Integrated Dell™ Remote Access Controller Firmware Version 1.00 User Guide

www.dell.com | support.dell.com

Notes and Notices

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

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

March 2008 Rev. A01

Contents

1

iDRAC Overview

The Integrated Dell™ Remote Access Controller (iDRAC) is a systems management hardware and software solution that provides remote management capabilities, crashed system recovery, and power control functions for Dell PowerEdge™ systems.

The iDRAC uses an integrated System-on-Chip microprocessor for the remote monitor/control system. The iDRAC co-exists on the system board with the managed PowerEdge server. The server operating system, which may be a Microsoft® Windows® or Linux operating system, is concerned with executing applications; the iDRAC is concerned with monitoring and managing the server's environment and state outside of the operating system.

You can configure the iDRAC to send you an e-mail or Simple Network Management Protocol (SNMP) trap alert for warnings or errors. To help you diagnose the probable cause of a system crash, iDRAC can log event data and capture an image of the screen when it detects that the system has crashed.

Managed servers are installed in a Dell M1000-e system enclosure (chassis) with modular power supplies, cooling fans, and a chassis management controller (CMC). The CMC monitors and manages all components installed in the chassis. Redundant CMCs can be added to provide hot failover if the primary CMC fails. The chassis provides access to the iDRACs through its LCD display, local console connections, and its web interface.

All network connections to the iDRAC are through the CMC network interface (CMC RJ45 connection port labelled "GB1"). The CMC routes traffic to the iDRACs on its servers through a private, internal network. This private management network is outside of the server's data path and outside of the operating system's control, that is, *out-of-band*. The managed servers' *inband* network interfaces are accessed through I/O modules (IOMs) installed in the chassis.

The iDRAC network interface is disabled by default. It must be configured before the iDRAC is accessible. After the iDRAC is enabled and configured on the network, it can be accessed at its assigned IP address with the iDRAC web interface, telnet or SSH, and supported network management protocols, such as Intelligent Platform Management Interface (IPMI).

iDRAC Management Features

The iDRAC provides the following management features:

- Dynamic Domain Name System (DDNS) registration
- Remote system management and monitoring using a Web interface, the local RACADM command line interface via console redirection, and the SM-CLP command line over a telnet/SSH connection
- Support for Microsoft Active Directory® authentication — Centralizes iDRAC user IDs and passwords in Active Directory using the standard schema or an extended schema
- Console Redirection — Provides remote system keyboard, video, and mouse functions
- Virtual Media — Enables a managed server to access a local media drive on the management station or ISO CD/DVD images on a network share
- Monitoring — Provides access to system information and status of components
- Access to system logs — Provides access to the system event log, the iDRAC log, and the last crash screen of the crashed or unresponsive system that is independent of the operating system state
- Dell OpenManage™ software integration — Enables you to launch the iDRAC Web interface from Dell OpenManage Server Administrator or IT Assistant
- iDRAC alert — Alerts you to potential managed node issues through an e-mail message or SNMP trap
- Remote power management — Provides remote power management functions, such as shutdown and reset, from a management console
- Intelligent Platform Management Interface (IPMI) support
- Secure Sockets Layer (SSL) encryption — Provides secure remote system management through the Web interface

- Password-level security management — Prevents unauthorized access to a remote system
- Role-based authority — Provides assignable permissions for different systems management tasks

iDRAC Security Features

The iDRAC provides the following security features:

- User authentication through Microsoft Active Directory (optional) or hardware-stored user IDs and passwords
- Role-based authority, which enables an administrator to configure specific privileges for each user
- User ID and password configuration through the Web interface or SM-CLP
- SM-CLP and Web interfaces, which support 128-bit SSL encryption and 40-bit SSL encryption (for countries where 128 bit is not acceptable)
- Session time-out configuration (in seconds) through the Web interface or SM-CLP
- Configurable IP ports (where applicable)

  NOTE: Telnet does not support SSL encryption.

- Secure Shell (SSH), which uses an encrypted transport layer for higher security
- Login failure limits per IP address, with login blocking from the IP address when the limit is exceeded
- Limited IP address range for clients connecting to the iDRAC

Supported Platforms

The iDRAC supports the following PowerEdge systems in the Dell PowerEdge M1000-e system enclosure:

- PowerEdge M600
- PowerEdge M605

Check the iDRAC Readme file and the *Dell PowerEdge Compatibility Guide* located on the Dell Support website at **support.dell.com** for the latest supported platforms.

Supported Operating Systems

Table 1-1 lists the operating systems that support the iDRAC.

See the *Dell OpenManage Server Administrator Compatibility Guide* located on the Dell Support website at **support.dell.com** for the latest information.

Table 1-1. Supported Operating Systems

Operating System Family	Operating System
Microsoft Windows	Microsoft® Windows Server® 2003 R2 Standard and Enterprise (32-bit x86) Editions with SP2
	Microsoft Windows Server 2003 Web, Standard and Enterprise (32-bit x86) Editions with SP2
	Microsoft Windows Server 2003 Standard and Enterprise (x64) Editions with SP2
	Microsoft Windows Storage Server 2003 R2 Express, Workgroup, Standard, and Enterprise x64 Editions
	Microsoft Windows Vista® Gold Business and Enterprise Editions
	Microsoft Windows Server 2008 Web, Standard, and Enterprise (32-bit x86) Editions
	Microsoft Windows Server 2008 Web, Standard, Enterprise and Datacenter (x64) Editions
	NOTE: When installing Windows Server 2003 with Service Pack 1, be aware of changes to DCOM security settings. For more information, see article 903220 from the Microsoft Support website at **support.microsoft.com/kb/903220**.
Red Hat® Linux®	Enterprise Linux WS, ES, and AS (version 3) (x86 and x86_64)
	Enterprise Linux WS, ES, and AS (version 4) (x86 and x86_64)
	Enterprise Linux 5 (x86 and x86-64)

Table 1-1. Supported Operating Systems *(continued)*

Operating System Family	Operating System
SUSE® Linux	Enterprise Server 9 with Update 2 and Update 3 (x86_64) Enterprise Server 10 (Gold) (x86_64)

Supported Web Browsers

NOTICE: Console Redirection and Virtual Media only support 32-bit Web browsers. Using 64-bit Web browsers will generate unexpected results or failure.

