Dell™ Remote Access Controller/ Modular Chassis Version 1.3

User's Guide

www.dell.com | support.dell.com

Notes, Notices, and Cautions

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.

⚠ **CAUTION: A CAUTION indicates a potential for property damage, personal injury, or death.**

February 2006 Rev. A00

Contents

DRAC/MC Overview

The Dell™ Remote Access Controller/Modular Chassis (DRAC/MC) is a systems management hardware and software solution designed to provide remote management capabilities, crashed system recovery, and power control functions for Dell PowerEdge™ modular server systems.

You can configure the DRAC/MC to send you e-mail alerts for warnings or errors related to voltages, temperatures, and fan speeds. A DRAC/MC module has its own baseboard management controller (BMC) that supports event data logging using the System Event Log (SEL). The event data can be obtained through the DRAC/MC Web-based interface or using RACADM commands.

Beginning with version 1.1, DRAC/MC supports the redundant DRAC feature. For more information, see "Understanding the Redundant DRAC/MC Environment."

To get started with the DRAC/MC, see "Installing and Setting Up the DRAC/MC."

What's New in DRAC/MC Version 1.3

The following changes in the DRAC/MC 1.3 are documented in this guide:

- Added support for the Dell PowerEdge 1955
- Modified the way power is budgeted to the various server blades through new redundancy policy selection
- Added support for user-configurable server names
- Added three new RACADM commands: "crdisconnect," "getmacaddress," and "vmdetach"
- Added object definitions to the new "cfgChassisPower" and "cfgServerInfo" property database groups
- Added support for remote RACADM
- Added support for backing up and restoring configuration objects
- Added new features to the Avocent Digital Access KVM module: multi-session CD/DVD support, virtual media (CD/DVD) software eject, viewer ID support, and user-configurable ports
- Added support for SUSE® LINUX Enterprise Server (version 9)

System Overview

Your system can include up to ten server modules (or blades). Each server module functions as an individual server encompassing up to two microprocessors, up to two hot-pluggable hard drives, and up to eight memory modules (see Figure 1-1 and Figure 1-2). The DRAC/MC monitors the server modules by communicating with the BMC in each server module. To function as a system, a server module is inserted into a Dell Modular Server Enclosure that supports power supplies, fan modules, a management module (DRAC/MC), a KVM switch or pass-through module, and at least one I/O module for network connectivity. The power supplies, fans, DRAC/MC, and I/O modules are shared resources of the server modules in the Dell Modular Server Enclosure. In addition, your system may also ship with an optional external universal serial bus (USB) diskette drive and/or an optional external USB CD drive, which you can use to set up and configure the server modules.

NOTE: To ensure proper operation and cooling, all bays must be populated with either a server module or a blank prior to turning on the system.

Figure 1-1. System Overview of a Dell PowerEdge 1855

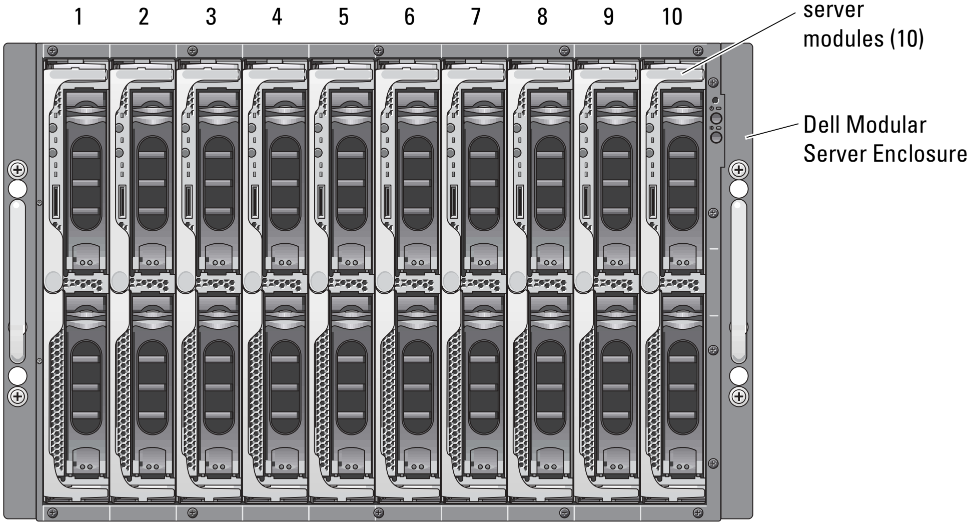
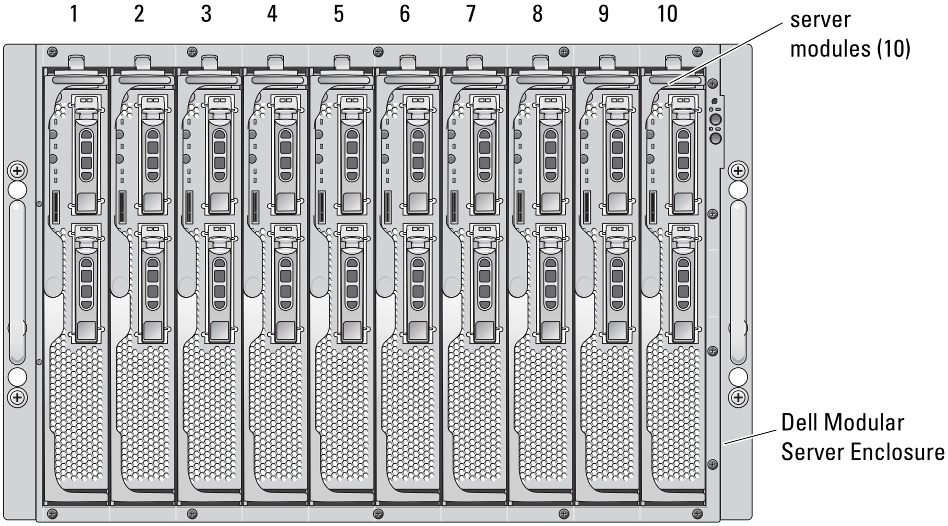


Figure 1-2. System Overview of a Dell PowerEdge 1955



The following sections describe the major hardware and software features of your system and provide information about the indicators on the system's front and back panels. They also provide information about other documents you may need when setting up your system and how to obtain technical assistance.

NOTE: The redundant DRAC/MC feature is only available for version 1.1 or later. For more information, see the *Installation and Troubleshooting Guide* and the *Hardware Owner's Manual* located on the Dell Support website at **support.dell.com**.

DRAC/MC Module Features

The DRAC/MC provides serial and Ethernet management ports, a status indicator when redundant DRAC/MCs are installed, and status indicators for the DRAC/MC (see Figure 1-3). See "Understanding the Redundant DRAC/MC Environment" for more information about dual configurations for DRAC/MC. See also "Using Text-Mode Serial Console Redirection" for specific information on serial port redirection of server modules and switches. Table 1-1 provides information about the status indicators.

NOTE: To support the redundant DRAC/MC configuration, both DRAC/MCs must have the same firmware version. The redundant DRAC/MC feature is only available for firmware version 1.1 or later.

Figure 1-3. DRAC/MC Module Features

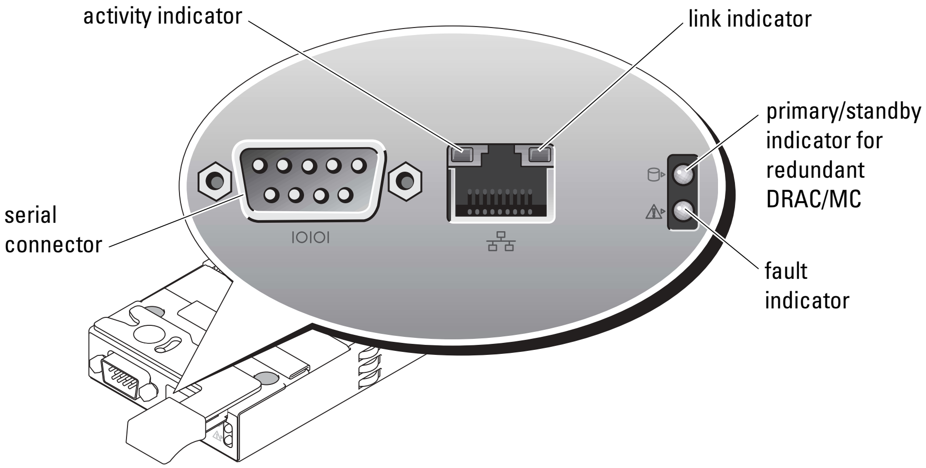


Table 1-1. DRAC/MC Module Indicators

Indicator Type	Icon	Activity Indicator	Indicator Code
Network interface controller link indicator	🖧	Off	LAN is not linked.
		Green	LAN is linked.
Network interface controller activity indicator		Off	LAN is not active.
		Amber blinking	Indicates that the system DRAC/MC and the LAN are communicating.
Primary/standby indicator	⛁▷	Off	The DRAC/MC is a backup for the primary DRAC/MC. **NOTE:** For more information about availability of redundant configurations for the DRAC/MC, see "Understanding the Redundant DRAC/MC Environment."
		Green	The DRAC/MC is active for system management.
		Green blinking	The DRAC/MC is in recovery mode or manufacturing mode.

Table 1-1. DRAC/MC Module Indicators *(continued)*

Indicator Type	Icon	Activity Indicator	Indicator Code
Fault indicator	⚠▷	Off	The DRAC/MC is operating normally.
		Amber	In a single (nonredundant) configuration, this DRAC/MC failed.
		Amber blinking	In a redundant configuration, this DRAC/MC failed.
Serial connector	10101	None	Used for a serial connection with a null modem cable.

NOTICE: When two DRAC/MC modules have different firmware (version 1.0 and version 1.1), the firmware upgrade will fail. To support redundant DRAC/MC, both modules must have firmware version 1.1 or later.

Hardware Specifications

Power Requirements

Table 1-2 lists the power requirements for the DRAC/MC.

Table 1-2. DRAC/MC Power Requirements

System Power
5V Standby 2.5-watt (maximum)

Connectors

NOTE: For information about installing the DRAC/MC hardware, see the *Installing a Remote Access Controller* document (available in the DRAC/MC kit), the *Installation and Troubleshooting Guide*, and the *Hardware Owner's Manual* that is included with your system.

The DRAC/MC provides a dedicated 10/100 Mbps RJ-45 Network Interface Controller (NIC), a 9-pin D-subminiature connector on the opposite end that connects the module to the Dell Modular Server Enclosure midplane.

DRAC/MC Ports

Table 1-3 identifies the ports used by the DRAC/MC. This information is required when opening firewalls for remote access to a DRAC/MC system.

Table 1-3. DRAC/MC Port Numbers

DRAC/MC Port Number	Used For
Ports listening for connection (server):	
23	telnet*
80	HTTP
161	SNMP agent
443	HTTPS
Ports that DRAC/MC uses as a client:	
25	SMTP
53	Dynamic DNS registration
68	DHCP Client
69	TFTP Firmware Upgrade
162	SNMP trap
389	Active Directory® authentication
636	Active Directory authentication
3269	Active Directory authentication
* Configurable Port	

Supported Remote Access Connections

Table 1-4 lists the features of each type of connection.

Table 1-4. Supported Remote Access Connections

Connection	Features
DRAC/MC NIC	• 10/100 Mbps Ethernet • DHCP support (static IP is the default) • SNMP traps and e-mail event notification • Dedicated network interface for the DRAC/MC • Support for telnet console and remote RACADM commands including system boot, reset, powerup, and shutdown commands
Serial port	• Support for serial console commands including system boot, reset, powerup, and shutdown commands • Support for text-only console redirection to a VT-100 terminal or terminal emulator

DRAC/MC System Features

The following is a list of features available on the DRAC/MC. Your system may have updates that enable additional features. Refer to the latest *Dell Remote Access Controller/Modular Chassis User's Guide* on the Dell Support website at **support.dell.com**.

- Remote system management, and monitoring through the DRAC/MC Web-based GUI, serial, remote RACADM, or telnet connection.
- Telnet text console redirection feature that allows you to directly access the DRAC/MC managed modules.
- Access to the Dell Modular Server Enclosure System Event Log (SEL) and DRAC/MC logs.
- Integrated launch of the DRAC/MC interface from the Dell OpenManage™ IT Assistant.
- Ability to alert you to potential problems on the DRAC/MC by sending either an e-mail message or an SNMP trap through the DRAC/MC NIC to a management station.
- Ability to configure DRAC/MC and update DRAC/MC firmware using a telnet session, a Web-based user interface, remote RACADM, or a terminal session (for example, a hyperterminal, remote RACADM, or a similar program).
- Ability to perform power management functions such as shutdown and reset, from a telnet session or the Web-based user interface, remote RACADM, and terminal session.
- Web-based interface password-level security management.
- Role-based authority that provides assignable permissions for different systems management tasks.
- Ability to address DRAC/MC modular system configuration issues that are associated with installing I/O modules and daughter cards. This feature is included in DRAC/MC version 1.1 and later.

- Ability to update firmware with redundant DRAC/MC modules. For more information, see "Understanding the Redundant DRAC/MC Environment."
- Support for Microsoft Active Directory, which enables you to secure your networked systems and user data more effectively.
- Ability to support remote, operating system-independent graphical console redirection and Virtual Media using the Avocent Digital Access KVM Module.

  NOTE: DRAC/MC firmware version 1.2 or later is required to use the Avocent Digital Access KVM Module.

DRAC/MC Security Features

The DRAC/MC provides the following security features:

- Role-based authority: This feature allows specific privileges to be configured for each user.
- User ID and password configuration: This feature allows User ID and password configuration through the Web-based and command line interfaces.
- Web-based and remote RACADM interface operation: This feature supports 128-bit SSL encryption.

  NOTE: Telnet does not support SSL encryption.
- Session time-out configuration (in minutes): This configuration is through the Web-based interface.
- Session time-out configuration setting: This feature is available using the command line interface object "cfgSerialConsoleIdleTimeout (Read/Write)."
- Support for Microsoft Active Directory: Active Directory provides added security for Web-based operations such as console redirection, virtual media sessions, and managing your systems using the DRAC/MC user interface.

Supported Platforms

The DRAC/MC is supported on the PowerEdge 1855 and 1955 systems.

Supported Web Browsers

The DRAC/MC supports the following Web browsers:

- Microsoft Internet Explorer 6.0 with Service Pack 1 and 2 on Microsoft Windows®
- Mozilla 1.7.8, 1.7.10, and 1.7.11 on Red Hat® Enterprise Linux (version 3 and version 4)
- Mozilla 1.7.8, 1.7.10, and 1.7.11 on SUSE LINUX Enterprise Server (version 9)

- Mozilla Firefox 1.0.7 on Red Hat Enterprise Linux (version 3 and version 4)
- Mozilla Firefox 1.0.7 on SUSE LINUX Enterprise Server (version 9)

NOTE: Cookies and JavaScript must be enabled.

NOTE: When you run multiple DRAC/MC sessions using Mozilla or Firefox browsers, each browser window shares the same session. To fix this issue in the Mozilla browser, configure the Mozilla Profile Manager to use separate profiles. Run the Mozilla Profile Manager from the operating system shell prompt by typing `mozilla -profilemanager`. To fix this issue in Firefox, set the environment variable `MOZ_NO_REMOTE` to `1`. Changing the environment variable creates a separate profile for each window (or session).

NOTE: Certain operations like saving files (log files or CSR files) to disk will be not successful if the following configuration setting in Microsoft Internet Explorer is selected:
Tools→Internet Options→Advanced→Security→Do not save encrypted pages to disk.
Deselect this option and restart Internet Explorer.

NOTE: For proper operation of the DRAC/MC Web-based GUI pages in the Microsoft Windows XP SP2 and Microsoft Windows Server 2003 SP1 operating systems, disable the Windows firewall.

See the latest DRAC/MC readme located on the Dell Support website at **support.dell.com** for an updated list of supported Web browsers.

Other Documents You May Need

In addition to this *User's Guide*, the following documents provide additional information about the setup and operation of the DRAC/MC in your system:

- The DRAC/MC online help provides information about using the Web-based graphical user interface.
- The *Dell OpenManage IT Assistant User's Guide* provides information about using IT Assistant.
- The *Dell OpenManage Baseboard Management Controller Utilities User's Guide* provides information about installing and using the BMC.
- The *Dell Integrated KVM Switch Module User's Guide* provides information about installing and configuring the integrated KVM switch module in the Dell Modular Server Enclosure.

The following system documents are also available to provide more information about the system in which your DRAC/MC is installed:

CAUTION: The *Product Information Guide* provides important safety and regulatory information. Warranty information may be included within this document or as a separate document.

- The Dell PowerEdge Expandable RAID Controller (PERC) documentation describes how to use the integrated mirroring features.
- *Installing a Remote Access Controller* provides instructions for installing DRAC/MC hardware. This document is available in the DRAC/MC kit.
- The *Rack Installation Guide* and *Rack Installation Instructions* included with your rack solution describes how to install your system into a rack.

- The *Getting Started Guide* provides an overview to initially set up your system.
- The *Installation and Troubleshooting Guide* describes how to troubleshoot the system and install or replace system components.
- The *Hardware Owner's Manual* (for *x9xx* systems) describes how to troubleshoot the system and install or replace system components.
- The *User's Guide* provides an overview of the system, descriptions of the Dell OpenManage Server Assistant and the System Setup program, and technical specifications.
- The *Configuration Guide* provides information on configuring your system and the server modules in your system. Additionally, the guide provides a starting point for system configuration.
- Systems management software documentation describes the features, requirements, installation, and basic operation of the software.
- The *Dell OpenManage Server Administrator SNMP Reference Guide* provides additional information about the use the simple network management protocol and agents.
- Operating system documentation describes how to install (if necessary), configure, and use the operating system software.
- Documentation for any components you purchased separately provides information to configure and install these options.
- Updates are sometimes included with the system to describe changes to the system, software, and/or documentation.

NOTE: Always read the updates first because they often supersede information in other documents.

Release notes or readme files may be included to provide last-minute updates to the system or documentation or advanced technical reference material intended for experienced users or technicians. See your DRAC/MC readme for more information about the DRAC/MC. This readme is available on the Dell Support website at **support.dell.com** along with this guide on the Systems Management documentation Web page.

2

Installing and Setting Up the DRAC/MC

This section provides information about how to install and set up your DRAC/MC module and software. Steps are provided to walk you through each task.

What You Need to Get Started

Locate the following items to install and configure the DRAC/MC software:

- DRAC/MC module (already installed or in the optional kit)
- The instructions for installing DRAC/MC in this section

Installing the DRAC/MC Hardware

The DRAC/MC module may be preinstalled on your system or available separately in a kit. To get started with the DRAC/MC module that is already installed on your system, see "Configuration Overview."

If a DRAC/MC is not installed on your system, see the *Installing a Remote Access Controller* document that is included with your DRAC/MC kit or see your platform *Installation and Troubleshooting Guide* or the *Hardware Owner's Manual* for hardware installation instructions before proceeding.

About DRAC/MC Modules

Among other controlling features, the DRAC/MC controls power to the system. When a functional DRAC/MC module is not installed, newly-installed server modules cannot be powered on and presently-installed server modules cannot have their power cycled.

⚠ **CAUTION: Many repairs may only be done by a certified service technician. You should only perform troubleshooting and simple repairs as authorized in your product documentation, or as directed by the online or telephone service and support team. Damage due to servicing that is not authorized by Dell is not covered by your warranty. Read and follow the safety instructions that came with the product.**

Removing a DRAC/MC Module

1. Disconnect any cables attached to the DRAC/MC module.
2. Press in the bottom of the release tab and pull out the release lever. See Figure 2-1.
3. Slide the DRAC/MC module out of the chassis.

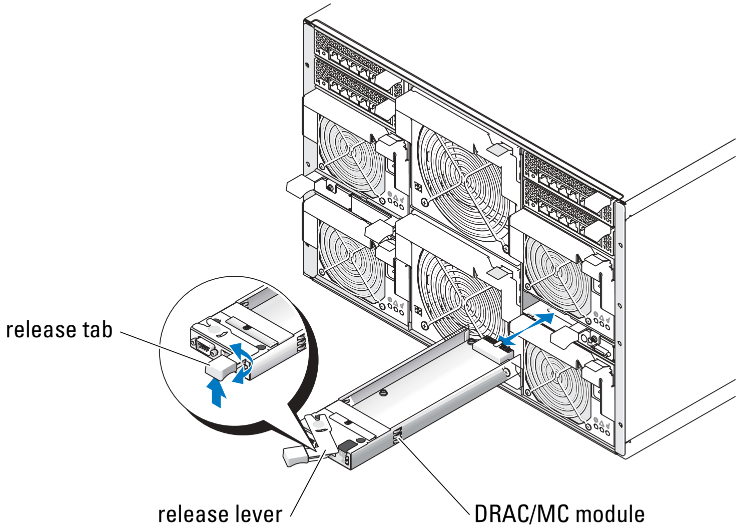
NOTE: Because DRAC/MC modules are hot pluggable, you can remove a module without powering down your system.

Installing a DRAC/MC Module

1. Ensure that the DRAC/MC module release lever is fully extended. See Figure 2-1.
2. Slide the module into the chassis until it is fully seated.
3. Close the release lever until it snaps securely into place.
4. Reconnect the cables that were attached to the module.

NOTE: For information about installing the redundant DRAC/MC firmware for version 1.1 or later, see "Understanding the Redundant DRAC/MC Environment."

Figure 2-1. Removing and Installing a DRAC/MC Module



Configuration Overview

This section provides a high-level overview of the DRAC/MC configuration process. You can perform all configuration steps using the Web-based interface, remote RACADM, or serial/telnet console.

To configure your DRAC/MC software, perform the following steps in their numbered order.

NOTICE: Unexpected results may occur—such as a runtime error—if you use the Web-based interface and the serial/telnet console simultaneously.

1. Configure the DRAC/MC network settings. See "Configuring the DRAC/MC Network Settings."
2. Add and configure DRAC/MC users. See "Adding and Configuring DRAC/MC Users."
3. Configure the Web browser to connect to the Web-based interface. See "Configuring a Supported Web Browser."

4 Update the DRAC/MC firmware. See "Updating the DRAC/MC Firmware."

5 Access the DRAC/MC through a network. See "Accessing the DRAC/MC Through a Network."

6 Update the KVM firmware. See "Updating the KVM Firmware."

Configuring a Supported Web Browser

The following sections provide instructions for configuring the supported Web browsers. For a list of supported Web browsers, see "Supported Web Browsers."

Configuring Internet Explorer to Connect to the Web-Based Interface

If you are connecting to the DRAC/MC Web-based interface from a management station that connects to the Internet through a proxy server, configure the Web browser accordingly for a proper connection.

To configure your Web browser, perform the following 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.

Viewing Localized Versions of the Web-Based Interface

NOTE: Localization is available for DRAC/MC version 1.1 or later, which includes English, Spanish, French, German, Japanese, and Simplified Chinese. However, localization is not available in version 1.0—the first release of DRAC/MC.

When using Internet Explorer on systems running Microsoft® Windows® to view localized versions of the DRAC/MC Web-based interface, perform the following steps:

1 Open the Windows **Control Panel** and double-click the **Regional Options** icon.

2 Select the location from **Your locale (location)**.

3 Click **OK** twice.

Configuring the DRAC/MC Serial or Telnet Text Console

Before using the serial/telnet consoles, perform the instructions in "Configuring a DRAC/MC to Use a Serial or Telnet Text Console."

Configuring the DRAC/MC Remote RACADM

Before using the remote RACADM utility, perform the instructions in "Using the RACADM CLI Remotely."

Configuring DRAC/MC Properties

You can configure all DRAC/MC properties (including network, users, and alerts) through the RACADM command line interface (CLI).

For more information about using the RACADM CLI through a serial console or telnet session, see "Using the DRAC/MC CLI Commands."

Configuring the DRAC/MC Network Settings

NOTICE: Changing your DRAC/MC network settings may disconnect your current network connection.

Configure the DRAC/MC network settings using one of the following tools:

- Web-based Interface — See "Configuring the DRAC/MC NIC."
- RACADM CLI— See "cfgLanNetworking."

Adding and Configuring DRAC/MC Users

Add and configure DRAC/MC users using one of the following tools:

- Web-based Interface — See "Managing and Recovering a Remote System" for information on how to access and use the Web-based interface.
- RACADM CLI — See "Using the DRAC/MC CLI Commands."

Adding and Configuring SNMP Alerts

NOTE: You can find DRAC/MC alert information in Management Information Base (MIB) format in the **rac_host MIB**.

NOTE: The SNMP agent defaults to the OFF state. If the SNMP agent is required, this agent must be turned ON by typing the following CLI command line:

```
racadm config -g cfgOobSnmp -o cfgOobSnmpAgentEnable 1
```

Add and configure SNMP alerts using one of the following tools:

- Web-based Interface — See "Installing and Setting Up the DRAC/MC."
- RACADM CLI — See "Using the DRAC/MC CLI Commands."

Updating the DRAC/MC Firmware

NOTICE: Updating your DRAC/MC firmware will disconnect your current network connection.

Use one of the following methods to update your DRAC/MC firmware:

- Web-based Interface — See "Using the DRAC/MC Web-based Firmware Update Interface."

  NOTICE: The DRAC/MC may not be accessible for up to 5 minutes after a firmware update. Since the DRAC/MC uses a different MAC address during a firmware update, it sends a gratuitous Address Resolution Protocol (ARP) after completing the update. A switch with Spanning Tree Protocol enabled may block the ARP packet transmission. To avoid this issue, disable the Spanning Tree Protocol on the switch ports that are connected to all DRAC/MC modules during a firmware update.

  NOTICE: DRAC/MC versions 1.1 and later use a common MAC address that is stored in the Dell Modular Server Enclosure. Since the common MAC address is different from the DRAC/MC version 1.0 MAC address, a Dynamic Host Configuration Protocol (DHCP)-assigned IP address can be changed after you upgrade the DRAC/MC firmware to version 1.1 or later.

- RACADM CLI — See "Using the RACADM Command Line Interface to Update Firmware."
- Firmware Recovery Console — See "Using the Firmware Recovery Console."

In firmware releases prior to version 1.2, the firmware update self-extracting .zip file includes the following files:

- **mgmt.bin** — Contains the DRAC/MC firmware image.
- **upload.exe** — Recovers the previous firmware version if the installed firmware is corrupted.
- **rac_host.mib** — Provides firmware information.

In firmware version 1.2 and later, the **upload.exe** and **rac_host.mib** files may be packaged separately from the firmware package.

Using the DRAC/MC Web-based Firmware Update Interface

NOTICE: To support redundant DRAC/MC, both modules must have firmware version 1.1 or later.

NOTICE: If you are updating your DRAC/MC module firmware to version 1.2 or later, install version 1.1 or version 1.1.1 before you install the new version (1.2 or later). Upgrading your firmware from version 1.0 directly to version 1.2 or later is not supported.

NOTICE: DRAC/MC version 1.0 does not support a redundant configuration. Dell does not support chassis configurations with two DRAC/MC version 1.0 modules or two DRAC/MC modules with version 1.0 and version 1.1 or later firmware.

1. Copy the binary file **mgmt.bin** to a TFTP server root directory.
2. Log on to the DRAC/MC Web-based user interface using "Supported Web Browsers."

   See "DRAC/MC System Features" for more information.

3. From the DRAC/MC Web-based user interface main window, click the **Update** tab.
4. In the **Firmware Update** window, enter the IP address of the TFTP server and the image name, `mgmt.bin`.

5 Click **Update Firmware**.

The TFTP download and firmware update process may take several minutes to complete. After the update completes, the DRAC/MC will reset.

6 If you installed firmware version 1.1 or version 1.1.1 and want to update your DRAC/MC firmware to version 1.2 or later, repeat step 2 through step 5. Otherwise, go to step 7.

7 If your system is not configured with two DRAC/MC modules in a redundant configuration, the firmware update is completed.

If your system is configured with two DRAC/MC modules in a redundant configuration and the DRAC/MC modules have firmware versions 1.1 or later, both the DRAC/MC modules will be updated from the same binary image. Perform the following steps if upgrading from firmware version 1.0:

a Remove the updated DRAC/MC module from the system.

b Insert the remaining DRAC/MC module into the system.

c Repeat step 2 through step 6.

After you perform a firmware update, perform the steps in the following subsections to clear the Web browser cache and ensure that all new Web-based interface pages are reloaded.

Using the RACADM Command Line Interface to Update Firmware

NOTICE: If you are updating your DRAC/MC module firmware to version 1.2 or later, install version 1.1 or version 1.1.1 before you install the new version (1.2 or later). Upgrading your firmware from version 1.0 directly to version 1.2 or later is not supported.

1 If your system is configured with two DRAC/MC firmware version 1.0 modules, remove one DRAC/MC module from the system.

2 Copy the binary file, `mgmt.bin`, to a TFTP server root directory.

3 Log on to the DRAC/MC telnet or serial interface.

4 From the telnet or serial interface, type a command line similar to the following example:

```
racadm fwupdate -a <TFTP IP Address> -d mgmt.bin
```

The TFTP download and firmware update process may take several minutes to complete. After the update completes, the DRAC/MC will reset.

From the remote RACADM interface, type a command line similar to the following example:

```
racadm -r <IP Address> -u <User name> -p <Password> fwupdate -a <TFTP
IP Address> -d mgmt.bin
```

The TFTP download and firmware update process may take several minutes to complete. After the update completes, the DRAC/MC will reset.

NOTE: The remote RACADM utility version 5.0.0 is compatible with DRAC/MC version 1.3 and later.

5 If you installed firmware version 1.1 or version 1.1.1 and want to update your DRAC/MC firmware to version 1.2 or later, repeat step 3 and step 4. Otherwise, go to step 6.

6 If your system is not configured with two DRAC/MC modules in a redundant configuration, the firmware update is completed.

   If your system is configured with two DRAC/MC modules in a redundant configuration and the DRAC/MC modules have firmware versions 1.1 or later, both the DRAC/MC modules will be updated from the same binary image. Perform the following steps if upgrading from firmware version 1.0:

   a Remove the updated DRAC/MC module from the system.

   b Insert the remaining DRAC/MC module into the system.

   c Repeat step 3 through step 5.

After you perform a firmware update, perform the steps in the following subsections to clear the Web browser cache and ensure that all new Web-based interface pages are reloaded.

Clearing the Web Browser Cache With Internet Explorer

1 From the drop-down menu, select **Tools**→**Internet Options**.

2 In the **Internet Options** window, click the **General** tab, and under **Temporary Internet Files**, click **Delete Files...**.

3 Select **Delete all offline content**.

4 Click **OK** twice.

5 Close and restart the Web browser.

Clearing the Web Browser Cache With Mozilla or Firefox

1 From the drop-down menu, select **Edit Preferences**.

2 In the **Preferences** window, select **Advanced**→**Cache**.

3 Select **Clear Disk Cache**.

4 Select **Clear Memory Cache**.

5 Click **OK**.

6 Close and restart the browser.

Understanding the Redundant DRAC/MC Environment

In a redundant configuration, two separate DRAC/MC modules are installed in a chassis:

- A primary DRAC/MC module, which actively monitors the chassis.
- A standby DRAC/MC module that monitors the active signal from the primary DRAC/MC module. The standby DRAC/MC module becomes the active primary DRAC/MC module if a failure occurs for more than five seconds.

Failover occurs and the standby DRAC/MC module becomes active when any of the following conditions occur:

1. The primary DRAC/MC network connection is broken. For example, a cable has been disconnected or is broken.
2. The user removes the primary DRAC/MC module from the chassis.
3. The primary DRAC/MC module is rebooting, or the user initiates a DRAC/MC reset.
4. The primary DRAC/MC module is in a nonresponsive state and fails to exchange a heartbeat signal with the standby DRAC/MC module.
5. The firmware is being updated, causing a temporary failover to occur. In this case, because the primary and standby DRAC/MCs use the same IP address, the console, telnet, and user interface are each rendered inactive.

NOTE: During a firmware update, the backup DRAC/MC monitors the chassis while the active DRAC/MC updates the firmware. When the primary DRAC/MC completes the firmware update, the backup DRAC/MC continues the TFTP update. The DRAC/MC network interface will not be available until the firmware update is complete.

NOTE: Both DRAC/MCs must be connected to the same subnet to support a single IP TFTP firmware update. This feature is available only with DRAC/MC version 1.1 or later. This feature will not work if one of the DRAC/MCs is version 1.0. See "Upgrading Both DRAC/MC Modules with a Single Firmware Package."

Primary DRAC/MC Election Process

When the chassis powers up for the first time, the DRAC/MC module that is located above power supply 1 (see Figure 3-1) becomes the primary module.

NOTE: The chassis orientation presumes that you are viewing the DRAC/MC chassis from the back, as shown in Figure 3-1. In this scenario, the primary module is located on the system's right side during initial powerup.

If a DRAC/MC is not installed in the first slot or if the DRAC/MC in the first slot is not connected to the network, the standby DRAC/MC module (the DRAC/MC in slot 2) becomes the primary module.

If the primary or secondary DRAC/MC module is configured with a firmware version prior to version 1.1, remove the updated DRAC/MC module from the Dell Modular Server Enclosure and update the firmware on the remaining DRAC/MC module. If both modules require a firmware update, remove one DRAC/MC module from the Dell Modular Server Enclosure and update each module one at a time.

NOTE: DRAC/MC version 1.1 or later uses a reserved MAC address stored in the chassis. Because of this feature, a DHCP-assigned IP address may change after updating the firmware to version 1.1. The DRAC/MC MAC address displayed by the RACADM **getsysinfo** command will also be changed with version 1.1.

You can also upgrade both DRAC/MC modules simultaneously by using a single firmware package. See "Upgrading Both DRAC/MC Modules with a Single Firmware Package."

Using DRAC/MC in Normal Operating Mode

In normal operating mode after you initialize the modules, the primary DRAC/MC module processes network requests from the Internet, SNMP, and telnet to communicate with the end user.

The primary module also synchronizes with the standby module internally to read and write date/time information while you change the settings. This information includes the UART baud rate synchronization and the NIC failover with the primary link.

Upgrading Both DRAC/MC Modules with a Single Firmware Package

Both the primary and standby DRAC/MC modules can be updated with a single firmware package from the same TFTP server.

To update the modules using a single firmware package, perform the following steps:

1. Initiate a TFTP firmware update using the **racadm fwupdate** command or through the Web-based user interface.
2. The primary DRAC/MC module starts the TFTP firmware update.
3. The standby DRAC/MC module monitors the chassis while the other DRAC/MC module is updated. At this time, the DRAC/MCs are not accessible through telnet, remote RACADM, or Web interfaces.
4. When the primary DRAC/MC module completes the TFTP update, the TFTP update starts on the other DRAC/MC module. The primary DRAC/MC module continues to monitor the chassis while the standby module is updating the firmware. The DRAC/MCs are not accessible through telnet, remote RACADM, or Web interfaces.
5. When the standby module completes the firmware update process, the primary module is available for network access and telnet, remote RACADM, and Web-based user interfaces become available.

   NOTE: During the firmware update process, both DRAC/MCs are accessible through the serial interface. The serial interfaces will display the firmware update status at that time.

Accessing the DRAC/MC Through a Network

This section provides information about how to access a DRAC/MC after the hardware is installed and the software is configured.

After you configure the DRAC/MC, you can remotely access the DRAC/MC system using one of four remote access interfaces. Table 2-1 describes each of the DRAC/MC interfaces.

Table 2-1. DRAC/MC Interfaces

Interface	Description
Web-based interface	Enables you to access the DRAC/MC using a supported Web browser through the DRAC/MC NIC. For a list of supported Web browsers, see "DRAC/MC System Features."
Telnet	Provides access to serial and RACADM CLI commands, and text console redirection through the DRAC/MC network interface.
Terminal emulation software	Provides access to serial and RACADM CLI commands, and text console redirection through the DRAC/MC external serial port.
Remote RACADM interface	Provides access to serial and RACADM CLI commands through the DRAC/MC network interface.

You can access the DRAC/MC Web-based interface through the DRAC/MC NIC by using a supported Web browser or through Dell OpenManage™ IT Assistant.

To access the DRAC/MC using a supported Web browser, perform the following steps:

1 Type the IP address of the DRAC/MC.

NOTE: The DRAC/MC default IP address is `192.168.0.120`, which is configurable by the user.

2 To log in, type your DRAC/MC user name and password.

NOTE: The DRAC/MC default user name is `root` and the default password is `calvin`.

For more information about using the DRAC/MC interface, see the remote access interface online help.

3

Using the DRAC/MC Chassis Configuration Verification Feature

This section provides information about how to prevent you from misconfiguring your Dell™ Modular Server Enclosure based on the following scenarios (see Table 3-1):

- Installing daughter cards on the server modules that are of a different fabric type than the chassis I/O modules installed in chassis I/O slots 3 and 4; (for example, Fibre Channel daughter cards installed on the server modules and Ethernet modules installed on chassis I/O slots 3 and 4).
- Installing an I/O module in one of the I/O module slots that is incorrect for that system.

Chassis Verification Procedure

The chassis verification feature varies depending on the DRAC/MC module firmware version.

NOTE: If the Dell Modular Server Enclosure is not configured properly, the Chassis Configuration Verification feature may not allow an I/O or server module to start up.

Table 3-1 provides the chassis verification procedures for the DRAC/MC firmware.

Table 3-1. Chassis Verification Procedure

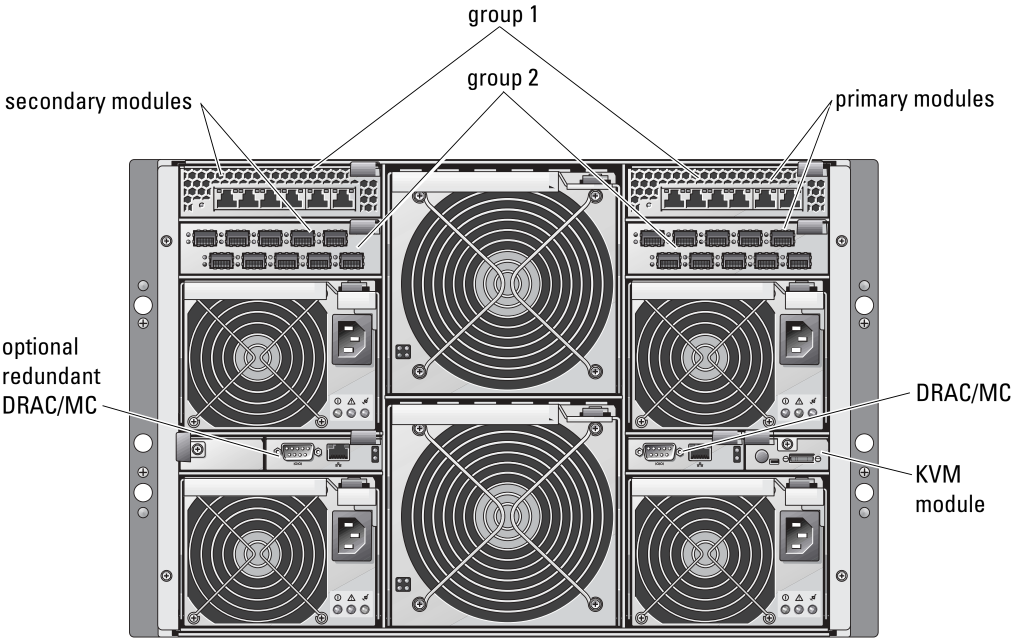
Firmware Version	Chassis Verification Procedure
Version 1.1	Does not allow unsupported hardware configuration to power on.
Version 1.2 and later	Allows unsupported hardware configuration to power on if the fabric type between the daughter cards is compatible with the Ethernet or Fibre Channel I/O module.

Chassis Management Architecture for I/O Modules

The server system supports up to four I/O slots that support and monitor a wide variety of I/O devices. The DRAC/MC monitors all of the I/O devices and daughter cards in the server modules to verify if the configuration is a valid configuration.

Figure 3-1 shows a back view of the Dell Modular Server Enclosure.

Figure 3-1. **Dell Modular Server Enclosure (back view)**



To understand daughter card and I/O module verification features, you must first consider the following assumptions:

- Chassis I/O module numbers are designated as shown in Table 3-2.

Table 3-2. Chassis I/O module numbers

	Primary Modules	Secondary Modules
Group 1	1	2
Group 2	3	4

- Chassis I/O module configuration takes precedence over the server module daughter cards.
- The server's I/O daughter card fabric type (for example, Fibre Channel) must match the fabric type of the chassis I/O module in chassis I/O slot 3 (and slot 4 if required).

NOTE: The chassis configuration verification feature is only supported for DRAC/MC version 1.1 or later.

Table 3-3 provides common scenarios for valid configuration and misconfiguration for the four bays, and how each configuration affects the DRAC/MC.

Table 3-3. Supported I/O Configuration Summary

I/O Modules	I/O Bay 1	I/O Bay 2	I/O Bay 3	I/O Bay 4
Dell PowerConnect™ 5316M Ethernet Switch	Valid	Valid: Must match bay 1	Valid: Requires gigabyte Ethernet (GbE) daughter cards or no daughter cards in server modules	Valid: Requires GbE daughter cards or no daughter cards in server modules and must match bay 3
GbE Pass Through	Valid	Valid: Must match bay 1	Valid: Requires GbE daughter cards or no daughter cards in server modules	Valid: Requires GbE daughter cards or no daughter cards in server modules and must match bay 3
Brocade Fibre Channel Switch	Invalid	Invalid	Valid: Requires Fibre Channel daughter cards or no daughter cards in server modules	Valid: Requires Fibre Channel daughter cards or no daughter cards in server modules and must match bay 3
McData 4314 Fibre Channel Switch	Invalid	Invalid	Valid: Requires Fibre Channel daughter cards or no daughter cards in server modules	Valid: Requires Fibre Channel daughter cards or no daughter cards in server modules and must match bay 3
Fibre Channel Pass Through	Invalid	Invalid	Valid: Requires Fibre Channel daughter cards or no daughter cards in server modules	Valid: Requires Fibre Channel daughter cards or no daughter cards in server modules and must match bay 3
Infiniband Pass Through	Invalid	Invalid	Valid: Requires Infiniband daughter cards or no daughter cards in server modules	Valid: Requires Infiniband daughter cards or no daughter cards in server modules and must match bay 3
Cisco Catalyst Ethernet Blade Switch 3030	Valid	Valid: Must match bay 1	Valid: Requires GbE daughter cards or no daughter cards in server modules	Valid: Requires GbE daughter cards or no daughter cards in server modules and must match bay 3

Table 3-3. Supported I/O Configuration Summary *(continued)*

I/O Modules	I/O Bay 1	I/O Bay 2	I/O Bay 3	I/O Bay 4
Brocade SilkWorm 4116 Fibre Channel Switch	Invalid	Invalid	Valid: Requires Fibre Channel daughter cards or no daughter cards in server modules	Valid: Requires Fibre Channel daughter cards or no daughter cards in server modules and must match bay 3
McData 4416 Fibre Channel Switch	Invalid	Invalid	Valid: Requires Fibre Channel daughter cards or no daughter cards in server modules	Valid: Requires Fibre Channel daughter cards or no daughter cards in server modules and must match bay 3

NOTE: The GbE pass-through module ports are preset to communicate at 1000 Mb and will not auto-negotiate to a slower speed. As a result, only connect the GbE pass-through module to 1000 Mb external switch ports. Do not use this module with 10 Mb or 100 Mb external switch ports.

I/O Misconfiguration Behavior

NOTE: You can use the RACADM CLI **getdcinfo** command to view the daughter card configuration.

If DRAC/MC modules do not conform to the parameters outlined in the preceding table and misconfiguration results, the server modules and the chassis may exhibit the following behaviors:

- The LED on the I/O module will be blinking.
- The I/O modules with an invalid configuration will not power on.
- An SEL entry will be created by the DRAC/MC.

Daughter Card Misconfiguration Behavior

If the daughter card on the server module does not match the group 2 fabric (on modules in bay 3 and bay 4), the server modules will exhibit the following behaviors:

- The server module cannot be powered on.
- An error LED on the server module will be blinking.
- A SEL entry will be created by the DRAC/MC.
- If the server module requests power on, the KVM LED will be blinking.

Chassis Misconfiguration Behavior

If the server modules contain different types of daughter cards, and if no I/O modules are present in bay 3 and bay 4, the behavior is a chassis misconfiguration. In this situation, the server modules containing daughter cards will not be powered on. If the server module requests power on, the KVM LED will be blinking.

4

Configuring a DRAC/MC to Use a Serial or Telnet Text Console

The DRAC/MC provides a serial and network interface designed to perform all the configuration and systems management functions using the DRAC/MC Web-based interface or the serial/telnet console.

The following section describes the serial/telnet text console features, and explains how to set up your system so you can perform systems management actions through a serial/telnet console.

Serial and Telnet Console Features

The DRAC/MC supports the following serial and telnet console features:

- Up to four client connections, including telnet connections
- Access to the DRAC/MC CLI through the system serial port and through the DRAC/MC NIC
- Console commands that allow you to power up, power down, power-cycle, reset, view logs, view chassis sensor status, or configure the DRAC/MC
- Connection through the **connect server-x** or **connect switch-x** command, allowing users to view and interact with the server or I/O module console (including BIOS, setup, and the operating system)

  If you are running Red Hat® Enterprise Linux (or SUSE® LINUX Enterprise Server) on the DRAC/MC, the **connect server-x** serial command provides a true Linux console stream interface.

  If you are running Microsoft® Windows Server™ 2003 on the server module where the console has been redirected through the **connect server-x** command, the Microsoft Special Administration Console (SAC) appears.

Text Mode Console Redirection

The text mode console redirection feature of the DRAC/MC is not available for the Windows® 2000 Server operating system. This feature is supported with the Windows Server 2003 operating system.

Supported RACADM CLI Commands

Because the RACADM CLI command does not have access to a file system on a serial or telnet console, several options (such as reading or writing a file) are not supported by the RACADM command through a serial or telnet console. For more information about supported RACADM CLI commands for the serial and telnet consoles, see "Using the DRAC/MC CLI Commands."

Enabling and Configuring the DRAC/MC to Use a Serial or Telnet Console

The following subsections provide information about how to enable and configure a serial/telnet console on the DRAC/MC.

NOTE: DRAC/MC firmware version 1.1 or later supports up to four telnet sessions.

NOTE: In DRAC/MC version 1.0, if a telnet client is connected to the DRAC/MC, and another client attempts a telnet connection, the second client will receive only a blank screen in response.

Enabling the Serial and/or Telnet Console on the DRAC/MC

NOTE: By default, telnet is disabled.

NOTE: You (the current user) must have **Configure DRAC/MC** permission in order to perform the steps in this section.

If the serial console is disabled, you can enable the console remotely through the telnet interface. To enable the serial console at the telnet console `DRAC/MC:` prompt, type the following serial CLI commands:

```
racadm config -g cfgSerial -o cfgSerialConsoleEnable 1
```

```
racadm config -g cfgSerial -o cfgSerialTelnetEnable 1
```

NOTE: For more information about how to use the RACADM CLI and serial/telnet commands, see "Using the DRAC/MC CLI Commands."

Using the RACADM CLI Command to Configure the Settings for the Serial and Telnet Console

The default settings may be reconfigured for serial/telnet console redirection. To configure the settings, open a command prompt and type the **racadm config** command using the appropriate group, object, and object value(s) for the setting that you want to configure. For a complete list of available telnet and serial/telnet console commands, see "Using the DRAC/MC CLI Commands."

To type RACADM CLI commands, type the commands from a command prompt on the serial or telnet session:

```
racadm config -g <group> -o <object> <value>
```

NOTE: To display all groups, type: `racadm getconfig -h`

Displaying Configuration Settings

To display the current settings for a particular group, type the following commands from the command prompt on the DRAC/MC:

```
racadm getconfig -g <group>
```

For example, to display a list of all of the settings for the **cfgSerial** group, type the following:

```
racadm getconfig -g cfgSerial
```

Connecting to the DRAC/MC Through the Local Serial Port or Telnet Management Station (Client System)

The DRAC/MC provides access between the DRAC/MC and the serial port on your system to enable you to start up, shut down, or reset the DRAC/MC, and access logs and sensors.

The serial console is available through the DRAC/MC serial connector. Only one serial client can be connected at any given time.

The telnet console is available on the DRAC/MC through the DRAC/MC NIC. In DRAC/MC version 1.0, only one telnet client can be connected at any given time.

The serial/telnet connection to the DRAC/MC serial or telnet console requires the management station terminal emulation software (see "Configuring the Management Station Terminal Emulation Software" for more information).

The following subsections explain how to connect your management station to the DRAC/MC through a DRAC/MC external serial port using terminal software and a null modem cable, or by telnet using terminal software through the DRAC/MC NIC.

Connecting the DB-9 Cable

To access the DRAC/MC using a serial text console, connect a DB-9 null modem cable to the COM port that you are using on the chassis. Not all DB-9 cables carry the pinout/signals that are necessary for this connection. The DB-9 cable for this connection must conform to the specification shown in Table 4-1.

Table 4-1. Required Pinout for DB-9 Null Modem Cable

Signal Name	DB-9 Pin	DB-9 Pin	Signal Name
FG (Frame Ground)	–	–	FG (Frame Ground)
TD (Transmit data)	3	2	RD (Receive Data)
RD (Receive Data)	2	3	TD (Transmit data)
RTS (Request To Send)	7	8	CTS (Clear To Send)
CTS (Clear To Send)	8	7	RTS (Request To Send)
SG (Signal Ground)	5	5	SG (Signal Ground)
DSR (Data Set Ready)	6	4	DTR (Data Terminal Ready)
DCD (Data Carrier Detect)	1	4	DTR
DTR (Data Terminal Ready)	4	6	DSR (Data Set Ready)
DTR	4	1	DCD (Data Carrier Detect)

Configuring the Management Station Terminal Emulation Software

Your DRAC/MC supports a serial or telnet text console from a management station running one of the following types of terminal emulation software:

- Red Hat Enterprise Linux or SUSE Linux Enterprise Server Minicom in an Xterm
- Hilgraeve's HyperTerminal Private Edition (version 6.3)
- Red Hat Enterprise Linux or SUSE Linux Enterprise Server Telnet in an Xterm
- Microsoft Telnet

Perform the steps in the following subsections to configure your type of terminal software. Configuration is not required when using Microsoft Telnet.

Configuring Red Hat Enterprise Linux and SUSE Linux Enterprise Server Minicom for Serial Console Emulation

Minicom is the serial port access utility for Red Hat Enterprise Linux and SUSE Linux Enterprise Server. The following steps are valid for configuring Minicom version 1.8. Other Minicom versions may differ slightly but require the same basic settings. Use the information in "Required Minicom Settings for Serial Console Emulation" to configure other versions of Minicom.

Configuring Minicom Version 1.8 for Serial Console Emulation

NOTE: To ensure that the text displays properly, Dell™ recommends that you use an Xterm window to display the telnet console instead of the default window provided by the Red Hat Enterprise Linux and SUSE Linux Enterprise Server installation.

1 To start a new Xterm session, type `xterm &` at the command prompt.

2 Drag the lower right corner of the window with the mouse to resize it to 80 x 25 prior to using telnet.

3 If you do not have a Minicom configuration file, go to the next step.

If you have a Minicom configuration file, type `minicom` *`<Minicom config file name>`* and then skip to step 20.

4 At the Xterm command prompt, type `minicom`.

5 Select **Serial Port Setup** and press <Enter>.

6 Press <a> and select the appropriate serial device (for example, **/dev/ttySo**).

7 Press <e> and set the **Bps/Par/Bits** option to **115200 8N1**.

8 Press <f> and set **Hardware Flow Control** to **Yes** and set **Software Flow Control** to **No**.

9 To exit the **Serial Port Setup** menu, press <Enter>.

10 To enter **Terminal Setup**, press <a>.

11 For the **Terminal Emulation** setting, select **VT100**.

12 To exit **Terminal Setup**, press <Enter>.

13 Select **Modem and Dialing** and press <Enter>.

14 In the **Modem Dialing and Parameter Setup** menu, press <Backspace> to clear the **init**, **reset**, **connect**, and **hangup** settings so that they are blank.

15 To save each blank value, press <Enter>.

16 When all specified fields are clear, press <Enter> to exit the **Modem Dialing and Parameter Setup** menu.

17 Select **Save setup as config_name** and press <Enter>.

18 Select **Exit From Minicom** and press <Enter>.

19 At the command shell prompt, type `minicom <Minicom config file name>`.

20 To expand the Minicom window to 80 x 25, drag the corner of the window.

21 To exit Minicom, press <Ctrl><a><z><x>.

The Minicom window displays a login screen. When the login screen is displayed, type your user name and password. Your connection to the DRAC/MC console should be successful.

NOTE: If you are using Minicom for serial text console redirection to configure the DRAC/MC BIOS, it may be useful to turn on color in Minicom. To turn on color, at the command prompt type `minicom -c on`.

Required Minicom Settings for Serial Console Emulation

Use Table 4-2 to configure any version of Minicom.

Table 4-2. Minicom Settings for Serial Console Emulation

Setting Description	Required Setting
Bits Per Second/Parity/Bits	115200 8N1
Hardware flow control	Yes
Software flow control	No
Terminal emulation	ANSI
Modem dialing and parameter settings	Clear the **init**, **reset**, **connect**, and **hangup** settings so that they are blank
Window size	80 x 25 (to resize, drag the lower-right corner of the window)

Configuring HyperTerminal for Serial Console Redirection

HyperTerminal is the Windows serial port access utility. To set the size of your console screen appropriately, use Hilgraeve's HyperTerminal Private Edition version 6.3.

To configure HyperTerminal for serial console redirection, perform the following steps:

1 Start the HyperTerminal program.

2 Type a name for the new connection and click **OK**.

3 In the **Connect using:** text box, select the COM port on the management station (for example, COM1) to which you have connected the DB-9 null modem cable and click **OK**.

4 Configure the COM port settings as shown in Table 4-3, and then click **OK**.

5 Click **File→Properties** and click the **Settings** tab.

6 Set the **Telnet terminal ID:** to **VT100**.

7 Click **Terminal Setup** and set **Screen Rows** to **25**.

8 Set **Columns** to 80 and click **OK**.

9 Click **ASCII Setup...**.

10 Select **Wrap lines that exceed terminal width**, and click **OK**.

Table 4-3. COM Properties Dialog Box Port Settings

Setting Description	Required Setting
Bits per second:	115200
Data bits:	8
Parity:	None
Stop bits:	1
Flow control:	Hardware

NOTE: If these settings are incorrect, the HyperTerminal window will not be displayed.

The HyperTerminal window displays a login screen. When the login screen is displayed, enter your user name and password. Your connection should be successful connecting to the DRAC/MC console.

Configuring Red Hat Enterprise Linux and SUSE Linux Enterprise Server XTerm for Telnet Console Redirection

NOTE: When you are using the **connect server-x** command through a telnet console to display the System Setup screens, set the terminal type to **VT100** in System Setup and for the telnet session.

NOTE: Telnet is disabled on the DRAC/MC by default. To enable telnet, use either the Web-based user interface **Configuration** tab, or use the **cfgSerial** object to configure using the RACADM CLI. For more information, see the "cfgSerial" object.

When running telnet with Red Hat Enterprise Linux or SUSE Linux Enterprise Server, perform the following steps:

NOTE: To ensure that the text is properly displayed, Dell recommends that you use an Xterm window to display the telnet console instead of the default window provided by the Red Hat Enterprise Linux and SUSE Linux Enterprise Server installation.

1 To start a new Xterm session, type `xterm &` at the command prompt.

2 Drag the lower right corner of the window with the mouse to resize it to 80 x 25 prior to using telnet.

Red Hat Enterprise Linux (or SUSE Linux Enterprise Server) Xterm is now ready to connect by Telnet to the DRAC/MC. To connect to the DRAC/MC, at the Xterm prompt, type `telnet <DRAC/MC IP address>`.

Enabling Microsoft Telnet for Telnet Console Redirection

Microsoft telnet requires that you first enable **Telnet** in **Windows Component Services**.

When telnet is enabled, connect to the DRAC/MC by performing the following steps:

1. Open a command prompt.
2. Type `telnet <DRAC/MC IP address>:<port number>` and press <Enter> (where *IP address* is the IP address for the DRAC/MC and *port number* is the telnet port number if it has been changed from its default value of 23).

Using a Serial or Telnet Console

NOTE: If you are running Windows XP or the Windows 2003 operating system and experiencing problems with characters in a DRAC/MC telnet session, see the Microsoft Knowledge Base article 824810 on the Microsoft Support site at **support.microsoft.com** for more information and an available hotfix. This problem may manifest itself as an apparently frozen login (the return key seems not to work and the password prompt does not appear).

NOTE: On a Windows 2000 management station, pressing the <F2> key does not enter BIOS setup. To resolve this problem, use the telnet client supplied with the Windows Services for UNIX® 3.5 recommended free download from Microsoft. You can download Windows Services for UNIX 3.5 from **www.microsoft.com/windows/sfu/downloads/default.asp**.

You can type serial commands and RACADM CLI commands in a serial or telnet console. For more information about the serial commands and RACADM CLI commands, see "Using the DRAC/MC CLI Commands."

5

Managing and Recovering a Remote System

The DRAC/MC provides a Web-based interface, remote RACADM, and a serial/telnet console that allows you to configure the DRAC/MC properties and users, perform remote management tasks, and troubleshoot a remote (managed) system for problems. Use the DRAC/MC Web-based interface for common systems management tasks. This section provides links to information about performing those types of tasks.

You can also perform all Web-based interface configuration tasks with the RACADM CLI commands. For a list of all remote RACADM CLI commands that you can use to perform the text-based equivalents of each task, see "Using the DRAC/MC CLI Commands."

NOTE: When you are working in the Web-based interface, see your DRAC/MC online help for context- sensitive information about each Web-based interface page.

Accessing the Web-Based Interface

To link to the DRAC/MC remote Web-based interface login window, perform the following steps:

Accessing the Login Window

1 Open a Web browser.

2 Type `https://<IP address>`

where *`<IP address>`* is the IP address for the DRAC/MC.

3 Press <Enter>.

4 The DRAC/MC **Log in** window appears.

Logging In

NOTE: To log in, you must have **Log In to DRAC/MC** permission.

You can log in as a DRAC/MC user. To log in, perform the following steps:

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

1 In the **Username** field, type your DRAC/MC user name. The DRAC/MC user name for local users is case sensitive.

2 In the **Password** field, type your DRAC/MC user password. This field is case sensitive. You can also use the <Tab> key to navigate to this field.

3 Click **OK** or press <Enter>.

Logging Out

Click **Log Out** in the upper-right corner of the main window.

NOTE: The **Log Out** link is not displayed until you log in.

NOTE: Closing the browser without gracefully logging out causes the session to remain open until it times out. It is strongly recommended that you click the **Log Out** button to end the session; otherwise, the session remains active until the session time-out is reached.

Adding and Configuring DRAC/MC Users and Alerts

To manage your system with the DRAC/MC, you can create unique users with specific administrative permissions (role-based authority). You can also configure alerts to be e-mailed to specified users.

This section provides instructions about how to perform the following tasks:

- Adding and Configuring DRAC/MC Users
- Configuring the DRAC/MC NIC
- Adding and Configuring SNMP Alerts

Adding and Configuring DRAC/MC Users

1 Click the **Configuration** tab and select **Users**.

2 Click [**Available**] under the **Username** column to add a new user, or click the user name under the **Username** column to edit an existing user.

3 In the **Add/Configure DRAC/MC User** page, configure the user name, password, access permissions, and e-mail alert settings for a new or existing DRAC/MC user.

Configuring a New User Name and Password

Use Table 5-1 to configure a new or existing DRAC/MC user name and password.

Table 5-1. User Properties

Property	Description
Username	Allows you to specify a DRAC/MC user name. (A new user must be created with a unique user name.)
Password	Allows you to specify or edit the DRAC/MC user's password.
Confirm New Password	Requires you to retype the DRAC/MC user's password to confirm.

Configuring User Permissions

Under **User Permissions**, click the **User Group** drop-down menu and select the permissions group for the user.

Use Table 5-2 to determine the **User Group** (permissions) for the user.

Table 5-2. User Group Permissions

User Group	Permissions Granted
Administrator	**Log in to DRAC/MC**, **Configure DRAC/MC**, **Configure Users**, **Clear Logs**, **Execute Server Control Commands**, **Access Console Redirection**, **Access Virtual Media**, **Test Alerts**, **Execute Diagnostic Commands**, and receive e-mail alerts (if **Enabled**)
Power User	**Log in to DRAC/MC**, **Clear Logs**, **Execute Server Control Commands**, **Access Console Redirection**, **Access Virtual Media**, **Test Alerts**, and receive e-mail alerts (if **Enabled**)
Guest User	**Log in to DRAC/MC**, and receive e-mail alerts (if **Enabled**)
E-mail Alerts Only	Receive e-mail alerts (if **Enabled**)
Custom	Allows you to select any combination of the following permissions: **Log in to DRAC/MC**, **Configure DRAC/MC**, **Configure Users**, **Clear Logs**, **Execute Server Action Commands**, **Access Console Redirection**, **Access Virtual Media**, **Test Alerts**, **Execute Diagnostic Commands**, and receive e-mail alerts (if **Enabled**)

Configuring User E-mail Alerts

Enabling User E-mail Alerts

Use the information in Table 5-3 to enable e-mail alerts.

Table 5-3. Enable E-mail Alert Properties

Property	Description
Enable e-mail Alerts	Enables the DRAC/MC e-mail alerts feature and allows you to select which events, according to their severity, will cause an e-mail alert to be sent.
E-mail Address	Specifies the e-mail address to which alerts are sent.
Message	Specifies the e-mail message text.

Configuring E-mail Alerts by Severity

The information under **e-mail Alerts** in the Web-based interface enables you to select which events, according to their severity, will cause an e-mail alert to be sent. Select the severity of the temperature, voltage, fan, or miscellaneous sensor for which you want an e-mail alert generated.

You can specify three severities: **Informational** (lowest severity), **Warning** (medium severity), and **Severe** (highest severity). Alerts are sent to the e-mail address that you typed in **e-mail Alerts**. For information about each e-mail alert severity type, see Table 5-4.

Table 5-4. E-mail Alert Severity

Severity	Description
Informational	Select the check boxes in this column to enable the DRAC/MC to send an alert if the corresponding event listed under **Alert Description** occurs with a severity of **Informational**.
Warning	Select the check boxes in this column to enable the DRAC/MC to send an alert if the corresponding event listed under **Alert Description** occurs with a severity of **Warning**.
Severe	Select the check boxes in this column to enable the DRAC/MC to send an alert if the corresponding event listed under **Alert Description** occurs with a severity of **Severe**.

The **Alert Description** lists the following events monitored by the DRAC/MC:

- **Select All** — Monitors all of the sensors available on the system.
- **System Temperature Sensors** — Monitors the system temperature sensors.
- **System Voltage Sensors** — Monitors the system voltage sensors.
- **System Fan Sensors** — Monitors the system fan speed (RPM).
- **System Miscellaneous Sensors** — Monitors other available system sensors, such as chassis intrusion.

A specified alert (either **Informational**, **Warning**, or **Severe**) is sent when the event is triggered at the level of severity you selected in the check boxes that are displayed to the left in the window.

Printing the Page

Click the **Print** button in the top-right corner of the screen to print the **Add/Configure DRAC/MC User** page.

Configuring the DRAC/MC NIC

1. Click the **Configuration** tab and select **Network**.
2. Use the **Network Configuration** page to configure the DRAC/MC NIC settings, and configure the e-mail alert settings and the telnet settings. Table 5-5 describes each NIC setting.
3. If you updated the DRAC/MC NIC settings in step 2 from their original settings, reconfigure the telnet and Web sessions with the updated IP address and gateway settings.

NOTE: To change any of the settings on the **Network Configuration** page, you must have **Configure DRAC/MC** permission.

Table 5-5. DRAC/MC NIC Settings

Setting	Description
MAC Address	Displays the DRAC/MC MAC address.
Enable NIC (Default: On)	Enables the DRAC/MC NIC and activates the remaining controls in this group.
Use DHCP (For NIC IP Address) (Default: Off)	Enables the DRAC/MC NIC to obtain the IP address from the DHCP server; deactivates the **Static IP Address**, **Static Subnet Mask**, and **Static Gateway** controls.
Static IP Address	Specifies or edits the Static IP address for the DRAC/MC NIC. To change this setting, first deselect the **Use DHCP (For NIC IP Address)** check box.
Static Gateway	Specifies or edits the static gateway for the DRAC/MC NIC. To change this setting, first deselect the **Use DHCP (For NIC IP Address)** check box.
Static Subnet Mask	Specifies or edits the static subnet mask for the DRAC/MC NIC. To change this setting, first deselect the **Use DHCP (For NIC IP Address)** check box.
Use DHCP to obtain DNS server addresses	Uses DHCP to obtain DNS server addresses. To use static IP addresses, deselect this box and enter the IP addresses in the **Static Preferred DNS Server** and **Static Alternate DNS Server** field(s).
Static Preferred DNS Server	Specifies the static IP address for the primary DNS server. To change this setting, deselect the **Use DHCP to obtain DNS server addresses** check box.
Static Alternate DNS Server	Specifies the static IP address for the backup DNS server. To change this setting, deselect the **Use DHCP to obtain DNS server addresses** check box.
Register DRAC/MC on DNS	Enables the DRAC/MC to register the DRAC/MC name on the DNS server. If disabled, the DRAC/MC will register the default name, **RAC-service tag**, on the DNS server.
DNS DRAC/MC Name	Specifies or edits the DRAC/MC name.
Use DHCP for DNS Domain Name	Enables the DRAC/MC to obtain the domain name from the DHCP server.
DNS Domain Name	Specifies or edits the DRAC/MC domain name.
Auto Negotiation	Determines whether the DRAC/MC automatically sets the **Duplex Mode** and **Network Speed** by communicating with the nearest router or hub (**On**) or allows you to set the **Duplex Mode** and **Network Speed** manually (**Off**).
Duplex Mode	Configures the duplex mode to full or half to match your network environment. This option is not available if **Auto Negotiation** is set to **On**.
Network Speed	Configures the network speed to 100 Mb or 10 Mb to match your network environment. This option is not available if **Auto Negotiation** is set to **On**.
GUI Session Time-out	Specifies the time (from 5 to 60 minutes in 5-minute intervals) before the session is forced to log out if input is not received.
E-mail Alert Settings	Enables e-mail messaging and activates the SMTP (e-mail) Server Address control.

Table 5-5. DRAC/MC NIC Settings *(continued)*

Setting	Description
SMTP (E-mail) Server Address	Specifies or edits the IP address of the SMTP server through which all e-mail messages will be sent.
Enable SNMP (Default: Disable)	Enables or disables the Simple Network Management Protocol (SNMP) service used for sending alerts.
Community	The community name used for the SNMP service.
Enable Telnet (Default: Enable)	Enables or disables the DRAC/MC telnet service so users can connect remotely through telnet.
Telnet Port Number	The port number that the DRAC/MC telnet service will use to communicate with the remote telnet application.

Other Options

The **Network Configuration** page provides the buttons in Table 5-6 in the top-right corner of the screen.

Table 5-6. Network Configuration Page Buttons (Top Right)

Button	Action
Print	Prints the **Network Configuration** page.
Refresh	Reloads the **Network Configuration** page.
Apply Changes	Saves the changes made to the network configuration.

Adding and Configuring SNMP Alerts

NOTE: You must have **Configure DRAC/MC** permission to add or delete an SNMP alert; otherwise, these options will not be available.

1 Click the **Configuration** tab and select **Alerts**.

2 Use the **Add/Configure SNMP Alerts** page to add, delete, configure, and test SNMP alerts.

NOTE: The DRAC/MC supports three severity levels: **Informational, Warning,** and **Severe**. Some events support only the informational severity level because they deliver only a message.

Adding an Alert Destination

1 In the **Destination IP Address** column, locate an available **Destination IP Address**.

If all **Destination IP Addresses** are populated with IP addresses, you have configured all of your existing alerts. To continue, delete an alert.

2 Click [**Available**] to open the **Add/Configure SNMP Alerts** page.

3 Under **General**, use Table 5-7 to configure the Alert properties.

4 Click **Apply Changes** to apply your changes or click **Go Back to SNMP Alerts Page** to return to the previous page.

Table 5-7. Alert Properties

Property	Description
Enable SNMP Alert	Determines whether you want to enable the current SNMP alert.
Community	Specifies or edits the community name to which the destination IP address belongs.
IP Address	Specifies or edits the destination IP address to which the alert is sent.

Configuring Alerts by Severity

1. Use the **Severity Configuration** section to select which events, according to their severity, will cause an SNMP alert to be sent to the IP address you typed in **Configuring Alert Properties**.
2. Select a check box under the severity of the sensor for which you want an SNMP alert generated.
3. Use Table 5-8 to configure the events that generate an SNMP alert.

Table 5-8. Severity Options

Option	Description
Informational	Select the check boxes in this column to enable the DRAC/MC to send an alert if the corresponding event listed under **Alert Description** occurs with a severity of **Informational** (lowest severity).
Warning	Select the check boxes in this column to enable the DRAC/MC to send an alert if the corresponding event listed under **Alert Description** occurs with a severity of **Warning** (medium severity).
Severe	Select the check boxes in this column to enable the DRAC/MC to send an alert if the corresponding event listed under **Alert Description** occurs with a severity of **Severe** (highest severity).

The **Alert Description** lists the following events monitored by the DRAC/MC:

- **Select All** — Monitors all available sensors on the system.
- **System Temperature Sensors** — Monitors the system temperature sensors.
- **System Voltage Sensors** — Monitors the system voltage sensors.
- **System Fan Sensors** — Monitors the system fan speed (RPM).
- **System Miscellaneous Sensors** — Monitors other available system sensors.

A specified alert (either **Informational**, **Warning**, or **Severe**) is sent when the event is triggered by the level of severity you selected in the check boxes.

For information about how to manage events, see the *Dell OpenManage™ Baseboard Management Controller's User's Guide*.

Viewing Information About Existing Alerts

Click an alert in the **SNMP Alert List to** display the following properties for existing SNMP alerts. See Table 5-9 for descriptions.

Table 5-9. SNMP Alert Properties

Property	Description
Enabled?	Displays (**Yes** or **No**) whether you have enabled SNMP alerts on the **Add/Configure SNMP Alerts** page.
Destination IP Address	Displays the destination IP address to which the corresponding alert is sent. Click the IP address to open the **Add/Configure SNMP Alerts** window. If the **Available** link appears under **Destination IP Address**, click the link to open the **Add/Configure SNMP Alerts** page, and configure a new alert.
Community	Displays the SNMP community for the **Destination IP Address**.

Testing an Alert

You can force an alert to be sent to the specified destination IP address. In the **SNMP Alert List**, select **Test Alert** for the alert you want to test. This action generates an alert to the specified IP address.

NOTE: Only users with **Test Alerts** permission will have the **Test Alert** option available next to their user name.

Deleting an Alert Destination

In the **SNMP Alert List**, select **Remove Alert** for the alert you want to delete.

Other Options

The **SNMP Alerts** and **Add/Configure SNMP Alerts** pages provide the buttons in Table 5-10 in the top-right corner of the screen.

Table 5-10. SNMP Alerts Page Buttons (Top Right)

Button	Action
Print	Prints the **SNMP Alerts** page.
Refresh	Reloads the **SNMP Alerts** page.

Managing a Remote System

This section provides instructions about how to perform the following systems management tasks to manage a remote system:

- Updating the DRAC/MC Firmware
- Viewing the Chassis Summary
- Troubleshooting a Remote System

Updating the DRAC/MC Firmware

Use the **Firmware Update** page to update the DRAC/MC firmware to the latest revision. When you run the update, the software retains your current DRAC/MC settings.

The following data is included in the DRAC/MC firmware package:

- A binary image file containing compiled DRAC/MC firmware code and data
- An executable program used in conjunction with the **Firmware Recovery Console** to install the firmware through the serial port
- The DRAC/MC SNMP **rac_host.mib** file

In firmware releases prior to version 1.2, the firmware update self-extracting .zip file included the following files:

- **mgmt.bin** — Contains the DRAC/MC firmware image.
- **upload.exe** — Recovers the previous firmware version if the installed firmware is corrupted.
- **rac_host.mib** — Provides firmware information.

In firmware version 1.2 and later, the **upload.exe** and **rac_host.mib** files may be packaged separately from the firmware package.

To update the DRAC/MC firmware, perform the following steps:

1. Download the latest DRAC/MC firmware and save the extracted file to your TFTP server.
2. Ensure that the chassis is powered on.
3. In the Web-based user interface, select the **Update** tab.
4. Enter the filename of the firmware image stored on your TFTP server in the **Image Name** text box.
5. Enter the IP address of your TFTP server in the **TFTP Server IP** text boxes.
6. Click **Update Firmware**.

   The firmware update may take several minutes to complete.

   During this procedure, the Web server, telnet server, and KVM module are not available, and the video is redisplayed on the monitor.

NOTICE: Avoid power cycling or resetting (remotely or locally) the DRAC/MC module during the update procedure, as these procedures will corrupt the firmware image in the DRAC/MC.

7. Reload the Web-based user interface to enter the login page.
8. Clear the Web browser cache.

   See "Clearing the Web Browser Cache With Internet Explorer" and "Clearing the Web Browser Cache With Mozilla or Firefox."

Using the Firmware Recovery Console

If the firmware becomes corrupted for any reason, the DRAC/MC will boot to the **Firmware Recovery Console**. The recovery console output is displayed only through the serial port. To view the console, attach a null modem cable from the DRAC/MC serial port to your management station and run a terminal emulation software package to attach to the DRAC/MC. The console allows you to install the firmware through a TFTP server or the DRAC/MC serial port.

The **Firmware Recovery Console** output is similar to following screen text. The console options are:

```
(1) Upgrade Firmware from Serial Port
(2) Upgrade Firmware from Network
(3) Network Parameters
Choose:__
```

Using the Serial Port to Upload Firmware

To upload the firmware through the serial port, perform the following steps:

1. Select option "`(1) Upgrade Firmware from Serial Port`".
2. After you have selected option `(1)`, characters appear on the DRAC/MC console. At this time, exit your terminal emulation software and start the UPLOAD executable that is included with the firmware upgrade package for your operating system.

The upload will take several minutes to complete. When the upload is complete, the DRAC/MC resets and the DRAC/MC login page is displayed on the serial console, if connected.

Using the Network to Upload the Firmware

To upload the firmware using a TFTP server, perform the following steps:

1. Select option "`(3) Network Parameters`".
2. The network setup page is displayed:

   ```
   (-) Hardware Version : B3A
   (-) MAC Address : 00 C0 9F 44 01 4A
   (1) IP Address : 10.111.250.50
   (2) TFTP Server Address : 10.111.250.51
   (3) Gateway Address : 10.111.254.254
   (4) Subnetmask : 255.255.0.0
   (5) TFTP File Name : mgmt.bin
   (0) EXIT

   Choose:__
   ```

3. This page allows you to configure the DRAC/MC IP address, TFTP server IP address, gateway address, subnet mask, and TFTP filename. Verify that the network configuration is correct, and when all data is verified or updated, select option "`(0) EXIT`".

4 You will be returned to the **Firmware Recovery Console** main menu.

5 Select option "`(2) Upgrade Firmware from Network`".

The upload will take several minutes to complete. When completed, the DRAC/MC will reset and the DRAC/MC login page displays.

Ensuring Network Security

The DRAC/MC uses certificate management to ensure security for your DRAC/MC network communications.

Certificate Management Overview

A certificate signing request (CSR) is a digital request to a certificate authority (CA) for a secure server certificate. Secure server certificates ensure the identity of a remote system and ensure that information exchanged with the remote system cannot be viewed or changed by others. To ensure the security for your DRAC/MC, it is strongly recommended that you generate a CSR, submit the CSR to a CA, and upload the certificate returned from the CA.

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

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

Viewing a Current Chassis Certificate

1 Log in to the DRAC/MC.

2 In the **Remote Access Controller/Modular Chassis** window, click the **Configuration** tab.

3 In the **Network Configuration** page, click **Security**.

4 In the **Certificate Management** page, in the **Option** box, select **View Current Chassis Certificate** and click **Next**.

The **View Current Chassis Certificate** page appears.

Use the **View Current Chassis Certificate** page to view a server certificate for your DRAC/MC. Table 5-11 provides information about the server certificate.

Table 5-11. Current Chassis Certificate Information

Field	Description
Type	Type of certificate; server certificate
Serial	Certificate serial number
Key Size	Encryption key size
Valid From	Issuance date of the certificate
Valid To	Expiration date of the certificate
Subject	Certificate attributes entered by the user
Issuer	Certificate attributes returned by the issuer

The buttons in Table 5-12 are available on the **View Current Chassis Certificate** page.

Table 5-12. View Current Chassis Certificate Page Buttons

Button	Action
Print	Prints the contents of the open window to your default printer.
Go Back to the Certificate Management Page	Returns to the previous page.
Refresh	Updates the chassis certificate values.

Generating, Uploading, and Viewing a Chassis Certificate

1. Click the **Configuration** tab and click **Security**.
2. Select one of the following CSR types:
   - **DRAC/MC** — Remote Access controller
   - **D-KVM** — Avocent Digital Access KVM
3. Use the **Certificate Management** page options (see Table 5-13) to generate a CSR to send to a CA. The CSR information is stored on the DRAC/MC firmware.

NOTE: You must have **Configure DRAC/MC** permission to generate or upload a server certificate.

Table 5-13. Certificate Management Page Options

Option	Action
Generate a New Certificate Signing Request (CSR)	Select this option and click **Next** to open the **Certificate Signing Request Generation** page that enables you to generate a CSR to send to a CA to request a secure Web certificate. **NOTICE:** Each generated CSR overwrites any previous CSR on the firmware. Before the DRAC/MC can accept your certificate, the last generated CSR in the firmware must match the certificate returned from the CA.
Upload Chassis Certificate	Select this option and click **Next** to upload an existing certificate that your company has title to, and uses to control access to the DRAC/MC. **NOTICE:** Only X509, Base 64 encoded certificates are accepted by the DRAC/MC; DER-encoded certificates are not accepted. Upload a new certificate to replace the default certificate you received with your DRAC/MC.
View Current Chassis Certificate	Select this option and click **Next** to view an existing server certificate.

Generating a Certificate Signing Request

Type a value in the field for each CSR attribute. Table 5-14 describes the valid values for each required field.

The **E-mail Address** field is optional. You may type your company's e-mail address, or any e-mail address that you want to have associated with the CSR.

NOTICE: Each new CSR overwrites any previous CSR on the firmware. Before the DRAC/MC can accept your certificate, the CSR in the firmware must match the certificate returned from the CA, or the DRAC/MC will not upload the certificate.

Table 5-14. Required CSR Fields

Field	Description
Common Name (CN)	The exact name being certified (usually the Web server's domain name, for example, **www.xyzcompany.com**). Only alphanumeric characters, hyphens, underscores, and periods are valid. Spaces are not valid.
Organization Unit (OU)	The name associated with an organizational unit, such as a department (for example, Enterprise Group). Only alphanumeric characters, hyphens, underscores, periods, and spaces are valid.
Organization (O)	The name associated with this organization (for example, XYZ Corporation). Only alphanumeric characters, hyphens, underscores, periods, and spaces are valid.
Country Code (C)	The name of the country where the entity applying for certification is located. Use the drop-down menu to select the country.

Table 5-14. Required CSR Fields *(continued)*

Locality (L)	The city or other location of the entity being certified (for example, Round Rock). Only alphanumeric characters and spaces are valid. Do not separate words using an underscore or some other character.
State (S)	The state or province where the entity who is applying for a certification is located (for example, Texas). Only alphanumeric characters and spaces are valid. Do not use abbreviations.

The buttons in Table 5-15 are available on the **Certificate Signing Request Generation** page.

Table 5-15. Certificate Signing Request Generation Page Buttons

Button	Action
Print	Prints the contents of the window's data area using the default printer for your system.
Go Back to Certificate Management Page	Returns to the previous page.
Generate	Generates a CSR and then prompts you to either open it or save it in the directory you specify.

Upload a Certificate

To upload your server certificate to the DRAC/MC firmware, perform the following steps:

1. In the **Remote Access Controller/Modular Chassis** window, click the **Configuration** tab.
2. In the **Network Configuration** page, click **Security**.
3. In the **Certificate Management** page in the **Option** box, select **Upload Chassis Certificate** and click **Next**.
4. In the **Upload Chassis Certificate** page in the **Attribute** box, type the path to the chassis certificate and click **Upload**.

NOTE: The **Full Path** value displays the file path of the certificate to be uploaded. Type the absolute file path (for example, the full path and the complete filename including the file extension).

The buttons in Table 5-16 are available on the **Upload Chassis Certificate** page.

Table 5-16. Certificate Management Page Buttons

Button	Action
Print	Prints the contents of the **Upload Certificate** page.
Go Back to the Certificate Management Page	Returns to the previous page.
Upload	Uploads the certificate to the DRAC/MC firmware.
Refresh	Updates the chassis certificate values.