Table 1-2 lists the Web browsers that are supported as iDRAC clients.

See the iDRAC Readme file and the *Dell OpenManage Server Administrator Compatibility Guide* located on the Dell Support website at **support.dell.com** for the latest information.

Table 1-2. Supported Web Browsers

Operating System	Supported Web Browser
Windows	Internet Explorer 6.0 (32-bit) with Service Pack 2 (SP2) for Windows XP and Windows 2003 R2 SP2 only
	Internet Explorer 7.0 for Windows Vista, Windows XP, and Windows 2003 R2 SP2 only
Linux	Mozilla Firefox 1.5 (32-bit) on SUSE Linux (version 10) only
	Mozilla Firefox 2.0 (32-bit)

Supported Remote Access Connections

Table 1-3 lists the connection features.

Table 1-3. Supported Remote Access Connections

Connection	Features
iDRAC NIC	• 10Mbps/100Mbs/1Gbps Ethernet via CMC Gb Ethernet port • DHCP support • SNMP traps and e-mail event notification • Support for SM-CLP (telnet or SSH) command shell, for operations such as iDRAC configuration, system boot, reset, power-on, and shutdown commands • Support for IPMI utilities, such as ipmitool and ipmishell

iDRAC Ports

Table 1-4 lists the ports iDRAC listens on for connections. Table 1-5 identifies the ports that the iDRAC uses as a client. This information is required when opening firewalls for remote access to an iDRAC.

Table 1-4. iDRAC Server Listening Ports

Port Number	Function
22*	Secure Shell (SSH)
23*	Telnet
80*	HTTP
443*	HTTPS
623	RMCP/RMCP+
3668*, 3669*	Virtual Media Service
3770*, 3771*	Virtual Media Secure Service
5900*	Console Redirection keyboard/mouse
5901*	Console Redirection video

* Configurable port

Table 1-5. iDRAC Client Ports

Port Number	Function
25	SMTP
53	DNS
68	DHCP-assigned IP address
69	TFTP
162	SNMP trap
636	LDAPS
3269	LDAPS for global catalog (GC)

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 iDRAC in your system:

- The iDRAC online help provides information about using the Web interface.
- The *Dell CMC Firmware Version 1.0 User's Guide* provides information about using the controller that manages all modules in the chassis containing your PowerEdge server.
- The *Dell OpenManage IT Assistant User's Guide* and the *Dell OpenManage IT Assistant Reference Guide* provide information about IT Assistant.
- The *Dell OpenManage Server Administrator User's Guide* provides information about installing and using Server Administrator.
- The *Dell Update Packages User's Guide* provides information about obtaining and using Dell Update Packages as part of your system update strategy.

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

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

- The *Rack Installation Guide* and *Rack Installation Instructions* included with your rack solution describe how to install your system into a rack.
- The *Getting Started Guide* provides an overview of system features, setting up your system, and technical specifications.
- The *Hardware Owner's Manual* provides information about system features and describes how to troubleshoot the system and install or replace system components.
- Systems management software documentation describes the features, requirements, installation, and basic operation of the software.
- 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.

2

Configuring the iDRAC

This section provides information about how to establish access to the iDRAC and to configure your management environment to use iDRAC.

Before You Begin

Gather the following items prior to configuring the iDRAC:

- *Dell Chassis Management Controller User's Guide*
- *Dell PowerEdge Installation and Server Management* CD
- *Dell Systems Management Consoles* CD
- *Dell PowerEdge Service and Diagnostic Utilities* CD
- *Dell PowerEdge Documentation* CD

Interfaces for Configuring the iDRAC

You can configure the iDRAC using the iDRAC Configuration utility, the iDRAC Web interface, the local RACADM CLI, or the SM-CLP CLI. The local RACADM CLI is available after you have installed the operating system and the Dell PowerEdge server management software on the managed server. Table 2-1 describes these interfaces.

NOTICE: Using more than one configuration interface at the same time may generate unexpected results.

Table 2-1. Configuration Interfaces

Interface	Description
iDRAC Configuration Utility	Accessed at boot time, the iDRAC Configuration utility is useful when installing a new PowerEdge server. Use it for setting up the network and basic security features and for enabling other features.

Table 2-1. Configuration Interfaces *(continued)*

Interface	Description
iDRAC Web Interface	The iDRAC Web interface is a browser-based management application that you can use to interactively manage the iDRAC and monitor the managed server. It is the primary interface for day-to-day tasks, such as monitoring system health, viewing the system event log, managing local iDRAC users, and launching the CMC Web interface and console redirection sessions.
CMC Web Interface	In addition to monitoring and managing the chassis, the CMC Web interface can be used to view the status of a managed server, configure iDRAC network settings, and to start, stop, or reset the managed server.
Chassis LCD Panel	The LCD panel on the chassis containing the iDRAC can be used to view the high-level status of the servers in the chassis. During initial configuration of the CMC, the configuration wizard allows you to enable DHCP configuration of iDRAC networking.
Local RACADM	The local RACADM command line interface runs on the managed server. It is accessed from either the iKVM or a console redirection session initiated from the iDRAC Web interface. RACADM is installed on the managed server when you install Dell OpenManage Server Administrator. RACADM commands provide access to nearly all iDRAC features. You can inspect sensor data, system event log records, and the current status and configuration values maintained in the iDRAC. You can alter iDRAC configuration values, manage local users, enable and disable features, and perform power functions such as shutting down or rebooting the managed server.
iVM-CLI	The iDRAC Virtual Media Command Line Interface (iVM-CLI) provides the managed server access to media on the management station. It is useful for developing scripts to install operating systems on multiple managed servers.

Table 2-1. Configuration Interfaces *(continued)*

Interface	Description
SM-CLP	SM-CLP is the Server Management Workgroup Server Management-Command Line Protocol (SM-CLP) implementation incorporated in the iDRAC. The SM-CLP command line is accessed by logging into the iDRAC using telnet or SSH. SM-CLP commands implement a useful subset of the local RACADM commands. The commands are useful for scripting since they can be executed from a management station command line. The output of commands can be retrieved in well-defined formats, including XML, facilitating scripting and integration with existing reporting and management tools. See "RACADM and SM-CLP Equivalencies" on page 295 for a comparison of the RACADM and SM-CLP commands.
IPMI	IPMI defines a standard way for embedded management subsystems such as the iDRAC to communicate with other embedded systems and management applications. You can use the iDRAC Web interface, SM-CLP, or RACADM commands to configure IPMI Platform Event Filters (PEFs) and Platform Event Traps (PETs). PEFs cause the iDRAC to perform selectable actions (for example, rebooting the managed server) when it detects a condition. PETs instruct the iDRAC to send e-mail or IPMI alerts when it detects specified events or conditions. You can also use standard IPMI tools such as **ipmitool** and **ipmishell** with iDRAC when you enable IPMI Over LAN.

Configuration Tasks

This section is an overview of the configuration tasks for the management station, the iDRAC, and the managed server. The tasks to be performed include configuring the iDRAC so that it can be used remotely, configuring the iDRAC features you want to use, installing the operating system on the managed server, and installing management software on your management station and the managed server.

The configuration tasks that can be used to perform each task are listed beneath the task.

NOTE: Before performing configuration procedures in this guide, the CMC and I/O modules must be installed in the chassis and configured, and the PowerEdge server must be physically installed in the chassis.

Configure the Management Station

Set up a management station by installing the Dell OpenManage software, a Web browser, and other software utilities.

- See "Configuring the Management Station" on page 41

Configure iDRAC Networking

Enable the iDRAC network and configure IP, netmask, gateway, and DNS addresses.

NOTE: Changing the iDRAC network settings terminates all current network connections to the iDRAC.

NOTE: The option to configure the server using the LCD panel is available *only* during the CMC initial configuration. Once the chassis is deployed, the LCD panel cannot be used to reconfigure the iDRAC.

NOTE: The LCD panel can be used to enable DHCP to configure the iDRAC network. If you want to assign static addresses, you must use the iDRAC Configuration Utility or the CMC Web interface.

- Chassis LCD Panel — see the *Dell Chassis Management Controller User's Guide*.
- iDRAC configuration utility — see "LAN" on page 199
- CMC Web interface — see "Configuring Networking Using the CMC Web Interface" on page 33
- RACADM — see "cfgLanNetworking" on page 255

Configure iDRAC Users

Set up the local iDRAC users and permissions. The iDRAC holds a table of sixteen local users in firmware. You can set usernames, passwords, and roles for these users.

- iDRAC configuration utility (configures administrative user only) — see "LAN User Configuration" on page 202
- iDRAC Web interface — see "Adding and Configuring iDRAC Users" on page 65
- RACADM — see "Adding an iDRAC User" on page 153

Configure Active Directory

In addition to the local iDRAC users, you can use Microsoft® Active Directory® to authenticate iDRAC user logins.

- See "Using the iDRAC with Microsoft Active Directory" on page 89

Configure IP Filtering and IP Blocking

In addition to user authentication, you can prevent unauthorized access by rejecting connection attempts from IP addresses outside of a defined range and by temporarily blocking connections from IP addresses where authentication has failed multiple times within a configurable timespan.

- iDRAC Web interface — see "Configuring IP Filtering and IP Blocking" on page 60
- RACADM — see "Configuring IP Filtering (IpRange)" on page 161, "Configuring IP Blocking" on page 163

Configure Platform Events

Platform events occur when the iDRAC detects a warning or critical condition from one of the managed server's sensors.

Configure Platform Event Filters (PEFs) to choose the events you want to detect, such as rebooting the managed server, when an event is detected.

- iDRAC Web interface — see "Configuring Platform Event Filters (PEF)" on page 62
- RACADM — see "Configuring PEF" on page 158

Configure Platform Event Traps (PETs) to send alert notifications to an IP address, such as a management station with IPMI software or to send an e-mail to a specified e-mail address.

- iDRAC Web interface — see "Configuring Platform Event Traps (PET)" on page 63
- RACADM — "Configuring PET" on page 159

Configure Serial Over LAN

Serial Over LAN (SOL) is an IPMI feature that allows you to redirect the managed server's serial port I/O over the network. SOL enables the iDRAC console redirection feature.

- iDRAC Web interface — see "Configuring Serial Over LAN" on page 81
- See also "Using GUI Console Redirection" on page 121

Configure iDRAC Services

Enable or disable the iDRAC network services — such as telnet, SSH, and the Web server interface — and reconfigure ports and other service parameters.

- iDRAC Web interface — see "Configuring iDRAC Services" on page 82
- RACADM — see "Configuring iDRAC Telnet and SSH Services Using Local RACADM" on page 165

Configure Secure Sockets Layer (SSL)

Configure SSL for the iDRAC web server.

- iDRAC Web interface — see "Secure Sockets Layer (SSL)" on page 69
- RACADM — see "cfgRacSecurity" on page 276, "sslcsrgen" on page 244, "sslcertupload" on page 245, "sslcertdownload" on page 246, "sslcertview" on page 247

Configure Virtual Media

Configure the virtual media feature so that you can install the operating system on the PowerEdge server. Virtual media allows the managed server to access media devices on the management station or ISO CD/DVD images on a network share as if they were devices on the managed server.

- iDRAC Web interface — see "Configuring and Using Virtual Media" on page 137
- iDRAC configuration utility — see "Virtual Media" on page 202

Install the Managed Server Software

Install the Microsoft Windows or Linux operating system on the PowerEdge server using virtual media and then install the Dell OpenManage software on the managed PowerEdge server and set up the last crash screen feature.

- Console redirection — see "Installing the Software on the Managed Server" on page 51
- iVM-CLI — see "Using the Virtual Media Command Line Interface Utility" on page 190

Configure the Managed Server for the Last Crash Screen Feature

Set up the managed server so that the iDRAC can capture the screen image after an operating system crash or freeze.