Viewing the Chassis Summary

The **Chassis Summary** page enables you to view summary information about the DRAC/MC, the host chassis, and the current session's status of the host chassis. The **Chassis Summary** page displays the following types of information:

- DRAC/MC information (see Table 5-17)
- Chassis information (see Table 5-18 and Table 5-19)
- Session status information (see Table 5-20)
- KVM information (see Table 5-21)
- Switch information (see Table 5-22)

Table 5-17. Fields for DRAC/MC Information

Field	Description
Date and Time	Displays the date and time in the following format: `Tue Mar 21 21:04:52 2006 GMT+00:00`
Primary DRAC/MC Version	Displays the current firmware version level of the primary DRAC/MC version.
Standby DRAC/MC Version	Displays the current firmware version level of the standby DRAC/MC version.
Firmware Updated	Displays the date and time the firmware was last updated. The field remains blank until a firmware update is performed.
Hardware Version	Displays the DRAC/MC hardware version level.
Current IP Address	Displays the IP address of the DRAC/MC.
Current IP Gateway	Displays the IP address of the switch or router currently servicing the DRAC/MC Ethernet port.
Current IP Netmask	Displays the IP address of the subnet to which the DRAC/MC Ethernet port is connected.
MAC Address	Displays the MAC address of the DRAC/MC.
DHCP Enabled?	Displays whether DHCP is enabled on the DRAC/MC. The default value is Disabled.

Table 5-18. Fields for Chassis Information

Field	Description
System-ID	Displays the system identifier for the chassis.
System Model	Displays the chassis model and type.
Service Tag	Displays the chassis service tag.
Asset Tag	Displays the chassis asset tag number if one has been assigned.
Chassis Name	Displays the chassis name if one has been assigned.
Chassis Location	Displays the chassis location if one has been assigned.

Table 5-19. Fields for DRAC/MC Firmware Status Flags

Field	Description
Global Reset Pending Flag	Displays reset status for the chassis.

Table 5-20. Fields for Session Status

Field	Description
Valid Sessions	Indicates the number of currently active sessions.
Session Type	Displays the connection type of the session.
Session User	Displays the name of the user initiating the session.
User's IP Address	Displays the IP address of the user initiating the session.
Login Date/Time	Displays the time and date that the user logged in according to the DRAC/MC internal clock.

NOTE: The DRAC/MC supports up to four simultaneous users (sessions) logged in at one time.

Table 5-21. Fields for KVM Status

Field	Description
KVM Presence	Indicates whether or not the KVM module is installed in the chassis.
KVM Model	Displays the KVM model and type.
KVM Firmware Version	Indicates the current KVM firmware version level.
KVM Hardware Version	Indicates the current KVM hardware version level.

Table 5-21. Fields for KVM Status *(continued)*

Field	Description
KVM Status	Indicates the status of the current KVM: **N/A**, **Ready**, and **Updating**.
Current IP Address	Indicates the current KVM IP address.
Current IP Gateway	Indicates the current KVM IP gateway IP address.
Current IP Netmask	Indicates the current KVM IP netmask IP address.
MAC Address	Indicates the KVM MAC address.
DHCP Enabled?	Displays whether DHCP is enabled on the Avocent Digital Access KVM. The default value is **Disabled**.

NOTE: Some KVM status fields appear only if an Avocent Digital Access KVM is installed in the Dell™ Modular Server Enclosure.

NOTE: The KVM status field properties do not appear if the Dell Modular Server Enclosure is powered off.

See "Using the KVM Modules" for a complete description of the KVM switches.

With version 1.1 and later, the DRAC/MC supports the following KVM information:

- Firmware version
- Model
- Presence

NOTE: The Dell KVM pass-through switch and the Avocent Analog KVM switch interact differently with the DRAC/MC modules. The KVM pass-through switch does not have a pin for the DRAC/MC to detect its presence, so it does not generate a log when the KVM pass-through is installed or removed. The Avocent Analog KVM switch has a pin for the DRAC/MC to detect its presence, so it generates a log when the KVM is installed or removed.

The KVM function includes a PS2 keyboard, mouse, and VGA signal switching for ten modules. KVM uses keyboard/mouse emulation in each module where the output KVM module switching to the KVM board is controlled by the DRAC/MC for each KVM module control circuit. For a complete description of the KVM switch integration function, see your system's *User's Guide* and *Installation and Troubleshooting Guide* or the *Hardware Owner's Manual*.

The DRAC/MC Web-based interface provides the following information:

- Displays the available server modules to select from and the status of a KVM session; for example, the module running a valid user session.
- Sets the KVM date and time as required, for example, identifying when the KVM is installed or when the DRAC/MC is rebooted, or when the chassis is powered down.

NOTE: Within the Dell Modular Server Enclosure and DRAC/MC document set, the Avocent Analog KVM switch is also referred to as Dell KVM switch with KVM-over-IP.

NOTE: If you have a KVM pass-through switch module, the chassis summary screen in the Web-based interface will indicate that the KVM is absent.

Table 5-22. Fields for Switch Information

Field	Description
Switch Location	Displays the slot number where the switch is installed.
Switch Type	Displays the switch model and/or type.
MAC Address	Displays the MAC address of the switch. **NOTE:** Not all I/O modules have a MAC address, and most that do, only have one MAC address. As a result, MAC addresses only display for devices whose specifications require a MAC address.

Viewing the Chassis Status

The Chassis Status page enables you to view the status of chassis modules and server modules. The Chassis Status page displays the following type of information. (See Table 5-23.)

Table 5-23. Fields for Chassis Status page

Field	Description
Severity	Displays a status icon that indicates the health of the module. There are four types of severity (see Table 5-30): • Normal (green check) • Warning (yellow triangle) • Critical (red x) • Not available (blank)
Name	Displays the name of the module.
Presence	Indicates whether or not the module is installed in the chassis.
Power State	Displays the current power status: **ON**, **OFF**, **Throttled,** or **N/A** (if the component is not present).
Service Tag	Displays the module's service tag if one is available.

Viewing the Power Budget Status

The **Power Budget Status** page enables you to view information about the overall power status, power consumption, and power sharing.

The **Power Budget Status** page displays the following type of information. (See Table 5-24.)

Table 5-24. Values for Power Budget Status

Attribute	Value
Overall Power Status	Displays the power status of the chassis, which is: **OK**, **Warning**, **Failed**, or **N/A**.
Redundancy Policy	Displays the selected Redundancy Policy, which is: **No Redundancy**, **3+1**, **2+2**. **No Redundancy**: In this mode, no power is kept in reserve and failure of a power supply may potentially cause the chassis and server modules to power down if enough power is not available. **3+1**: In this mode, the capacity of the highest rated power supply is kept in reserve so that the chassis and server modules have enough power in the event of failure of any one power supply. **NOTE:** 3+1 is the default **Redundancy Policy** setting. **2+2**: In this mode, the capacity of the two highest rated power supplies is kept in reserve so that failure of any two power supplies will not cause the chassis to power down.
Redundancy	Displays if the power configuration of the system is in redundant state.
Total Available Power	Indicates the sum of the 12V DC wattage capacity of all the installed power supplies in the enclosure.
Redundancy Reserve	Indicates the power kept in reserve to satisfy the configured redundancy policy.
Load Sharing Overhead	Indicates the reduction in power when multiple power supplies are sharing a load in parallel.
Chassis Base Consumption	Indicates the power required for the chassis to boot up.
Server Consumption	Indicates the total power consumption of all server modules installed and powered on in the enclosure.
Total Consumption	Indicates the total power that the system has consumed. This value is the sum of Server Consumption, Chassis Base Consumption, and Load Sharing Overhead.
Remaining Power (excluding reserve)	Indicates the remaining power available for powering on additional server modules in the enclosure. This value excludes the power kept in reserve to satisfy the Redundancy Policy requirements (see Redundancy Reserve).
Chassis Power Supply Status Table	Displays the status and rated wattage for each installed power supply module.
Server Module Power Consumption Table	Displays the wattage that each server module has consumed.

NOTE: The values for Power Budget Status are *static* values, which reflect the maximum potential power consumption for each module/system. These values do *not* reflect the actual dynamic power consumption levels for each module/system.

Power Supply Redundancy

DRAC/MC firmware version 1.3 introduces a new power supply redundancy implementation. Key features are:

- Support for 2+2 and 3+1 power supply redundancy modes.
- CPU throttling of Dell PowerEdge™ 1955 server modules in 2+2 redundant mode if power requirement exceeds remaining power.

Key Requirement

- Four 2100 W power supplies (or greater) need to be installed in the chassis for the redundancy policy selections to be available.

Description

- No Redundancy: In this mode, power from all the power supplies can be used to power on the server modules and failure of any one power supply might cause server modules to lose power.
- 3+1 Redundancy Mode: In this mode, the capacity of the highest-rated power supply in the chassis is kept in reserve so that the failure of any one power supply will not cause any server modules or the chassis to power down. Server modules are prevented from powering up if the power consumption of the chassis exceeds the rated power of the remaining three power supplies.

  Failure of two power supplies in this mode may cause some or all server modules in the chassis to power down.

  Server modules are not throttled in this mode.

  NOTE: 3+1 is the default **Redundancy Policy** setting.
- 2+2 Redundancy Mode: In this mode, the capacity of the two highest-rated power supplies in the chassis is kept in reserve so that the failure of any two power supplies will not cause any server modules or the chassis to power down. PowerEdge 1955 server modules in the chassis will be throttled if the power consumption of the chassis exceeds the rated power of the remaining two power supplies. In this way, the total power consumption of the chassis will be kept below the rated capacities of the two lowest-rated power supplies.

  Failure of two power supplies in this mode will not cause any server modules to lose power.

  Only PowerEdge 1955 server modules might be throttled in this mode. Throttling reduces the power consumption of the server modules by changing the CPU duty cycle. This mode will reduce the blade performance by approximately 50%.

  To have true 2+2 redundancy, two power supplies should be connected to one AC circuit while the other two power supplies should be connected to a different AC circuit. When connected in this way, and with 2+2 redundancy policy selected, the chassis power will be maintained in the event of failure of one AC circuit.

  In this mode, already powered-on PowerEdge 1955 server modules can be throttled to allow a new server module to power up. The PowerEdge 1955 server modules are throttled starting from the highest slot number and unthrottled starting from the lowest slot number.

Viewing Server Summary

This new feature in the DRAC/MC version 1.3 allows you to configure the server names. The servers are named based on the slot they are in, that is, Server-1, Server-2, … , Server-10.

With DRAC/MC version 1.3, the server names will default to the same values as in earlier DRAC/MC firmware versions. However, they can be changed from both the Web and CLI interfaces.

The maximum length of each server name is 15 characters. The server names that are configured are specific to the slot in the chassis and not the servers themselves. So, if a server is moved from one slot to another, the server name will not follow the server. Server names are configurable even if a server is not present in a slot.

NOTE: A server cannot be renamed Server-<n>, if *n* is not the slot number for the server.

The **Server Summary** page enables you to view summary information about the server blades in your system.

The **Server Summary** page displays the following information:

Table 5-25. Fields for Server Summary

Field	Description
Server Location	Indicates the slot where the server module is installed
Service Tag	Displays the server module service tag
Server Name	Displays the user-assigned name of the server module
BMC MAC Address	Displays the MAC address of the BMC (when available)
BMC Baud Rate	Displays the current baud rate of the BMC
Network 1 MAC Address	Displays the first MAC address of the server module (when available)
Network 2 MAC Address	Displays the second MAC address of the server module (when available) **NOTE:** This option is not available on the PowerEdge 1855 modules

Configuring Server Names

1 Click the **Configuration** tab and the **Server** subtab.

2 Click the server name you want to edit.

3 In the **Change Server Name** page, edit the value of the server name.

   NOTE: If all characters in the server name field are deleted, the server name is reset to its default value.

4 Click **Apply Changes**.

Viewing the Sensor Status

The **Sensor Status** page enables you to view the status of sensors in the system. The **Sensor Status** page displays the following types of information: (See Table 5-26.)

- Temperature
- Fan
- Power Supply

Table 5-26. Fields for Sensor Status

Field	Description
Severity	Displays a status icon that indicates the health of the sensor.
Probe location	Displays the location of the sensor.
Reading	Displays the current reading of the sensor.
Minimum Warning Threshold	Minimum value that triggers a **Warning** alert.
Maximum Warning Threshold	Maximum value that triggers a **Warning** alert.
Minimum Failure Threshold	Minimum value that triggers a **Severe** alert.
Maximum Failure Threshold	Maximum value that triggers a **Severe** alert.

Recovering and Troubleshooting the DRAC/MC

This section explains how to perform the following tasks related to recovering and troubleshooting a crashed remote system by using the DRAC/MC Web-based interface:

- Troubleshooting a Remote System
- Managing Power on a Remote System
- Using the SEL
- Using the DRAC/MC Log
- Using the Diagnostic Console

Troubleshooting a Remote System

The following questions are commonly used to troubleshoot high-level problems in the DRAC/MC:

1. Is the system powered on or off?
2. If powered on, is the operating system functioning, crashed, or just frozen?
3. If powered off, did the power turn off unexpectedly?

For crashed systems, you can use console redirection (see "Using Console Redirection From a Management Station") and remote power management (see "Managing Power on a Remote System") to restart the system and watch the reboot process.

Managing Power on a Remote System

The DRAC/MC allows you to remotely perform several power management actions on the server modules and chassis to try to recover after a system crash or other problem. Use the **Server Control** page, which is located in the left window pane under **Power**, to perform an orderly shutdown through the operating system when rebooting, and then power the module on or off.

NOTE: You must have **Execute Server Action Commands** permission to perform power management actions.

Selecting Chassis Control Actions

1. Select the **Shutdown Operating System First** option (only for the **Reboot System**, **Power Off System**, and **Power Cycle System**).

   NOTE: All systems in the chassis must have Advanced Configuration and Power Interface (ACPI) enabled and must be configured properly for the **Shutdown Operating System First** option to work on the whole chassis. If any server module is not correctly ACPI-enabled, the chassis will not complete the chassis action.

2. Select one of the following **Chassis Control Actions**.
   - **Power On System** — Turns on the system power (equivalent to pressing the power button).
   - **Power Off System** — Turns off the system power (equivalent to pressing the power button).
   - **Power Cycle** — Turns off the system power and, after a delay, turns it on again (equivalent to pressing the power button twice).
3. Click **Apply Changes** to perform the power management action (for example, cause the system to power cycle).

Other Options

The **Chassis Control** page provides buttons (see Table 5-27) in the top-right corner of the screen.

Table 5-27. Chassis Control Page Buttons (Top Right)

Button	Action
Print	Prints the **Chassis Control** page.
Refresh	Reloads the **Chassis Control** page.

Selecting Server Control Actions

1. Select a server module on which to perform an action.
2. Select the **Shutdown Operating System First** option (only for the **Reboot System**, **Power Off System**, and **Server Control Actions**).

   If you want to make the system perform an orderly shutdown through the operating system before the selected **Server Control Action**, first shut down the operating system.

   NOTE: To perform the **Shutdown Operating System First** option, you must have an ACPI-enabled operating system that is correctly configured to accept ACPI commands.

   NOTE: The Microsoft® Windows Server™ operating system default policy does not allow you to use a login prompt to shutdown your server module(s). To modify the system default policy, navigate to the **Control Panel**, open **Administrator Tools**, select **Local Security Policy**, and edit the security options.

3. Select one of the following **Server Control Actions**.
   - **Reboot System** — Resets the system (equivalent to pressing the reset button); the power is not turned off by using this function.
   - **Power Cycle** — Turns off the system power and, after a delay, turns it on again (equivalent to pressing the power button twice).
   - **Power Off System** — Turns off the system power (equivalent to pressing the power button).
   - **Power On System** — Turns on the system power (equivalent to pressing the power button).
   - **NMI** — Causes a nonmaskable interrupt (NMI) to occur on the server module (which is useful when a system is locked and needs to be debugged or a memory dump is saved).

   NOTICE: Applying NMI on a running server module causes the operating system to crash, resulting in possible data loss.

4. Click **Apply** to perform the power management action (for example, cause the system to power cycle).

Other Options

The **Server Control** page provides buttons (see Table 5-28) in the top-right corner of the screen.

Table 5-28. Server Control Page Buttons (Top Right)

Button	Action
Print	Prints the **Server Control** page.
Refresh	Reloads the **Server Control** page.

Selecting Switch Control Actions

1 Select a switch module on which to perform an action. Only one **Control Action** can be performed on a switch module:

   Power Cycle — Turns off the switch and, after a delay, turns it on again.

2 Click **Apply** to perform the power management action (for example, cause the system to power cycle).

Other Options

The **Switch Control** page provides buttons (see Table 5-29) in the top-right corner of the screen.

Table 5-29. Switch Control Page Buttons (Top Right)

Button	Action
Print	Prints the **Switch Control** page.
Refresh	Reloads the **Switch Control** page.

Using the SEL

The **System Event Log (SEL)** displays system-critical events that occur on the chassis. This page displays the date, time, and a description of each event generated by the DRAC/MC. You can configure the DRAC/MC to send e-mail or SNMP alerts when specified events occur.

NOTE: When the SEL is full, it cannot accept additional alerts. The SEL will warn users by sending SNMP alerts when the log is at 80%, 90%, and 100% capacity. To allow additional alerts to be stored, clear the SEL.

The SEL displays the event severity information in Table 5-30.

Table 5-30. Status Indicator Icons

Icon	Status
✓	A green check mark indicates a healthy (normal) status condition.
⚠	A yellow triangle containing an exclamation point indicates a warning (noncritical) status condition.
✗	A red X indicates a critical (failure) status condition.
🟦	A blank space indicates that the status is unknown.

The SEL also provides the following information:

- **Date/Time** — The date and time that the event occurred.
- **Description** — A brief description of the event.

The SEL provides buttons (see Table 5-31) in the top-right corner of the screen.

NOTE: The **Clear Log** button only appears if you have **Clear Logs** permission.

Table 5-31. SEL Buttons (Top Right)

Button	Action
Print	Prints the **SEL**.
Clear Log	Clears the **SEL**.
Save As	Opens a pop-up window that enables you to save the **SEL** to a directory of your choice.
Refresh	Reloads the **SEL** page.

Table 5-32 provides a list of SEL messages, and their corresponding severity levels.

Table 5-32. SEL Messages

ID #	Log Messages	Severity
1	Module Added	Informational
	DRAC/MC-x module sensor presence was detected.	Informational
	<*Server name*> module sensor presence was detected.	Informational
	Switch-x module sensor presence was detected.	Informational
	Fan-x module sensor presence was detected.	Informational
	PS-x module sensor presence was detected.	Informational
2	Module Removed	Informational
	DRAC/MC-x module sensor was removed.	Warning
	<*Server name*> module sensor was removed.	Warning
	Switch-x module sensor was removed.	Warning
	Fan-x module sensor was removed.	Critical
	PS-x module sensor was removed.	Critical
3	Module Sensor Returned to Normal	Informational
	Chassis module sensor returned to normal.	Informational
	DRAC/MC-x module sensor returned to normal.	Informational
	<*Server name*> module sensor returned to normal.	Informational
	Switch-x module sensor returned to normal.	Informational
	Fan-x module sensor returned to normal.	Informational
	PS-x module sensor returned to normal.	Informational
4	<*Module name*> module sensor was not available or failure was detected.	Warning
	Chassis module sensor failure was detected.	Warning
	DRAC/MC-x module sensor failure was detected.	Warning

Table 5-32. SEL Messages *(continued)*

ID #	Log Messages	Severity
	<*Server name*> module sensor failure was detected.	Warning
	Switch-x module sensor failure was detected.	Warning
	Fan-x module sensor failure was detected.	Warning
	PS-x module sensor failure was detected.	Warning
5	Module Sensor Returned to Failure	Warning
	Chassis module sensor returned to failure.	Warning
	DRAC/MC-x module sensor returned to failure.	Warning
	<*Server name*> module sensor returned to failure.	Warning
	Switch-x module sensor returned to failure.	Warning
	Fan-x module sensor returned to failure.	Warning
	Power-x module sensor returned to failure.	Warning
6	Module Sensor Detected Nonrecoverable Events	Critical
	Chassis module sensor detected a nonrecoverable event.	Critical
	DRAC/MC-x module sensor detected a nonrecoverable event.	Critical
	<*Server name*> module sensor detected a nonrecoverable event.	Critical
	Switch-x module sensor detected a nonrecoverable event.	Critical
	Fan-x module sensor detected a nonrecoverable event.	Critical
	Power-x module sensor detected a nonrecoverable event.	Critical
9	Sensor Returned to Normal	Informational
	Fanx-Fan-x RPM fan sensor returned to normal (5000 RPM).	Informational
	Housing-Left temperature sensor returned to normal (25).	Informational
	Switch-3 voltage sensor returned to normal (3.3V).	Informational
10	Sensor Failure Was Detected	Warning
	Fan-x RPM fan sensor failure was detected (3000 RPM).	Warning
	Housing-Left temperature sensor failure was detected (60).	Warning
	Switch-x voltage sensor failure was detected (3.5V).	Warning
11	Sensor Returned to Failure	Warning
	Fan-x RPM fan sensor returned to failure (3000 RPM).	Warning
	Housing-Left temperature sensor returned to failure (60).	Warning
	Switch-x voltage sensor returned to failure (3.5V).	Warning

Table 5-32. SEL Messages *(continued)*

ID #	Log Messages	Severity
12	Sensor Detected Nonrecoverable Event	Critical
	Fan-x RPM fan sensor detected nonrecoverable event (0 RPM).	Critical
	Housing-Left temperature sensor detected nonrecoverable event (80).	Critical
	Switch-x voltage sensor detected nonrecoverable event (3.7V).	Critical
13	Power Supply Sensor Power Lost	Warning
	PS-x power supply sensor power was lost.	Warning
14	Power Supply A/C Recovery	Informational
	PS-x power supply sensor power was restored.	Informational
15	Minimum System Power Output Wattage Less Than the Required 3600W	Warning
16	Minimum System Power Output Wattage Returned To Normal	Informational
17	DRAC/MC SEL Log Was Cleared	Informational
18	Switch-x I/O module is not the same model as the remaining slave or master I/O module.	Warning
19	Switch-x slave I/O module must be installed with the master I/O module.	Warning
20	Switch-x I/O module fabric does not support the I/O module group.	Warning
21	Switch-x I/O module configuration does not match one or more existing server module configurations.	Warning
22	<*Server name*> daughter card configuration does not match the I/O module configuration.	Warning
23	<*Server name*> daughter card configuration does not match the existing server module configurations.	Warning
24	Server daughter card configurations are not identical.	Warning
25	The DRAC/MC system event log is 80% full.	Informational
26	The DRAC/MC system event log is 90% full.	Informational
27	The DRAC/MC system event log is 100% full.	Informational
28	DRAC/MC-1 and DRAC/MC-2 module firmware versions are not identical.	Warning
29	<*Server name*> unknown server blade type detected. DRAC/MC firmware may need to be upgraded.	Warning
30	1200 W power supply is not recommended with <*server name*>.	Warning

Using the DRAC/MC Log

The **DRAC/MC Log** is a persistent log maintained in the DRAC/MC firmware. The log contains a list of user actions (such as log in and log out) and alerts issued by the DRAC/MC. The oldest entries are overwritten when the log becomes full. The **DRAC/MC Log** provides the information in Table 5-33.

Table 5-33. Status Indicator Icons

Icon	Status
✓	A green check mark indicates a healthy (normal) status condition.
⚠	A yellow triangle containing an exclamation point indicates a warning (noncritical) status condition.
✗	A red X indicates a critical (failure) status condition.
🟦	A blank space indicates that the status is unknown.

The DRAC/MC log also contains the following information:

- **Date and Time** — The date and time (for example, `Tue Mar 21 16:55:47 2006`). When the DRAC/MC is unable to communicate with the server, the letters DSU (DRAC/MC startup) appear before the time, followed by the time elapsed since the DRAC/MC was started.
- **User** — The name of the user logging into the DRAC/MC.
- **Description** — A brief description of the event.

Using the DRAC/MC Log Buttons

The **DRAC/MC Log** provides the following buttons:.

Table 5-34. DRAC/MC Log Buttons

Button	Action
Print	Prints the **DRAC/MC Log** page.
Clear Log	Clears the **DRAC/MC Log** entries. **NOTE:** The **Clear Log** button only appears if you have **Clear Logs** permission.
Save As	Opens a pop-up window that enables you to save the **DRAC/MC Log** to a directory of your choice.
Refresh	Reloads the **DRAC/MC Log** page.

DRAC/MC Log Messages

DRAC/MC Log messages can be used by administrators to debug alerting from the DRAC/MC. Table 5-35 provides a list of the DRAC/MC users, messages, descriptions, and severity levels.

Table 5-35. DRAC/MC Log Messages

User	Message	Description	Severity
<User>	Requested chassis powercycle.	User requested chassis power cycle	Informational
<User>	Requested chassis powerdown.	User requested chassis power down	Informational
<User>	Requested chassis powerup.	User requested chassis power up	Informational
<User>	Requested chassis Graceful Shutdown.	User requested chassis graceful shutdown	Informational
<User>	Requested switch-x powercycle.	User requested switch power cycle	Informational
System	An invalid SSL certificate has been uploaded.	User uploaded an invalid SSL certificate	Warning
<User>	[Serial, Web, Telnet, or RACADM] Login successful.(xxx.xxx.xxx.xxx)	User login successful	Informational
<User>	[Serial, Web, Telnet, or RACADM] Login authentication failed.(xxx.xxx.xxx.xxx)	User authentication failure	Warning
<User>	[Serial, Web, Telnet, or RACADM] Logout (xxx.xxx.xxx.xxx)	User logout	Informational
<User>	[Serial, Web, Telnet, or RACADM] Session cancelled due to inactivity. (xxx.xxx.xxx.xxx)	Session cancelled due to inactivity and automatic logout occurred	Informational
<User>	[Serial, Web, Telnet, or RACADM] Session cancelled because client IP address changed. (xxx.xxx.xxx.xxx)	IP address changed; session cancelled	Informational
Unknown	[Serial, Web, Telnet, or RACADM] Session cancelled due to an invalid session ID from xxx.xxx.xxx.xxx	Invalid session ID caused session to be cancelled	Informational
System	Smtp: mail server xxx.xxx.xxx.xxx unreachable	Mail Server unreachable	Critical
<User>	Snmp: trap sent to xxx.xxx.xxx.xxx	User sent a test trap	Informational
<User>	Smtp: send test mail	User sent a test mail	Informational
<User>	Requested <*servername*> performed hard-reset	User requested server reset	Informational
<User>	Requested <*servername*> performed a powercycle	User requested server power cycle	Informational

Table 5-35. DRAC/MC Log Messages *(continued)*

User	Message	Description	Severity
<User>	Requested <*servername*> performed a powerdown	User requested server to power down	Informational
<User>	Requested <*servername*> performed powerup	User requested server to power up	Informational
<User>	Requested <*servername*> ACPI – Graceful Operating System Shutdown	User requested server ACPI – Graceful Operating System Shutdown	Informational
<User>	DRAC/MC IP changed	User changed DRAC/MC IP address	Informational
System	DRAC/MC-x Powered On	DRAC/MC booted up	Informational
System	DRAC/MC SSL certificate expired	DRAC/MC SSL certificate expired	Warning
<User>	DRAC/MC-x firmware update started	User started a DRAC/MC firmware update	Informational
<User>	DRAC/MC-x reset	User reset DRAC/MC module	Informational
System	DRAC/MC-x assumed primary role	DRAC/MC changed to primary role	Informational
<User>	DRAC/MC set time	User set DRAC/MC time	Informational
<User>	DRAC/MC SEL log was cleared	User cleared SEL	Informational
<User>	DRAC/MC log was cleared	User cleared DRAC/MC log	Informational
System	<*Servername*> power-on request failed because over power budget	One server module powered up and failed because over power budget	Warning
System	<*Servername*> powered off because of a power over budget issue.	One server module powered down due to insufficient power	Warning
System	<*Module Name*> service tag duplicated	Detected an I/O module with duplicated service tag	Warning
System	<*Module Name*> does not have a service tag	Detected an I/O module without service tag	Warning
System	<*Module Name*> configured with an invalid FRU	Detected an I/O module without validated FRU	Warning
System	<*Module Name*> detected an unknown I/O module.	Detected unknown type I/O module	Warning
System	DRAC/MC-x firmware update successful	DRAC/MC firmware update success	Informational
System	DRAC/MC-x firmware update failed because the TFTP server is unreachable.	DRAC/MC firmware update fail	Warning
<User>	Requested <*servername*> NMI	User requested server NMI	Informational
System	ENABLE throttle command that was sent to <*servername*> performed successfully.	Enabling throttle command on <*servername*> successful	Informational

Table 5-35. DRAC/MC Log Messages *(continued)*

User	Message	Description	Severity
System	ENABLE throttle command that was sent to <*servername*> failed.	Enabling throttle command on <*servername*> failed	Warning
System	DISABLE throttle command that was sent to <*servername*> performed successfully.	Disabling throttle command on <*servername*> successful	Informational
System	DISABLE throttle command that was sent to <*servername*> failed.	Disabling throttle command on <*servername*> failed	Warning
<User>	KVM firmware update started	Started the KVM firmware transaction	Informational
<User>	KVM firmware update successful	The KVM firmware update successful	Informational
<User>	KVM firmware update failed because the TFTP server is unreachable.	The DRAC/MC cannot reach the TFTP server; KVM firmware update failed	Warning
<User>	KVM firmware update failed because the image is unavailable.	Unavailable image; KVM firmware update failed	Warning
<User>	KVM firmware update failed because the TFTP server timed-out.	The TFTP server timed-out; KVM firmware update failed	Warning
<User>	KVM firmware update failed because the image is invalid.	Invalid image or packets; KVM firmware update failed	Warning
<User>	KVM firmware update failed because of an open virtual media session.	The Virtual Media session is open; KVM firmware update failed	Warning
<User>	The KVM firmware file transfer is complete.	The KVM firmware file transfer is complete.	Informational
<User>	KVM firmware update failed because the TFTP server is unreachable.	The KVM firmware update failed because the TFTP server is unreachable.	Warning
<User>	KVM firmware update failed because the image is unavailable.	The KVM firmware update failed because the image is unavailable.	Warning
<User>	KVM firmware update failed because the TFTP server timed-out.	The KVM firmware update failed because the TFTP server timed out.	Warning
<User>	KVM firmware update failed because the image is invalid.	The KVM firmware update failed because the image is invalid.	Warning
<User>	The DRAC/MC-1 changed role because of Ethernet disconnection.	The DRAC/MC-1 changed role because of the ethernet disconnection.	Warning
<User>	The DRAC/MC-1 firmware update failed because the image is unavailable.	The DRAC/MC-1 firmware update failed because the image is unavailable.	Warning
<User>	The DRAC/MC-1 firmware update failed because the image is invalid.	The DRAC/MC-1 firmware update failed because the image is invalid.	Warning
<User>	The DRAC/MC-1 firmware update failed because the TFTP server timed out	The DRAC/MC-1 firmware update failed because the TFTP server timed out.	Warning

Table 5-35. DRAC/MC Log Messages *(continued)*

User	Message	Description	Severity
System	Failed to read the FRU from Server-1.	Failed to read the server blade FRU.	Warning
<User>	The PowerEdge 1855 server module %d must be running BIOS version A04 or later to support the DRAC/MC Virtual Media feature.	The PowerEdge 1855 server module %d must be running BIOS version A04 or later to support the DRAC/MC Virtual Media feature	Warning
<User>	KVM firmware update failed because of an authentication error.	The KVM firmware update failed because of authentication error.	Warning
<User>	KVM firmware update failed because of unknown error.	The KVM firmware update failed because of unknown error.	Warning
<User>	The requested server-1 performed a graceful reset.	Requested server-%d performed a graceful reboot.	Informational
<User>	Requested KVM power-cycle.	The user requested KVM to do a power-cycle.	Warning
<User>	The Active Directory certificate was uploaded successfully.	The Active Directory certificate was uploaded successfully.	Informational
<User>	The Digital KVM settings are reset to factory defaults.	The Digital KVM settings are reset to factory defaults.	Warning
<User>	DRAC/MC detected an unknown blade ID for server-1.	The DRAC/MC detected an unknown blade ID for server-1.	Informational
<User>	The user initiated a Console Redirection session.	The user initiated a console redirection session.	Informational
<User>	The user initiated a Virtual Media session.	The user initiated a virtual media session.	Informational
<User>	The Active Directory Certificate upload failed because the file was invalid.	The Active Directory Certificate upload failed because the file was invalid.	Informational
<User>	The Web Certificate upload failed because the file was invalid.	The Web Certificate upload failed because the file was invalid.	Informational

Using the Diagnostic Console

The **Diagnostic Console** page enables advanced users or users under the direction of technical support to diagnose issues relating to the DRAC/MC hardware.

Use the diagnostic commands in Table 5-36 to display specific information about the DRAC/MC, and click **Submit**.

Table 5-36. Diagnostic Commands

Command	Description
`arp`	Displays the contents of the Address Resolution Protocol (ARP) table. ARP entries may not be added or deleted.
`ifconfig`	Displays the contents of the network interface table.
`netstat`	Prints the contents of the routing table. If the optional interface number is provided in the text field to the right of the **NetStat** option, then NetStat prints additional information regarding the traffic across the interface, buffer usage, and other network interface information.
`ping` <*IP Address*>	Verifies that the destination IP address is reachable from the DRAC/MC with the current routing-table contents. A destination IP address must be typed in the field to the right of this option. An ICMP (Internet control message protocol) echo packet is sent to the destination IP address based on the current routing-table contents.

The **Diagnostic Console** provides buttons (see Table 5-37) in the top-right corner of the screen.

Table 5-37. Diagnostic Console Page Buttons (Top Right)

Button	Action
Print	Prints the **Diagnostic Console** page.
Refresh	Reloads the **Diagnostic Console** page.

Troubleshooting Alerting Problems

Because SNMP does not confirm delivery of traps, it is best to trace the packets on the DRAC/MC using a network analyzer or a tool such as the Microsoft **snmputil** tool.

Frequently Asked Questions

Table 5-38 lists frequently asked questions and answers.

Table 5-38. Managing and Recovering a Remote System: Frequently Asked Questions

Question	Answer
When accessing the DRAC/MC Web-based interface, I get a security warning stating that the host name of the SSL certificate does not match the host name of the DRAC/MC.	DRAC/MC includes a default DRAC/MC server certificate to ensure network security for the Web-based interface and remote RACADM features. When this certificate is used, the Web browser displays a security warning because the default certificate is issued to **RAC default certificate** which does not match the host name of the DRAC/MC (for example, the IP address). To address this security concern, upload a DRAC/MC server certificate issued to the IP address of the DRAC/MC. When generating the CSR to be used for issuing the certificate, ensure that the common name (CN) of the CSR matches the IP address of the DRAC/MC (for example, 192.168.0.120).
When accessing the DRAC/MC Web-based interface, I get a security warning stating that the SSL certificate was issued by a CA that is not trusted.	DRAC/MC includes a default DRAC/MC server certificate to ensure network security for the Web-based interface and remote RACADM features. This certificate was not issued by a trusted CA. To address this security concern, upload a DRAC/MC server certificate issued by a trusted CA (for example, Thawte or Verisign).

6

Using the DRAC/MC With Microsoft® Active Directory®

A directory service is used to maintain a common database of all information needed for controlling users, computers, printers, etc. on a network.

If your company uses the Microsoft Active Directory service software, it can be configured to give you access to the DRAC/MC, allowing you to add and control DRAC/MC user privileges to your existing users in your Active Directory software. To access the DRAC/MC, your system must be running Microsoft Windows® 2000 or the Windows Server™ 2003 operating system.

NOTE: The DRAC/MC user interface only allows one Active Directory user login at a time.

Active Directory Schema Extensions

The Active Directory data can be conceptualized as a distributed database of Attributes and Classes. The rules for what data can be added or included in the database is the Active Directory schema. An example of a Class that is stored is the user class. Some example attributes of the user class are the user's first name, last name, phone number, and so on. Companies can extend the Active Directory database by adding their own unique Attributes and Classes to solve environment–specific needs. Dell has extended the schema to include the necessary changes to support remote management Authentication and Authorization.

Every Attribute or Class that is added to an existing Active Directory Schema must be defined with a unique ID. To maintain unique IDs across the industry, Microsoft maintains a database of Active Directory Object Identifiers (OIDs) so that when companies add extensions to the schema, they can be guaranteed to be unique and not to conflict with each other. To extend the schema in Active Directory, Dell received unique OIDs, unique name extensions, and unique linked attribute IDs for our attributes and classes that are added into the directory service.

Dell extension is: dell

Dell base OID is: 1.2.840.113556.1.8000.1280

RAC 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 RAC Schema Extensions

To provide the greatest flexibility in the multitude of customer environments, Dell provides a group of objects that can be configured by the user depending on the desired results. Dell has extended the schema to include an Association, Device, and Privilege object. The Association object is used to link together the users or groups with a specific set of privileges to one or more RAC devices. This model provides an Administrator maximum flexibility over the different combinations of users, RAC privileges, and RAC devices on the network without adding too much complexity.

Active Directory Object Overview

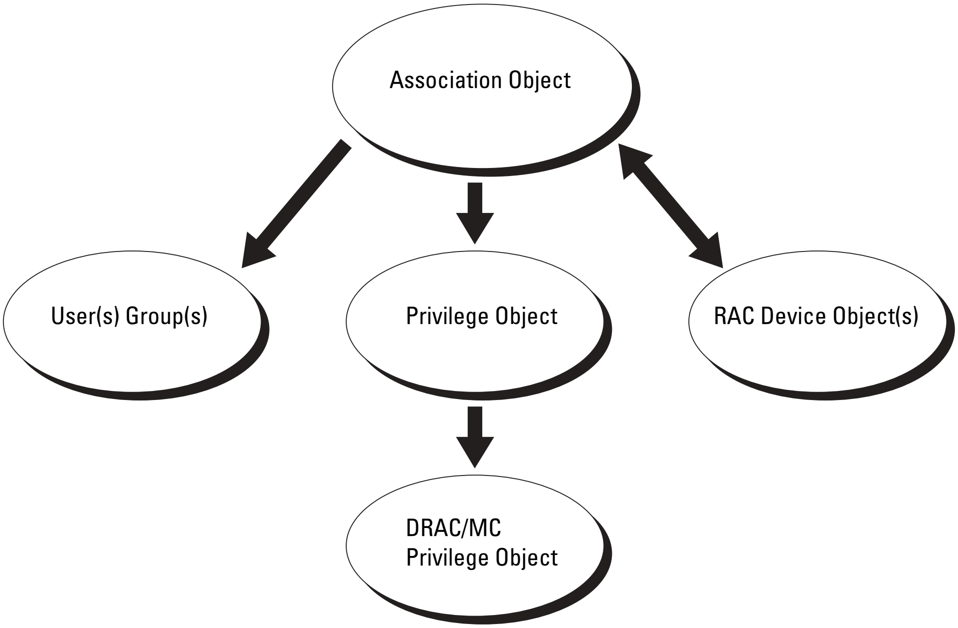
For each of the physical RACs on the network that you want to integrate with Active Directory for Authentication and Authorization, create at least one Association Object and one RAC Device Object. You can create as many Association Objects as you want, and each Association Object can be linked to as many users, groups of users, or RAC Device Objects as desired. The users and RAC Device Objects can be members of any domain in the enterprise.

However, each Association Object may be linked (or, may link users, groups of users, or RAC Device Objects) to only one Privilege Object. This allows an Administrator to control which users have what kind of privileges on specific RACs.

The RAC Device object is the link to the RAC firmware for querying Active Directory for authentication and authorization. When a RAC is added to the network, the Administrator must configure the RAC and its device object with its Active Directory name so that users can perform authentication and authorization with Active Directory. The Administrator will also need to add the RAC to at least one Association Object in order for users to authenticate.

Figure 6-1 illustrates that the Association Object provides the connection that is needed for all of the Authentication and Authorization.

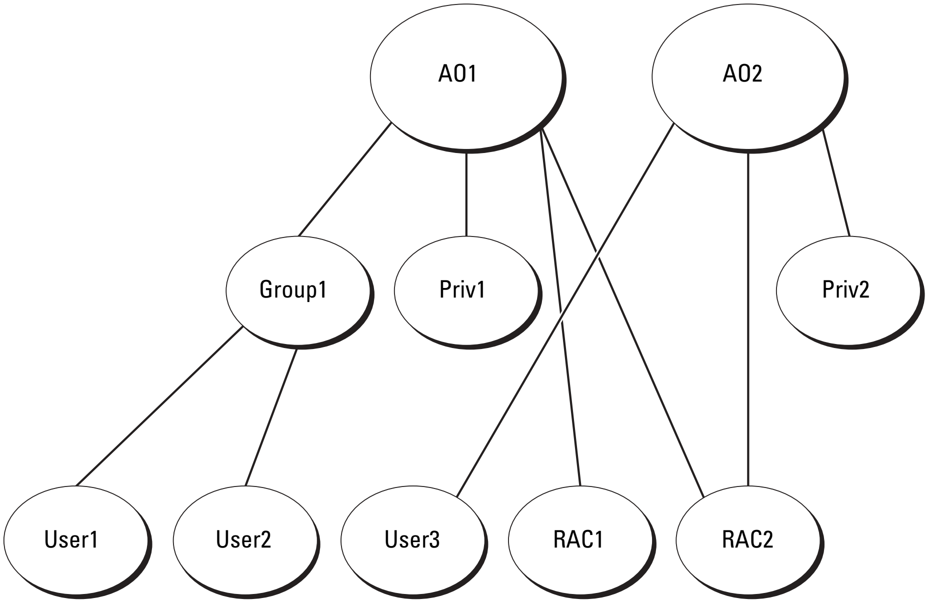
Figure 6-1. Typical Setup for Active Directory Objects



You can create as many or as few association objects as you want or need. However, you must create at least one Association Object, and you must have one RAC Device Object for each RAC (DRAC/MC) on the network that you want to integrate with Active Directory for Authentication and Authorization with the RAC (DRAC/MC). The Association Object allows for as many or as few users and/or groups as well as RAC Device Objects. However, the Association Object only has one Privilege Object per Association Object. The Association Object connects the *Users* who have *Privileges* on the RACs (DRAC/MCs).

In addition, you can set up Active Directory objects in a single domain or in multiple domains. For example, you have two Dell PowerEdge™ systems that are configured with DRAC/MC modules (RAC1 and RAC2) and three existing Active Directory users (user1, user2, and user3). You want to give user1 and user2 an administrator privilege to the DRAC/MC modules in the two PowerEdge systems and give user3 a login privilege to the RAC2 module. Figure 6-2 shows how you set up the Active Directory objects in this scenario.

Figure 6-2. 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 Device Objects, RAC1 and RAC2, to represent the DRAC/MC modules in the PowerEdge systems.

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.

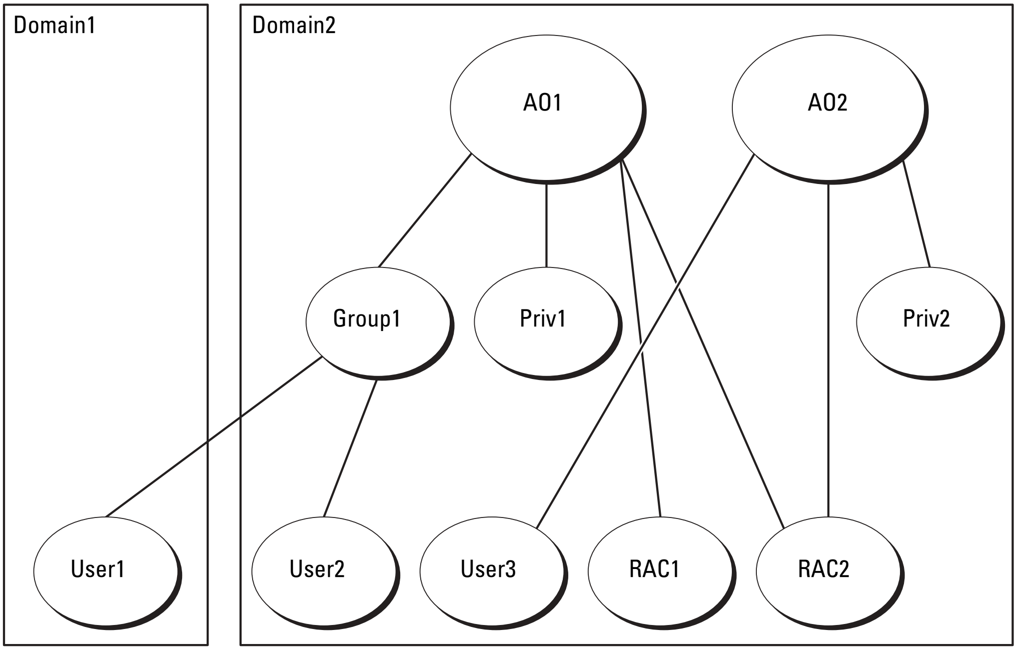
5 Add Group1 as Members in Association Object 1 (AO1), Priv1 as Privilege Objects in AO1, and RAC1, RAC2 as RAC Devices in AO1.

6 Add User3 as Members in Association Object 2 (AO2), Priv2 as Privilege Objects in AO2, and RAC2 as RAC Devices in AO2.

See "Adding DRAC/MC Users and Privileges to Active Directory" for detailed instructions.

Figure 6-3 shows how you can set up the Active Directory objects in multiple domains. In this scenario, you have two DRAC/MC modules (RAC1 and RAC2) and three existing Active Directory users (user1, user2, and user3). User1 is in Domain1; user2 and user 3 are in Domain2. You want to give user1 and user 2 administrator privileges to both DRAC/MC modules and give user3 login privileges to the RAC2 module.

Figure 6-3. Setting Up Active Directory Objects in Multiple Domains



To set up the objects for the 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 DRAC/MC modules.
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 RAC1, RAC2 as RAC Devices in AO1.
7. Add User3 as Members in Association Object 2 (AO2), Priv2 as Privilege Objects in AO2, and RAC2 as RAC Devices in AO2.

Configuring Active Directory to Access Your DRAC/MC

NOTE: The DRAC/MC does not support secure DNS security extensions. In Active Directory-enabled networks, the default DNS server settings must be configured to accept unsecure DDNS entries to support the DRAC/MC DDNS feature.

Before you can use Active Directory to access your DRAC/MC, configure the Active Directory software and the DRAC/MC by performing the following steps in their numbered order:

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 DRAC /MC users and their privileges to Active Directory (see "Adding DRAC/MC Users and Privileges to Active Directory").
4. Enable SSL on each of your domain controllers (see "Enabling SSL on a Domain Controller").
5. Configure the DRAC/MC Active Directory properties using either the DRAC /MC Web-based interface or the RACADM CLI (see "Configuring the DRAC/MC").

Extending the Active Directory Schema

Extending your Active Directory schema will add a Dell organizational unit, schema classes and attributes, and example privileges and association objects to the Active Directory 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 LDAP Data Interchange Format (LDIF) script file.

NOTE: The Dell organizational unit will not be added if you use the LDIF script file.

The LDIF files and Dell Schema Extender are located on your *Dell OpenManage Systems Management Consoles* CD in the following respective directories:

- *CD drive*:**\support\OMActiveDirectory Tools\RAC4\LDIF Files**
- *CD drive*:**\support\OMActiveDirectory Tools\RAC4\Schema Extender**

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**.

The schema is extended. To verify the schema extension, use the Microsoft Management Console (MMC), the Active Directory Schema snap-in, to verify the existence of the following classes (listed in Table 6-1, Table 6-2, Table 6-3, Table 6-4, Table 6-5, and Table 6-6) and attributes (listed in Table 6-7). See your Microsoft documentation for more information on how to enable and use the Active Directory Schema snap-in the MMC.

Table 6-1. Class Definitions for Classes Added to the Active Directory Schema

Class Name	Assigned Object Identification Number (OID)
dellRacDevice	1.2.840.113556.1.8000.1280.1.1.1.1
dellAssociationObject	1.2.840.113556.1.8000.1280.1.1.1.2
dellRAC4Privileges	1.2.840.113556.1.8000.1280.1.1.1.3
dellPrivileges	1.2.840.113556.1.8000.1280.1.1.1.4
dellProduct	1.2.840.113556.1.8000.1280.1.1.1.5

Table 6-2. 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/MC to send Lightweight Directory Access Protocol (LDAP) queries to Active Directory.
Class Type	Structural Class
SuperClasses	dellProduct
Attributes	**dellSchemaVersion** **dellRacType**

Table 6-3. 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.
Class Type	Structural Class
SuperClasses	Group
Attributes	**dellProductMembers** **dellPrivilegeMember**

Table 6-4. dellRAC4Privileges Class

OID	1.2.840.113556.1.8000.1280.1.1.1.3
Description	This class is used to define the privileges for the Authorization Rights for the DRAC/MC device.
Class Type	Auxiliary Class
SuperClasses	None
Attributes	**dellIsLoginUser** **dellIsCardConfigAdmin** **dellIsUserConfigAdmin** **dellIsLogClearAdmin** **dellIsServerResetUser** **dellIsConsoleRedirectUser** **dellIsVirtualMediaUser** **dellIsTestAlertUser** **dellIsDebugCommandAdmin**

Table 6-5. 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**

Table 6-6. 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 6-7. List of Attributes Added to the Active Directory Schema

Attribute Name/Description	Assigned OID/Syntax Object Identifier	Single Valued
dellPrivilegeMember	1.2.840.113556.1.8000.1280.1.1.2.1	FALSE
List of dellPrivilege Objects that belong to this Attribute.	Distinguished Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	
dellProductMembers	1.2.840.113556.1.8000.1280.1.1.2.2	FALSE
List of dellRacDevices Objects that belong to this role. This attribute is the forward link to the dellAssociationMembers backward link. Link ID: 12070	Distinguished Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	
dellIsLoginUser	1.2.840.113556.1.8000.1280.1.1.2.3	TRUE
TRUE if the user has Login rights on the device.	Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
dellIsCardConfigAdmin	1.2.840.113556.1.8000.1280.1.1.2.4	TRUE
TRUE if the user has Card Configuration rights on the device.	Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
dellIsUserConfigAdmin	1.2.840.113556.1.8000.1280.1.1.2.5	TRUE
TRUE if the user has User Configuration rights on the device.	Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
delIsLogClearAdmin	1.2.840.113556.1.8000.1280.1.1.2.6	TRUE
TRUE if the user has Log Clearing rights on the device.	Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
dellIsServerResetUser	1.2.840.113556.1.8000.1280.1.1.2.7	TRUE
TRUE if the user has Server Reset rights on the device.	Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
dellIsConsoleRedirectUser	1.2.840.113556.1.8000.1280.1.1.2.8	TRUE
TRUE if the user has Console Redirection rights on the device.	Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	

Table 6-7. List of Attributes Added to the Active Directory Schema *(continued)*

Attribute Name/Description	Assigned OID/Syntax Object Identifier	Single Valued
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 Admin 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
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

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 RAC (DRAC/MC) devices, Users and User Groups, RAC Associations, and RAC Privileges. 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 OpenManage Systems Management Consoles* CD.

NOTE: Install the Administrator Pack on each system that is managing the Active Directory DRAC/MC 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 Dell RAC Object in the container.

NOTE: For more information about the Active Directory Users and Computers snap-in, see your Microsoft documentation.

NOTE: If your system is running Microsoft Windows 2003 x64, you must manually install the x64 (64-bit) Active Directory snap-in files to configure your DRAC/MC components with Active Directory. To install the x64 snap-in files on your management station, navigate to the <***CD_Drive***>**\support\OMActiveDirectory_SnapIn64** directory on the *Dell OpenManage Systems Management Consoles* CD and run the installer.

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**.

NOTE: If you are using Microsoft Windows x64 edition, include the -32 switch with the **MMC** command to be able to effectively work with the Active Directory schema extension and computer snap-in.

This opens the Microsoft Management Console (MMC).

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 DRAC/MC Users and Privileges to Active Directory

The Dell-extended Active Directory Users and Computers snap-in allows you to add DRAC/MC users and privileges by creating RAC, Association, and Privilege objects. To add each type of object, perform the steps in each subsection.

Creating a RAC Device Object

1 In the **Console Root** (MMC) window, right-click a container.

2 Select **New**→**Dell RAC Object**.

This opens the **New Object** window.

3 Type a name for the new object. This name must match the DRAC/MC Name that you will type in step 4 of "Configuring the DRAC/MC."

4 Select **RAC Device Object**.

5 Click **OK**.

Creating a Privilege Object

Privilege Objects must be created in the same domain as the Association Object to which it is associated.

1. In the **Console Root** (MMC) window, right-click a container.
2. Select **New→Dell RAC Object**.

   This selection opens the **New Object** window.
3. Type a name for the new object.
4. Select **Privilege Object**.
5. Click **OK**.
6. Right-click the privilege object that you created and select **Properties**.
7. Click the **RAC/MC Privileges** tab and select the DRAC/MC privileges that you want the user to have.

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, 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→Dell RAC Object**.

   This opens the **New Object** window.
3. Type a name for the new object.
4. Select **Association Object**.
5. Select the scope for the **Association Object**.
6. Click **OK**.

Adding Objects to an Association Object

By using the **Association Object Properties** window, you can associate users or user groups, privilege objects, and RAC devices or RAC device groups.

NOTE: When using Windows 2000 mode or higher, use Universal Groups to span domains with your users or RAC objects.

You can add groups of Users and RAC devices. Creating Dell-related groups is done the same way you create 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 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 RAC device.

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 and click **OK**.

Click the **Products** tab to add one or more RAC devices to the association. The associated devices specify the RAC devices connected to the network that are available for the defined users or user groups.

NOTE: You can add multiple RAC devices to an association object.

To add RAC devices or RAC device groups:

1 Select the **Products** tab and click **Add.**

2 Type the RAC device or RAC device group name and click **OK**.

3 In the **Properties** window, click **Apply** and then **OK**.

Enabling SSL on a Domain Controller

If you plan to use Microsoft Enterprise Root Certificate Authority (CA) to automatically assign all your domain controllers SSL certificates, 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 and right-click **Automatic Certificate Request Settings**. Select **New,** 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

NOTE: The following steps may vary slightly if you are using Windows 2000.

NOTE: The Microsoft Enterprise Certification Authority (CA) MMC snap-in may fail to provide a certificate for the DRAC/MC-generated certificate signing request (CSR). To obtain a certificate, use the Microsoft Enterprise CA Web interface or the Microsoft Stand-Alone CA.

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 systems running Windows 2000) 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/MC. To do this, open the DRAC/MC Web-based interface, click the **Configuration** tab, and then click **Active Directory**.

Alternately, you may use the RACADM CLI commands. See "Configuring the DRAC/MC Active Directory Settings Using the CLI."

15 Click **Finish** and click **OK**.

Importing the DRAC/MC Firmware SSL Certificate to All Domain Controllers Trusted Certificate Lists

NOTE: If the DRAC/MC 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 Locate the DRAC/MC SSL certificate. The DRAC/MC SSL certificate is the same certificate that is used for the DRAC/MC Web server. All DRAC/MC controllers are shipped with a default self-signed certificate. You can get this certificate from the DRAC/MC by clicking **Download DRAC/MC Server Certificate** (see the DRAC/MC 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 Authority is not in the list, 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 the DRAC/MC

Configuring the DRAC/MC Active Directory Settings Using the Web-Based Interface

1 Log in to the Web-based interface using the default user, `root`, and the default password.

2 Click the **Configuration** tab and select the **Active Directory** subtab.

3 Select the **Enable Active Directory** check box.

4 Type the **DRAC/MC Name**. This name must be the same as the common name of the RAC object that you created in your Domain Controller (see step 3 of "Creating a RAC Device Object").

5 Type the **ROOT Domain Name**. The **ROOT Domain Name** is the fully qualified root domain name for the forest.

6 Type the **DRAC/MC Domain Name** (for example, `dracmc.com`). Do not use the NetBIOS name. The **DRAC/MC Domain Name** is the fully qualified domain name of the sub-domain where the RAC Device Object is located.

7 Click **Apply Changes** to save the Active Directory settings.

8 Click **Upload the Active Directory CA Certificat**e to upload your domain forest Root CA certificate into the DRAC/MC. 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"). Specify the full path and filename of the root CA certificate and click **Upload** to upload the root CA certificate to the DRAC/MC firmware. The DRAC/MC Web server automatically restarts after you click **Upload**. Log in again to complete the DRAC/MC Active Directory feature configuration.

9 In the **Configuration** tab, click the **Network** subtab.

10 If the **Use DHCP (for the NIC IP Address)** is enabled, select the **Use DHCP to obtain DNS server addresses**. If you want to enter a DNS server IP address manually, deselect the **Use DHCP to obtain DNS server addresses** and enter your primary and alternate DNS Server IP addresses.

11 Click **Apply Changes** to complete the DRAC/MC Active Directory feature configuration.

Configuring the DRAC/MC Active Directory Settings Using the CLI

Use the RACADM CLI and the Web-based interface to configure the DRAC/MC Active Directory feature.

1 Open a telnet or serial console session to the DRAC/MC 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>
```

2 Open a Web browser.

3 Log in to the Web-based interface using the default user, `root`, and the default password, `calvin`.

4 Click the **Configuration** tab and select **Active Directory**.

5 Click **Upload an Active Directory CA Certificat**e to upload your domain forest Root CA certificate into the DRAC/MC. 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"). Specify the full path and filename of the root CA certificate and click **Upload** to upload the root CA certificate to the DRAC/MC firmware. The DRAC/MC Web server automatically restarts after you click **Upload**. Log in again to complete the DRAC/MC Active Directory feature configuration.

6 Close the Web browser.

7 If DHCP is enabled on the DRAC/MC and you want to use the DNS provided by the DHCP server, type the following command:

```
racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 1
```

8 If DHCP is disabled on the DRAC/MC or you want to manually specify the 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>
```

9 Press **Enter** to complete the DRAC /MC Active Directory feature configuration.

Using Active Directory to Log In To the DRAC/MC

You can use Active Directory to log in to the DRAC/MC through the Web-based interface or the serial or telnet console.

The login syntax is consistent for all three methods:

<username@domain> or *<domain>\<username>* or *<domain>/<username>* (where *username* is an ASCII string of 1–256 bytes). No white space and no special characters (such as \, /, or @) are allowed in either the user name or the domain name.

NOTE: You cannot specify NetBIOS domain names, such as "Finance", because those names cannot be resolved.

Frequently Asked Questions

Table 6-8 lists frequently asked questions and answers.

Table 6-8. Using the DRAC/MC With Active Directory: Frequently Asked Questions

Question	Answer
Can I log into the DRAC/MC using Active Directory across multiple forests?	The DRAC/MC's Active Directory querying algorithm only supports a single tree in a single forest.
Does the login to the DRAC/MC using Active Directory work in mixed mode (that is, the domain controllers in the forest run different operating systems, such as Microsoft Windows NT® 4.0, Windows 2000, or Windows Server 2003)?	Yes. In mixed mode, all objects used by the DRAC/MC querying process (among user, RAC Device Object, and Association Object) have to be in the same domain. The Dell-extended Active Directory Users and Computers snap-in checks the mode and limits users in order to create objects across domains if in mixed mode.
Does using the DRAC/MC with Active Directory support multiple domain environments?	Yes. The domain forest function level must be in Native mode or Windows 2003 mode. In addition, the groups among Association Object, RAC user objects, and RAC Device Objects (including Association Object) must be universal groups.

Table 6-8. Using the DRAC/MC With Active Directory: Frequently Asked Questions *(continued)*

Question	Answer
Can these Dell-extended objects (Dell Association Object, Dell RAC Device, and Dell Privilege Object) be in different domains?	The Association Object and the Privilege Object must be in the same domain. The Dell-extended Active Directory Users and Computers snap-in forces you to create these two objects in the same domain. Other objects can be in different domains.
Are there any restrictions on Domain Controller SSL configuration?	Yes. All Active Directory servers' SSL certificates in the forest must be signed by the same root CA since DRAC/MC only allows uploading one trusted CA SSL certificate.
I created and uploaded a new RAC certificate and now the Web–based interface does not launch.	If you use Microsoft Certificate Services to generate the RAC certificate, one possible cause of this is you inadvertently chose **User Certificate** instead of **Web Certificate** when creating the certificate. To recover, create a new Web certificate from Microsoft Certificate Services and load it using the DRAC/MC GUI from the managed system.
What can I do if I cannot log into the DRAC/MC using Active Directory authentication? How do I troubleshoot the issue?	Troubleshoot as follows: • Ensure that you have checked the **Enable Active Directory** box on the **DRAC/MC Active Directory Configuration** page. • Ensure that the DNS setting is correct on the DRAC/MC Network configuration page. • Ensure that you have uploaded the Active Directory certificate from your Active Directory root CA to the DRAC/MC. • Check the Domain Controller SSL certificates to ensure that they have not expired. • Ensure that DRAC/MC Name, ROOT Domain Name, and DRAC/MC Domain Name match your Active Directory environment configuration. • Ensure that you use the correct user domain name during a login and not the NetBIOS name.

7

Using Text-Mode Serial Console Redirection

Overview

The DRAC/MC console redirection feature allows you to access the local server or switch console remotely in text mode only.

Currently, with the power of networking and the Internet, you do not have to sit in front of each server to perform all the routine maintenance. Using Intranet access, you can manage the servers from another city or even from the other side of the world from your desktop or laptop computer. You can also share the information with others—remotely and instantly.

When redirecting the server console, for the Microsoft® Windows Server™ 2003, Red Hat® Enterprise Linux, or SUSE® Linux Enterprise Server operating systems, each has a different display during the operating system boot process. For Microsoft Windows Server 2003, the Special Administration Console (SAC) appears after the operating system boots. For Red Hat Enterprise Linux and SUSE Linux Enterprise Server, the command shell appears after the operating system boots.

NOTE: The SAC is not available for the Microsoft Windows® 2000 Server operating system. This feature is supported with the Windows Server 2003 operating system.

NOTE: Due to the default Carriage Return+Line Feed (CRLF) settings in Windows-based telnet clients, the text mode console redirection feature may not function properly on server modules running the Linux operating system. This issue can also occur when connecting to I/O modules using console redirection. To fix this issue, configure the `CRLF` option on the telnet client to only send CR (carriage return) characters with the Windows telnet command `unset crlf`.

Configuring the System Setup Program on the Server Module

Perform the following steps to configure your System Setup program to redirect output to a serial port.

NOTE: Configure the System Setup Program in conjunction with the **connect serial/telnet** command.

NOTE: Perform the following sequence of commands locally on each module. When you have completed these steps, you can redirect the server console to the DRAC/MC remotely.

1 Turn on or restart your server module.

2 Press <F2> immediately after you see the following message:

```
<F2> = System Setup
```

3 Scroll down and select **Console Redirection**.

NOTE: If your system has Dell™ PowerEdge™ 1955 server modules, select **Serial Communication**.

4. Set the **Console Redirection** screen to the following settings:

   Console Redirection – DRAC/MC and **BMC Serial Over LAN (SOL)**

   NOTE: For PowerEdge 1955 server modules, set the **Serial Communication** screen to the following setting: **Serial Communication – On with Console Redirection via Com2**.

   Remote Terminal Type – ANSI or **VT100/VT200** depending on your specific needs

   Redirection After Boot – Enabled

   NOTE: If your terminal is in VT100 mode and you are unable to see the proper selection, go to the **Properties** menu and change the terminal to **VT200**. Your selection should now be visible. Any cursor movement causes you to lose the selection. If you lose your selection, switch back to **VT100**, and the selection is displayed again.

5. Verify that the BIOS fail-safe baud rate value is the same as the DRAC/MC object "cfgRacTuneHostCom2BaudRate (Read/Write)" (default = 57600).

6. For the PowerEdge 1955 server modules, verify that the BIOS fail-safe baud rate value is same as DRAC/MC object "cfgServerBMCBaudRate (Read Only)" (default = 57600).

7. Press <Esc> to exit the server module's System Setup program to complete the server module's System Setup program configuration.

Using Console Redirection

The BIOS in the server modules has the following options for console redirection:

- **DRAC/MC** enables server module console redirection.

  NOTE: For the DRAC/MC `connect <servername>` feature to work, set the BIOS console redirection to DRAC/MC before the server is booted. If it is set to any other value, you will be presented with an `Attempting connection` message when the **connect** command is executed to that server, and you will not be connected.
  In PowerEdge 1955 server modules, for the DRAC/MC `connect <servername>` feature to work, turn on the **Console Redirection** feature.

  NOTE: The BIOS Console Redirection Fail-Safe Baud Rate and the DRAC/MC redirection port baud rate must match. To set the DRAC/MC baud rate to match the BIOS Fail-Safe Baud rate, change the value in the **cfgRacTuneHostCom2BaudRate** database object. For more details on the object, see "cfgRacTuneHostCom2BaudRate (Read/Write)."

- **BMC SOL** enables the BMC serial over a LAN connection.

  NOTE: This option is not available on the PowerEdge 1955 server modules.

- **Off** disables console redirection from the server module.

  NOTE: If the console redirection option is set to BMC SOL on a PowerEdge 1855 server module, executing the `connect -F <`*`servername`*`>` command will force a connection to the DRAC/MC. This feature is available with DRAC/MC firmware version 1.2 and later.

Using the Serial Connector

The DRAC/MC module serial connector uses a 9-pin D-subminiature connector. See the documentation for the DRAC/MC controller for information on using the serial port for configuration.

Using a Serial Connection to Access the DRAC/MC Help Commands

Use the DRAC/MC console redirection to perform the following steps:

1. Open a DRAC/MC session. To start a HyperTerminal program, see "Configuring HyperTerminal for Serial Console Redirection." The DRAC/MC login screen is displayed.
2. Type your user name and password. The default user name is `root` and the default password is `calvin`.

   The `DRAC/MC:` command prompt is displayed.
3. To access information about a command, at the `DRAC/MC:` prompt, type:

   ```
   help <command_name>
   ```

   For example, `help getsysinfo` returns the syntax for the **getsysinfo** command.
4. To display a list of **RACADM** commands, at the `DRAC/MC:` prompt, type:

   ```
   racadm help
   ```

Using Console Redirection From a Management Station

Use telnet or a terminal emulation application to attach and log into the DRAC/MC console. To redirect a server console, type:

```
connect <Server name>
```

For example, if you are connecting to server module 6, you would type the following command line:

```
connect server-6
```

To redirect a switch console, type:

```
connect switch-<switchnumber>.
```

For example, if you are connecting to switch module 1, you would type the following at the command line:

```
connect switch-1
```

You are now connected to the specified module.

To return to the DRAC/MC console, press <Enter>, press the tilde (~) key, and then press the period (.) key.

NOTE: The escape sequence can be changed by modifying the **cfgSerialConsoleQuitKey** property default value. See "DRAC/MC Object and Command Properties" for a list of all default property values.

Using the BMC and PERC Utilities with Console Redirection

During console redirection, use the procedures described in the following sections. Note the changes implemented for key sequences in each utility.

Baseboard Management Controller Configuration

The BMC configuration is a utility that enables you to configure, monitor, and recover server modules remotely. BMC provides the following features:

- Uses the server's primary integrated NIC port.
- Provides fault logging and SNMP alerting.
- Provides access to event log and sensor status.
- Controls system functions including power up and power down.
- Provides independent support of the server module's power or operating state.
- Implements text console redirection for system setup, text-based utilities, and the operating system console.

  Use the following key sequences when you access the BMC utility during console redirection.

  a To access the BMC, press and hold the <Ctrl> and <E> keys when you are prompted following the power-on self-test (POST).

  b To exit, press <Esc>.

For additional information on using the BMC, see the *Dell OpenManage™ Baseboard Management Controller User's Guide* and the documentation for the systems management applications.

PERC/SCSI Setup Configuration

This integrated RAID solution is a utility that provides benefits for the server or workstation market where extra performance, storage capacity, and/or redundancy of a RAID configuration are required.

The PERC/SCSI configuration enables you to configure hard drives using both RAID and SCSI modes. You can perform a PERC/SCSI configuration using the PERC/SCSI Setup Utility during system startup.

To enter the PERC/SCSI Setup Utility during console redirection, perform the following steps:

1. Power on or restart your system after console redirection begins.
2. Press <Esc>, and then press the <Ctrl> and <M> keys when you are prompted following the power-on self-test (POST).

   NOTE: On a PowerEdge 1955, for a SAS 5i/R, press <Esc>, and then press the <Ctrl> and <C> keys when you are prompted following the power-on self-test.

3. To exit, press <Esc>.

For additional information on using the PERC/SCSI Setup Utility, see "DRAC/MC Security Features."

8

Using the DRAC/MC CLI Commands

The DRAC/MC provides CLI commands that allow you to manage and configure the DRAC/MC locally or remotely.

The following sections provide information about using the CLI commands. Examples of the CLI commands for configuring your DRAC/MC are also provided.

Using a Serial or Telnet Console

You can run the CLI commands in Table 8-1 from the serial or telnet console command prompt.

Logging In to the DRAC/MC

After you have configured your management station terminal emulator software, such as Minicom or HyperTerminal, perform the following steps to log in to the DRAC/MC:

1 Connect to the DRAC/MC using your management station terminal emulation software.

2 Type your DRAC/MC user name and press <Enter>.

3 Type your DRAC/MC password and press <Enter>.

You are now logged in to the DRAC/MC.

NOTE: Configure the terminal emulator software's connection settings to match the settings of the DRAC/MC for attributes such as baud rate, flow control, and so on.

NOTE: Before using the command prompt using telnet, configure the DRAC/MC to contain a proper IP address. Use either a statically assigned IP address or an IP address obtained from a DHCP server.

Starting a Console Redirection Session

After you have logged in to the DRAC/MC through your management station terminal software or by telnet, you can redirect the DRAC/MC console to the server or switch console by using the **connect** CLI command. Only one **connect** ***<servername>*** and one **connect switch-x** client is supported at a time (out of four total sessions shared with the DRAC/MC Web-based interface).

Perform the steps in the following subsections to redirect the DRAC/MC text console.

1 To redirect the server console through the DRAC/MC console, type `connect <servername>` from the DRAC/MC command prompt, which is displayed through the terminal emulator software.

2 To redirect the switch console through the DRAC/MC console, type `connect switch-x` from the DRAC/MC command prompt.

NOTE: Console redirection occurs when users go through **connect** ***<servername>*** or **switch-x**, where ***x*** represents a module slot number on the chassis.

NOTE: When accessing a DOS console through console redirection, characters in the output may be dropped during the output of large amounts of data (for example, the dump of large files greater than 30 lines or more). This event can cause incorrect displays during telnet sessions. Red Hat® Enterprise Linux, SUSE® Linux Enterprise Server, and the Microsoft® Windows® Special Administration Console (SAC) work correctly.

Viewing the Console Commands

Type `help` to display the entire **serial** console command list. Commands that are not supported on the system or interface that you are using are labeled as such.

For example, if you type a command that is a serial console command and not a RACADM command, it will fail:

```
racadm connect: UNSUPPORTED COMMAND
```

Table 8-1 lists the serial console commands. Most of these commands are also supported as RACADM CLI commands. The descriptions and *man page* information, including required syntax for the serial console commands, are identical for the RACADM CLI commands. You do not need to type RACADM before typing a serial console command because the serial console commands are not RACADM CLI commands. They are at the same *level*. For detailed information about the required syntax for each RACADM CLI command, see "Subcommand Man Pages."

Table 8-1. Serial/Telnet Commands

Command	Description
chassisaction	Executes a chassis or switch module to powerup/powerdown/powercycle.
clrraclog	Clears the DRAC/MC log entries.
clrsel	Clears the SEL entries.
connect	Redirects the DRAC/MC to a server module or switch console (serial port).
logout/exit/quit	Logs user out of a DRAC/MC session, and then displays a new login prompt.
getdcinfo	Displays configuration information about the daughter card that is installed in a server module
getioinfo	Displays general I/O status information.
getkvminfo	Displays information about the KVM module in a Dell™ Modular Server Enclosure.
getled/setled	Sets and displays LED settings on a module.

Table 8-1. Serial/Telnet Commands *(continued)*

Command	Description
getmodinfo	Gets module configuration and status information.
getpbinfo	Displays information about the system's power status and power consumption.
getraclog	Displays DRAC/MC log entries.
getsel	Displays SEL entries.
getsensorinfo	Gets sensor readings from specified sensors.
getsysinfo	Displays general DRAC/MC and system information.
help	Lists DRAC/MC commands with a one-line description.
help <*command*>	Lists the usage statement for the specified command.
racadm	Executes the RACADM command (for `username`: `root` or `racadmuser`).
serveraction	Executes a server reset/powerdown/graceful powerdown/powerdown/powerup/powercycle.

Using the RACADM CLI

The RACADM CLI commands can be run using the remote RACADM CLI or from the serial or telnet console command prompt.

Use the RACADM CLI command to configure DRAC/MC properties, perform remote management tasks, or recover a crashed system. Table 8-2 lists the RACADM CLI command that you can type into the serial/telnet console.

When using the serial/telnet console, type `racadm help` to display the entire RACADM CLI subcommand list, which lists all the commands supported by the DRAC/MC. The following sections provide information about how to use the RACADM CLI commands.

racadm CLI Command Description

Table 8-2. racadm CLI Command

Command	Description
racadm	command line status and configuration utility for the DRAC/MC.

Using the Serial/Telnet Console Remotely

NOTICE: Configure the IP address on your DRAC/MC before using the RACADM remote capability. For more information about initially configuring your DRAC/MC, including a list of other documents you may need, see "Installing and Setting Up the DRAC/MC."

racadm CLI Subcommand Descriptions

The following subsections provide descriptions of subcommands that you can run under the serial/telnet console. Table 8-3 briefly describes each RACADM CLI subcommand. For a detailed listing of every RACADM CLI subcommand including syntax and valid entries, see the "Subcommand Man Pages."

Table 8-3. racadm CLI Subcommands

Command	Description
chassisaction	Executes a chassis or switch module powerup/powerdown/powercycle.
clrraclog	Clears the DRAC/MC log completely.
clrsel	Clears the SEL entries.
config/getconfig	Configures the DRAC/MC and displays the DRAC/MC configuration.
crdisconnect	Disconnects a Web-based console redirection session.
fwupdate	Executes or displays status on DRAC/MC firmware updates.
getdcinfo	Displays information about the chassis configuration verification feature.
getioinfo	Displays general I/O status information.
getkvminfo	Displays information about the KVM.
getpbinfo	Displays information about the system's power status and power consumption.
getmacaddress	Displays the server NIC MAC addresses.
getmodinfo	Displays module configuration and status information.
getraclog	Displays DRAC/MC log entries.
getractime	Displays the DRAC/MC time.
getsel	Displays SEL entries.
getsensorinfo	Displays DRAC/MC sensor readings and information.
getssninfo	Displays information about active sessions.
getsvctag	Displays service tags.
getsysinfo	Displays general DRAC/MC and system information.
help	Lists **racadm** subcommand descriptions.
help <*command*>	Lists usage statement for the specified command.
racdump	Displays system, session, and sensor information.
racreset	Resets the DRAC/MC.
racresetcfg	Resets the DRAC/MC to the default configuration.
serveraction	Executes a server reset/powerdown/graceful powerdown/powerdown/power-cycle.
setassettag/getassettag	Displays asset tags and sets asset tags.

Table 8-3. racadm CLI Subcommands *(continued)*

Command	Description
getled/setled	Sets LED status and displays LED status.
setniccfg/getniccfg	Sets or displays the current DRAC/MC IP configuration.
setractime	Sets the DRAC/MC time.
setsysinfo	Sets the chassis name and chassis location properties.
sslcertview	Views a CA certificate or server certificate in the DRAC/MC.
testemail (see also "E-mail Test Command")	Forces the DRAC/MC to send an e-mail over the DRAC/MC NIC.
testtrap (see also "Trap Test Command")	Forces the DRAC/MC to send an SNMP test trap over the DRAC/MC NIC.
?	Displays the racadm subcommand descriptions.
vmdetach	Detaches an active virtual media session.

CLI Commands History

With version 1.1 or later, DRAC/MC stores the last six RACADM CLI commands that were executed from the serial or telnet console command prompt. Each time you close a session, the CLI or telnet commands history is deleted. When you access a history session, you can use the arrow keys to navigate through the history file. Additionally, you can use the backspace key, spacebar, delete key, and the left and right arrow keys to edit the history file.

RACADM Error Messages

For information about the serial/telnet console error messages, see "Frequently Asked Questions."

Using the RACADM CLI Remotely

NOTICE: Configure the IP address on your DRAC/MC before using the RACADM remote capability. For more information about initially configuring your DRAC/MC, including a list of other documents you may need, see "Installing and Setting Up the DRAC/MC."

The RACADM CLI provides a remote capability option (**-r**) that allows you to connect to the managed system and execute **RACADM** subcommands from a remote console or management station. To use the remote capability, you need a valid user name (**-u** option) and password (**-p** option), and the IP address of the managed system.

NOTE: The RACADM remote capability is supported only on management stations running Windows 2000 Server, Windows 2000 Professional, Windows Server™ 2003, Red Hat Enterprise Linux, and SUSE Linux Enterprise Server operating systems.

NOTE: RACADM version 5.0.0 or later supports remote operation with DRAC/MC. This utility is available on *Dell OpenManage Systems Management Consoles CD* version 5.0.

racadm Synopsis

`racadm [-u <user name>] -p <password> -r <racIpAddr> <subcommand>`

`racadm -i -r <racIpAddr> <subcommand>` or
`racadm -i -r <racIpAddr>:<new port number> <subcommand>` use this command if the DRAC/MC HTTPS port number has been changed.

racadm Options

Table 8-4 lists the options for the **racadm** command.

Table 8-4. racadm Command Options

Option	Description
-r <*racIpAddr*> or -r <*racIpAddr*>:<*port number*> if the DRAC/MC port number has been changed	Specifies the remote IP address of the controller.
-i	Tells **RACADM** to interactively query the user for the user's user name and password.
-u <*usrName*>	Specifies the user name that is used to authenticate the command transaction. If not specified, the default user name, racadmusr, is used. If the **-u** option is used, the **-p** option must be used, and the **-i** option (interactive) is not allowed.
-p <*password*>	Specifies the password used to authenticate the command transaction. If the **-p** option is used, the **-i** option is not allowed.

If you use the **-r** option, you must also use the **-u** and **-p** options to configure the DRAC/MC to accept **RACADM** commands. Using the **-r** option without the previously listed options will result in a command failure.

Enabling and Disabling the RACADM Remote Capability

NOTE: It is recommended that you run these commands on your local system.

The RACADM CLI remote capability is enabled by default. If you have disabled it, type the following command to enable the remote capability:

```
racadm config -g cfgRacTuning -o cfgRacTuneRemoteRacadmEnable 1
```

Type the following command to disable the remote capability:

```
racadm config -g cfgRacTuning -o cfgRacTuneRemoteRacadmEnable 0
```

RACADM Subcommand Descriptions

The following subsections provide descriptions of subcommands that you can run under the RACADM CLI. For a detailed listing of every **RACADM** subcommand including syntax and valid entries, see the "Subcommand Man Pages."

Configuring Multiple DRAC/MCs

One of the major features of the RACADM CLI is the ability to configure a DRAC/MC using a configuration file. The RACADM CLI parses the DRAC/MC configuration file, **racadm.cfg**, and then sends individual configuration requests to one or more DRAC/MCs.

This method may be used to configure multiple DRAC/MC database properties. First run the RACADM CLI to query a configured DRAC/MC for its database properties, which are accessed using their object group IDs and object IDs. The RACADM CLI creates the **racadm.cfg** file from the retrieved information. You can then configure other cards with the same database information by exporting this file out to the other DRAC/MCs.

NOTE: Some configuration files contain unique DRAC/MC information (such as the static IP address) that must be modified before configuring other cards.

Configuration File Overview

To use the configuration file, perform the following high-level steps:

1. Get the configuration from the DRAC/MC that contains the appropriate configuration.
2. Modify the configuration (optional).
3. Push the configuration to a target DRAC/MC.
4. Reset the target DRAC/MC.

The **getconfig -f racadm.cfg** subcommand requests the configuration of the DRAC/MC and generates a **racadm.cfg** file (you can choose any name for this file).

NOTE: The generated .cfg file does not contain user passwords.

Other options for the **getconfig** command enable you to perform such actions as:

- Displaying all configuration properties in a group (specified by group name and index)
- Displaying all configuration properties for a user by user name

The **config** subcommand loads the information into other DRAC/MCs. Other options for **config** enable you to perform such actions as:

- Removing passwords in the **racadm.cfg** file used to configure the card
- Synchronizing the user name and password database with Dell OpenManage™ Server Administrator

The initial configuration file, **racadm.cfg**, is named by the user. In the following example, the configuration file is named **myfile.cfg**. To obtain this file, type the following command at the command prompt:

```
racadm getconfig -f myfile.cfg
```

NOTICE: It is recommended that you edit this file with a simple text editor; the RACADM utility uses an ASCII text parser, and any formatting confuses the parser and might corrupt the RACADM database.