- Managed Server — see "Configuring the Managed Server to Capture the Last Crash Screen" on page 52, "Disabling the Windows Automatic Reboot Option" on page 53

Configuring Networking Using the CMC Web Interface

NOTE: You must have Chassis Configuration Administrator privilege to set up iDRAC network settings from the CMC.

NOTE: The default CMC user is **root** and the default password is **calvin**.

NOTE: The CMC IP address can be found in the iDRAC Web interface by clicking **System→ Remote Access→ CMC**. You can also launch the CMC Web interface from this page.

1. Use your web browser to log in to the CMC web user interface using a URL of the form https://<*CMC-IP-address*> or https://<*CMC-DNS-name*>.
2. Enter the CMC username and password and click **OK**.
3. Click the plus (+) symbol next to **Chassis** in the left column, then click **Servers**.
4. Click **Setup→ Deploy**.
5. Enable the LAN for the server by checking the checkbox next to the server beneath the **Enable Lan** heading.
6. Enable or disable IPMI over LAN by checking the or unchecking the checkbox next to the server beneath the **Enable IPMI over LAN** heading.
7. Enable or disable DHCP for the server by checking or unchecking the checkbox next to the server under the **DHCP Enabled** heading.
8. If DHCP is disabled, enter the static IP address, netmask, and default gateway for the server.
9. Click **Apply** at the bottom of the page.

Updating the iDRAC Firmware

Updating the iDRAC firmware installs a new firmware image in the iDRAC flash memory. You can update the firmware using any of the following methods:

- SM-CLP **load** command
- iDRAC Web interface
- Dell Update Package (for Linux or Microsoft Windows)
- DOS iDRAC Firmware update utility
- CMC Web interface (only if iDRAC firmware is corrupted)

Downloading the Firmware or Update Package

Download the firmware from **support.dell.com**. The firmware image is available in several different formats to support the different update methods available.

To update the iDRAC firmware using the iDRAC Web interface or SM-CLP, or to recover the iDRAC using the CMC Web interface, download the binary image, packaged as a self-extracting archive.

To update the iDRAC firmware from the managed server, download the operating system-specific Dell Update Package (DUP) for the operating system running on the server whose iDRAC you are updating.

To update the iDRAC firmware using the DOS iDRAC Firmware update utility, download both the update utility and the binary image, which are packaged in self-extracting archive files.

Execute the Firmware Update

NOTE: When the iDRAC firmware update begins, all existing iDRAC sessions are disconnected and new sessions are not permitted until the update process is completed.

NOTE: The chassis fans run at 100% during the iDRAC firmware update. When the update is complete, normal fan speed regulation resumes. This is normal behavior, designed to protect the server from overheating during a time when it cannot send sensor information to the CMC.

To use a Dell Update Package for Linux or Microsoft Windows, execute the operating-specific DUP on the managed server.

When using the SM-CLP **load** command, place the firmware binary image in a directory where a Trivial File Transfer Protocol (TFTP) server can serve it to the iDRAC. See "Updating the iDRAC Firmware Using SM-CLP" on page 184.

When using the iDRAC Web interface or the CMC Web interface, place the firmware binary image on a disk that is accessible to the management station from which you are running the Web interface. See "Updating the iDRAC Firmware" on page 85.

NOTE: The iDRAC Web interface also allows you to reset the iDRAC configuration to the factory defaults.

You can use the CMC Web interface to update the firmware *only* when the CMC detects that the iDRAC firmware is corrupted, as could occur if the iDRAC firmware update progress is interrupted before it completes. See "Recovering iDRAC Firmware Using the CMC" on page 86.

Using the DOS Update Utility

To update the iDRAC firmware using the DOS update utility, boot the managed server to DOS, and execute the **idrac16d** command. The syntax for the command is:

```
idrac16d [-f] [-i=<filename>] [-l=<logfile>]
```

When executed with no options, the **idrac16d** command updates the iDRAC firmware using the firmware image file **firmimg.imc** in the current directory.

The options are as follows:

`-f` — forces the update. The `-f` option can be used to *downgrade* the firmware to an earlier image.

`-i=<filename>` — specifies the filename image that contains the firmware image. This option is required if the firmware filename has been changed from the default name **firmimg.imc**.

`-l=<logfile>` — logs output from the update activity. This option is used for debugging.

NOTICE: If you enter incorrectly arguments to the **idrac16d** command, or supply the `–h` option, you may notice an additional option, `-nopresconfig` in the usage output. This option is used to update the firmware without preserving any configuration information. You should **not** use this option, since it *deletes* all of your existing iDRAC configuration information such as IP addresses, users, and passwords.

Verifying the Digital Signature

A digital signature is used to authenticate the identity of the signer of a file and to certify that the original content of the file has not been modified since it was signed.

If you do not already have it installed on your system, you must install the Gnu Privacy Guard (GPG) to verify a digital signature. To use the standard verification procedure, perform the following steps:

1 Download the Dell Linux public GnuPG key, if you do not already have it, by navigating to **lists.us.dell.com** and clicking the **Dell Public GPG key** link. Save the file to your local system. The default name is **linux-security-publickey.txt**.

2 Import the public key to your gpg trust database by running the following command:

```
gpg --import <Public Key Filename>
```

NOTE: You must have your private key to complete the process.

3 To avoid a distrusted-key warning, change the trust level for the Dell Public GPG key.

a Type the following command:

```
gpg --edit-key 23B66A9D
```

b Within the GPG key editor, type `fpr`. The following message appears:

```
pub 1024D/23B66A9D 2001-04-16 Dell, Inc.
(Product Group) <linux-security@dell.com>
Primary key fingerprint: 4172 E2CE 955A 1776
A5E6 1BB7 CA77 951D 23B6 6A9D
```

If the fingerprint of your imported key is the same as above, you have a correct copy of the key.

c While still in the GPG key editor, type `trust`. The following menu appears:

```
Please decide how far you trust this user to
correctly verify other users' keys (by looking
at passports, checking fingerprints from
different sources, etc.)

  1 = I don't know or won't say
  2 = I do NOT trust
  3 = I trust marginally
  4 = I trust fully
  5 = I trust ultimately
```

```
   m = back to the main menu

Your decision?
```

d Type 5 <Enter>. The following prompt appears:

```
Do you really want to set this key to ultimate
trust? (y/N)
```

e Type `y` <Enter> to confirm your choice.

f Type `quit` <Enter> to exit the GPG key editor.