Creating a DRAC/MC Configuration File

The DRAC/MC configuration file <*filename*>**.cfg** is used with the **racadm config -f** ***<filename>*.cfg** command. The configuration file is a simple text file that allows the user to build a configuration file (similar to an **.ini** file) and configure the DRAC/MC from this file. You may use any file name, and the file does not require a **.cfg** extension (although it is referred to by that designation in this subsection). The **.cfg** file can be:

- Created
- Obtained from a **racadm getconfig -f** ***<filename>*.cfg** command
- Obtained from a **racadm getconfig -f** ***<filename>*.cfg** command, and then edited

NOTE: See "config/getconfig" for information about the **getconfig** command.

The **.cfg** file is first parsed to verify that valid group and object names are present and that some simple syntax rules are being followed. Errors are flagged with the line number in which the error was detected, and a simple message explains the problem. The entire file is parsed for correctness, and all errors are displayed. Writes are not performed to the DRAC/MC if an error is found in the **.cfg** file. The user must correct *all* errors before any configuration can take place. The **-c** option may be used in the **config** subcommand, which verifies syntax only and does *not* perform writes to the DRAC/MC.

Remember the following important points:

- If the parser encounters an indexed group, it is the value of the anchored object that differentiates the various indexes.

  The parser reads in all of the indexes from the DRAC/MC for that group. Any objects within that group are simple modifications at configuration time. If a modified object represents a new index, the index is created on the DRAC/MC during configuration.

- The user cannot specify a desired index in a **.cfg** file.

  Indexes may be created and deleted, so over time the group may become fragmented with used and unused indexes. If an index is present, it is modified. If an index is not present, the first available index is used. This method allows flexibility when adding indexed entries, where the user does not need to make exact index matches between all the RACs being managed; new users are added to the first available index. A **.cfg** file that parses and runs correctly on one DRAC/MC may not run correctly on another if all indexes are full and a new user is to be added.

- Use the **racresetcfg** subcommand to keep all DRAC/MCs the same.

  To keep all DRAC/MCs the same, use the **racresetcfg** subcommand to reset the DRAC/MC to original defaults, and then run the **racadm config -f** ***<filename>*.cfg** command. Ensure that the **.cfg** file has all the required objects, users, indexes, and other parameters.

NOTICE: Use the **racresetcfg** subcommand to reset the database and the DRAC/MC NIC settings to the original default settings and remove all users and user configurations. While the root user is available, other users' settings are also reset to the default settings.

Parsing Rules

- All lines that start with '#' are treated as comments.

  A comment line *must* start in column one. A '#' character in any other column is treated as a # character. (Some modem parameters may have # characters as part of their string. An escape character is not required. You may want to generate a **.cfg** from a **racadm getconfig -f <*filename*>.cfg** command, and then perform a **racadm config -f <*filename*>.cfg** command to a different DRAC/MC, without adding escape characters).

  Example:

  ```
  #
  # This would be a comment
  [cfgUserAdmin]
  cfgUserAdminPageModemInitString=<Modem init # not a comment>
  ```

- All group entries must be surrounded by "[" and "]" characters.

  The starting "[" character denoting a group name *must* start in column one. This group name *must* be specified before any of the objects in that group. Objects that do not have an associated group name generate an error. The configuration data is organized into groups as defined in "DRAC/MC Property Database Group and Object Definitions."

  The following example displays a group name, object, and the object's property value.

  Example:

  ```
  [cfgLanNetworking]
  cfgNicIpAddress=143.154.133.121
  ```

- All parameters are specified as "object=value" pairs without any white space between the object, =, or value.

  White spaces after the value are ignored. A white space inside a value string is left unmodified. Any character to the right of the '=' is taken as is (for example, a second '=', or a '#', '[', ']', and so forth). All of these characters are valid modem chat script characters.

  See the example in the previous bullet point.

- An indexed object entry is ignored by the **.cfg** parser.

  The user *cannot* specify which index is used. If the index already exists, it is used, or else the new entry is created in the first available index for that group.
  The **racadm getconfig -f <*filename*>.cfg** command places a comment in front of index objects, which allows the user to see which comments are being used.

  NOTE: You can create an indexed group manually, using the following command:

  ```
  racadm config -g <groupName> -o <anchored object> -i <index 1-16>
  <unique anchor name>
  ```

- The line for an indexed group *cannot* be deleted from a **.cfg** file.

  The user must remove an indexed object manually using the following command:

  ```
  racadm config -g <groupName> -o <objectName> -i <index 1-16> ""
  ```

  NOTE: A NULL string (two "" characters) directs the DRAC/MC to delete the index for the specified group.

  To view the contents of an indexed group, use the following command:

  ```
  racadm getconfig -g <groupName> -i <index 1-16>
  ```

- For indexed groups the object anchor *must* be the first object after the brackets ([ ]) pair. The following are examples of the current indexed groups:

  ```
  [cfgUserAdmin]

  cfgUserAdminUserName=<USER_NAME>

  "

  [cfgTraps]

  cfgTrapsDestIpAddr=<IP_ADDRESS>

  '

  '
  ```

  NOTE: Type `racadm getconfig -f <myexample>.cfg`. This command builds a **.cfg** file for the current DRAC/MC configuration. This configuration file can be used as an example and as a starting point for your unique **.cfg** file.

Configuration File Example

The following example describes the IP address of the DRAC/MC. Remove all unnecessary <*variable*>=**value** entries. In this situation, only the actual variable group's label with "[" and "]" will remain along with the two <*variable*>=**value** entries pertaining to the IP address change.

The file contents are as follows:

```
#

#   Object Group "cfgLanNetworking"

#

[cfgLanNetworking]

cfgNicIpAddress=10.35.10.110

cfgNicGateway=10.35.10.1
```

This file will be updated as follows:

```
#
#   Object Group "cfgLanNetworking"
#
[cfgLanNetworking]
cfgNicIpAddress=10.35.9.143
# comment, the rest of this line is ignored
cfgNicGateway=10.35.9.1
```

The command **racadm config -f myfile.cfg** parses this file and identifies any errors by line number. A correct file will update the proper entries. You may use the same **getconfig** command used in the previous example to confirm the update.

You can use this file to download company-wide changes or to configure new systems over the network.

Using the RACADM Utility to Configure the DRAC/MC

The DRAC/MC Web-based interface is the fastest way to configure a DRAC/MC. If you prefer using a command line interface, use the serial/telnet console or the remote RACADM interface.

Before Adding a DRAC/MC User

The DRAC/MC allows up to 16 users to be configured into the DRAC/MC property database. Before manually adding the DRAC/MC user, you need to know which users, if any, exist. If the DRAC/MC is new, or the **racadm racresetcfg** command has been run, then the only user is `root` with the password `calvin`. The **racresetcfg** subcommand resets the DRAC/MC back to the original defaults.

NOTICE: Use caution when using this command because *all* configuration parameters are reset to the original defaults; any previous changes are lost.

NOTE: Users can be added and deleted over time, so it is possible that users on the DRAC/MC do not have the same index number as the same user on a different DRAC/MC.

To find out if a user exists, you can type the following command at the command prompt:

```
racadm getconfig -u <username>
```

or you can type the following command once for each index of 1–16:

racadm getconfig -g cfgUserAdmin -i <*index*>

Several parameters and object IDs are displayed along with their current values. The two objects of interest are:

```
# cfgUserAdminIndex=XX
cfgUserAdminUserName=
```

If the **cfgUserAdminUserName** object has no value, the index number, which is indicated by the **cfgUserAdminIndex** object, is available for use. If a name appears after the = (equal sign), that index is taken by the specified user name.

NOTE: If a configuration object name is displayed by prefixing the # (number character), that means the object list is read-only.

NOTE: When you manually add or remove a user with the **racadm config** subcommand, you *must* specify the index with the **-i** option. Observe that the **cfgUserAdminIndex** object displayed in the previous example contains a '#' character.

Adding a DRAC/MC User Without Alert Capabilities

To add a simple user without any alert information, first locate an available user index by performing the steps in "Before Adding a DRAC/MC User." Next, type the following two command lines with the new user name and password:

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i <index> <username>

racadm config -g cfgUserAdmin -o cfgUserAdminPassword -i <index> <password>
```

Example:

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i 2 john

racadm config -g cfgUserAdmin -o cfgUserAdminPassword -i 2 123456
```

A user name "john" with the password of "123456" is created. This user name and password can now be used to log into the Web-based remote access interface. You can verify the new user with either of the following two commands:

```
racadm getconfig -u john

racadm getconfig -g cfgUserAdmin -i 2
```

Deleting a DRAC/MC User

All users must be deleted manually. The following command is used to delete users:

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i <index> ""
```

Example (to delete user `john` from the previous example):

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i 2 ""
```

A null string of double quote characters ("") indicates to the DRAC/MC that you want to delete the index for the specified group.

Adding a DRAC/MC User With Alerting Capabilities

To add a DRAC/MC user that is able to receive e-mail and SNMP traps, first locate an available DRAC/MC user index by performing the steps in "Before Adding a DRAC/MC User." The following example has an available user index at index 2.

NOTE: See "DRAC/MC Property Database Group and Object Definitions" for details about each specific object.

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i 2 john

racadm config -g cfgUserAdmin -o cfgUserAdminPassword -i 2 123456

racadm config -g cfgUserAdmin -o cfgUserAdminEmailAddress -i 2
"john@yz.com"

racadm config -g cfgUserAdmin -o cfgUserAdminEmailCustomMsg -i 2
"this is a custom message"

racadm config -g cfgUserAdmin -o cfgUserAdminEmailEnable -i 2 1

racadm config -g cfgUserAdmin -o cfgUserAdminAlertFilterRacEventMask -i 2
0x0

racadm config -g cfgUserAdmin -o cfgUserAdminAlertFilterSysEventMask -i 2
0x0

racadm config -g cfgTraps -o cfgTrapsSnmpCommunity -i 2 public

racadm config -g cfgTraps -o cfgTrapsEnable -i 2 1

racadm config -g cfgTraps -o cfgTrapsFilterRacEventMask -i 2 0x0

racadm config -g cfgTraps -o cfgTrapsFilterSysEventMask -i 2 0x0

racadm config -g cfgTraps -o cfgTrapsDestIpAddr -i 2 <SNMP trap destination>

racadm config -g cfgOobSnmp -o cfgOobSnmpTrapsEnable 1

racadm config -g cfgRemoteHosts -o cfgRhostsSmtpServerIpAddr
143.166.224.254

racadm racreset
```

NOTE: After you manually type the commands, test the alerts to ensure proper functionality.

Testing E-mail Alerting

E-mail alerting is enabled by the following command. A "0" disables this feature; a "1" enables it.

```
racadm config -g cfgUserAdmin -o cfgUserAdminEmailEnable -i 2 1

racadm testemail -i 2
```

Testing SNMP Trap Alerting

SNMP traps are enabled by the following command. A "0" disables this feature; a "1" enables it.

```
racadm config -g cfgTraps -o cfgTrapsEnable -i 2 1
```

```
racadm testtrap -i 2
```

Adding a DRAC/MC User With Permissions

To add a user with specific administrative permissions (role-based authority), first locate an available user index by performing the steps in "Before Adding a DRAC/MC User." Next, type the following command lines with the new user name and password.

NOTE: See Table B-1 for a list of the Bit Mask numbers to enable specific user permissions. The default user permission is 0, which provides full administrative permission.

```
racadm config -g cfgUserAdmin -o cfgUserAdminPrivilege -i <index>
<Bit Mask Number for specific user permissions>
```

Configuring DRAC/MC Network Properties

Type the following command to get a list of the available network properties:

```
racadm getconfig -g cfgLanNetworking
```

If you want to use DHCP to obtain an IP address, you can use the command to write the object **cfgNicUseDhcp** to enable it. You may also type a static IP address, netmask, and gateway.

The following is an example of how the command may be used to configure desired LAN network properties.

```
racadm config -g cfgLanNetworking -o cfgNicEnable 1

racadm config -g cfgLanNetworking -o cfgNicIpAddress 192.168.0.120

racadm config -g cfgLanNetworking -o cfgNicNetmask 255.255.255.0

racadm config -g cfgLanNetworking -o cfgNicGateway 192.168.0.120

racadm config -g cfgLanNetworking -o cfgNicUseDhcp 0
```

NOTE: If **cfgNicEnable** is set to **0**, the DRAC/MC LAN is disabled even if DHCP is enabled.

Frequently Asked Questions

Table 8-5 lists frequently asked questions and answers.

Table 8-5. Using the DRAC/MC CLI Commands: Frequently Asked Questions

Question	Answer
When I use the RACADM CLI commands and subcommands, I get errors that I don't understand.	You may encounter local error messages when using the RACADM CLI commands and subcommands. These errors occur when problems occur with syntax, typographical errors, incorrect names, and so on. Example: `racadm <subcmd>: ERROR: <message>`

9

Using the KVM Modules

This section provides information about installing, configuring, and using your supported keyboard, video, and mouse (KVM) modules.

Overview

The Dell™ Modular Server Enclosure supports the following KVM modules:

- Dell Integrated KVM Switch Module
- DRAC/MC-Supported KVM modules

NOTE: If you are connected to a server module in the DRAC/MC user interface and the DRAC/MC resets for any reason, the selected server module after restart changes to server module 1.

Dell Integrated KVM Switch Module

The Dell Integrated KVM switch module allows you to configure and manage your system's server modules by providing keyboard, monitor, and mouse functions to the Dell PowerEdge™ server modules in a Dell Modular Server Enclosure as if you were directly connected to the module. You can connect to the KVM switch module from either a common access point or across an IP network.

The server modules can be accessed through any one of the following:

- Local keyboard, monitor, and mouse (or *crash cart*)
- External Dell analog KVM switch
- External Dell digital KVM switch
- Web-based console redirection through the DRAC/MC

The module includes a local KVM cable (or *dongle*) that provides two PS2 connections and a video connection. The local KVM cable connects to the custom connector on the module.

See the *Dell Integrated KVM Switch Module User's Guide* and your system's *Installation and Troubleshooting Guide* or *Hardware Owner's Manual* for more information.

DRAC/MC-Supported KVM Modules

The DRAC/MC supports the following KVM modules in a Dell Modular Server Enclosure:

- Dell KVM pass-through module
- Avocent Analog KVM switch module
- Avocent Digital Access KVM module

Table 9-1 lists a feature summary of the DRAC/MC-supported KVM modules.

Table 9-1. DRAC/MC-Supported KVM Module Features

Dell KVM Pass-Through Module	Avocent Analog KVM Module	Avocent Digital Access KVM Module
KVM connector only.	ACI (RJ-45) and KVM connectors.	Ethernet and KVM connectors.
No network interface.	No network interface.	Network interface supports static IP address or DHCP.
No OSCAR support.	Supports OSCAR.	Supports OSCAR.
No support for Web-based console redirection.	No support for Web-based console redirection.	Supports Web-based console redirection through the DRAC/MC.
No Virtual Media support.	No Virtual Media support.	Supports Virtual Media through the DRAC/MC.

The following subsections provide descriptions of each DRAC/MC-supported KVM module for your Dell Modular Server Enclosure.

Dell KVM Pass-Through Module

NOTE: The Dell KVM pass-through module is not configured with an RJ-45 connector. This module does not report the <*presence*> status to the DRAC/MC. As a result, the chassis summary screen and the RACADM commands `getkvminfo` and `getmodinfo` indicates that the KVM is absent. Additionally, the DRAC/MC does not generate a log entry when the KVM pass-through is installed or removed.

The Dell KVM Pass-Through Module provides a KVM connection from the server modules in the Dell Modular Server Enclosure to a local KVM.

This module can be configured by connecting a local KVM cable from the custom connector to a local keyboard, monitor, and mouse.

See the documentation included with your module to identify the custom connector.

Avocent Analog KVM Switch Module

The Avocent Analog KVM switch module provides a KVM connection from the server modules in the Dell Modular Server Enclosure to a local KVM or an external Dell KVM switch.

This module can be configured using one of the following methods:

- Connect a local KVM cable from the custom connector to a local KVM.
- Connect a CAT 5 cable from the Analog Console Interface (ACI) port to an external Dell analog or digital KVM switch.

See the documentation included with your module to identify the custom connector and ACI port.

Avocent Digital Access KVM Module

The Avocent Digital Access KVM Module provides a KVM connection from the server modules in the Dell Modular Server Enclosure to a local KVM or an external Dell KVM switch. The module also provides Web-based console redirection and virtual media through the DRAC/MC.

This module can be configured using one of the following methods:

- Connect a local KVM cable from the custom connector (see Figure 9-2) to a local KVM.
- Connect a local KVM cable from the custom connector (see Figure 9-2) to a Server Interface Pod (SIP) and a CAT 5 cable from the SIP to an external Dell Analog or Digital KVM switch.
- Connect a CAT 5 cable from the NIC connector (see Figure 9-2) to the same subnet as the DRAC/MC.

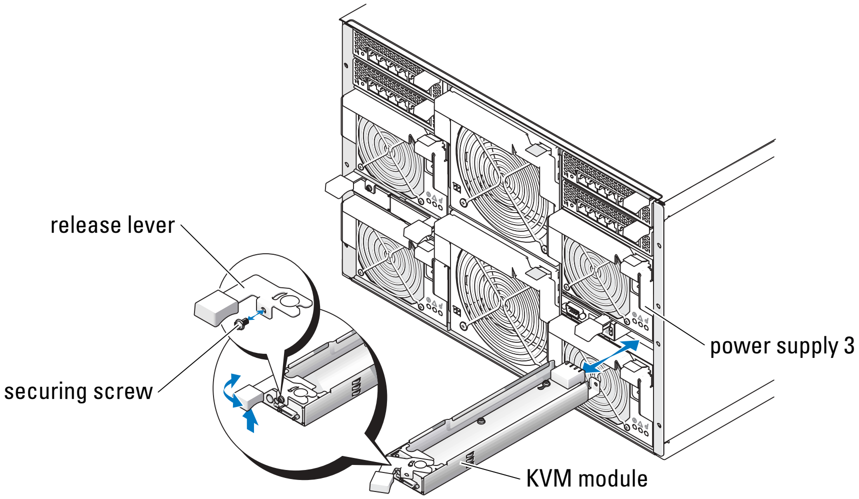
NOTE: The Avocent Digital Access KVM module default IP address is 192.168.0.121.

Installing the KVM Module

1. Ensure that the KVM module release lever is fully extended.
2. Slide the module into the chassis until it is fully seated.
3. Close the release lever until it seats securely into place.
4. Install the Phillips head screw that secures the release lever to the module.
5. Connect the cables to the module.

NOTE: The KVM module can only be installed in the KVM slot under power supply 3, as shown in Figure 9-1.

Figure 9-1. Removing and Installing a KVM Module



Avocent Digital Access KVM Module Features

The Avocent Digital Access KVM Module includes a custom cable (or *dongle*) that ships with your system, which provides two PS/2 connectors and one video connector. The KVM module also includes an identification indicator (see Figure 9-2). Table 9-2 lists the indicator status.

See the online help for additional information.

Figure 9-2. Avocent Digital Access KVM Module Features

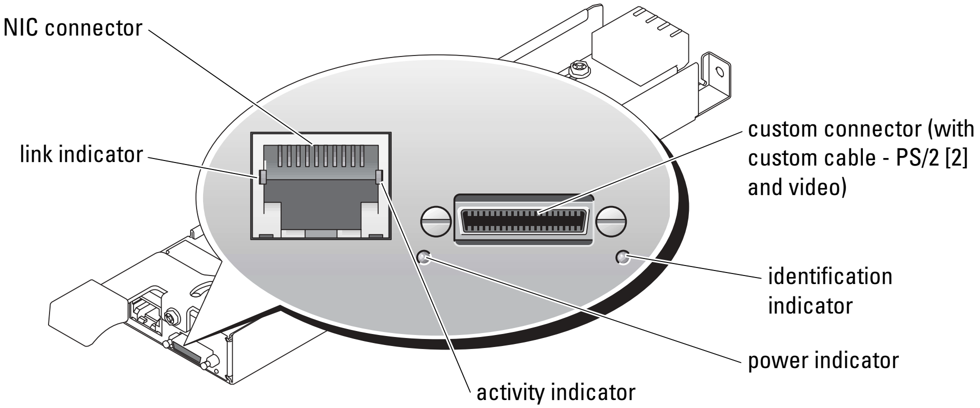


Table 9-2. KVM Switch Module Features

Indicator	Activity Indicator	Indicator Code
Identification indicator	Off	Dell Server Module Enclosure is not being identified.
	Green blinking	Dell Server Module Enclosure is being identified.
Power indicator	Off	KVM switch does not have power.
	Green	KVM switch has power.
Custom connector	None	Allows two PS/2 connectors and one video device to be connected to the system.
Link indicator	Off	The NIC is not connected to the network.
	Green	The NIC is connected to a valid link partner on the network.
Activity indicator	Off	Network data is not being sent or received.
	Amber blinking	Network data is being sent or received.

Identifying the KVM Type Using the User Interface

To identify the KVM type using the user interface, click the **Properties** tab and then click **Chassis Summary**. The KVM module appears under **KVM Information**.

Table 9-3 provides a description of the **KVM Information** fields in the user interface.

Table 9-3. Fields for KVM Information

Field	Description
KVM Presence	Indicates whether or not the KVM module is installed in the chassis.
KVM Model	Displays the KVM model and type.
KVM Firmware Version	Indicates the current KVM firmware version level.
KVM Hardware Version	Indicates the current KVM hardware version level.
KVM Status	Indicates the status of the current KVM, which can be **N/A**, **Ready**, **OFF**, and **Updating**.
Current IP Address	Indicates the current KVM IP address.
Current IP Gateway	Indicates the current KVM IP gateway IP address.
Current IP Netmask	Indicates the current KVM IP netmask IP address.
MAC Address	Indicates the KVM MAC address.
DHCP Enabled?	Displays whether DHCP is enabled on the Avocent Digital Access KVM. The default value is **Disabled**.

NOTE: Some KVM status fields will appear only if an Avocent Digital Access KVM is installed in the Dell Modular Server Enclosure.

NOTE: The KVM status field properties will not appear if the Dell Modular Server Enclosure is powered off.

Identifying the KVM Type Using the CLI

To identify the KVM using the CLI, use the following command:

```
racadm getkvminfo
```

Configuring the Avocent Digital Access KVM Module

Use the DRAC/MC GUI to configure the Avocent Digital Access KVM Module in the Dell Server Module Enclosure.

To access the DRAC/MC from the management station:

1 Open a web browser.

2 In the **Address** field, type the IP address of the DRAC/MC that is connected to the Avocent Digital Access KVM Module, and then press <Enter>.

3 In the **Logon** box, type your user name and password, and then click **OK**.

NOTE: The default user name is `root`; the default password is `calvin`.

The following sections provide information on configuring your Avocent Digital Access KVM Module from the management station using the DRAC/MC user interface.

NOTE: The Avocent Digital Access KVM Module is the only KVM module that must be configured through the DRAC/MC user interface.

Configuring Your Network

1 Press the power button on the Dell Modular Server Enclosure to turn on the system (if required). Ensure that the system power indicator is green before proceeding to step 2.

2 Click the **Configuration** tab and select **Digital Access KVM Settings**.

Table 9-4 describes the Network settings.

NOTE: To ensure proper communications between the Avocent Digital Access KVM Module and the DRAC/MC, configure your Avocent Digital Access KVM Module's IP address in the same subnet as the DRAC/MC.

NOTE: To change any of the settings on the **Digital Access KVM Settings** page, you must have **Configure DRAC/MC** permission.

Table 9-4. Digital Access KVM Settings

Setting	Description
MAC Address	Displays the KVM MAC address.
Use DHCP **(For NIC IP Address)** **(Default: Off)**	Causes Avocent Digital Access KVM NIC to obtain the IP address from the DHCP server; deactivates the **Static IP Address**, **Static Subnet Mask**, and **Static Gateway** controls.
Static IP Address	Specifies or edits the Static IP address for the Avocent Digital Access KVM module NIC. This option is not available if **Use DHCP** is selected.
Static Gateway	Specifies or edits the static gateway for the Avocent Digital Access KVM NIC. This option is not available if **Use DHCP** is selected.
Static Subnet Mask	Specifies or edits the static subnet mask for the Avocent Digital Access KVM NIC. This option is not available if **Use DHCP** is selected.
Auto Negotiation	Determines whether the DRAC/MC automatically sets the **Duplex Mode** and **Network Speed** by communicating with the nearest router or hub (**On**) or allows you to set the **Duplex Mode** and **Network Speed** manually (**Off**).
Duplex Mode	Configures the duplex mode to full or half to match your network environment. This option is not available if **Auto Negotiation** is set to **On**.
Network Speed	Configures the network speed to 100 Mb or 10 Mb to match your network environment. This option is not available if **Auto Negotiation** is set to **On**.

Configuring Your Port Settings

The **Digital Access KVM Settings** page also enables you to set the DKVM port numbers settings. Table 9-5 describes the port number settings and identifies the ports used by the DKVM.

Table 9-5. Digital KVM Port Number Setting

Setting	Description
Console	
Keyboard/Mouse Port	Displays the user-assigned port for the keyboard and the mouse. Default port is 2068 (configurable only with DRAC/MC firmware version 1.3 and Digital Access KVM firmware version 01.10.*xx*.).
Video Port	Displays the user-assigned port for the video. Default port is 8192 (configurable only with DRAC/MC firmware version 1.3 and Digital Access KVM firmware version 01.10.*xx*.).
Media	
Virtual Media Port	Displays the user-assigned port for the virtual media. Default port is 3668 (configurable only with DRAC/MC firmware version 1.3 and Digital Access KVM firmware version 01.10.*xx*.).

Other Options

The **Digital Access KVM Settings** page also provides other buttons as shown in Table 9-6.

Table 9-6. Digital Access KVM Settings Page Buttons

Button	Action
Print	Prints the **Digital Access KVM Settings** page.
Refresh	Reloads the **Digital Access KVM Settings** page.
Apply Changes	Saves the changes made to the **Digital Access KVM Settings** page.

Configuring Network Security

Ensuring Network Security

The DRAC/MC and KVM use certificate management to secure your DRAC/MC and KVM network communications.

Certificate Management Overview

A certificate signing request (CSR) is a digital request to a certificate authority (CA) for a secure server certificate. Secure server certificates ensure the identity of a remote system and ensure that information exchanged with the remote system cannot be viewed or changed by others. To ensure DRAC/MC and KVM security, it is strongly recommended that you generate a CSR, submit the CSR to a CA, and upload the certificate returned from the CA.

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

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

See "Managing and Recovering a Remote System" for more information.

Using Graphical User Interface (GUI) Console Redirection

The DRAC/MC and KVM console redirection feature allows you to access the local server console remotely in either graphic or text mode.

Today with the power of networking and the Internet, you do not have to sit in front of each server to perform all the routine maintenance. You can manage the servers from another city or even from the other side of the world from your desktop or laptop computer. You can also share the information with others— remotely and instantly.

NOTE: Your Dell Modular Server Enclosure must be turned on and configured with a KVM to use this feature.

NOTE: Console redirection requires a minimum available network bandwidth of 128 Kbps.

Using Console Redirection

NOTICE: Before you can use console redirection, all browsers must have a Sun Java Virtual Machine Plug-in (version 1.4.2 and later) installed, and the Java cache must be cleared and disabled from the Java plug-in control panel in your operating system. For more information, see "DRAC/MC System Features."

NOTE: When you open a console redirection session, the managed system does not indicate that the console has been redirected.

NOTE: After you click **Launch** in the **Console Redirection** page, the Digital Access KVM keeps the DRAC/MC user session key for up to 3 minutes so the KVM Viewer application can launch. The Console Redirection **Launch** button in the DRAC/MC Web page is disabled for 3 minutes, even if you cancel the Console Redirection certificate acceptance message boxes. If you click the **Launch** button and then click any other link before the DRAC/MC Web page is refreshed, the **Launch** button may be disabled for the next 3 minutes.

The **Console Redirection** page enables you to manage the remote system by using the keyboard, video, and mouse on your local management station to control the corresponding devices on a remote managed system. This feature can be used in conjunction with the Virtual Media feature to perform remote software installations.

The following rules apply to a console redirection session:

- Only one console redirection session is supported.
- A console redirection session can only be connected to one target system.
- When a console redirection viewer application is running, the **Server Selection** option is unavailable. To select another server, close the application, select another server, and then reopen the application.

Opening a Console Redirection Session

When you open a console redirection session, the Dell Digital KVM Viewer Application starts and the remote system's desktop appears in the viewer. Using the Digital KVM Viewer Application, you can control the system's mouse and keyboard functions from a local or remote management station.

To open a console redirection session, perform the following steps:

1. On your management station, open a Web browser.
2. Connect and log into the DRAC/MC.

   The default user name is `root`; the default password is `calvin`.

3. In the left window pane, expand **DRAC/MC** and click **Console**.
4. In the **Console Redirection** screen under **Select a server blade**, select the target PowerEdge system.

   NOTE: This procedure may take a few seconds to complete, depending on your network connection speed.

5. Click **Launch Viewer Application**.

   NOTE: Multiple message boxes may appear after you launch the application. To prevent unauthorized access to the application, navigate through these message boxes within 3 minutes. Otherwise, you will be prompted to relaunch the application.

   NOTE: After clicking **Launch Viewer Application**, the Digital Access KVM locks the DRAC/MC user session for up to 3 minutes. During this time, the **Launch Viewer Application** button is disabled, even if you cancel the Console Redirection certificate acceptance pop-up windows.

   NOTE: If one or more **Security Alert** windows appear in the following steps, read the information in the window and click **Yes** to continue.

   The **Dell Digital KVM Viewer Application** window appears with the remote system's desktop in the application window.

6. If two mouse pointers appear on the remote system's desktop, synchronize the mouse pointers on the management station and the remote system. See "Synchronizing the Mouse Pointers."

NOTE: With DRAC/MC version 1.2 and earlier, if a user had multiple Console Redirection or Virtual Media sessions opened to different Digital KVMs from the same client, it was not easy to distinguish between these sessions. DRAC/MC version 1.3 and later have the capability to display an identification in the Console Redirection/ Virtual Media application title bar in the format <*chassisname-servername*>. If the <*chassisname*> field is not configured, the identification is in the form of <*chassisservicetag-servername*>. This format is only available with Digital Access KVM firmware version 01.10.*xx* or later.

Using the Digital KVM Viewer Application

The Java-powered Dell Digital KVM Viewer Application provides a user interface between the management station and the remote system, allowing you to see the remote system's desktop and control its mouse and keyboard functions from your management station. When you connect to the remote system, the Digital KVM Viewer Application starts in a separate window.

The Digital KVM Viewer Application provides various control adjustments such as video calibration, mouse acceleration, and snapshots. Click **Help** for more information on these functions.

When you start a console redirection session and the Digital KVM Viewer Application window appears, you may be required to adjust the following controls in order to view and control the remote system properly. These adjustments include:

- Adjusting the video quality
- Synchronizing the mouse pointers

Adjusting the Video Quality

The Digital KVM Viewer Application provides video adjustments that allow you to optimize the video for the best possible view.

To adjust the video quality, perform the following steps:

1. At the bottom of the **Digital KVM Viewer Application** window, click **Calibrate**.
2. To adjust the video quality automatically, click the **Automatic Video Adjustment** button.
3. To manually adjust or fine tune the video quality, including the screen position, click each video adjustment button in the window and adjust the controls as needed.

   NOTE: The recommended server module video resolution for optimal console redirection performance is 1024 by 768 pixels and 60Hz refresh rate.

   Click **Help** for more information.

   NOTE: Reducing the **Pixel Noise Ratio** setting to zero causes multiple video refresh commands that generates excessive network traffic and flickering video in the **Dell Digital KVM Viewer Application** window. Dell recommends that you adjust the **Pixel Noise Ratio** setting at a level that provides optimal system performance and pixel enhancement while minimizing network traffic.

   NOTE: The display on the console redirection viewer may occasionally get corrupted due to loss of video synchronization. Click **Refresh** in the viewer application to fix this issue and clear the video corruption.

Synchronizing the Mouse Pointers

When you connect to a remote PowerEdge system using Console Redirection, the mouse acceleration speed on the remote system may not synchronize with the mouse pointer on your management station, causing two mouse pointers to appear in the **Dell Digital KVM Viewer Application** window.

To synchronize the mouse pointers, disable mouse acceleration on the target server module, the management station, and the **Dell Digital KVM Viewer** application. When you complete these procedure, the remote system mouse pointer and the management station mouse pointer move together (or *shadow*) as one mouse pointer.

To synchronize the mouse pointers, perform the following steps. See Table 9-7 for the procedure that is appropriate for your operating system.

1 Open a console redirection session and start the **Dell Digital KVM Viewer Application** on the target server module.

2 Identify the operating system that is running on both the target server module and your management station.

3 In the **Dell Digital KVM Viewer Application** window, disable the mouse acceleration speed on the target server module. See Table 9-7.

4 On your management station, disable the mouse acceleration speed. See Table 9-7.

5 In the **Dell Digital KVM Viewer Application** window in the **Mouse Acceleration** box, click the drop-down menu arrow and select **None**.

6 In the **Dell Digital KVM Viewer Application window**, move your management station mouse pointer to the top left corner of the screen until both mouse pointers move together (or *shadow*) as one mouse pointer.

NOTE: Synchronizing the mouse pointers may take several seconds to complete, depending on your network connection.

Table 9-7. Disabling Mouse Acceleration

Remote System's Operating System	Procedure
Microsoft® Windows® 2000	1 On the remote system's desktop, click **Start** and select **Run.** 2 In the **Run** field, type `regedit` and click **OK**. 3 In the **Registry Editor** left window pane, expand **HKEY_USERS→DEFAULT→Control Panel.** 4 Click **Mouse**. 5 In the **Registry Editor** right window pane, right-click **MouseSpeed** and select **Modify**. 6 In the **Edit String** window in the **Value data** field, change the current value from **1** to **0** and click **OK**. 7 Close the R**egistry Editor** window. 8 On the Windows desktop, click **Start** and select **Control Panel→Mouse**. 9 In the **Mouse Properties** window, click the **Motion** tab. 10 In the **Acceleration** box, click **None** and then click **OK**.

Table 9-7. Disabling Mouse Acceleration *(continued)*

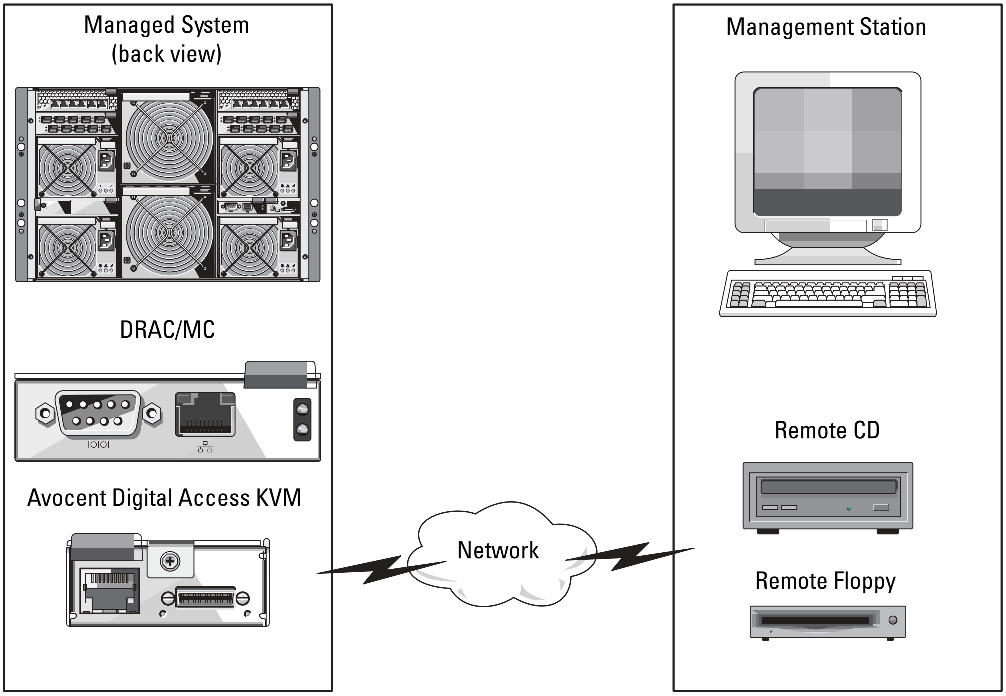
Remote System's Operating System	Procedure
Windows Server™ 2003	1 On the remote system's desktop, click **Start** and select **Run.** 2 In the **Run** field, type `regedit` and click **OK**. 3 In the **Registry Editor** left window pane, expand **HKEY_USERS→DEFAULT→Control Panel.** 4 Click **Mouse**. 5 In the **Registry Editor** right window pane, right-click **MouseSpeed** and select **Modify**. 6 In the **Edit String** window in the **Value data** field, change the current value from **1** to **0** and click **OK**. 7 Close the **Registry Editor** window. 8 On the Windows desktop, click **Start** and select **Control Panel→Mouse**. 9 In the **Mouse Properties** window, click the **Pointer Options** tab. 10 In the **Motion** box, deselect **Enhance pointer precision** and then click **OK**.
Red Hat® Enterprise Linux (version 3) with a command line interface Red Hat Enterprise Linux (version 4) with a command line interface	1 At the command prompt, type the following and press <Enter>: `xset m 0` **NOTE:** When you restart your system, the value resets to the default setting. 2 In the **Dell Digital KVM Viewer Application** window in the **Mouse Configuration** box drop-down menu, select **None**. 3 Move the mouse until the mouse pointer and the curser shadow each other.
Red Hat Enterprise Linux (version 3) with the X Window System	1 Click the Red Hat icon and select **Preferences→Control Center** 2 In the **Control Center** window, double click the **Mouse** icon. 3 In the **Mouse Preferences** window, click the **Motion** tab. 4 In the **Speed** box under **Acceleration**, adjust the toggle halfway between **Slow** and **Fast**, and then click **OK**. 5 In the **Dell Digital KVM Viewer Application** window in the **Mouse Configuration** box drop-down menu, select **None**.
Red Hat Enterprise Linux (version 4) with the X Window System	1 Click the Red Hat icon and select **Preferences→Mouse**. 2 In the **Mouse Preferences** window, click the **Motion** tab. 3 In the **Speed** box under **Acceleration**, adjust the acceleration speed bar halfway between **Slow** and **Fast**. 4 Click **Close**.
SUSE® Linux Enterprise Server (version 9) SP3 with the X Window System	1 Click the Novell® icon and select **Control Center→Peripherals→Mouse**. 2 In the **Mouse** window, click the **Advanced** tab. 3 In the **Pointer Acceleration** dialog box, set the acceleration value to 1.0x. 4 Click **Apply** and close the window.

Using Virtual Media

Overview

The Virtual Media feature provides the managed system with a virtual CD and virtual floppy drive, which can use standard media from anywhere on the network. Figure 9-3 shows the overall architecture of virtual media.

Figure 9-3. Overall Architecture of Virtual Media



Using Virtual Media, administrators can remotely boot their managed systems, install applications, update drivers, or even install new operating systems remotely from the virtual CD/DVD and diskette drives.

NOTE: Virtual Media requires a minimum available network bandwidth of 128 Kbps.

NOTE: Digital Access KVM firmware version 1.10.*xx* or later support the CD and DVD media recorded in a multi-session format.

The management station provides the physical media or image file across the network.

NOTE: JAVA Runtime Environment (JRE) version 1.4.2 (or later) must be installed on the management station to run a virtual media session.

When Virtual Media is connected, all virtual CD/floppy drive access requests from the managed system are directed to the management station across the network. When Virtual Media is not connected, virtual devices on the managed system behave just like two drives without media present.

Currently, the virtual floppy drive can be connected to a legacy 1.44 MB floppy drive with a 1.44 MB floppy diskette, a USB floppy drive with a 1.44 MB floppy diskette, a 1.44 MB floppy image, and Dell USB keys. The virtual CD/DVD drive can be connected to a CD/DVD or ISO image.

Managed System Requirements

Table 9-8 provides the management station system requirements to run Console Redirection and Virtual Media sessions.

Table 9-8. Management Station System Requirements

Component	Minimum Requirements
Processor	Intel® Pentium™ 650 MHz or equivalent
RAM	128 MB
Network connection	10BaseT or 100BaseT (100BaseT recommended)
Operating System	• Windows 2000 Workstation, Server, or Terminal Server with Service Pack 4 or later **NOTE:** When using Virtual Media to install Windows 2000 Server, the installation CD must have a built-in Service Pack 4, which is required to access the virtual drives. This requirement also applies to using the virtual drives with Windows 2000 Server. The drives will not appear until Service Pack 4 has been successfully installed. • Windows XP Home or Professional Edition • Windows Server 2003, Standard, Enterprise, or Web Edition • Red Hat Enterprise Linux (version 3) Advanced Server (ES, AS, and WS) • Red Hat Enterprise Linux (version 4) Advanced Server (ES, AS, and WS) • SUSE Linux Enterprise Server (version 9, SP3)
Video	• XGA video with a graphics accelerator • 800 x 600 resolution • Color palette of at least 256 colors

Using the Virtual Media Feature

To use the Virtual Media feature, perform the following procedures from your management station:

1. Open a console redirection session.
2. Attach the Virtual Media device to the remote system.
3. Connect the virtual media to the Virtual Media device.

The following subsections provide the necessary steps to perform these procedures.

Opening a Console Redirection Session

1. Perform the procedures in "Opening a Console Redirection Session."
2. In the **Console Redirection** page in the **Select a server blade** column, record the server name that you selected as the target remote system. This information is required in the following section.

Attaching the Virtual Media Device to the Remote System

1. In the **Remote Access Controller/Modular Chassis** window's left window pane, expand **DRAC/MC** and click **Media**.

   All the available server modules are listed under **Select a server blade**.

2. In the **Virtual Media** screen under **Select a server blade**, select the server that you chose in "Opening a Console Redirection Session" and click **Attach**.
3. Click **Launch Media Application**.

   NOTE: If one or more **Security Alert** windows appear, read the information in the window and click **Yes** to continue.

   The virtual media session starts and the **Virtual Media** window appears.

   The **Status** box displays the target drives and the corresponding connection status for each drive.

   NOTE: A USB memory key or a floppy image file is also listed under **Floppy Drive** because they could be virtualized as a virtual floppy.

   NOTE: The drive letters of virtual devices on the managed system have no correlation to the drive letters of physical drives on the management station.

4. In the **Dell Digital Access KVM Viewer Application** window, verify that the virtual media device is attached to the remote system.

Connecting the Virtual Media to the Virtual Media Device

NOTE: A valid media should be present in the floppy or CD/DVD drive before the respective virtual media device can be connected.

1. In the **Floppy Drive** box or the **CD/DVD Drive** box, select the virtual media that you want to connect to the virtual media device.
2. Click **Browse** and select the appropriate drive.
3. Click **Connect**.

   The **Connected To** column displays the connection status for the selected target drive. The **Read Bytes** column displays the data transfer speed.

Changing the Virtual Media Device

NOTE: Changing virtual media while connected could stop the system boot sequence.

1 In the **Virtual Media** window, click **Disconnect**.

2 Remove the CD or DVD from the management station CD drive (if applicable).

3 Perform one of the following procedures:

- Insert another CD or DVD into the management station CD drive.
- In the **Floppy Drive** or **CD/DVD drive** box, click **Browse** and select another floppy drive or ISO image.

4 Click **Connect**.

Disconnecting the Virtual Media Device From the Virtual Media Device

1 In the **Virtual Media** window, click **Disconnect**.

In the **Status** box, the target drive status in the **Connected To** column changes to **Not connected** and the data transfer rate for each disconnected drive in the **Read Bytes** column change to **n/a**.

2 Close the **Virtual Media** window.

3 In the **Close program request** window, click **Yes** to close the virtual media window.

Detaching the Virtual Media Device from the Remote System

1 Navigate to the **Dell Remote Access Controller/Modular Chassis** window.

2 In the **Virtual Media** screen, click **Detach**.

3 When prompted, click **OK** to close the virtual media connection.

In the **Virtual Media** screen, the **Select a server module** selection changes to **None** and the **Detach** button changes to **Attach**.

4 Close the **Dell Digital KVM Viewer Application**.

In the **Dell Digital KVM Viewer Application** window, click **Close**.

5 Close the Console Redirection session.

In the **Dell Remote Access Controller/Modular Chassis** window, click **Log Out**.

Booting From the Virtual Media

On supported systems, the system BIOS allows you boot from virtual CD or virtual floppy drives. You need to enter the BIOS setup window to ensure that the virtual drives are enabled in the boot sequence menu and that bootable devices are in the correct order.

To change the BIOS setting, perform the following steps:

1 Boot the managed system.

2 Press <F2> to enter the BIOS setup window.

3. Scroll to the boot sequence and press <Enter>.

   In the pop-up window, the virtual CD and virtual floppy (USB) drives are listed along with other regular boot devices.

4. Ensure that the virtual drive is enabled and that it is the first device with bootable media present among the listed devices. If it is not the first device, you can change the boot order by following the instructions on the screen.

5. Save the changes and exit.

   The managed system reboots.

   The managed system attempts to boot from a bootable device based on the boot order. If the virtual device is connected and a bootable media is present, the system boots to this virtual device. Otherwise, the system ignores the device, just like a physical device without bootable media.

Installing Operating Systems Using Virtual Media

1. Ensure that your operating system installation CD is inserted in the management station's CD drive.
2. Ensure that you have selected your local CD drive and that you have connected to the virtual drives.
3. Follow the steps for booting from the virtual media in the preceding section to ensure that the BIOS is set to boot from the CD drive that you are installing from.
4. Follow the instructions on the screen to complete the installation.

Using Virtual Media When the Server's Operating System is Running

On Windows systems, the virtual media drives are mounted and given a drive letter.

Using the virtual drives from within Windows is similar to using your physical drives. When you connect to the media at a management station, the media is available at the system by simply clicking the drive and browsing its content.

On a Red Hat Enterprise Linux or SUSE Linux Enterprise Server system, the virtual drives must be mounted before the drives can be accessed. Before mounting the drive, first connect to the media at the management station.

Red Hat Enterprise Linux automatically creates mount points in the **/etc/fstab** file for the virtual floppy and CD drives.

On a system running Red Hat Enterprise Linux or SUSE Linux Enterprise Server, type the following command to quickly identify the assigned virtual media devices:

```
cat /var/log/messages | grep Virtual
```

Updating the KVM Firmware

NOTICE: The DRAC/MC remains available until the KVM firmware update is complete. Dell recommends that you avoid using the DRAC/MC Web-based user interface and the telnet interface until the KVM firmware update is complete.

NOTE: Downgrading the Digital Access KVM firmware version will reset the KVM configuration to its default values.

Use one of the following methods to update your KVM firmware.

- Web-based interfaces
- RACADM CLI — See "fwupdate"

Using the DRAC/MC Web-based Interface to Update the KVM Firmware

1. Copy the KVM binary file to update the TFTP root directory.
2. Log on to the DRAC/MC Web-based user interface using a supported Internet browser.
3. Select **KVM Update** for the module to be updated.
4. From the DRAC/MC Web-based user interface main window, click the **Update** tab. The **Firmware Update** window is displayed.
5. On the **Firmware Update** window, enter the IP address of the TFTP server and the KVM firmware image name and select the KVM firmware as the option to update.

   NOTE: The Digital KVM firmware image name length is limited to 20 characters.
6. Click **Update Firmware**.
7. The TFTP download and firmware update process may take several minutes. After the update completes, the KVM will reset.

Using the RACADM Command Line Interface to Update KVM Firmware

1. Copy the KVM firmware binary file to a TFTP server root directory.
2. Log on to the DRAC/MC telnet or serial interface.
3. From the telnet or serial interface, using the **racadm fwupdate** command, type a command line similar to the following example:

   ```
   racadm fwupdate -a <TFTP_IP_Address> -d <kvm_firmware_name> -m kvm
   ```
4. The TFTP download and firmware update process may take several minutes. After the update completes, the KVM resets.

Frequently Asked Questions

Table 9-9 lists frequently asked questions and answers.

Table 9-9. Using Virtual Media: Frequently Asked Questions

Question	Answer
Do I need to install drivers on the server to make the Virtual Media feature work?	No. Drivers are not required on either the managed system or the management station. The operating system provides what is required for this feature. See "Managed System Requirements" for a list of supported operating systems.

How do I find my device names on Linux systems so I can mount them?	You can look at the **/etc/fstab** file which lists the device names for all your devices. When you know the device name, then you can use the **mount** and **unmount** command to mount and unmount your CD or floppy drives.
	To manually identify the virtual media devices, type the following command:
	`cat /var/log/messages | grep Virtual`
	Then look for mount points for those devices in the **/etc/fstab** file.
	Finally, use the associated mount point on the **mount** command, for example:
	`mount /mnt/cdrom1`

Subcommand Man Pages

This section provides descriptions of the subcommands that you can run in the RACADM CLI.

Table A-1 and Table A-2 contain general information about CLI RACADM and CLI serial command permissions, respectively. Some commands in both tables may apply to both serial and RACADM command permissions.

Table A-1. CLI RACADM Command Permissions

Command Name	Permission
chassisaction	Execute Server Control Commands
clrraclog	Clear Logs
clrsel	Clear Logs
config	Configure DRAC/MC
crdisconnect	Administrator
fwupdate	Configure DRAC/MC
getassettag	Log in to DRAC/MC
getconfig	Log in to DRAC/MC
getdcinfo	Log in to DRAC/MC
getioinfo	Log in to DRAC/MC
getkvminfo	Log in to DRAC/MC
getled	Log in to DRAC/MC
getmacaddress	Log in to DRAC/MC
getmodinfo	Log in to DRAC/MC
getniccfg	Log in to DRAC/MC
getpbinfo	Log in to DRAC/MC
getraclog	Log in to DRAC/MC
getractime	Log in to DRAC/MC
getsel	Log in to DRAC/MC
getsensorinfo	Log in to DRAC/MC
getssninfo	Log in to DRAC/MC

Table A-1. CLI RACADM Command Permissions *(continued)*

Command Name	Permission
getsvctag	Log in to DRAC/MC
getsysinfo	Log in to DRAC/MC
help	Log in to DRAC/MC
racdump	Log in to DRAC/MC
racreset	Configure DRAC/MC
racresetcfg	Configure DRAC/MC
serveraction	Execute Server Control Commands
sslcertview	Configure DRAC/MC
setassettag	Configure DRAC/MC
setled	Configure DRAC/MC
setniccfg	Configure DRAC/MC
setractime	Configure DRAC/MC
setsysinfo	Configure DRAC/MC
testemail	Test Alerts
testtrap	Test Alerts
vmdetach	Administrator

Table A-2. CLI Serial Command Permissions

Command Name	Permission
chassisaction	Execute Server Control Commands
clrraclog	Clear Logs
clrsel	Clear Logs
connect	Access Console Redirection
exit	Log in to DRAC/MC
getdcinfo	Log in to DRAC/MC
getioinfo	Log in to DRAC/MC
getkvminfo	Log in to DRAC/MC
getled	Log in to DRAC/MC
getpbinfo	Log in to DRAC/MC
getmodinfo	Log in to DRAC/MC

Table A-2. CLI Serial Command Permissions *(continued)*

Command Name	Permission
getraclog	Log in to DRAC/MC
getsel	Log in to DRAC/MC
getsensorinfo	Log in to DRAC/MC
getsysinfo	Log in to DRAC/MC
help	Log in to DRAC/MC
logout	Log in to DRAC/MC
quit	Log in to DRAC/MC
serveraction	Execute Server Control Commands

help

NOTE: To use this subcommand, you must have **Log In DRAC/MC** permission.

Table A-3 describes the **help** subcommand.

Table A-3. Help Subcommand

Command	Definition
help	Lists all of the subcommands available to use with **RACADM** and provides a short description for each.

Synopsis

```
racadm help
```

```
racadm help <command>
```

Description

The **help** subcommand lists all of the subcommands that are available under the RACADM CLI along with a one-line description. You can also type a command after **help** to get the syntax for a specific subcommand.

Output

The **racadm help** subcommand displays a complete list of subcommands.

The **racadm help** <*command*> command displays information for the specified subcommand only.

logout/exit/quit

Synopsis

```
logout
```

```
exit
```

```
quit
```

Description

The **logout**, **exit**, and **quit** subcommands log the current user out of the serial/telnet command shell and then display a new login prompt.

Output

The **logout, exit, and quit** subcommands return no output (if successful).

connect

NOTE: To use the **connect** subcommand, you must have **Access Console Redirection** permission.

Table A-4 describes the **connect** subcommand.

Table A-4. connect Subcommand

Subcommand	Definition
connect	Connects the console to a server module or switch port.

Synopsis

```
connect <module>
```

```
connect [-F] <module>
```

Description

The **connect** command enables the DRAC/MC serial port to connect to the serial port on the target server or switch module (<*module*>). See Table A-5.

When the system BIOS console redirection setting is set to BMC, the **-F** option forces the serial console redirection session to switch from **BMC** to **DRAC/MC**. When the system is rebooted, the BIOS console redirection setting returns to the default setting.

When the connection is in text mode, the connection is terminated by typing <Enter><~><.>.

If the host terminal connection to the DRAC/MC serial port is disconnected when the connection is in secure mode, console redirection is terminated, and you are logged out from the serial command shell.

To terminate the connection, type the following sequence:

<Enter><~><.>

Input

Table A-5 describes the **connect** subcommand options.

Table A-5. connect Subcommand Options

Option	Description
`<module>`	The module has the following legal values: `<servername>` `switch-<n>` where `n = 1 to 4` (for example, `switch-1`)
–F	forces the SOL multiplexer (mux) to be switched to DRAC/MC.

Output

Prints a single output line and connects to the targeted module port.

For example:

```
Connected to server-1
```

When the connection is terminated, the DRAC/MC generates the following output:

```
Connection to <module> terminated.
DRAC/MC:
```

Examples

```
connect server-1
connect switch-1
```

config/getconfig

NOTE: To use the **config** subcommand, you must have **Configure DRAC/MC** permission.

NOTE: To use the **getconfig** subcommand, you must have **Log In To DRAC/MC** permission.

Table A-6 describes the **config** and **getconfig** subcommands.

Table A-6. config/getconfig Subcommand Options

Subcommand	Definition
config	Configures the DRAC/MC.
getconfig	Gets the DRAC/MC configuration data.

Synopsis

```
racadm config -g <groupName> -o <objectName> [-i <index>] <Value>

racadm getconfig -g <groupName> [-i <index>]

racadm getconfig -u <username>

racadm getconfig -h
```

config Subcommand Description

The **config** subcommand allows you to set DRAC/MC configuration parameters individually. If the data is different, that DRAC/MC object is written with the new value.

Input

Table A-7 describes the **config** subcommand options.

NOTE: The **-f**, **-s**, and **-p** options are not supported for the serial RACADM console.

Table A-7. config Subcommand Options and Descriptions

Option	Description
-g	The **-g <*groupName*>**, or group option, must be used with the **-o** option. The <*groupName*> specifies the group containing the object that is to be set.
-o	The **-o <*objectName*> <*Value*>**, or object option, must be used with the **-g** option. This option specifies the object name that is written with the string <*value*>. For more information on groups and their associated object names, see "Configuring a DRAC/MC to Use a Serial or Telnet Text Console."
-i	The **-i <*index*>**, or index option, is only valid for indexed groups and can be used to specify a unique group. The <*index*> is a decimal integer from 1 through 16. The index is specified here by the index value, not a named value.

Output

This subcommand generates error output when invalid syntax, group name, object name, index, or other invalid database members are encountered.

getconfig Subcommand Description

The **getconfig** subcommand allows you to retrieve DRAC/MC configuration parameters on an individual basis.

Input

Table A-8 describes the **getconfig** subcommand options.

NOTE: The -f option is not supported for the serial/telnet console.

Table A-8. getconfig Subcommand Options and Descriptions

Option	Description
-g	The **-g** ***<groupName>***, or *group* option, can be used to display the configuration for a single group. The **groupName** is the name for the group used in the **racadm.cfg** files. If the group is an indexed group, use the **-i** option.
-h	The **-h**, or **help** option, displays a list of all available configuration groups that you can use. This option is useful when you do not remember exact group names.
-i	The **-i** ***<index>***, or **index** option, is valid only for indexed groups and can be used to specify a unique group. The <*index*> is a decimal integer from 1 through 16. If **-i** <*index*> is not specified, a value of 1 is assumed for groups, which are tables that have multiple entries. The index is specified by the index value, not a named value.
-u	The **-u** ***<username>***, or **user name** option, can be used to display the configuration for the specified user. The <*username*> option is the log in user name for the user.

Output

This subcommand generates error output upon encountering either of the following:

- Invalid syntax, group name, object name, index, or other invalid database members
- Serial/telnet console transport failures

If errors are not encountered, this subcommand displays the contents of the specified configuration.

Examples

- `racadm getconfig -g cfgLanNetworking` – Displays all of the configuration parameters (objects) that are contained in the group cfgLanNetworking.
- `racadm config -g cfgLanNetworking -o cfgNicIpAddress 10.35.10.100 –` Sets the **cfgNicIpAddress** configuration parameter (object) to the value 10.35.10.110. This IP address object is contained in the group cfgLanNetworking.

- `racadm getconfig -h` – Displays a list of the available configuration groups on the DRAC/MC.
- `racadm getconfig -u root` – Displays the configuration parameters for the user named `root`.

crdisconnect

NOTE: To use the **crdisconnect** subcommand, you must have **Administrator** permission.

Table A-9 describes the **crdisconnect** subcommand.

Table A-9. crdisconnect Subcommand

Subcommand	Definition
crdisconnect	Closes the Web console redirection session.

Synopsis

```
racadm crdisconnect
```

Description

The **crdisconnect** command enables a user with administrator permission to disconnect a Web-based console redirection session.

This command returns an error if no console redirection session is active.

fwupdate

NOTE: To use this subcommand, you must have **Configure DRAC/MC** permission.

Table A-10 describes the **fwupdate** subcommand.

Table A-10. fwupdate Subcommand

Subcommand	Definition
fwupdate	Allows the caller to update the firmware on the DRAC/MC.

Synopsis

```
racadm fwupdate -a <TFTP IP Address> -d <directory and filename> [-D]
[-m kvm/drac]
```

Description

The **fwupdate** subcommand allows the caller to update the firmware on the DRAC/MC or the Avocent Digital Access KVM module. The user can instruct the DRAC/MC or Digital Access KVM firmware to get the firmware update file from a TFTP server and load it into the DRAC/MC or the Avocent Digital Access KVM flash.

NOTICE: Running the **fwupdate** subcommand prompts the DRAC/MC to reboot into a fwupdate mode, which causes all telnet and web connections to be dropped. To see the progress of the update, you must be connected to the serial console through the serial connection on the DRAC/MC.

Input

Table A-11 describes the **fwupdate** subcommand options.

Table A-11. fwupdate Subcommand Options and Descriptions

Option	Description
-a	The **IP Address** option specifies the IP address of the TFTP server.
-d	The **-d** option specifies the path and filename of the firmware update file on the TFTP server.
-D	After the update is complete, reset all firmware configuration parameters to the default values. For more information, see "racresetcfg."
-m kvm/drac	Indicates which module is to be updated. **NOTE:** This option is available only in DRAC/MC version 1.1 or later. If the **-m** option is not provided, the default is `drac`.

Output

Status of the TFTP upload can only be seen from a serial connection to the DRAC/MC as the DRAC/MC telnet and web server services are shut down during the upload to ensure that the card does not receive interrupts that might impact the firmware update.

getioinfo

NOTE: To use this subcommand, you must have **Log In To DRAC/MC** permission.

Table A-12 describes the **getioinfo** subcommand.

Table A-12. getioinfo Subcommand

Subcommand	Definition
getioinfo	Retrieves I/O status information.

Synopsis

```
racadm getioinfo
```

Description

The **getioinfo** subcommand displays the following information about the I/O modules in a chassis:

- Module name
- Type
- POST result
- Runtime status
- Power control
- Temperature
- Voltage

Output

Table A-13 provides an example of output from the **getioinfo** subcommand. The default is to display information about all I/O modules in the chassis.

Table A-13. getioinfo Sample Output

# I/O	Module Name	Type	POST Results	<Runtime Status>	<Power Control>	Temperature	Voltage
1	GbE Switch	3	OK	OK	ON	24	N/A
2	GbE Switch	3	OK	OK	ON	23	N/A
3	N/A	0	N/A	N/A	OFF	0	N/A
4	N/A	0	N/A	N/A	OFF	0	N/A

NOTE: The information under the *Voltage* heading will only be populated if you have a Fibre Channel Pass-Through module installed.

Examples

The <*module*> has the following values:

- Fibre Channel Pass-Through
- Gigagbit Ethernet (GbE) Switch
- GbE Pass-Through
- Fibre Channel Switch
- Infiniband Pass-Through

getmacaddress

NOTE: To use the **getmacaddress** subcommand, you must have **Login** permission.

Table A-14 describes the **getmacaddress** subcommand.

Table A-14. getmacaddress Subcommand

Subcommand	Definition
getmacaddress	Gets the MAC address for a server module's network interface adapter.

Synopsis

```
racadm getmacaddress
```

Default

All server module information is displayed.

Options

```
-m <servername>
```

getpbinfo

NOTE: To use the **getpbinfo** subcommand, you must have **Log In DRAC/MC** permission.

Table A-15 describes the **getpbinfo** subcommand.

Table A-15. getpbinfo Subcommand

Subcommand	Definition
getpbinfo	Displays the system power status and power consumption values.

Synopsis

```
racadm getpbinfo
```

Description

The **getpbinfo** subcommand displays the following information about the system's power status and power consumption:

- Overall Power Status
- Redundancy Policy
- Redundant
- Total Available Power

- Redundancy Reserve
- Load Sharing Overhead
- Chassis Base Consumption
- Server Consumption
- Total Consumption
- Remaining Power (excluding reserve)

Examples

Below is a sample output of the **getpbinfo** subcommand.

```
[Power Budget Status]
Overall Power Status                  OK
Redundancy Policy                     3+1
Redundant                             Yes
Total Available Power                 8400W
Redundancy Reserve                    2100W
Load Sharing Overhead                 336W
Chassis Base Consumption              400W
Server Consumption                    1446W
Total Consumption                     2182W
Remaining Power (excluding reserve)   4118W

[Chassis Power Supply Status Table]
<Name>  <Presence>    <Power State><Value>       <Firmware Version>
PS-1    Present       ON           2100W         S21
PS-2    Present       ON           2100W         S21
PS-3    Present       ON           2100W         S21
PS-4    Present       ON           2100W         S21
```

```
[Server Module Power Consumption Table]
<Slot#> <Server Name> <Blade Type>  <Power State> <Current/Max
                                                  Consumption>
1       Server-1      PE1955        ON            241/241W
2       Server-2      N/A           N/A           N/A
3       Server-3      PE1955        ON            241/241W
4       Server-4      PE1855        OFF           0/300W
5       Server-5      PE1955        ON            241/241W
6       Server-6      PE1955        ON            241/241W
7       Server-7      PE1855        OFF           0/300W
8       Server-8      PE1955        ON            241/241W
9       Server-9      N/A           N/A           N/A
10      Server-10     PE1955        ON            241/241W
```

getssninfo

NOTE: To use this subcommand, you must have **Log In To DRAC/MC** permission.

Table A-16 describes the **getssninfo** subcommand.

Table A-16. getssninfo Subcommand

Subcommand	Definition
getssninfo	Retrieves session information for one or more currently active or pending sessions from the Session Manager's session table.

Synopsis

```
racadm getssninfo [-A] [-u <username> | *]
```

Description

The **getssninfo** subcommand returns a list of currently active or pending users and optionally includes summary session table information. The summary information provides the total number of sessions in each of the defined Session Manager states:

- Valid
- Available

Input

Table A-17 describes the **getssninfo** subcommand options.

Table A-17. getssninfo Subcommand Options and Descriptions

Option	Description
-A	The **-A** option eliminates the printing of data headers.
-u	The **-u** <*username*> option limits the printed output to only the detail session records for the given user name. If an "*" symbol is given as the user name, all users are listed. Summary information is not displayed when this option is specified.

Examples

- **racadm getssninfo**

  Session table summary status:

  ```
  1 VALID
  ```

  ```
  3 AVAILABLE
  ```

Table A-18 provides an example of output from the **racadm getssninfo** subcommand.

Table A-18. getssninfo Subcommand Output Example

Type	User	IP Address	Login Date/Time
Serial	root	0.0.0.0	Fri 01 Mar 03 23:31:17 2000 GMT+00:00

- **racadm getssninfo -A**

  ```
  1 3
  ```

  ```
  "Serial" "root" 0.0.0.0 "Fri Mar 03 23:31:17 2000 GMT+00:00"
  ```

- **racadm getssninfo -A -u** *

  ```
  "Serial" "root" 0.0.0.0 "Fri Mar 03 23:31:17 2000 GMT+00:00"
  ```

getsysinfo

NOTE: To use this subcommand, you must have **Log In To DRAC/MC** permission.

Table A-19 describes the **getsysinfo** subcommand.

Table A-19. getsysinfo Subcommand

Command	Definition
getsysinfo	Displays DRAC/MC information and other system information.

Synopsis

```
racadm getsysinfo [-d] [-r] [-c] [-A] [-f]
```

Description

The **getsysinfo** subcommand displays DRAC/MC information and other system information.

Input

Table A-20 describes the **getsysinfo** subcommand options.

Table A-20. getsysinfo Subcommand Options and Descriptions

Option	Description
-d or **-r**	Displays controller information. (These options have equivalent meanings for compatibility purposes.)
-r	Displays controller information.
-c	Displays chassis information.
-A	Eliminates the printing of headers/labels.
-f	Displays firmware status flags.

NOTE: If you are running DRAC/MC firmware version 1.2 or later, the **getsysinfo** command displays the standby DRAC/MC version number.

If the **-d** or **-c** options are not specified, the other RAC information and chassis information are displayed.

Enumeration values or bitmaps are defined for these elements. When the **-A** application programming interface (API) option is included on the command, the enumeration or bit value of the element is listed in the output. Otherwise, the enumeration or bit value is mapped to a string before being output.

setsysinfo

NOTE: To use this subcommand, you must have **Configure DRAC/MC** permission.

Table A-21 describes the **setsysinfo** subcommand.

Table A-21. setsysinfo Subcommand

Command	Definition
setsysinfo	Sets the chassis name and location

Synopsis

```
racadm setsysinfo chassis_name=<value>
racadm setsysinfo chassis_location=<value>
```

Description

Use the **setsysinfo** subcommand to set chassis name and chassis location properties.

Input

Table A-22 describes the **setsysinfo** subcommand options.

Table A-22. setsysinfo Subcommand

Option	Description
<value>	Specifies the N-byte ASCII chassis name or location.

Output

You can view the chassis name and location in the **getsysinfo** subcommand chassis status field.

Restrictions

None

getractime

NOTE: To use this subcommand, you must have **Log In DRAC/MC** permission.

Table A-23 describes the **getractime** subcommand.

Table A-23. getractime Subcommand

Subcommand	Definition
getractime	Displays the time from the controller.

Synopsis

```
racadm getractime [-u]|[-d]
```

Description

The **getractime** subcommand displays the time in one of the following two formats:

- **-u** – The UTC hexidecimal value followed by the offset in signed decimal (default).
- **-d** – The *yyyymmddhhmmss.mmmmmms*off string with no option is displayed in the same format as the UNIX® date command.

Output

The **getractime** subcommand displays the output on one line.

setractime

NOTE: To use the **setractime** subcommand, you must have **Configure DRAC/MC** permission.

Table A-24 describes the **setractime** subcommand.

Table A-24. setractime Subcommand

Subcommand	Definition
setractime	Sets the time on the server module.

Synopsis

```
racadm setractime -u <utctime> [-o <offset>]
```

racadm setractime -d *yyyymmddhhmmss.mmmmmmsoff*

Description

The **setractime** subcommand sets the time on the DRAC/MC. The time can be specified using one of the options, as described in Table A-25.

Input

Table A-25 describes the **setractime** subcommand options.

Table A-25. setrac Subcommand Options and Descriptions

Option	Description
-u	The time is specified by the user in UTC (Universal Time Coordinated), which is the seconds since 1/1/1970 (0) and before 12/31/2003 (1924991999).
-o	The offset used with the -u option, which indicates the seconds offset from Greenwich Mean Time (GMT) (a signed value).
-d	The time specified as a string: *yyyymmddhhmmss.mmmmmmsoff* where: • *yyyy* is a four-digit integer • *mm* is the month • *dd* is the day • *hh* is the hour • *mm* is the minute • *ss* is the second • *mmmmmm* is the number of microseconds • *s* is a + (plus) sign or a - (minus) sign, which indicates the sign of the offset • *off* is the offset in minutes **NOTE:** The *off* is the offset in minutes from GMT and the offset must be in 15-minute increments.

Output

The **setractime** subcommand returns with no output if successful and the **getractime** subcommand displays the output on one line.

Example

The **setractime** subcommand supports dates ranging from 1/1/1970 00:00:00 to 12/31/2030 23:59:59. For example, Monday, May 25, 1998 at 1:30:15 PM EST would be represented as:

```
racadm setractime -d 19980525133015.000000-300
```

setniccfg/getniccfg

NOTE: To use the **setniccfg** subcommand, you must have **Configure DRAC/MC** permission.

NOTE: To use the **getniccfg** subcommand, you must have **Log In To DRAC/MC** permission.

Table A-26 describes the **setniccfg** and **getniccfg** subcommands.

Table A-26. setniccfg/getniccfg Subcommands

Subcommand	Definition
setniccfg	Sets the IP configuration for the controller.
getniccfg	Displays the current IP configuration for the controller.

NOTE: The terms NIC and Ethernet management port may be used interchangeably.

Synopsis

```
racadm setniccfg -d
racadm setniccfg -s [<ipAddress> <netmask> <gateway>]
racadm setniccfg -o
racadm getniccfg
```

Description for setniccfg

The **setniccfg** subcommand sets the controller IP address.

- The **-d** option enables DHCP for the Ethernet management port (default is DHCP disabled).
- The **-s** option enables static IP settings. The IP address, netmask, and gateway can be specified. Otherwise, the existing static settings are used.
- The **-o** option disables the Ethernet management port completely.

`<ipAddress>`, `<netmask>`, and `<gateway>` must be typed as dot-separated strings.

Description for getniccfg

The **getniccfg** subcommand displays the current Ethernet management port settings.

Output

The **setniccfg** subcommand returns without output if successful. The **getniccfg** subcommand output displays the following information:

```
Network adapter = Enabled/Disabled
DHCP = Enabled/Disabled
Static IP Settings: <ipAddress> <netmask> <gateway>
Current IP Settings: <ipAddress> <netmask> <gateway>
```

getsvctag

NOTE: To use this subcommand, you must have **Log In To DRAC/MC** permission.

Table A-27 describes the **getsvctag** subcommand.

Table A-27. getsvctag Subcommand

Subcommand	Definition
getsvctag	Displays the Service Tag.

Synopsis

```
racadm getsvctag [-m <module>]
```

Description

The **getsvctag** subcommand allows you to display one or more server module service tags. By default, the DRAC/MC displays the service tags for all of the server modules in the Dell™ Modular Server Enclosure.

Input

Table A-28 describes the getsvctag options.

Table A-28. getsvctag Subcommand Option

Option	Description
-m	Module for the service tag command. The legal values include the following: • chassis • switch-<*n*> where *n* equals the switch number up to a maximum of four switches. For example: `racadm getsvctag switch-1`

Example

Type `getsvctag` at the command prompt. An example of the output is displayed as follows:

```
Y76TP0G
```

The command returns `0` on success and nonzero on errors.

racdump

NOTE: To use this subcommand, you must have **Log In DRAC/MC** permission.

Table A-29 describes the **racdump** subcommand.

Table A-29. racdump Subcommand

Subcommand	Definition
racdump	Displays status and general DRAC/MC information.

Synopsis

```
racadm racdump
```

Description

The **racdump** subcommand provides a single command to get system, session, and sensor information from the DRAC/MC.

The following subcommands are executed as a result of the single **racdump** subcommand:

- **getsysinfo**
- **getssninfo**
- **getsensorinfo**

Output

The output of the individual commands are displayed.

racreset

NOTE: To use this subcommand, you must have **Configure DRAC/MC** permission.

Table A-30 describes the **racreset** subcommand.

Table A-30. racreset Subcommand

Subcommand	Definition
racreset	Resets the DRAC/MC.

NOTICE: Wait until the DRAC/MC reset is completed before issuing another command. If the DRAC/MC reset is not completed, you may receive the following message: `reset in progress`
The user interface is not accessible until the reset is complete.

Synopsis

```
racadm racreset [hard | soft | graceful] [delay in seconds]
```

Description

The **racreset** subcommand issues a reset to the DRAC/MC. The user is allowed to select how many seconds of delay occur before the reset sequence is started. The reset event is written into the DRAC/MC log.

NOTICE: For compatibility purposes, these three options (hard, soft, and graceful) have the same result on the DRAC/MC.

Input

Table A-31 describes the **racreset** subcommand options.

Table A-31. racreset Subcommand Options and Descriptions

Option	Description
hard **soft** **graceful**	A *hard, soft, or graceful* reset resets the entire DRAC/MC and is as close to a powerup reset as can be achieved using software. The DRAC/MC log, database, and selected daemons are shut down gracefully prior to the reset, and the PCI configuration is lost. Implementing these options should be considered as a final effort.
<*delay*>	The user is allowed to select how many seconds of delay occur before the reset sequence is started. A valid delay entry is between 1-60 seconds. The default is 3 seconds.

racresetcfg

NOTE: To use this subcommand, you must have **Configure DRAC/MC** permission.

Table A-32 describes the **racresetcfg** subcommand.

Table A-32. racresetcfg Subcommand

Subcommand	Definition
racresetcfg	Resets all database configuration parameters to default values, and then resets the DRAC/MC or KVM.
-m <*module*>	Indicates which module is to be reset to the default settings.

Synopsis

```
racadm racresetcfg [-m drac/kvm]
```

Description

The **racresetcfg** subcommand removes all database property entries that have been configured by the user. The database has default properties for all entries that are used to restore the card back to its original default settings. After resetting the database properties, the DRAC/MC or KVM resets automatically.

If `-m kvm` is specified, the Digital KVM will be reset to the default settings.

NOTICE: Before using this subcommand, ensure that you want to restore your database to its original default state with default user `root` and default password `calvin`.

NOTE: This option is available only in DRAC/MC version 1.2 or later. If the `-m` option is not provided, the default is `drac`.

NOTE: This command may take several minutes to complete. After the system resets to the default settings, the DRAC/MC or KVM reboots.

setassettag/getassettag

NOTE: To use the **setassettag** subcommand, you must have **Configure DRAC/MC** permission.

NOTE: To use the **getassettag** subcommand, you must have **Log In To DRAC/MC** permission.

Table A-33 describes the **setassettag** and **getassettag** subcommands.

Table A-33. setassettag/getassettag Subcommand

Subcommand	Definition
setassettag	Sets the specified asset tag.
getassettag	Displays asset tags.

Synopsis

```
racadm setassettag -m <module> <assetTag>
racadm getassettag [-m <module>]
```

Description for setassettag

Use the **setassettag** subcommand to set the asset tag for the specified module.

- The `<module>` option has the following legal values:
  `chassis`
- The `<assetTag>` option is the N-byte ASCII asset tag.

Description for getassettag

Use the **getassettag** subcommand to display the asset tag for a module or all modules with unique asset tags. The default is all modules (that have asset tags):

Example

Input: `getassettag`

Output: `chassis 78373839-33`

Both subcommands return 0 on success and nonzero on errors.

Restrictions

The **setassettag** subcommand does not work on the server module.

getled/setled

NOTE: To use the **getled** subcommand, you must have **Log In To DRAC/MC** permission.

NOTE: To use the **setled** subcommand, you must have **Configure DRAC/MC** permission.

Table A-34 describes the **setled** and **getled** subcommands.

Table A-34. setled/getled Subcommands and Definitions

Subcommand	Definition
getled	Displays the LED settings on a module.
setled	Sets the state of the LEDs on a module.

Synopsis

```
racadm getled -m <module> [-l <ledState>]
racadm setled -m <module> [-l <ledState>] <VALUE>
```

Description for getled

The **getled** subcommand displays the current state of the specified LED on a module, where module and LED state have the same meaning as they do for the **setled** subcommand. When a LED's state is ON, then the LED will blink; when the LED's state is OFF, the LED will stay lit.

Input

Table A-35 describes the **getled** subcommand option values.

Table A-35. getled Options

Option	Definition
-m <*module*>	The module has the following legal values: `server-<n>` where *n* = `1 to 10` (for example, `server-1`) `switch-<n>` where *n* = `1 to 4` (for example, `switch-1`)

-l <*ledState*>	The module has the following values:
	`1 = Locate LED state (default)`
	`2 = Fault LED state`

Examples

The following command will display the state of the Fault LED on Server 9:

```
racadm getled -m server-9 -l 2
```

The following command will display the state of the default LED (ON or OFF).

```
racadm getled -m server-1
```

Description for setled

The **setled** subcommand sets the state of the specified LED on a module. When the LED's state is ON, the LED blinks; when the LED's state is OFF, the LED will stay lit.

Input

Table A-36 describes the **setled** subcommand option values.

Table A-36. setled Options

Option	Definition
-m <*module*>	The module has the following legal values: `server-<n>` where *n* = `1 to 10` (for example, `server-1`) `switch-<n>` where *n* = `1 to 4`(for example, `switch-1`)

-l <*ledState*>	The module has the following legal values:
	`1 = locate LED state (default)`
	`2 = fault LED state`
	When the -l option is omitted, the setled command sets the default LED.

<*value*>	`ON or OFF`

Example

The following command string sets the Locate LED on Server 1 to ON.