You must import and validate the public key only once.

4 Obtain the package you need, for example the Linux DUP or self-extracting archive) and its associated signature file from the Dell Support website at **support.dell.com/support/downloads**.

NOTE: Each Linux Update Package has a separate signature file, which is shown on the same web page as the Update Package. You need both the Update Package and its associated signature file for verification. By default, the signature file is named the same as the DUP filename with a **.sign** extension. For example, if a Linux DUP is named **PE1850-BIOS-LX-A02.BIN**, its signature filename is **PE1850-BIOS-LX-A02.BIN.sign**. The iDRAC firmware image also has an associated **.sign** file, which is included in the self-extracting archive with the firmware image. To download the files, right-click on the download link and use the **Save Target As...** file option.

5 Verify the Update Package:

```
gpg --verify <Linux Update Package signature
filename> <Linux Update Package filename>
```

The following example illustrates the steps that you follow to verify a 1425SC BIOS Update Package:

1 Download the following two files from **support.dell.com**:

- PESC1425-BIOS-LX-A01.bin.sign
- PESC1425-BIOS-LX-A01.bin

2 Import the public key by running the following command line:

```
gpg --import <linux-security-publickey.txt>
```

The following output message appears:

```
gpg: key 23B66A9D: "Dell Computer Corporation
(Linux Systems Group) <linux-
security@dell.com>" not changed
gpg: Total number processed: 1
gpg: unchanged: 1
```

3 Set the GPG trust level for the Dell public key. if you haven't done so previously.

   a Typing the following command:

   ```
   gpg --edit-key 23B66A9D
   ```

   b At the command prompt, type the following commands:

   ```
   fpr
   trust
   ```

   c Type 5 <Enter> to choose `I trust ultimately` from the menu.

   d Type `y` <Enter> to confirm your choice.

   e Type `quit` <Enter> to exit the GPG key editor.

   This completes validation of the Dell public key.

4 Verify the PESC1425 BIOS package digital signature by running the following command:

   ```
   gpg --verify PESC1425-BIOS-LX-A01.bin.sign
   PESC1425-BIOS-LX-A01.bin
   ```

   The following output message appears:

   ```
   gpg: Signature made Thu 14 Apr 2005 04:25:37 AM
   IST using DSA key ID 23B66A9D
   gpg: Good signature from "Dell Computer
   Corporation (Linux Systems Group) <linux-
   security@dell.com>"
   ```

NOTE: If you have not validated the key as shown in step 3, you will receive additional messages:

```
gpg: WARNING: This key is not certified with a
trusted signature!
gpg: There is no indication that the signature
belongs to the owner.
Primary key fingerprint: 4172 E2CE 955A 1776
A5E6 1BB7 CA77 951D 23B6 6A9D
```

3

Configuring the Management Station

A management station is a computer used to monitor and manage the PowerEdge servers and other modules in the chassis. This section describes software installation and configuration tasks that set up a management station to work with the iDRAC. Before you begin configuring the iDRAC, follow the procedures in this section to ensure that you have installed and configured the tools you will need.

Management Station Set Up Steps

To set up your Management Station, perform the following steps:

1. Set up the management station network.
2. Install and configure a supported Web browser.
3. Install a Java Runtime Environment (JRE) (optional for Windows).
4. Install telnet or SSH clients, if required.
5. Install a TFTP server, if required.
6. Install Dell OpenManage IT Assistant (optional).

Management Station Network Requirements

To access the iDRAC, the management station must be on the same network as the CMC RJ45 connection port labelled "GB1". It is possible to isolate the CMC network from the network the managed server is on, so that your management station may have LAN access to the iDRAC but not to the managed server.

Using the iDRAC console redirection feature (see "Using GUI Console Redirection" on page 121), you can access the managed server's console even if you do not have network access to the server's ports. You can also perform several management functions on the managed server, such as rebooting the computer, using iDRAC facilities. To access network and application services hosted on the managed server, however, you may need an additional NIC in the management computer.

Configuring a Supported Web Browser

The following sections provide instructions for configuring the supported Web browsers for use with the iDRAC Web interface. For a list of supported Web browsers, see "Supported Web Browsers" on page 23.

NOTE: The iDRAC Web interface is not supported on 64-bit Web browsers. If you open a 64-bit browser, access the Console Redirection page, and attempt to install the plug-in, the installation procedure fails. If this error was not acknowledged and you repeat this procedure, the Console Redirect Page loads even though the plug-in installation fails during your first attempt. This issue occurs because the Web browser stores the plug-in information in the profile directory even though the plug-in installation procedure failed. To fix this issue, install and run a supported 32-bit Web browser and log in to the iDRAC.

Configuring Your Web Browser to Connect to the Web Interface

If you are connecting to the iDRAC Web interface from a management station that connects to the Internet through a proxy server, you must configure the Web browser to access the Internet from this server.

To configure the Internet Explorer Web browser to access a proxy server, perform the following steps:

1 Open a Web browser window.

2 Click **Tools**, and click **Internet Options**.

3 From the **Internet Options** window, click the **Connections** tab.

4 Under **Local Area Network (LAN) settings**, click **LAN Settings**.

5 If the **Use a proxy server** box is selected, select the **Bypass proxy server for local addresses** box.

6 Click **OK** twice.

Adding iDRAC to the List of Trusted Domains

When you access the iDRAC Web interface through the Web browser, you may be prompted to add the iDRAC IP address to the list of trusted domains if the IP address is missing from the list. When completed, click **Refresh** or relaunch the Web browser to establish a connection to the iDRAC Web interface.

Viewing Localized Versions of the Web Interface

The iDRAC Web interface is supported on the following operating system languages:

- English
- French
- German
- Spanish
- Japanese
- Simplified Chinese

Internet Explorer 6.0 (Windows)

To view a localized version of the iDRAC Web interface in Internet Explorer, perform the following steps:

1. Click the **Tools** menu and select **Internet Options**.
2. In the **Internet Options** window, click **Languages**.
3. In the **Language Preference** window, click **Add**.
4. In the **Add Language** window, select a supported language.

   To select more than one language, press <Ctrl>.

5. Select your preferred language and click **Move Up** to move the language to the top of the list.
6. In the **Language Preference** window, click **OK**.
7. Click **OK**.

Firefox 1.5 (Linux)

To view a localized version of the iDRAC Web interface in Firefox, perform the following steps:

1. Click **Edit→ Preferences**, then click the **Advanced** tab.
2. In the **Language** section, click **Choose**.
3. Click **Select a language to add...**.
4. Select a supported language and click **Add**.
5. Select your preferred language and click **Move Up** to move it to the top of the list.
6. In the Languages menu, click **OK**.
7. Click **OK**.

Setting the Locale in Linux

The console redirection viewer requires a UTF-8 character set to display correctly. If your display is garbled, check your locale and reset the character set if needed.

The following steps show how to set the character set on a Red Hat® Enterprise Linux® client with a Simplified Chinese GUI:

1. Open a command terminal.
2. Type `locale` and press <Enter>. Output similar to the following output appears:

```
LANG=zh_CN.UTF-8
LC_CTYPE="zh_CN.UTF-8"
LC_NUMERIC="zh_CN.UTF-8"
LC_TIME="zh_CN.UTF-8"
LC_COLLATE="zh_CN.UTF-8"
LC_MONETARY="zh_CN.UTF-8"
LC_MESSAGES="zh_CN.UTF-8"
LC_PAPER="zh_CN.UTF-8"
LC_NAME="zh_CN.UTF-8"
LC_ADDRESS="zh_CN.UTF-8"
LC_TELEPHONE="zh_CN.UTF-8"
```

```
LC_MEASUREMENT="zh_CN.UTF-8"
LC_IDENTIFICATION="zh_CN.UTF-8"
LC_ALL=
```

3 If the values include `"zh_CN.UTF-8"`, no changes are required. If the values do not include `"zh_CN.UTF-8"`, go to step 4.

4 Edit the **/etc/sysconfig/i18n** file with a text editor.

5 In the file, apply the following changes:

Current entry:

```
LANG="zh_CN.GB18030"
SUPPORTED="zh_CN.GB18030:zh_CH.GB2312:zh_CN:zh"
```

Updated entry:

```
LANG="zh_CN.UTF-8"
SUPPORTED="zh_CN.UTF-
8:zh_CN.GB18030:zh_CH.GB2312:zh_CN:zh"
```

6 Log out and then log in to the operating system.

When you switch from any other language, ensure that this fix is still valid. If not, repeat this procedure.

Disabling the Whitelist Feature in Firefox

Firefox has a "whitelist" security feature that requires user permission to install plugins for each distinct site that hosts a plugin. If enabled, the whitelist feature requires you to install a console redirection viewer for each iDRAC you visit, even though the viewer versions are identical.

To disable the whitelist feature and avoid unnecessary plugin installations, perform the following steps:

1 Open a Firefox Web browser window.

2 In the address field, type `about:config` and press <Enter>:

3 In the **Preference Name** column, locate and double-click **xpinstall.whitelist.required**.

The values for **Preference Name**, **Status**, **Type**, and **Value** change to bold text. The **Status** value changes to **user set** and the **Value** value changes to **false**.

4 In the **Preferences Name** column, locate **xpinstall.enabled**.

Ensure that **Value** is **true**. If not, double-click **xpinstall.enabled** to set **Value** to **true**.

Installing a Java Runtime Environment (JRE)

NOTE: If you use the Internet Explorer browser, an ActiveX control is provided for the console viewer. You can also use the Java console viewer with Internet Explorer if you install a JRE and configure the console viewer in iDRAC web interface before you launch the viewer. See "Configuring Console Redirection in the iDRAC Web Interface" on page 123 for more information.

You can choose to use the Java viewer instead before you launch the viewer.

If you use the Firefox browser you must install a JRE (or a Java Development Kit [JDK]) to use the console redirection feature. The console viewer is a Java application that is downloaded to the management station from the iDRAC Web interface and then launched with Java Web Start on the management station.

Go to **java.sun.com** to install a JRE or JDK. Version 1.6 (Java 6.0) or higher is recommended.

Installing Telnet or SSH Clients

By default, the iDRAC telnet service is disabled and the SSH service is enabled. Since telnet is an insecure protocol, you should use it only if you cannot install an SSH client or your network connection is otherwise secured.

NOTE: There can be only one active telnet or SSH connection to the iDRAC at a time. When there is an active connection, other connection attempts are denied.

Telnet with iDRAC

Telnet is included in Microsoft® Windows® and Linux operating systems and can be run from a command shell. You may also choose to install a commercial or freely available telnet client with more convenience features than the standard version included with your operating system.

If your management station is running Windows XP or Windows 2003, you may experience an issue with the characters in an iDRAC telnet session.This issue may occur as a frozen login where the return key does not respond and the password prompt does not appear.

To fix this issue, download hotfix 824810 from the Microsoft Support website at **support.microsoft.com**. See Microsoft Knowledge Base article 824810 for more information.

Configuring the Backspace Key For Your Telnet Session

Depending on the telnet client, using the <Backspace> key may produce unexpected results. For example, the session may echo `^h`. However, most Microsoft and Linux telnet clients can be configured to use the <Backspace> key.

To configure Microsoft telnet clients to use the <Backspace> key, perform the following steps:

1. Open a command prompt window (if required).
2. If you are not running a telnet session, type:

   ```
   telnet
   ```

   If you are running a telnet session, press <Ctrl><]>.
3. At the prompt, type:

   ```
   set bsasdel
   ```

   The following message appears:

   ```
   Backspace will be sent as delete.
   ```

To configure a Linux telnet session to use the <Backspace> key, perform the following steps:

1 Open a shell and type:

```
stty erase ^h
```

2 At the prompt, type:

```
telnet
```

SSH With iDRAC

Secure Shell (SSH) is a command line connection with the same capabilities as a telnet session, but with session negotiation and encryption to improve security. The iDRAC supports SSH version 2 with password authentication. SSH is enabled by default on the iDRAC.