```
racadm setled -m server-1 -l 1 ON
```

The following command string sets the default LED (Locate LED) on Server 2 to OFF

```
racadm setled -m server-2 OFF
```

getmodinfo

NOTE: To use this subcommand, you must have **Log In To DRAC/MC** permission.

Table A-37 describes the **getmodinfo** subcommand.

Table A-37. getmodinfo Subcommand

Subcommand	Definition
getmodinfo	Displays module configuration and status information.

Synopsis

```
getmodinfo [-m <module>] [-A] [-G <generation>]
```

Description

The **getmodinfo** subcommand displays the following information about the major modules in the chassis:

- Module name
- Presence status
- Power status
- System health
- Module Service Tag

Input

Table A-38 describes the **getmodinfo** subcommand option values.

Table A-38. getmodinfo Options

String	Definition
-m <*module*>	The chassis has the following legal values: • `server-<n> (where n = 1 to 10)` (for example, `server-1)` • `switch-<n> (where n = 1 to 4)` (for example, `switch-1)` • `DRAC/MC-<n> (where n = 1 or 2)` (for example, `DRAC/MC-1)` • `fan-<n> (where n = 1 or 2)` (for example, `fan-1)` • `ps-<n> (where n = 1 to 4)` (for example, `ps-2)` The default is to display information about all the major modules in the chassis.
-A	Suppresses the header and the outputs <`presence`>, <`pwrState`>, and <`health`> as a numeric enumerated.
-G <*generation*>	Returns a value of 1 if <`generation`> matches the current generation of the module resources table (indicating that there were no changes since the last call). If the generation is new and the **-G** option was used, the following line is displayed before the rest of the module information: `Generation: <n>` where <`n`> is the generation number. A <`generation`> value of 0 always causes a mismatch, and as a result, new output.

Output

The **getmodinfo** subcommand prints a line of output for each module specified.

getsensorinfo

NOTE: To use this subcommand, you must have **Log In To DRAC/MC** permission.

Table A-39 describes the **getsensorinfo** subcommand.

Table A-39. getsensorinfo Subcommand

Subcommand	Definition
getsensorinfo	Dumps the current reading and enable status for the specified sensors.

Synopsis

```
racadm getsensorinfo [-s <sensorNum>] [-G <generation>]
```

Description

The **getsensorinfo** subcommand dumps the current reading and enable status for the specified sensors. The list of sensors output is platform-dependent and corresponds to the sensor readings generated by the **getsensorinfo** subcommand.

Input

Table A-40 describes the **getsensorinfo** subcommand option values.

Table A-40. getsensorinfo Options

String	Definition
-s	Allows a specific sensor to be specified by the Intelligent Platform Management Interface (IPMI) sensor number.
-G <*generation*>	Returns a value of 1 if `<generation>` matches the current generation of the module resources table (indicating that there were no changes since the last call). If the generation is new and the **-G** option was used, the following line is displayed before the rest of the module information: `Generation: <n>` where `<n>` is the generation number. A `<generation>` value of 0 always causes a mismatch, and as a result, new output.

Output

The **getsensorinfo** output values correspond with the IPMI definitions. One line of output is generated for each sensor.

serveraction

NOTE: To use this subcommand, you must have **Executive Server Control Commands** permission.

Table A-41 describes the **serveraction** subcommand.

Table A-41. serveraction Subcommand

Subcommand	Definition
serveraction	Executes a system reset or powerup/down/cycle.

Synopsis

```
racadm serveraction [-s <system-n>] [-d <delay>] [-w <cycleWait>] <action>
```

Description

The **serveraction** subcommand provides an interface to control system reset and power control.

- `<action>` is the string that specifies the action
- `<system-n>` is the system number that corresponds to the module number; for example: `server-1` = `system-1`
- `<system-n>` `= ALL` applies the specified action to all server modules

Input

Table A-42 describes the **serveraction** subcommand option values.

Table A-42. serveraction Subcommand Options

String	Definition
<*action*>	Specifies the action. The options for the <*action*> string are: • **powerdown** – Powers down the server. • **powerup** – Powers up the server. • **powercycle** – Issues a power cycle to the server. **NOTE:** The `-w <cycleWait>` option can be used with **powercycle.** • **hardreset** – Issues a hard reset to the server. • **graceshutdown** – Powers down the server module gracefully.
-d <*delay*>	Specifies the time in seconds after the command is received before the action is executed. The default is 1 second and the maximum is 1800 seconds.
-w <*cycleWait*>	Used only when <*action*> is **powercycle**. Specifies the time in seconds at which a **powerup** action is performed after a **powerdown** is initiated. The default setting is 15 seconds. The maximum setting is 1800 seconds (30 minutes).

Output

If successful, the **serveraction** subcommand returns no output.

chassisaction

NOTE: To use this subcommand, you must have **Execute Server Control Commands** permission.

Table A-43 describes the **chassisaction** subcommand.

Table A-43. chassisaction Subcommand

Subcommand	Definition
chassisaction	Sets chassis or switch to powerup/down/cycle.

Synopsis

```
racadm chassisaction [-m <module>] [-d <delay>] [-w <cycleWait>] <action>
```

Description

The **chassisaction** subcommand provides an interface to manage module reset and power.

NOTE: The **chassisaction** subcommand is supported only on Digital Access KVMs.

Table A-44 describes the **chassisaction** subcommand option values.

Table A-44. chassisaction Subcommand Options

Option	Definition
-m	The `-m <module>` for the chassisaction has the following legal values: • `chassis` • `<switch-n>` where `n` = 1 to 4 (for example, `switch-1`) • `kvm`
<action>	Specifies the action. The options for the *<action>* string are: • **powerdown** – Powers down the module. • **powerup** – Powers up the module. **NOTE:** The **powerdown** and **powerup** options are valid only for the chassis; these options are not available for I/O modules or KVM. • **powercycle** – Power cycles the module. **NOTE:** The `-w <cycleWait>` option can be used with **powercycle**. • **graceshutdown** – Graceful shutdown of the module.
-d *<delay>*	Specifies the time in seconds after the command is received before the action is executed. The default is 1 second and the maximum is 1800 seconds.
-w *<cycle wait>*	Used only when *<action>* is **powercycle**. Specifies the time in seconds at which a **powerup** action is performed after a **powerdown** is initiated. The default setting is 15 seconds. The maximum setting is 1800 seconds (30 minutes).

Output

If successful, the **chassisaction** subcommand returns no output.

getraclog

NOTE: To use this subcommand, you must have **Log In DRAC/MC** permission.

Table A-45 describes the **getraclog** subcommand.

Table A-45. getraclog Commands

Command	Definition
getraclog -i	Displays the number of entries in the DRAC/MC log.
getraclog	Displays the DRAC/MC log entries.

Synopsis

```
racadm getraclog -i
```

```
racadm getraclog [-A] [-c count] [-d delay-seconds]\[-s start-record]
[-v] [-V] [-m]
```

Description

NOTE: The command name and the **racadm** subcommand names may be different, which is normal.

The **getraclog -i** subcommand displays the number of entries in the DRAC/MC log.

The options in Table A-46 allow the **getraclog** subcommand to read entries.

Table A-46. getraclog Options

Option	Definition
-A	Provides API-formatted output (no header).
-c	Provides the maximum count of entries to be returned.
<*blank*>	Displays the entire log; racadm and serial only (default).
-d	Provides the number of seconds to delay the display of log entries.
-s	Provides the associated number of the first displayed entry (default = 0 [list begins with the first DRAC/MC log entry]).
-v	Provides *verbose* output. **NOTE:** This option is not available with DRAC/MC version 1.3 and later.
-V	Provides *very verbose* output. **NOTE:** This option is not available with DRAC/MC version 1.3 and later.
-m	Displays 24 rows at a time, and queries for more (similar to the UNIX **more** command).

Output

One line of output is displayed for each DRAC/MC log entry.

Restrictions

The output buffer size is too big for execution across IPMI transport.

clrraclog

NOTE: To use this subcommand, you must have **Clear Logs** permission. See Table A-1 for more information.

Synopsis

```
racadm clrraclog
```

Description

The **clrraclog** subcommand completely clears the DRAC/MC log. A single entry is made to indicate the user and time that the log was cleared.

getsel

NOTE: To use this subcommand, you must have **Log In To DRAC/MC** permission.

Table A-47 describes the **getsel** subcommand.

Table A-47. getsel Subcommands

Command	Definition
getsel -i	Displays the number of entries in the System Event Log.
getsel	Displays SEL entries.

Synopsis

```
racadm getsel -i
```

```
racadm getsel [-A] [-E] [-R] [-c count] [-d delay-seconds]\[-s count]
[-v] [-V] [-m]
```

Description

The **getsel -i** subcommand displays the number of entries in the SEL.

The **getsel** options in Table A-48 (without the **-i** option) are used to read entries.

Table A-48. getsel Options

Option	Definition
<*blank*>	Default is to display the entire log **racadm** and **serial** commands only (default).
-A	Provides API-formatted output (no header).
-E	Places the system event log (SEL) output in hexidecimal at the end of each output line.
-R	Prints only the raw data.
-c	Provides the maximum count of entries to be returned.
-d	Provides the number of seconds to delay the recording of any new log entries.
-m	Displays 24 rows at a time, and queries for more (similar to the UNIX **more** command)
-s	Provides the number of records to skip before returning entries (default=0).
-v	Provides *verbose* output.
-V	Provides *very verbose* output.

Output

One line of output is displayed for each SEL entry.

getkvminfo

NOTE: To use the **getkvminfo** subcommand, you must have **Log In To DRAC/MC** permission.

Table A-49 describes the **getkvminfo** subcommand.

Table A-49. getkvminfo Subcommand

Subcommand	Definition
getkvminfo	Retrieves the KVM status information.

Synopsis

```
racadm getkvminfo
```

Description

The **getkvminfo** subcommand displays the following information about the KVM module in a chassis:

- module
- presence
- model
- firmware version
- status

Output

Below is an output example using the **getkvminfo** subcommand.

Table A-50. getkvminfo Output Example

```
<module>      <presence>     <model>           <FW Version>     <status>
KVM           present        Avocent Analog    1.0              Ready
```

getdcinfo

NOTE: To use the **getdcinfo** subcommand, you must have **Log In To DRAC/MC** permission.

Table A-51 describes the **getdcinfo** subcommand.

Table A-51. getdcinfo Subcommand

Subcommand	Definition
getdcinfo	Retrieves the daughter card and I/O module misconfiguration information.

Synopsis

```
racadm getdcinfo
```

Description

The **getdcinfo** subcommand displays the following information about the daughter card that is installed in a chassis:

- Group candidate I/O type
- I/O module name
- I/O module power control
- Daughter card type
- Server module power control

Table A-52 lists the legal value definitions for each candidate I/O type.

Table A-52. Legal Value Definitions

Legal Value	Definition
FC	Fibre Channel
FC-PT	Fibre Channel pass-through module
GbE	Gigabit Ethernet
GbE-SW	Gigabit Ethernet switch
GbE-PHY	Gigabit Ethernet pass-through module
IB	Infiniband

Table A-53 lists the valid candidate I/O type legal values.

Table A-53. Valid Candidate I/O Type Legal Values

Candidate	Legal Values
Group 1 Candidate I/O Type	• GbE-PHY • GbE-SW • Unknown
Group 2 Candidate I/O Type	• FC • FC-PT • FC-SW • GbE • GbE-PHY • GbE-SW • IB • Unknown
I/O module ***<name>***	• FC • GbE • IB • Fail • N/A • OK • Unknown
Server module ***<state>***	• Fail • N/A • OK

Output

The **getdcinfo** command returns no output (if successful) and prints the following output for each specified I/O module and server module:

Table A-54. getdcinfo Output

#	<IO>	<Name>	<State>
1		Gbe Pass-Through	OK
2		GbE Switch	FAIL
3		FC Pass-Through	OK
4		FC Pass-Through	OK

Table A-55. getdcinfo Output

#	<Server>	<Daughter Card>	<State>
1	N/A	N/A	
2	N/A	N/A	
3	N/A	N/A	
4	N/A	N/A	
5	None	OK	
6	N/A	N/A	
7	N/A	N/A	
8	Unknown	FAIL	
9	N/A	N/A	
10	Unknown	FAIL	

clrsel

NOTE: To use this subcommand, you must have **Clear Logs** permission.

Synopsis

```
racadm clrsel
```

Description

The **clrsel** subcommand completely clears the SEL. A single entry is made to indicate the time that the log was cleared.

sslcertview

NOTE: To use this subcommand, you must have **Configure DRAC/MC** permission.

Table A-56 describes the **sslcertview** subcommand.

Table A-56. sslcertview Subcommand

Subcommand	Description
sslcertview	Displays a CA certificate or server certificate that is located in the DRAC/MC.

Synopsis

```
racadm sslcertview -t <type> [-A]
```

Input

Table A-57 describes the **sslcertview** subcommand options.

Table A-57. sslcertview Subcommand Options

Option	Description
-t <*type*>	Specifies the type of certificate to upload, either the CA certificate or server certificate. 1 = server certificate 2 = CA certificate
-A	Prevents printing headers/labels.

Output Examples

For the **racadm sslcertview -t 1** subcommand, you receive output similar to the following example, where **C** is the country, **CN** is the common name, **O** is the organization, **OU** is the organizational unit, **L** is the locality, **S** is the state, and **E** is the e-mail address:

```
certificate type=1
serial number=00
key size=1024
valid from=DSU+12:34:31
valid to=DSU+15:34:31
subject.C=US
subject.CN=RMC Default Certificate
subject.O=Dell Inc.
subject.OU=BVS
subject.L=Round Rock
subject.S=Texas
subject.E=john@dell.com
```

```
issuer.C=US
issuer.CN=RMC Default Certificate
issuer.O=Dell Inc.
issuer.OU=BVS
issuer.L=Round Rock
issuer.S=Texas
issuer.E=john@dell.com
```

For the **racadm sslcertview -t 1 -A** subcommand, you receive output similar to the following example:

```
1
00
1024
DSU+12:34:31
DSU+15:34:31
US
RMC Default Certificate
Dell Inc.
BVS
Round Rock
Texas
john@dell.com
US
RMC Default Certificate
Dell Inc.
BVS
Round Rock
Texas
john@dell.com
```

testemail

NOTE: To use this subcommand, you must have **Test Alerts** permission.

Table A-58 describes the **testemail** subcommand.

Table A-58. testemail Subcommand

Subcommand	Description
testemail	Tests an e-mail alert.

Synopsis

```
racadm testemail -i <index> | -u <username>
```

Description

The testemail subcommand forces the DRAC/MC to send an e-mail over the DRAC/MC network adapter.

Input

Table A-59 describes the **testemail** subcommand options.

Table A-59. testemail Subcommand Options

Option	Description
-u <*username*>	Specifies the user who receives the e-mail. The necessary properties must be set up to correctly send e-mail messages.
-i <*index*>	Specifies the index of the user.

Output

None.

testtrap

NOTE: To use this subcommand, you must have **Test Alerts** permission.

Table A-60 describes the **testtrap** subcommand.

Table A-60. testtrap Subcommand

Subcommand	Description
testtrap	Tests an SNMP trap.

Synopsis

```
racadm testtrap -i <index>
```

Description

The **testtrap** subcommand forces the DRAC/MC to send an SNMP trap over the DRAC/MC NIC.

Input

Table A-61 describes the **testtrap** subcommand options.

Table A-61. testtrap Subcommand Options

Option	Description
-i <*index*>	Specifies the index of the trap.

vmdetach

NOTE: To use the **vmdetach** subcommand, you must have **Administrator** permission.

Table A-62 describes the **vmdetach** subcommand.

Table A-62. vmdetach Subcommand

Subcommand	Definition
vmdetach	Detaches an active virtual media session

Synopsis

```
racadm vmdetach
```

Description

The **vmdetach** command detaches an active virtual media session. This command returns an error if no virtual media session is active.

B

DRAC/MC Property Database Group and Object Definitions

The DRAC/MC property database contains the configuration information for the DRAC/MC. Data is organized by associated object, and objects are organized by object group. The IDs for the groups and objects that the property database supports are listed in this section.

Use the group and object IDs with the RACADM utility to configure the DRAC/MC. The following sections describe each object and indicate whether the object is readable, writable, or both.

idRacInfo

This group contains display parameters to provide information about the specifics of the DRAC/MC being queried.

One instance of the group is allowed. The following subsections describe the objects in this group.

idRacType (Read Only)

Legal Values

Always report 0x7.

Default

0x7

Description

Identifies the remote access controller type as the DRAC/MC.

idRacProductInfo (Read Only)

Legal Values

String of up to 63 ASCII characters.

Default

Remote Access Controller/Modular Chassis.

Description

Uses a text string to identify the product.

idRacDescriptionInfo (Read Only)

Legal Values

String of up to 255 ASCII characters.

Default

This system component provides a complete set of remote management functions for a server.

Description

A text description of the DRAC type.

idRacVersionInfo (Read Only)

Legal Values

String of up to 63 ASCII characters.

Default

DRAC Firmware Version *x.x* Build (mm.dd)

Description

A string containing the current firmware version of the product, where *x* is the current revision.

idRacName (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC/MC** permission.

Legal Values

String of up to 15 ASCII characters.

Default

DRAC

Description

A user assigned name to identify this controller.

idRacMisc (Read/Write)

Legal Values

String of up to 64 ASCII characters.

Default

Null string

Description

Generic property undefined at this release.

cfgActiveDirectory

This group contains parameters to configure the DRAC/MC Active Directory feature.

cfgADEnable (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC/MC** permission.

Legal Values

Boolean, either 1 or 0 (True or False).

Default

0

Description

0 = disable

1 = enable

This object sets the Active Directory authentication to enable (1) or disable (0).

cfgRacDomain (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC/MC** permission.

Legal Values

A string of up to 255 characters.

Default

""

Description

The DRAC/MC domain name is the fully qualified domain name of the subdomain where the RAC device object is located. Do not use the NetBIOS name.

cfgRootDomain (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC/MC** permission.

Legal Values

A string of up to 255 ASCII characters.

Default

""

Description

Root domain of the domain forest.

cfgRacName

NOTE: To modify this property, you must have **Configure DRAC/MC** permission.

Legal Values

A string up of up to 255 ASCII characters.

Default

""

Description

The name must be identical to the RAC object common name you created in your domain controller.

cfgLanNetworking

This group contains parameters to configure the DRAC/MC NIC.

One instance of the group is allowed. All objects in this group will require the DRAC/MC NIC to be reset, which may cause a brief loss in connectivity. Objects that change the DRAC/MC NIC IP address settings will close all active user sessions and require users to reconnect using the updated IP address settings.

cfgNicEnable (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC/MC** permission.

Legal Values

Boolean, either 1 or 0 (TRUE or FALSE).

Default

1

Description

0=Disable.

1=Enable the DRAC/MC NIC.

cfgNicIpAddress (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC/MC** permission.

Legal Values

A string of "." separated numeric fields containing the static IP address.

Default

192.168.0.120

Description

The IP address of the DRAC/MC NIC.

cfgNicNetmask (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC/MC** permission.

Legal Values

A string of "." separated numeric fields containing the static network mask.

Default

255.255.255.0

Description

The network mask used by the DRAC/MC NIC.

cfgNicGateway (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC/MC** permission.

Legal Values

A string of "." separated numeric fields containing the static gateway.

Default

192.168.0.1

NOTE: The previous default IP address was 192.168.0.120.

Description

The gateway used by the DRAC/MC NIC.

cfgNicUseDhcp (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC/MC** permission.

Legal Values

Boolean, either 1 or 0 (TRUE or FALSE).

Default

0

Description

0=Use the static DRAC/MC NIC parameters described above.

1=Use DHCP and obtain the necessary parameters from the DHCP server for the DRAC/MC NIC.

cfgDNSDomainNameFromDHCP (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC/MC** permission.

Legal Values

Boolean, either 1 or 0 (TRUE or FALSE).

Default

0

Description

0 = Use the static DRAC/MC network adapter parameters described above.

1 = Use DHCP and obtain the domain name parameter from the DHCP server for the DRAC/MC network adapter.

cfgDNSDomainName (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC/MC** permission.

Legal Values

String of up to 254 ASCII characters. At least one character must be a letter.

Default

MYDOMAIN

Description

A string containing the DNS domain name.

cfgDNSRacName (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC/MC** permission.

Legal Values

A string of up to 63 ASCII characters. At least one character must be a letter.

Default

NULL

Description

A string containing the DNS RAC name.

cfgDNSRegisterRac (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC/MC** permission.

Legal Values

Boolean, either 1 or 0 (TRUE or FALSE).

Default

0

Description

0 = Use the static DRAC/MC network adapter parameters described above.

1 = Registers the DRAC/MC name on the DNS server.

cfgDNSServersFromDHCP (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC/MC** permission.

Legal Values

Boolean, either 1 or 0 (TRUE or FALSE).

Default

0

Description

Retrieves DNS server addresses from the DHCP server.

cfgDNSServer1 (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC/MC** permission.

Legal Values

Any legal IP address, including 0.0.0.0.

Default

192.168.0.5

Description

The static IP address for DNS server 1.

cfgDNSServer2 (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC/MC** permission.

Legal Values

Any legal IP address, including 0.0.0.0.

Default

192.168.0.6

Description

The static IP address for DNS server 2.

cfgCurrentLanNetworking

This group contains parameters that are currently in use by the DRAC/MC NIC.

One instance of the group is allowed. The following subsections describe the objects in this group.

cfgNicCurrentIpAddress (Read Only)

Legal Values

A string of "." separated numeric fields containing the IP address

Default

192.168.0.120

Description

The current IP address of the Avocent Digital Access KVM NIC.

cfgNicCurrentNetmask (Read Only)

Legal Values

A string of "." separated numeric fields containing the network mask.

Default

255.255.255.0

Description

The current network mask used by the Avocent Digital Access KVM NIC.

cfgNicCurrentGateway (Read Only)

Legal Values

A string of "." separated numeric fields containing the gateway address.

Default

192.168.0.1

Description

The current gateway used by the Avocent Digital Access KVM NIC.

cfgNicCurrentDhcpWasUsed (Read Only)

Legal Values

Boolean, either 1 or 0 (TRUE or FALSE).

Default

0

Description

Indicates whether or not DHCP was used to configure the NIC.

0 = IP address is static

1 = IP address was obtained from a DHCP server.

cfgDNSCurrentServer1 (Read Only)

Legal Values

A string of "." separated numeric fields containing the IP address.

Default

192.168.0.5

Description

The current primary DNS server IP address.

cfgDNSCurrentServer2 (Read Only)

Legal Values

A string of "." separated numeric fields containing the IP address.

Default

192.168.0.6

Description

The current secondary DNS server IP address.

cfgDNSCurrentDomainName (Read Only)

Legal Values

A string of "." separated numeric fields containing the IP address.

Default

MYDOMAIN

Description

The current DNS domain name.

cfgNetTuning

This group contains parameters for tuning the DRAC/MC NIC.

One instance of the group is allowed. The following subsections describe the objects in this group.

cfgNetTuningNicAutoneg (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC/MC** permission.

Legal Values

Boolean, either 1 or 0 (TRUE or FALSE).

Default

1

Description

0 = Disable.

1 = Enable.

If enable, autonegotiation takes priority over values set in the **cfgNetTuningNic100MB** and **cfgNetTuningNicFullDuplex** objects.

cfgNetTuningNic100MB (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC/MC** permission.

Legal Values

Boolean, either 1 or 0 (TRUE or FALSE).

Default

1

Description

0 = Disable.

1 = Enable the object link speed to 100 Mb (1) or 10 Mb (0).

cfgNetTuningNicFullDuplex (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC/MC** permission.

Legal Values

Boolean, either 1 or 0 (TRUE or FALSE).

Default

1

Description

0 = Disable

1 = Enable the object and set the duplex to full duplex (1) or half duplex (0).

cfgKvmLanNetworking

This group contains parameters to configure the Avocent Digital Access KVM NIC.

One instance of the group is allowed. All objects in this group will require the Avocent Digital Access KVM NIC to be reset, which may cause a brief loss in connectivity. Objects that change the Avocent Digital Access KVM NIC IP address settings will close all active user sessions and require users to reconnect using the updated IP address settings.

cfgKvmNicIpAddress (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC/MC** permission.

Legal Values

A string of "." separated numeric fields containing the static IP address.

Default

192.168.0.121

Description

The IP address of the Avocent Digital Access KVM NIC.

cfgKvmNicNetmask (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC/MC** permission.

Legal Values

A string of "." separated numeric fields containing the static network mask.

Default

255.255.255.0

Description

The network mask used by the Avocent Digital Access KVM NIC.

cfgKvmNicGateway (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC/MC** permission.

Legal Values

A string of "." separated numeric fields containing the static gateway.

Default

192.168.0.1

Description

The gateway used by the Avocent Digital Access KVM NIC.

cfgKvmNicUseDhcp (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC/MC** permission.

Legal Values

Boolean, either 1 or 0 (TRUE or FALSE).

Default

1

Description

0=Use the static Avocent Digital Access KVM NIC parameters described above.

1=Use DHCP and obtain the necessary parameters from the DHCP server for the Avocent Digital Access KVM NIC.

cfgKvmNicMacAddress (Read Only)

Legal Values

MAC address.

Default

The unique MAC address value that is assigned to the KVM.

Description

The Avocent Digital Access KVM MAC address.

cfgKvmCurrentLanNetworking

This group contains parameters that are currently in use by the Avocent Digital Access KVM NIC. One instance of the group is allowed. The following subsections describe the objects in this group.

cfgKvmNicCurrentIpAddress (Read Only)

Legal Values

A string of "." separated numeric fields containing the IP address.

Default

192.168.0.121

Description

The current IP address of the Avocent Digital Access KVM NIC.

cfgKvmNicCurrentNetmask (Read Only)

Legal Values

A string of "." separated numeric fields containing the network mask.

Default

255.255.255.0

Description

The current network mask used by the Avocent Digital Access KVM NIC.

cfgKvmNicCurrentGateway (Read Only)

Legal Values

A string of "." separated numeric fields containing the gateway address.

Default

192.168.0.1

Description

The current gateway used by the Avocent Digital Access KVM NIC.

cfgKvmNicCurrentDhcpWasUsed (Read Only)

Legal Values

Boolean, either 1 or 0 (TRUE or FALSE).

Default

0

Description

Indicates whether or not DHCP was used to configure the NIC.

0 = IP address is static

1 = IP address was obtained from a DHCP server.

cfgKvmNetTuning

The group contains parameters to tune the Avocent Digital Access KVM network configuration.

One instance of the group is allowed. All objects in this group require a Avocent Digital Access KVM reset before they become active. The following subsections describe the objects in this group.

cfgKvmNetTuningNicAutoneg (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC/MC** permission.

Legal Values

Boolean, either 1 or 0 (TRUE or FALSE).

Default

1

Description

0 = Disable

1 = Enable

If enabled, autonegotiation takes priority over values set in the **cfgNetTuningNic100MB** and **cfgNetTuningNicFullDuplex** objects.

cfgKvmNetTuningNic100MB (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC/MC** permission.

Legal Values

Boolean, either 1 or 0 (TRUE or FALSE).

Default

1

Description

0 = Disable

1 = Enable

The DRAC/MC link speed is set to 100 Mbit (**1**) or 10 Mbit (**0**).

cfgKvmNetTuningNicFullDuplex (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC/MC** permission.

Legal Values

Boolean, either 1 or 0 (TRUE or FALSE).

Default

1

Description

This object sets the duplex to full duplex(**1**) or half duplex (**0**).

cfgKvmNetTuningEnableDebug (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC/MC** permission.

NOTE: This option is for Dell internal use only. When this object is set to 1, a Dell Support technician can diagnose the Avocent Digital Access KVM interface by opening a telnet session to the KVM.

Legal Values

Boolean, either 1 or 0 (TRUE or FALSE).

Default

1

Description

0 = Disable

1 = Enable

The DRAC/MC sets the Avocent Digital Access KVM debug console to enable or disable.

cfgRacConsoleRedirection

This group contains parameters for configuring console redirection.

One instance of the group is allowed. The following subsections describe the objects in this group

cfgConsoleRedirectionEnable (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC/MC** permission.

Legal Values

Boolean, either 1 or 0 (TRUE or FALSE).

Default

1

Description

0 = Disable

1 = Enable

Enables or disables RAC console redirection.

cfgMaxSessions (Read Only)

Legal Values

1

Default

1

Description

Lists the maximum number of supported console redirection sessions for the Avocent Digital Access KVM.

cfgCurrentSessions (Read Only)

Legal Values

0 or 1

Default

0

Description

Lists the current number of active console redirection sessions.

cfgRemoteHosts

The group contains parameters to configure various firmware update loading, IP addresses, enables, and so on.

One instance of the group is allowed. The following subsections describe the objects in this group.

cfgRhostsSmtpEmailEnable (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC/MC** permission.

Legal Values

Boolean, either 1 or 0 (TRUE or FALSE).

Default

1

Description

0=disable, 1=enable the SMTP protocol to send e-mail alerts.

cfgRhostsSmtpServerIpAddr (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC/MC** permission.

Legal Values

A string of "." separated numeric fields containing the IP address.

Default

127.0.0.1

Description

The IP address of the server used in e-mail alerts.

cfgRhostsFwUpdateTftpEnable (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC/MC** permission.

Legal Values

Boolean either 1 or 0 (TRUE or FALSE).

Default

1

Description

0=Disable, 1=Enable loading the firmware update file through TFTP.

cfgRhostsFwUpdateIpAddr (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC/MC** permission.

Legal Values

A string of "." separated numeric fields containing the IP address.

Default

192.168.0.4

Description

The address of the TFTP server where the firmware update image is located.

cfgRhostsFwUpdatePath (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC/MC** permission.

Legal Values

String of up to 255 ASCII characters that designate a valid path name.

Default

""

Description

The path name pointing to the firmware update binary file. If this is a filename only, then the path needs to be specified in the TFTP server. Otherwise, the entire path can be specified here.

NOTE: The server may still require you to specify the drive (for example, **C**).

cfgUserAdmin

This group contains parameters that you can use to configure which users are allowed access to the DRAC/MC.

Sixteen instances of the group are allowed, which corresponds to a user for each index. The following subsections describe the objects in this group.

cfgUserAdminPrivilege (Read/Write)

NOTE: To modify this property, you must have **Configure Users** permission.

Legal Values

0x80000000 to 0x800001ff, and 0x0

Default

0

Description

Use the bit mask numbers in Table B-1 to set role-based authority privileges for a DRAC/MC user.

Table B-1. Bit Masks for User Privileges

User Privilege	Bit Mask
Log Into DRAC/MC	0x80000001
Configure DRAC/MC	0x80000002
Configure Users	0x80000004
Clear Logs	0x80000008
Execute Server Control Commands	0x80000010
Access Console Redirection	0x80000020
Access Virtual Media	0x80000040
Test Alerts	0x80000080
Execute Debug Commands	0x80000100

cfgUserAdminUserName (Read/Write)

NOTE: To modify this property, you must have **Configure Users** permission.

Legal Values

A string of up to 19 ASCII characters.

Default

None

Description

The name of the user for this index. The user index is created by writing a string into this name field if the index is empty. Writing a string of double quotes ("") deletes the user at that index. You cannot change the name. You must delete and then recreate the name. The string must not contain "/" (forward slash, "\" (backslash), "." (period), "@" (at symbol) or quotations marks.

NOTE: This command is the anchor for this indexed group.

cfgUserAdminPassword (Write Only)

NOTE: To modify this property, you must have **Configure Users** permission.

Legal Values

A string of up to 20 ASCII characters.

Default

None

Description

The password for this user. The user passwords are encrypted and cannot be seen or displayed after this property is written.

cfgUserAdminAlertFilterSysEventMask (Read/Write)

NOTE: To modify this property, you must have **Configure Users** permission.

Legal Values

See "System-Generated Alert Mask Definitions."

Default

0x777777

Description

See "System-Generated Alert Mask Definitions." (Type hexadecimal values.)

cfgUserAdminEmailEnable (Read/Write)

NOTE: To modify this property, you must have **Configure Users** permission.

Legal Values

Boolean either 1 or 0 (TRUE or FALSE).

Default

0

Description

0=Disable, 1=Enable e-mail alerting on a per user basis.

cfgUserAdminEmailAddress (Read/Write)

NOTE: To modify this property, you must have **Configure Users** permission.

Legal Values

A string of up to 63 ASCII characters.

Default

""

Description

Standard e-mail address, such as john_doe@mycompany.com.

cfgUserAdminEmailCustomMsg (Read/Write)

NOTE: To modify this property, you must have **Configure Users** permission.

Legal Values

A string of up to 31 ASCII characters.

Default

""

Description

User-defined message to be sent on a e-mail alert.

cfgTraps

This group contains parameters to configure the delivery of SNMP traps.

Sixteen instances of this group are allowed, which represent sixteen unique trap destinations. The following subsections describe the objects in this group.

cfgTrapsDestIpAddr (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC/MC** permission.

Legal Values

A string of "." separated numeric fields containing the IP.

Default

0.0.0.0

Description

IP address of an SNMP trap daemon.

NOTE: This object is the "anchor" for this indexed group.

cfgTrapsEnable (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC/MC** permission.

Legal Values

Boolean, either 1 or 0 (TRUE or FALSE).

Default

0

Description

0=Disabled, 1=Enabled for this indexed entry.

cfgTrapsSnmpCommunity (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC/MC** permission.

Legal Values

A string of up to 31 ASCII characters.

Default

""

Description

An SNMP community name.

cfgTrapsFilterSysEventMask (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC/MC** permission.

Legal Values

See "System-Generated Alert Mask Definitions."

Default

0x77777

Description

See "System-Generated Alert Mask Definitions." (Type hexadecimal values.)

cfgSessionManagement

This group contains parameters to configure the number of sessions that can connect to the DRAC/MC.

One instance of the group is allowed. All objects in this group require a DRAC/MC reset before they become active. The following subsections describe the objects in this group.

cfgSsnMgtMaxSessions (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC/MC** permission.

Legal Values

0x1 through 0x4

Default

0x4

Description

The maximum number of simultaneous sessions that are allowed at one time from the DRAC/MC Web-based remote access interface. (Type hexadecimal values.)

cfgSsnMgtMaxSessionsPerUser (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC/MC** permission.

Legal Values

0x1 through 0x4

Default

0x4

Description

The maximum number of simultaneous sessions allowed per user. (Type hexadecimal values.)

cfgSerial

This group contains configuration parameters for the system external serial port.

One instance of the group is allowed. The following subsections describe the objects in this group.

cfgSerialBaudRate

NOTE: To modify this property, you must have **Configure DRAC/MC** permission.

NOTE: For best results redirecting BIOS System Setup screens, Dell recommends using 115200.

Legal Values

9600, 28800, 57600, 115200

Default

115200

Description

Sets the baud rate on the external serial port. (Type decimal values).

cfgSerialConsoleEnable

NOTE: To modify this property, you must have **Configure DRAC/MC** permission.

Legal Values

Boolean, either 1 or 0 (TRUE or FALSE).

Default

1

Description

0=Disabled, 1=Enabled. Enables the serial port and terminal interface.

cfgSerialConsoleQuitKey (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC/MC** permission.

Legal Values

A string of 3 or fewer characters.

Default

The <CR><~><.> key combination

The <CR> key represents a carriage return; press <Enter> as a substitute for <CR>.

Description

This key sequence terminates text console redirection when using VT-100.

cfgSerialConsoleIdleTimeout (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC/MC** permission.

Legal Values

Integer from 1 to any positive number. Type hexadecimal values.

Default

0x12c

Description

The maximum number of times (in seconds) of line idle time before the line is disconnected. (Type hexadecimal values.)

cfgSerialConsoleShellType (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC/MC** permission.

Legal Values

1 = VT100 block screen interface, has limited command function compared to type 2.

2 = UNIX®-style command line data stream interface.

Default

2

NOTE: Only option 2 is supported in the DRAC/MC.

Description

Sets the serial console shell type. (Type hexadecimal values.)

cfgSerialConsoleNoAuth (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC/MC** permission.

Legal Values

0 – Login prompt is **Enabled** on the serial shell.

1 – Login prompt is **Disabled** on serial shell.

Default

0

Description

Allows you to disable authentication on the serial shell.

cfgSerialConsoleCommand (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC/MC** permission.

Default

Empty string (no command).

Description

The **serial** command runs after login at the start of a session and allows you to set up a command such as **connect com2** that autoruns when a session begins.

Example

connect com2

cfgSerialTelnetEnable (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC/MC** permission.

Legal Values

0=disabled, 1=enabled

Description

Enables/disables telnet console.

Default

0=telnet disabled

cfgOobSnmp

The group contains parameters to configure the SNMP agent and trap capabilities of the DRAC/MC.

One instance of the group is allowed. The following subsections describe the objects in this group.

cfgOobSnmpAgentCommunity

NOTE: To modify this property, you must have **Configure DRAC/MC** permission. This object requires a DRAC/MC reset before it becomes active.

Legal Values

A string of up to 31 ASCII characters.

Default

public

Description

Use this object to modify the SNMP community name.

cfgOobSnmpTrapsEnable (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC/MC** permission. This object requires a DRAC/MC reset before it becomes active.

Legal Values

Boolean, either 1 or 0 (TRUE or FALSE)

Default

1

Description

0=Disable, 1=Enable transmission of SNMP traps.

cfgOobSnmpAgentEnable (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC/MC** permission. This object requires a DRAC/MC reset before it becomes active.

Legal Values

Boolean either 1 or 0 (TRUE or FALSE).

Default

0

Description

0=Disable, 1=Enable the DRAC/MC SNMP agent.

cfgRacTuning

The group contains various tuning configuration parameters.

One instance of the group is allowed. The following subsections describe the objects in this group.

cfgRacTuneConRedirPort (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC/MC** permission.

Legal Values

A number between 0 and 65535.

Default

0x814

Description

The port used by console redirection (keyboard and mouse data).

cfgRacTuneConRedirVideoPort (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC/MC** permission.

Legal Values

A number between 0 and 65535.

Default

0x2000

Description

The port used by console redirection video.

cfgRacTuneRemoteRacadmEnable (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC/MC** permission.

Legal Values

Boolean, either 1 or 0 (TRUE or FALSE).

Default

0

NOTE: For DRAC/MC version 1.3 and later, the default value of this property is 1.

Description

0=Disable, 1=Enable

cfgRacTuneHostCom2BaudRate (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC/MC** permission.

Legal Values

115200, 57600, 19200, and 9600

Default

57600

NOTE: For best results when redirecting BIOS System Setup screens, Dell recommends setting this baud rate to 57600.

Description

0=Disable, 1=Enable

If enabled, autonegotiation takes priority over the values that are set in the **cfgNetTuningNic100MB** and **cfgNetTuningNicFullDuplex** objects.

cfgRacTuneTelnetPort

NOTE: To modify this property, you must have **Configure DRAC/MC** permission.

Legal Values

Integer from 1 to any positive number. Type hexadecimal values.

1 – Port 65536 and deny the following ports:

Table B-2. Denied Ports

Protocol	Port Number
SMTP	6400
HTTP	80
HTTPS	443
SSH	22
LDAP	389
SSL LDAP	686

Default

0x17

Description

Use this property to configure the DRAC/MC telnet port.

cfgRacTuneD3debugEnable (Read/Write)

NOTE: This property is not supported by DRAC/MC.

Legal Values

Boolean, either 1 or 0 (TRUE or FALSE).

Default

1

Description

Enables or disables the RAC debug command. This object requires a RAC reset before it becomes active.

cfgRacVirtual

This group contains parameters to configure the DRAC/MC Virtual Media feature. One instance of the group is allowed. The following subsections describe the objects in this group.

cfgVirAtapiSvrPort (Read Only)

Legal Value

A number between 0 and 65535.

Default

0xe54

Description

The port that is used for the virtual media connection.

cfgRacVirtualMediaDisable

NOTE: This property is not available with DRAC/MC version 1.3 and later.

Legal Value

Boolean, either 1 or 0 (TRUE or FALSE).

Default

0 (Virtual Media is enabled).

Description

This property is used to enable or disable Virtual Media.

cfgChassisPower

This group contains parameters to configure the DRAC/MC power budget feature. Only one instance of the group is allowed. The following subsections describe the objects in this group.

cfgChassisRedundancyPolicy (Read/Write)

Legal Value

0 - No Redundancy

1 - 3+1 Redundancy

2 - 2+2 Redundancy

Default

1 - 3+1 Redundancy

Description

Sets the redundancy policy for the power supplies. In the default 3+1 redundancy mode, the capacity of the highest-rated power supply is kept in reserve so that the chassis and server modules have enough power in the event of failure of any one power supply.

cfgChassisRedundantState (Read Only)

Legal Value

Boolean, either 1 or 0

Default

None

Description

1=Yes (system is redundant)

0=No (system is not redundant)

cfgChassisPowerStatus (Read Only)

Legal Value

OK and Warning

Default

None

Description

OK = No Redundancy

Warning = Redundancy is lost

cfgChassisAvailablePower (Read Only)

Legal Value

in watts

Default

None

Description

This value is the sum of 12V DC wattage capacity of all the installed power supplies in the enclosure.

cfgChassisRedundancyReserve (Read Only)

Legal Value

in watts

Default

None

Description

This value is the power kept in reserve to satisfy the configured redundancy policy.

cfgChassisLoadSharing (Read Only)

Legal value

in watts

Default

None

Description

This value is the reduction in power when multiple power supplies are sharing a load in parallel.

cfgChassisBaseConsumption (Read Only)

Legal value

in watts

Default

400W

Description

This value is the power required for the chassis to boot.

cfgChassisServerConsumption (Read Only)

Legal value

in watts

Default

None

Description

This value is the total power consumption of all the server modules installed and powered on in the enclosure.

cfgChassisTotalConsumption (Read Only)

Legal value

in watts

Default

None

Description

This value is the total power that the system has consumed. It is the sum of cfgChassisBaseConsumption, cfgChassisServerConsumption, CfgChassisLoadSharing.

cfgChassisRemainingPower (Read Only)

Legal value

in watts

Default

3152W

Description

This value is the remaining power available for powering on additional server modules in the enclosure. This excludes the power kept in reserve to satisfy the redundancy policy requirements.

cfgServerInfo

This group contains parameters to configure the server blades in your modular system. Up to ten instances (corresponding to the number of server blades in your system) of the group are allowed. The following subsections describe the objects in this group.

cfgServerSlotNumber (Read Only)

NOTE: This object is Read/Write when using the remote RACADM utility with the config command and a configuration file.

Legal Value

1–10

Description

Specifies the slot that the server module occupies.

cfgServerServiceTag (Read Only)

Legal Value

Strings

Description

Specifies the service tag of the server module.

cfgServerName

Legal Value

Strings

Default

Server-*n*

Description

Specifies the user-configurable server name. The maximum number of characters allowed in this value is 15.

NOTE: This value is specific to the slot and not to the server module. If this value is blank or has only spaces, the `cfgservername` is reset to the default value.

cfgServerBMCMacAddress (Read Only)

Description

Specifies the MAC address of the baseboard management controller (BMC) on the modular system.

cfgServerNic1MacAddress (Read Only)

Description

Specifies the MAC address of the first network adapter, LOM1, on the server module.

cfgServerNic2MacAddress (Read Only)

NOTE: This property is not available on the PowerEdge 1855 server modules.

Description

Specifies the MAC address of the second network adapter, LOM2, on the server module.

cfgServerBMCBaudRate (Read Only)

Description

Specifies the baud rate of the BMC on the server modules.

Event Filter Operation and Event Mask Properties

The DRAC/MC alert filter scans all of the objects in the **alert enable** property group **cfgUserAdmin**. If this object's property values are **TRUE**, it scans the event masks in the User table.

NOTE: Throughout this document, objects are always referred to by group name *and* object name, separated by a space.

The DRAC/MC alert filter operates according to the following general steps:

- The DRAC/MC alert filter scans all of the objects in the **alert enable** property group **cfgUserAdmin**. If this object's property value is TRUE, it scans the event masks in the User table.
- The DRAC/MC alert filter scans the **cfgTraps cfgTrapsEnable** object. If this object's property value is **TRUE**, it scans the event masks in the Trap table.

The following subsections describe the event masks for DRAC/MC-generated events and managed-system-generated events defined in the User table and the Trap table.

System-Generated Alert Mask Definitions

The **cfgTraps cfgTrapsFilterSysEventMask** properties are an unsigned 32-bit integer property that holds the filter information for managed-system generated events. The bit definitions in Table B-3 apply.

Table B-3. System-Generated Alert Mask Bit Definitions

Bits	Data	Type
28–31	System undefined	reserved
24–27	System undefined	reserved
20–23	System undefined	reserved
16–19	System status alerts	<*statMask*>
12–15	System miscellaneous sensor	<*senMask*>
8–11	System fan sensors	<*senMask*>
4–7	System voltage sensors	<*senMask*>
0–3	System temperature sensors	<*senMask*>

where <*senMask*> has the following bit definitions:

- Bit-0: 1 = Send alert for informational events (such as a return to lower severity range or normal).
- Bit-1: 1 = Send alert for warning (noncritical) events.
- Bit-2: 1 = Send alert for critical events.
- Bit-3: Reserved.

where <*statMask*> has the following bit definitions:

- Bit-0: 1 = Send alert when system transitions to a powered-on state.
- Bit-1: 1 = Send alert when system transitions to a powered-off state.
- Bit-2: 1 = Send alert when watchdog timer detects a system hang.
- Bit-3: Reserved.

Alert Test Commands

You can test alerts using test commands. The **RACADM** command has subcommands that test the different types of alert interfaces. These object ID sets cause the firmware to execute the subcommand with the option that indicates the test alert type to test. The test message is preset in properties for each test alert type. The types of alerts are e-mail and trap.

The following subsection describes the command interfaces and the operation of the subcommand for each option.

E-mail Test Command

Synopsis