You can use PuTTY (Windows) or `OpenSSH` (Linux) on a management station to connect to the managed server's iDRAC. When an error occurs during the login procedure, the **ssh** client issues an error message. The message text is dependent on the client and is not controlled by the iDRAC.

NOTE: `OpenSSH` should be run from a VT100 or ANSI terminal emulator on Windows. Running `OpenSSH` at the Windows command prompt does not result in full functionality (that is, some keys do not respond and no graphics are displayed).

Only one telnet or SSH session is supported at any given time. The session timeout is controlled by the `cfgSsnMgtSshIdleTimeout` property as described in "iDRAC Property Database Group and Object Definitions" on page 253.

The iDRAC SSH implementation supports multiple cryptography schemes, as shown in Table 3-1.

NOTE: SSHv1 is not supported.

Table 3-1. Cryptography Schemes

Scheme Type	Scheme
Asymmetric Cryptography	Diffie-Hellman DSA/DSS 512-1024 (random) bits per NIST specification
Symmetric Cryptography	• AES256-CBC • RIJNDAEL256-CBC • AES192-CBC • RIJNDAEL192-CBC • AES128-CBC • RIJNDAEL128-CBC • BLOWFISH-128-CBC • 3DES-192-CBC • ARCFOUR-128
Message Integrity	• HMAC-SHA1-160 • HMAC-SHA1-96 • HMAC-MD5-128 • HMAC-MD5-96
Authentication	• Password

Installing a TFTP Server

NOTE: If you use only the iDRAC Web interface to transfer SSL certificates and upload new iDRAC firmware, no TFTP server is required.

Trivial File Transfer Protocol (TFTP) is a simplified form of the File Transfer Protocol (FTP). It is used with the SM-CLP and RACADM command line interfaces to transfer files to and from the iDRAC.

The only times when you need to copy files to or from the iDRAC are when you update the iDRAC firmware or install certificates on the iDRAC. If you choose to use SM-CLP or RACADM when you perform these tasks, a TFTP server must be running on a computer the iDRAC can access by IP number or DNS name.

You can use the **netstat -a** command on Windows or Linux operating systems to see if a TFTP server is already listening. Port 69 is the TFTP default port. If no server is running, you have the following options:

- Find another computer on the network running a TFTP service
- If you are using Linux, install a TFTP server from your distribution
- If you are using Windows, install a commercial or free TFTP server

Installing Dell OpenManage IT Assistant

Your system includes the Dell OpenManage System Management Software Kit. This kit includes, but is not limited to, the following components:

- *Dell Systems Management Consoles* CD — Contains all the latest Dell systems management console products, including Dell OpenManage IT Assistant.
- *Dell PowerEdge Service and Diagnostic Utilities* CD — Provides the tools you need to configure your system and delivers firmware, diagnostics, and Dell-optimized drivers for your system.
- *Dell PowerEdge Documentation* CD — Helps you stay current with documentation for systems, systems management software products, peripherals, and RAID controllers.
- Dell Support website and Readme files — Check Readme files and the Dell Support website at **support.dell.com** for the most recent information about your Dell products.

Use the *Dell System Management Consoles* CD to install the management console software, including Dell OpenManage IT Assistant, on the management station. For instructions on installing this software, see your *Quick Installation Guide*.

4

Configuring the Managed Server

This section describes tasks to set up the managed server to enhance your remote management capabilities. These tasks include installing the Dell Open Manage Server Administrator software and configuring the managed server to capture the last crash screen.

Installing the Software on the Managed Server

The Dell management software includes the following features:

- Local RACADM CLI — allows you to configure and administer the iDRAC from the managed system. It is a powerful tool for scripting configuration and management tasks.
- Server Administrator is required to use the iDRAC last crash screen feature.
- Server Administrator — a Web interface that allows you to administer the remote system from a remote host on the network.
- Server Administrator Instrumentation Service — provides access to detailed fault and performance information gathered by industry-standard systems management agents and allows remote administration of monitored systems, including shutdown, startup, and security.
- Server Administration Storage Management Service — provides storage management information in an integrated graphical view.
- Server Administrator Logs — displays logs of commands issued to or by the system, monitored hardware events, POST events, and system alerts. You can view logs on the home page, print or save them as reports, and send them by e-mail to a designated service contact.

Use the *Dell PowerEdge Installation and Server Management* CD to install Server Administrator. For instructions on installing this software, see your *Quick Installation Guide*.

Configuring the Managed Server to Capture the Last Crash Screen

The iDRAC can capture the last crash screen so that you can view it in the Web interface to help troubleshoot the cause of the managed system crash. Follow these steps to enable the last crash screen feature.

1. Install the managed server software. For more information about installing the managed server software, see the *Server Administrator User's Guide*.
2. If you are running a Microsoft® Windows® operating system, ensure that the Automatically Reboot feature is deselected in the **Windows Startup and Recovery Settings**. See "Disabling the Windows Automatic Reboot Option" on page 53.
3. Enable the Last Crash Screen (disabled by default) in the iDRAC Web interface.

   To enable the Last Crash Screen in the iDRAC Web interface, click **System**→ **Remote Access**→ **iDRAC**→ **Network/Security**→ **Services**, then check the **Enable** checkbox under the Automatic System Recovery Agent Settings heading.

   To enable the Last Crash Screen using local RACADM, open a command prompt on the managed system and type the following command:

   ```
   racadm config -g cfgRacTuning -o
   cfgRacTuneAsrEnable 1
   ```
4. In the Server Administrator web-based interface, enable the **Auto Recovery** timer and set the **Auto Recovery** action to **Reset**, **Power Off**, or **Power Cycle**.