```
racadm testemail –i <index>

racadm testemail –u <username>
```

Alert Data Definitions

The e-mail alert contains the following information: message (including test message, if a paging test), event description, date, time, severity, system ID, model, BIOS version, asset tag, service tag, and BMC version. The following is an example test e-mail (fields shown are examples only and may not reflect actual observed output for your environment):

```
Subject: Alert from Dell Remote Access Controller/Modular Chassis:
10.35.10.108

Message: TEST PAGE

Event: E-mail paging test to user 1

Date: 06-mar-2005

Time: 00:01:37

Severity: Info/Normal

Model: Dell PowerEdge 1855

BIOS version: A00

Asset tag: 181676

Service tag: 6X713

DRAC/MC Version: 1.3
```

Trap Test Command

Synopsis

```
racadm testtrap –i <trap index>
```

Alert Data Definitions

The "alertMessage" string (up to 1 KB) provides the specific information describing the cause and specific source of the event, which includes:

- Sensor identification: entity/IPMBsecondaryAddress
- Sensor number
- Sensor ID string (if possible)
- Current reading and range (normal/warning/critical)

For more information, see the *Server Administrator SNMP Reference Guide*.

DRAC/MC Object and Command Properties

The following tables provide detailed information about DRAC/MC default values, permissions, and command database support.

Table C-1. Property Default Values

Property	Default Value	Legal Value
	idRacInfo	
idRacName	DRAC	Maximum length 15 characters
idRacMisc	Null	Maximum length 64 characters
idRacProductInfo	Remote Access Controller/Modular Chassis	Maximum of 63 characters
idRacDescriptionInfo	The system component provides a complete set of remote management functions for a server.	Maximum of 255 characters
idRacVersionInfo	DRAC Firmware Version *x.x* Build (mm.dd)	Maximum of 63 characters.
idRacType	0x7	N/A
	cfgActiveDirectory	
cfgADEnable	0 (Disabled)	0 (Disabled) or 1 (Enabled)
cfgRacName	""	Maximum length 255 characters
cfgRacDomain	""	Maximum length 255 characters
cfgRootDomain	""	Maximum length 255 characters
	cfgLanNetworking	
cfgNicEnable	1 (Enabled)	0 (Disabled or 1 (Enabled)
cfgNicIpAddress	192.168.0.120	Valid IP address
cfgNicNetmask	255.255.255.0	Valid IP mask
cfgNicGateway	192.168.0.1	Valid IP address
cfgNicUseDhcp	0 (Disabled)	0 (Disabled) or 1 (Enabled)
cfgDNSDomainNameFromDHCP	0 (Disabled)	0 (Disabled) or 1 (Enabled)

Table C-1. Property Default Values *(continued)*

Property	Default Value	Legal Value
cfgDNSDomainName	"MYDOMAIN"	Maximum length 254 characters. At least one character must be alphabetic.
cfgDNSRacName	""	Maximum length 63 characters
cfgDNSRegisterRac	0 (Disabled)	0 (Disabled) or 1 (Enabled)
cfgDNSServersFromDHCP	0 (Disabled)	0 (Disabled) or 1 (Enabled)
cfgDNSServer1	192.168.0.5	Any legal IP address, including 0.0.0.0
cfgDNSServer2	192.168.0.6	Any legal IP address, including 0.0.0.0
	cfgKvmLanNetworking	
cfgKvmNicIpAddress	192.168.0.121	A string of "." separated numeric fields containing the static IP address.
cfgKvmNicNetmask	255.255.255.0	A string of "." separated numeric fields containing the static IP address.
cfgKvmNicGateway	192.168.0.1	A string of "." separated numeric fields containing the static IP address.
cfgKvmNicUseDhcp	0 (Disabled)	0 (Disabled) or 1 (Enabled)
cfgKvmNicMacAddress	None	Avocent Digital Access KVM MAC address
	cfgCurrentLanNetworking	
cfgNicCurrentIpAddress	192.168.0.120	Valid IP address
cfgNicCurrentNetmask	255.255.255.0	Valid IP Mask
cfgNicCurrentGateway	192.168.0.1	Valid IP address
cfgNicCurrentDhcpWasUsed	0 (Disabled)	0 (Disabled) or 1 (Enabled)
cfgDNSCurrentServer1	192.168.0.5	Any legal IP address, including 0.0.0.0.
cfgDNSCurrentServer2	192.168.0.6	Any legal IP address, including 0.0.0.0.
cfgDNSCurrentDomainName	"MYDOMAIN"	Maximum length 254 characters. At least one character must be alphabetic.
	cfgKvmCurrentLanNetworking	
cfgKvmNicCurrentIpAddress	192.168.0.121	A string of "." separated numeric fields containing the static IP address.
cfgKvmNicCurrentNetmask	255.255.255.0	A string of "." separated numeric fields containing the static IP address.

Table C-1. Property Default Values *(continued)*

Property	Default Value	Legal Value
cfgKvmNicCurrentGateway	192.168.0.1	A string of "." separated numeric fields containing the static IP address.
cfgKvmNicCurrentDhcpWasUsed	0 (Disabled)	0 (Disabled) or 1 (Enabled)
	cfgRacConsoleRedirection	
cfgConsoleRedirectionEnable	1 (Enable)	0 (Disabled) or 1 (Enabled)
cfgMaxSessions	1	Maximum of 255 characters
cfgCurrentSessions	0	Maximum of 255 characters
	cfgRacVirtual	
cfgVirAtapiSvrPort	0xe54	A number between 0 and 65535
cfgRacVirtualMediaDisable	0 (Virtual Media is enabled)	0 (Disabled) or 1 (Enabled)
NOTE: This property is not available on DRAC/MC version 1.3 and later.		
	cfgRemoteHosts	
cfgRhostsSmtpEmailEnable	1 (Enabled)	0 (Disabled) or 1 (Enabled)
cfgRhostsSmtpServerIpAddr	127.0.0.1	Valid IP
cfgRhostsFwUpdateTftpEnable	1 (Enabled)	0 (Disabled) or 1 (Enabled)
cfgRhostsFwUpdateIpAddr	192.168.0.4	Valid IP
cfgRhostsFwUpdatePath	Null	Maximum length 255 characters
	cfgUserAdmin	
cfgUserAdminPrivilege	0x0	0x80000000 to 0x800001ff, and 0x0
cfgUserAdminUserName	First instance is `root`, and all other occurrences are Null	Maximum length 19 characters
cfgUserAdminPassword	First instance is `calvin`. All other occurrences are Null	Maximum length 20 characters
cfgUserAdminAlertFilterSysEventMask	0x777777	-
cfgUserAdminEmailEnable	0 (Disabled)	0 (Disabled) or 1 (Enabled)
cfgUserAdminEmailAddress	Null	Maximum length 63 characters
cfgUserAdminEmailCustomMsg	Null	Maximum length 31 characters

Table C-1. Property Default Values *(continued)*

Property	Default Value	Legal Value
	cfgTraps	
cfgTrapsDestIpAddr	0.0.0.0	Valid IP & 0.0.0.0
cfgTrapsEnable	0 (Disabled)	0 (Disabled) or 1 (Enabled)
cfgTrapsSnmpCommunity	Null	Maximum length 31 characters
cfgTrapsFilterSysEventMask	0x777777	-
	cfgSessionManagement	
cfgSsnMgtMaxSessions	4	0x01 to 0x04
cfgSsnMgtMaxSessionsPerUser	4	0x01 to 0x04
	cfgSerial	
cfgSerialBaudRate	115200	9600, 28800, 57600, and 115200
cfgSerialConsoleEnable	1 (Enabled)	0 (Disabled) or 1 (Enabled)
cfgSerialConsoleQuitKey	<CR><~><.>	A string of 3 or fewer characters
cfgSerialConsoleIdleTimeout	0x12c (300 seconds)	Integer from 0x1 to 0xffff. Entering hexadecimal 0x0 indicates a disable time-out.
cfgSerialConsoleShellType	2	1 - VT100 block screen interface 2 - UNIX® command line data stream interface
cfgSerialConsoleNoAuth	0 (Disabled)	0 (Disabled) or 1 (Enabled)
cfgSerialConsoleCommand	Null	Maximum length 128 characters
cfgSerialTelnetEnable	0 (Disabled)	0 (Disabled) or 1 (Enabled)
	cfgOobSnmp	
cfgOobSnmpAgentCommunity	public	Maximum length 31 characters
cfgOobSnmpTrapsEnable	1 (Enabled)	0 (Disabled) or 1 (Enabled)
cfgOobSnmpAgentEnable	0 (Disabled)	0 (Disabled) or 1 (Enabled)
	cfgNetTuning	
cfgNetTuningNicAutoneg	1 (Enabled)	0 (Disabled) or 1 (Enabled)
cfgNetTuningNic100MB	1 (Enabled)	0 (Disabled) or 1 (Enabled)
cfgNetTuningFullDuplex	1 (Enabled)	0 (Disabled) or 1 (Enabled)

Table C-1. Property Default Values *(continued)*

Property	Default Value	Legal Value
	cfgKvmNetTuning	
cfgKvmNetTuningNicAutoneg	1 (Enabled)	0 (Disabled) or 1 (Enabled)
cfgKvmNetTuningNic100MB	1 (Enabled)	0 (Disabled) or 1 (Enabled)
cfgKvmNetTuningNicFullDuplex	1 (Enabled)	0 (Disabled) or 1 (Enabled)
cfgKvmNetTuningEnableDebug	0 (Disabled)	0 (Disabled) or 1 (Enabled)
	cfgRacTuning	
cfgRacTuneD3debugEnable	This property is not supported by DRAC/MC.	
cfgRacTuneRemoteRacadmEnable	0 (Disabled) **NOTE:** For DRAC/MC version 1.3 and later, the default value is 1 (Enabled).	0 (Disabled) or 1 (Enabled)
cfgRacTuneHostCom2BaudRate	57600	115200, 57600, 19200, and 9600
cfgRacTuneTelnetPort	0x17	Any number between 0 and 65535
cfgRacTuneConRedirPort	0x170c	A number between 0 and 65535
cfgRacTuneConRedirVideoPort	0x2000	A number between 0 and 65535
	cfgServerInfo	
cfgServerSlotNumber		
cfgServerServiceTag		
cfgServerName	Server–*n*	Strings
cfgServerBMCMacAddress		
cfgServerBMCBaudRate	19200 for Dell™ PowerEdge™ 1855 57600 for PowerEdge 1955	9600, 19200, 57600, and 115200
cfgServerNic1MacAddress		
cfgServerNic2MacAddress		
	cfgChassisPower	
cfgChassisRedundancyPolicy	1	0, 1, and 2
cfgChassisRedundantState		0 or 1
cfgChassisPowerStatus		OK and Warning
cfgChassisAvailablePower		in watts

Table C-1. Property Default Values *(continued)*

Property	Default Value	Legal Value
cfgChassisRedundancyReserve		in watts
cfgChassisLoadSharing		in watts
cfgChassisBaseConsumption	400W	in watts
cfgChassisServerConsumption		in watts
cfgChassisTotalConsumption		in watts
cfgChassisRemainingPower		in watts

Table C-2. Property Access Permissions

Property	Read Permission	Write Permission
	IdRacInfo	
idRacType	Log in to DRAC/MC	N/A
idRacProductInfo	Log in to DRAC/MC	N/A
idRacDescriptionInfo	Log in to DRAC/MC	N/A
idRacVersionInfo	Log in to DRAC/MC	N/A
idRacName	Log in to DRAC/MC	Configure DRAC/MC
idRacMisc	Log in to DRAC/MC	Configure DRAC/MC
	cfgActiveDirectory	
cfgADEnable	Log in to DRAC/MC	Configure DRAC/MC
cfgRacName	Log in to DRAC/MC	Configure DRAC/MC
cfgRacDomain	Log in to DRAC/MC	Configure DRAC/MC
cfgRootDomain	Log in to DRAC/MC	Configure DRAC/MC
	cfgLanNetworking	
cfgDNSServersFromDHCP	Log in to DRAC/MC	Configure DRAC/MC
cfgDNSServer1	Log in to DRAC/MC	Configure DRAC/MC
cfgDNSServer2	Log in to DRAC/MC	Configure DRAC/MC
cfgDNSDomainNameFromDHCP	Log in to DRAC/MC	Configure DRAC/MC
cfgDNSDomainName	Log in to DRAC/MC	Configure DRAC/MC
cfgDNSRacName	Log in to DRAC/MC	Configure DRAC/MC
cfgDNSRegisterRac	Log in to DRAC/MC	Configure DRAC/MC
cfgNicEnable	Log in to DRAC/MC	Configure DRAC/MC

Table C-2. Property Access Permissions *(continued)*

Property	Read Permission	Write Permission
cfgNicIpAddress	Log in to DRAC/MC	Configure DRAC/MC
cfgNicNetmask	Log in to DRAC/MC	Configure DRAC/MC
cfgNicGateway	Log in to DRAC/MC	Configure DRAC/MC
cfgNicUseDhcp	Log in to DRAC/MC	Configure DRAC/MC
cfgNicMacAddress	This property is not supported by DRAC/MC.	
	cfgCurrentLanNetworking	
cfgDNSCurrentServer1	Log in to DRAC/MC	N/A
cfgDNSCurrentServer2	Log in to DRAC/MC	N/A
cfgDNSCurrentDomainName	Log in to DRAC/MC	N/A
cfgNicCurrentIpAddress	Log in to DRAC/MC	N/A
cfgNicCurrentNetmask	Log in to DRAC/MC	N/A
cfgNicCurrentGateway	Log in to DRAC/MC	N/A
cfgNicCurrentDhcpWasUsed	Log in to DRAC/MC	N/A
cfgDNSCurrentDhcpWasUsed	This property is not supported by DRAC/MC.	
CfgDNSCurrentServer1	This property is not supported by DRAC/MC.	
CfgDNSCurrentServer2	This property is not supported by DRAC/MC.	
	cfgRemoteHosts	
cfgRhostsSmtpEmailEnable	Log in to DRAC/MC	Configure DRAC/MC
cfgRhostsSmtpServerIpAddr	Log in to DRAC/MC	Configure DRAC/MC
cfgRhostsFwUpdateTftpEnable	Log in to DRAC/MC	Configure DRAC/MC
cfgRhostsFwUpdateIpAddr	Log in to DRAC/MC	Configure DRAC/MC
cfgRhostsFwUpdatePath	Log in to DRAC/MC	Configure DRAC/MC
	cfgUserAdmin	
cfgUserAdminPrivilege	Log in to DRAC/MC	Configure Users
cfgUserAdminUserName	Log in to DRAC/MC	Configure Users
cfgUserAdminPassword	N/A	Configure Users
cfgUserAdminAlertFilterRacEventMask	This property is not supported by DRAC/MC.	
cfgUserAdminAlertFilterSysEventMask	Log in to DRAC/MC	Configure Users
cfgUserAdminEmailEnable	Log in to DRAC/MC	Configure Users
cfgUserAdminEmailAddress	Log in to DRAC/MC	Configure Users

Table C-2. Property Access Permissions *(continued)*

Property	Read Permission	Write Permission
cfgUserAdminEmailCustomMsg	Log in to DRAC/MC	Configure Users
cfgUserAdminIndex	Log in to DRAC/MC	N/A
	cfgTraps	
cfgTrapsDestIpAddr	Log in to DRAC/MC	Configure DRAC/MC
cfgTrapsEnable	Log in to DRAC/MC	Configure DRAC/MC
cfgTrapsSnmpCommunity	Log in to DRAC/MC	Configure DRAC/MC
cfgTrapsFilterRacEventMask	This property is not supported by DRAC/MC.	
cfgTrapsFilterSysEventMask	Log in to DRAC/MC	Configure DRAC/MC
cfgTrapsIndex	Log in to DRAC/MC	N/A
	cfgSessionManagement	
cfgSsnMgtMaxSessions	Log in to DRAC/MC	Configure DRAC/MC
cfgSsnMgtMaxSessionsPerUser	Log in to DRAC/MC	Configure DRAC/MC
	cfgSerial	
cfgSerialBaudRate	Log in to DRAC/MC	Configure DRAC/MC
cfgSerialConsoleEnable	Log in to DRAC/MC	Configure DRAC/MC
cfgSerialConsoleQuitKey	Log in to DRAC/MC	Configure DRAC/MC
cfgSerialConsoleIdleTimeout	Log in to DRAC/MC	Configure DRAC/MC
cfgSerialConsoleShellType	Log in to DRAC/MC	Configure DRAC/MC
cfgSerialConsoleNoAuth	Log in to DRAC/MC	Configure DRAC/MC
cfgSerialConsoleCommand	Log in to DRAC/MC	Configure DRAC/MC
cfgSerialTelnetEnable	Log in to DRAC/MC	Configure DRAC/MC
cfgSerialTelnetEnableCom2RedirEnable	This property is not supported by DRAC/MC.	
CfgSerialTelnet7flsBackspace	This property is not supported by DRAC/MC.	
	cfgNetTuning	
cfgNetTuningNicAutoneg	Log in to DRAC/MC	Configure DRAC/MC
cfgNetTuningNic100MB	Log in to DRAC/MC	Configure DRAC/MC
cfgNetTuningFullDuplex	Log in to DRAC/MC	Configure DRAC/MC
cfgRacTuneConRedirPort	Log in to DRAC/MC	Configure DRAC/MC
cfgRacTuneConRedirVideoPort	Log in to DRAC/MC	Configure DRAC/MC

Table C-2. Property Access Permissions *(continued)*

Property	Read Permission	Write Permission
	cfgOobSnmp	
cfgOobSnmpAgentCommunity	This property is not supported by DRAC/MC.	
cfgOobSnmpTrapsEnable	Log in to DRAC/MC	Configure DRAC/MC
cfgOobSnmpAgentEnable	Log in to DRAC/MC	Configure DRAC/MC
	cfgRacTuning	
cfgRacTuneHttpPort	This property is not supported by DRAC/MC.	
cfgRacTuneHttpsPort	This property is not supported by DRAC/MC.	
cfgRacTuneTelnetPort	This property is not supported by DRAC/MC.	
cfgRacTuneFwUpdateResetDelay	This property is not supported by DRAC/MC.	
cfgRacTuneD3debugEnable	This property is not supported by DRAC/MC.	
cfgRacTuneRemoteRacadmEnable	Log in to DRAC/MC	Configure DRAC/MC
cfgRacTuneHostCom2BaudRate	Log in to DRAC/MC	Configure DRAC/MC
cfgRacTuneTelnetPort	Log in to DRAC/MC	Configure DRAC/MC
cfgRacTuneConRedirPort	Log in to DRAC/MC	Configure DRAC/MC
cfgRacTuneConRedirVideoPort	Log in to DRAC/MC	Configure DRAC/MC
	cfgKvmLanNetworking	
cfgKvmNicIpAddress	Log in to DRAC/MC	Configure DRAC/MC
cfgKvmNicNetmask	Log in to DRAC/MC	Configure DRAC/MC
cfgKvmNicGateway	Log in to DRAC/MC	Configure DRAC/MC
cfgKvmNicUseDhcp	Log in to DRAC/MC	Configure DRAC/MC
cfgKvmNicMacAddress	Log in to DRAC/MC	N/A
	cfgKvmCurrentLanNetworking	
cfgKvmNicCurrentIpAddress	Log in to DRAC/MC	N/A
cfgKvmNicCurrentNetmask	Log in to DRAC/MC	N/A
cfgKvmNicCurrentGateway	Log in to DRAC/MC	N/A
cfgKvmNicCurrentDhcpWasUsed	Log in to DRAC/MC	N/A
	cfgKvmNetTuning	
cfgKvmNetTuningNicAutoneg	Log in to DRAC/MC	Configure DRAC/MC
cfgKvmNetTuningNic100MB	Log in to DRAC/MC	Configure DRAC/MC

Table C-2. Property Access Permissions *(continued)*

Property	Read Permission	Write Permission
cfgKvmNetTuningNicFullDuplex	Log in to DRAC/MC	Configure DRAC/MC
cfgKvmNetTuningEnableDebug	Log in to DRAC/MC	Configure DRAC/MC
	cfgRacConsoleRedirection	
cfgConsoleRedirectionEnable	Log in to DRAC/MC	Configure DRAC/MC
cfgMaxSessions	Log in to DRAC/MC	N/A
cfgCurrentSessions	Log in to DRAC/MC	N/A
	cfgServerInfo	
cfgServerSlotNumber	Log in to DRAC/MC	Configure DRAC/MC
cfgServerServiceTag	Log in to DRAC/MC	N/A
cfgServerName	Log in to DRAC/MC	Configure DRAC/MC
cfgServerBMCMacAddress	Log in to DRAC/MC	N/A
cfgServerBMCBaudRate	Log in to DRAC/MC	N/A
cfgServerNic1MacAddress	Log in to DRAC/MC	N/A
cfgServerNic2MacAddress	Log in to DRAC/MC	N/A
	cfgChassisPower	
cfgChassisRedundancyPolicy	Log in to DRAC/MC	Configure DRAC/MC
cfgChassisRedundantState	Log in to DRAC/MC	N/A
cfgChassisPowerStatus	Log in to DRAC/MC	N/A
cfgChassisAvailablePower	Log in to DRAC/MC	N/A
cfgChassisRedundancyReserve	Log in to DRAC/MC	N/A
cfgChassisLoadSharing	Log in to DRAC/MC	N/A
cfgChassisBaseConsumption	Log in to DRAC/MC	N/A
cfgChassisServerConsumption	Log in to DRAC/MC	N/A
cfgChassisTotalConsumption	Log in to DRAC/MC	N/A
cfgChassisRemainingPower	Log in to DRAC/MC	N/A
	***icRacManageNodeOs (Not supported)**	
*All properties are not supported by DRAC/MC.		
	***CfgRacSecurity (Not supported)**	
*All properties are not supported by DRAC/MC.		

Table C-2. Property Access Permissions *(continued)*

Property	Read Permission	Write Permission
***CfgRacVirtual (Not supported)**		
*All properties are not supported by DRAC/MC.		
***CfgActiveDirectory (Not supported)**		
*All properties are not supported by DRAC/MC.		

Table C-3. Property Database Group, Object, and Default Values

No	Item	Property Database Group and Object	Default Value
1	**TFTP server IP**	cfgRemoteHosts→cfgRhostsFwUpdateIpAddr	192.168.0.4
2	**TFTP update path**	cfgRemoteHosts→cfgRhostsFwUpdatePath	Null
3	**Manage module Mask**	cfgLanNetworking→cfgNicNetmask	255.255.255.0
4	**Manage module IP**	cfgLanNetworking→cfgNicIpAddress	192.168.0.120
5	**Manage module Gateway**	cfgLanNetworking→cfgNicGateway	192.168.0.120
6	**Physical Control**	Only in Web interface	Auto Negotiation
7	**Console Baud Rate**	cfgSerial→cfgSerialBaudRate	115200
8	**NIC Enable**	cfgLanNetworking→cfgNicEnable	Enabled
9	**DHCP Enable**	cfgLanNetworking→cfgNicUseDhcp	Disabled
10	**Time Zone**	Only in Web interface	GMT+0
11	**SNMP Enable**	cfgOobSnmp→cfgOobSnmpAgentEnable	Enabled
12	**SNMP Trap Enable**	cfgOobSnmp→cfgOobSnmpTrapsEnable	Enabled
13	**SMTP Enable**	cfgRemoteHosts→cfgRhostsSmtpEmailEnable	Enabled
14	**TELNET Enable**	cfgserial→cfgSerialTelnetEnable	Disabled
15	**Debug Enable**	cfgRacTuning→cfgRacTuneD3debugEnable	Enabled
16	**Console Enable**	cfgSerial→cfgSerialConsoleEnable	Enabled
17	**Allow user to disable authentication on serial shell**	cfgSerial→cfgSerialConsoleNoAuth	Disabled
18	**Telnet Port No.**	cfgRacTuning→cfgRacTuneTelnetPort	0x17
19	**SMTP server IP**	cfgRemoteHosts→cfgRhostsSmtpServerIpAddr	127.0.0.1
20	**Console Timeout**	cfgSerial→cfgSerialConsoleIdleTimeout	300 Seconds
21	**HTTP timeout**	Only in Web interface	5 Minutes
22	**Date Time Format**	Only in Web interface	24 hours

Table C-3. Property Database Group, Object, and Default Values *(continued)*

No	Item	Property Database Group and Object	Default Value
23	**Console Redirection Baud Rate**	cfgRacTuning→cfgRacTuneHostCom2BaudRate	57600
24	**Shell Type**	cfgSerial→cfgSerialConsoleShellType	2 (UNIX is always 2.)
25	**Console Redirection Quit Key**	cfgSerial→cfgSerialConsoleQuitKey	<CR><~><.>
26	**The serial command run after login.**	cfgSerial→cfgSerialConsoleCommand	Null
27	**Login Name**	cfgUserAdmin→cfgUserAdminUserName	First instance is `root`, and all other occurrences are Null.
28	**Login Password**	cfgUserAdmin→cfgUserAdminPassword	First instance is `calvin`, and all other occurrences are Null.
29	**User Permission**	cfgUserAdmin→cfgUserAdminPrivilege	First instance is `Administrator permission 0x800001FF`, and all other occurrences are `Guest permission 0x80000001`.
30	**User group**	Only in Web interface	First instance is `Administrator`, and all other occurrences are `Guest`.
31	**User Filter (Informational, Warning, or Severe)**	cfgUserAdmin→cfgUserAdminAlertFilterSys EventMask	All are Enabled 0x777777.
32	**User E-mail Alert Enable**	cfgUserAdmin→cfgUserAdminEmailEnable	Disabled
33	**User E-mail Address**	cfgUserAdmin→cfgUserAdminEmailAddress	Null
34	**User E-mail Custom Message**	cfgUserAdmin→cfgUserAdminEmailCustomMsg	Null
35	**SNMP Trap Destination IP**	cfgTraps→cfgTrapsDestIpAddr	0.0.0.0
36	**SNMP Trap Alert Enable**	cfgTraps→cfgTrapsEnable	Disabled
37	**SNMP Trap Community**	cfgTraps→cfgTrapsSnmpCommunity	Null
38	**Trap Filter (Informational, Warning, or Severe)**	cfgTraps→cfgTrapsFilterSysEventMask	All are Enabled 0x777777.

Table C-3. Property Database Group, Object, and Default Values *(continued)*

No	Item	Property Database Group and Object	Default Value
39	**Generic property (undefined)**	idRacInfo→idRacMisc	Null
40	**A User-assigned Name**	idRacInfo→idRacName	DRAC
41	**Chassis Name**	`chassisname` in getsysinfo command	Null
42	**Chassis Location**	`chassislocation` in getsysinfo command	Null
43	**Maximum Sessions per User**	cfgSessionManagement→ cfgSsnMgtMaxSessionsPerUser	4
44	**DRAC/MC Maximum Session**	cfgSessionManagement→cfgSsnMgtMaxSessions	4

D

OSCAR Refresh Rates

Table D-1 provides the refresh rates for the On-Screen Configuration and Activity Reporting interface (OSCAR®).

Table D-1. OSCAR Refresh Rates

Resolution	Refresh Rate
640 x 480	70 Hz
640 x 480	72 Hz
640 x 480	75 Hz
640 x 480	85 Hz
800 x 600	70 Hz
800 x 600	72 Hz
800 x 600	75 Hz
800 x 600	85 Hz
1024 x 768	60 Hz
NOTE: This resolution is the recommended server video setting for optimal console redirection performance.	
1024 x 768	**70 Hz**
1024 x 768	72 Hz
1024 x 768	75 Hz
1024 x 768	85 Hz
1280 x 768	70 Hz
1280 x 768	85 Hz
1280 x 1024	70 Hz
1280 x 1024	75 Hz
1280 x 1024	85 Hz

NOTE: Using unsupported video settings may result in a blank video and a distorted OSCAR flag on the monitor when invoking the OSCAR menu.

Glossary

ACI

Abbreviation for Analog Console Interface, a KVM switch port that allows you to connect the switch to an external KVM device using a CAT 5 cable.

ACPI-enabled

Abbreviation for Advanced Configuration and Power Interface-enabled, which is a power management specification that makes hardware status information available to the operating system. ACPI enables a PC to turn its peripherals on and off for improved power management.

ANSI

Abbreviation for American National Standards Institute.

API

Abbreviation for Application Programming Interface, which is a language and message format used by an application program to communicate with the operating system or some other control program such as a database management system (DBMS) or communications protocol.

ARP

Acronym for Address Resolution Protocol, which is a method for finding a host's Ethernet address from its Internet address.

ASCII

Acronym for American Standard Code for Information Interchange, which is a code representation used for displaying or printing letters, numbers, and other characters.

baud rate

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

BIOS

Acronym for basic input/output system, which is the part of system software that provides the lowest-level interface to peripheral devices and which controls the first stage of the system boot process, including installation of the operating system into memory.

BMC

Abbreviation for baseboard management controller, which is the controller interface between the DRAC/MC and the managed system's BMC. Each module has its own BMC containing the DRAC/MC chassis management system that logs event data through the serial and RACADM System Event Log (SEL).

bus

A set of conductors connecting the various functional units in a computer. Buses are named by the type of data they carry, such as data bus, address bus, or PCI bus.

CA

Abbreviation for certificate authority. See *CSR*.

cache

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

CIM

Acronym for Common Information Model, which is a protocol designed for managing systems on a network.

CLI

Abbreviation for command line interface.

command

The combination of an option and argument, or just an option if no argument is required; for example:

```
racadm config -g <groupName>
```

CR

Abbreviation for carriage return. CR is one of the control characters in ASCII code, unicode, or EBCDIC that commands a display to move the position of the cursor to the first position on the same line. It is mostly used along with line feed, a move to the next line, while carriage return precedes line feed to indicate a new line.

CRLF

Abbreviation for Carriage Return+Line Feed.

CSR

Abbreviation for certificate signing request, which is a digital request to a CA for a secure server certificate. *See* CA.

console redirection

Console redirection is a function that directs a managed system's display screen, mouse functions, and keyboard functions to the corresponding devices on a management station. You may then use the management station's system console to control the managed system.

DHCP

Abbreviation for Dynamic Host Configuration Protocol, which is a protocol that provides a means to dynamically allocate IP addresses to computers on a local area network (LAN).

DLL

Abbreviation for Dynamic Link Library, which is a library of small programs, any of which can be called when needed by a larger program that is running in the system. The small program that lets the larger program communicate with a specific device such as a printer or scanner is often packaged as a DLL program (or file).

DRAC/MC

Abbreviation for Dell™ Remote Access Controller/Modular Chassis, which is a systems management hardware and software solution designed to provide remote management capabilities, crashed system recovery, and power control functions for Dell PowerEdge™ systems.

DSU

Abbreviation for disk storage unit.

firmware

Software (programs or data) that is written onto read-only memory (ROM). Firmware can boot and operate a device. Each controller contains firmware that helps provide the controller's functionality.

FRU

Abbreviation for field-replaceable unit, which is a part that can be easily removed and replaced by the user or by a technician without having to send the entire product or system to a repair facility.

GbE

Abbreviation for Gigabit Ethernet.

GMT

Abbreviation for Greenwich Mean Time, which is the standard time common to every place in the world. GMT nominally reflects the mean solar time along the prime meridian (0 longitude) that runs through the Greenwich Observatory outside of London, UK.

GPIO

Abbreviation for general purpose input/output.

GUI

Abbreviation for graphical user interface, which refers to a computer display interface that uses elements such as windows, dialog boxes, and buttons as opposed to a command prompt interface, in which all user interaction is displayed and typed in text.

hardware log
Records events generated by the DRAC/MC and the BMC.

hot plug
To remove a component from a system and plug in a new one while the power is still on and the unit is still operating. Redundant systems can be designed to swap drives, circuit boards, power supplies, virtually anything that is duplexed within the computer.

HTTP
Abbreviation for Hypertext Transfer Protocol. HTTP is the client server TCP/IP protocol used on the Web for the exchange of HTML documents.

HTTPS
Abbreviation for Hypertext Transfer 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 Web addresses with SSL, whereas you will continue to use `http://` for HTTP URLs without SSL.

ICMB
Abbreviation for Intelligent Chassis Management Bus.

ICMP
Abbreviation for Internet Control Message Protocol, which is a TCP/IP protocol used to send error and control messages.

ID
Abbreviation for identifier, commonly used when referring to a user identifier (user ID) or object identifier (object ID).

IP
Abbreviation for Internet Protocol, which is the network layer for TCP/IP. IP provides packet routing, fragmentation, and reassembly.

IPMB
Abbreviation for intelligent system management bus, which is a bus used in systems management technology.

IPMI
Abbreviation for Intelligent Platform Management Interface, which is a part of systems management technology.

JVM
Abbreviation for Java Virtual Machine, which is a system-independent execution environment that converts compiled Java code (byte code) for a system processor so that it can perform a Java program instructions.

Kbps
Abbreviation for kilobits per second, which is a data transfer rate.

KVM
Abbreviation for keyboard video mouse, which is a switch used to connect keyboard, video, mouse, and monitor to two or more computers.

LAN
Abbreviation for local area network.

LDAP
Abbreviation for Lightweight Directory Access Protocol.

LDIF
Abbreviation for LDAP Data Interchange Format.

LED
Abbreviation for light-emitting diode.

MAC
Acronym for media access control, which is a network sublayer between a network node and the network physical layer.

MAC address
Acronym for media access control address, which is a unique address embedded in the physical components of a NIC.

managed system
The managed system is the system in which the DRAC 4 is installed or embedded.

management station
The management station is a system that remotely accesses the DRAC/MC.

Mbps
Abbreviation for megabits per second, which is a data transfer rate.

MIB
Abbreviation for management information base.

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 systems 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.

NAS
Abbreviation for network attached storage.

NIC
Acronym for network interface controller, which is an adapter circuit board installed in a computer to provide a physical connection to a network.

NMI
Abbreviation for nonmaskable interrupt.

OID
Abbreviation for Object Identifiers.

OSCAR
Abbreviation for On-Screen Configuration and Activity Reporting interface.

PERC/SCSI
Abbreviation for PowerEdge Expandable RAID Controller, which is a configuration that enables you to configure hard drives using both RAID and SCSI modes. You can perform a PERC/SCSI configuration using the PERC/SCSI Setup Utility during system startup. *See* SCSI.

PCI
Abbreviation for Peripheral Component Interconnect, which is a standard interface and bus technology for connecting peripherals to a system and for communicating with those peripherals.

POST
Acronym for power-on self-test, which is a sequence of diagnostic tests that are run automatically by a system when it is powered on.

PPP
Abbreviation for Point-to-Point Protocol, which is the Internet standard protocol for transmitting network layer datagrams (such as IP packets) over serial point-to-point links.

RAID
Abbreviation for redundant array of independent drives.

RAM
Acronym for random-access memory. RAM is general-purpose readable and writable memory on systems and the DRAC/MC.

RAM disk
A memory-resident program which emulates a hard drive. The DRAC/MC maintains a RAM disk in its memory.

RAC

Abbreviation for remote access controller.

Redundant DRAC/MC

In a redundant configuration, there are two DRAC/MCs in a chassis: the primary DRAC/MC, which monitors the chassis and the standby DRAC/MC, which is in standby mode that monitors the active signal from the primary module. The standby DRAC/MC will become the active primary DRAC/MC if failover occurs for more than five seconds.

NOTE: To support the redundant DRAC/MC configuration, both DRAC/MCs must have the same firmware version.

ROM

Acronym for read-only memory, which is memory from which data may be read, but to which data cannot be written.

RPM

Abbreviation for Red Hat® Package Manager, which is a package-management system for the Red Hat Enterprise Linux operating system that helps installation of software packages. It is similar to an installation program.

SAC

Acronym for the Microsoft® Special Administration Console.

SCSI

Acronym for small computer system interface. An I/O bus interface with faster data transmission rates than standard ports.

SEL

Abbreviation for System Event Log, which displays system-critical events that occur on the chassis. This log displays the date, time, and a description of each event generated by the DRAC/MC.

SIP

Abbreviation for Server Interface Pod, a device that drives standard KVM analog signals over a single CAT 5 cable to another computer, thereby eliminating the KVM cable.

SMI

Abbreviation for systems management interrupt.

SMTP

Abbreviation for Simple Mail Transfer Protocol, which is a protocol used to transfer electronic mail between systems, usually over an Ethernet.

SNMP

Abbreviation for Simple Network Management Protocol, which is a protocol designed to manage nodes on an IP network. DRAC/MCs are SNMP-managed devices (nodes).

SNMP trap

A notification (event) generated by the DRAC/MC or the BMC that contains information about state changes on the managed system or about potential hardware problems.

SOL

Abbreviation for Serial Over LAN, which enables suitably designed servers to transparently redirect the serial character stream of a baseboard UART to/from a remote client over a shared LAN. The architecture requires software running on the managed system's BMC and client software running on management station and/or a central network proxy.

SSH

Abbreviation for Secure SHell.

SSL

Abbreviation for secure sockets layer.

TAP

Abbreviation for Telelocator Alphanumeric Protocol, which is a protocol used for submitting requests to a pager service.

TCP/IP

Abbreviation for Transmission Control Protocol/Internet Protocol, which represents the set of standard Ethernet protocols that includes the network layer and transport layer protocols.

TFTP

Abbreviation for Trivial File Transfer Protocol, which is a simple file transfer protocol used for downloading boot code to diskless devices or systems.

UART

Acronym for universal asynchronous receiver-transmitter. The UART is a system component that handles asynchronous serial communication by converting parallel bytes from the processor into serial bits for transmission (vice versa).

USB

Abbreviation for universal serial bus, which is a hardware interface for low-speed peripherals such as a keyboard, mouse, scanner, printer, external diskette drive, or telephony device.

UPS

Abbreviation for uninterruptible power supply.

UTC

Abbreviation for Universal Coordinated Time. The international time standard (formerly Greenwich Mean Time, or GMT). Zero hours UTC is midnight in Greenwich, England, which is located at 0 degrees longitude. Everything east of Greenwich (up to 180 degrees) is later in time; everything west is earlier. There are 42 time authorities around the world that are constantly synchronizing with each other. In the U.S., the time authorities are located at the U.S. Naval Observatory (USNO) and the National Institute of Standards & Technology (NIST). *See* GMT.

utility

A program used to manage system resources, for example, memory, disk drives, or printers.

VNC

Abbreviation for virtual network computing.

VT-100

Abbreviation for Video Terminal 100, which is used by the most common terminal emulation programs.

Web server

A secure port server that makes Web pages available for viewing by Web browsers using the HTTP or HTTPS protocol.

WAN

Abbreviation for wide area network.

Windows® SAC

Abbreviation for Windows Special Administration Console. Windows 2003 allows operating system installation, configuration, and recovery by directing a text-based console screen (or SAC) over the serial port, with access provided by a connected console server.

Index