   For information about how to configure the **Auto Recovery** timer, see the *Server Administrator User's Guide*. To ensure that the last crash screen can be captured, the **Auto Recovery** timer should be set to 60 seconds. The default setting is 480 seconds.

   The last crash screen is not available when the **Auto Recovery** action is set to **Shutdown** or **Power Cycle** if the managed server is powered off.

Disabling the Windows Automatic Reboot Option

To ensure that the iDRAC can capture the last crash screen, disable the **Automatic Reboot** option on managed servers running Microsoft Windows Server® or Windows Vista®.

1. Open the Windows **Control Panel** and double-click the **System** icon.
2. Click the **Advanced** tab.
3. Under **Startup and Recovery**, click **Settings**.
4. Deselect the **Automatically Reboot** check box.
5. Click **OK** twice.

5

Configuring the iDRAC Using the Web Interface

The iDRAC provides a Web interface that enables you to configure the iDRAC properties and users, perform remote management tasks, and troubleshoot a remote (managed) system for problems. For everyday systems management, use the iDRAC Web interface. This chapter provides information about how to perform common systems management tasks with the iDRAC Web interface and provides links to related information.

Most Web interface configuration tasks can also be performed with local RACADM commands or with SM-CLP commands.

Local RACADM commands are executed from the managed server. For more information about local RACADM, see "Using the Local RACADM Command Line Interface" on page 149.

SM-CLP commands are executed in a shell that can be accessed remotely with a telnet or SSH connection. For more information about SM-CLP, see "Using the iDRAC SM-CLP Command Line Interface" on page 173.

Accessing the Web Interface

To access the iDRAC Web interface, perform the following steps:

1 Open a supported Web browser window.

See "Supported Web Browsers" on page 23 for more information.

2 In the **Address** field, type `https://<iDRAC-IP-address>` and press <Enter>.

If the default HTTPS port number (port 443) has been changed, type:

```
https://<iDRAC-IP-address>:<port-number>
```

where *iDRAC-IP-address* is the IP address for the iDRAC and *port-number* is the HTTPS port number.

The iDRAC **Login** window appears.

Logging In

You can log in as either an iDRAC user or as a Microsoft® Active Directory® user. The default user name and password are **root** and **calvin**, respectively.

You must have been granted **Login to iDRAC** privilege by the administrator to log in to the iDRAC.

To log in, perform the following steps:

1. In the **Username** field, type one of the following:
   - Your iDRAC user name.

     The user name for local users is case sensitive. Examples are `root`, `it_user`, or john_doe.
   - Your Active Directory user name.

     Active Directory names can be entered in any of the forms <*domain*>\<*username*>, <*domain*>/<*username*>, or <*user*>@<*domain*>. They are not case sensitive. Examples are `dell.com\john_doe,`or `JOHN_DOE@DELL.COM`.
2. In the **Password** field, type your iDRAC user password or Active Directory user password. Passwords are case sensitive.
3. Click **OK** or press <Enter>.

Logging Out

1. In the upper-right corner of the main window, click **Logout** to close the session.
2. Close the browser window.

NOTE: The **Logout** button does not appear until you log in.

NOTE: Closing the browser without gracefully logging out may cause the session to remain open until it times out. It is strongly recommended that you click the logout button to end the session; otherwise, the session may remain active until the session timeout is reached.

NOTE: Closing the iDRAC Web interface within Microsoft Internet Explorer using the close button ("x") at the top right corner of the window may generate an application error. To fix this issue, download the latest Cumulative Security Update for Internet Explorer from the Microsoft Support website, located at support.microsoft.com.

Configuring the iDRAC NIC

This section assumes that the iDRAC has already been configured and is accessible on the network. See "Configure iDRAC Networking" on page 30 for help with the initial iDRAC network configuration.

Configuring the Network and IPMI LAN Settings

NOTE: You must have **Configure iDRAC** privilege to perform the following steps.

NOTE: Most DHCP servers require a server to store a client identifier token in its reservations table. The client (iDRAC, for example) must provide this token during DHCP negotiation. The iDRAC supplies the client identifier option using a one-byte interface number (0) followed by a six-byte MAC address.

1. Click **System**→ **Remote Access**→ **iDRAC**.
2. Click the **Network/Security** tab to open the **Network Configuration** page.

   Table 5-1 and Table 5-2 describe the **Network Settings** and **IPMI LAN Settings** on the **Network** page.
3. When you have completed entering the required settings, click **Apply**.
4. Click the appropriate button to continue. See Table 5-3.

Table 5-1. Network Settings

Setting	Description
Enable NIC	When checked, indicates that the NIC is enabled and activates the remaining controls in this group. When a NIC is disabled, all communication to and from the iDRAC via the network is blocked. The default is **off**.
Media Access Control (MAC) Address	Displays the Media Access Control (MAC) address that uniquely identifies each node in a network. The MAC address cannot be changed.

Table 5-1. Network Settings *(continued)*

Setting	Description
Use DHCP (For NIC IP Address)	Prompts the iDRAC to obtain an IP address for the NIC from the Dynamic Host Configuration Protocol (DHCP) server. Also deactivates the **Static IP Address**, **Static Subnet Mask**, and **Static Gateway** controls. The default is **off**.
Static IP Address	Allows you to enter or edit a static IP address for the iDRAC NIC. To change this setting, deselect the **Use DHCP (For NIC IP Address)** checkbox.
Static Subnet Mask	Allows you to enter or edit a subnet mask for the iDRAC NIC. To change this setting, first deselect the **Use DHCP (For NIC IP Address)** checkbox.
Static Gateway	Allows you to enter or edit a static gateway for the iDRAC NIC. To change this setting, first deselect the **Use DHCP (For NIC IP Address)** checkbox.
Use DHCP to obtain DNS server addresses	Enable DHCP to obtain DNS server addresses by selecting the **Use DHCP to obtain DNS server addresses** checkbox. When not using DHCP to obtain the DNS server addresses, provide the IP addresses in the **Static Preferred DNS Server** and **Static Alternate DNS Server** fields. The default is **off**. **NOTE:** When the **Use DHCP to obtain DNS server addresses** checkbox is selected, IP addresses cannot be entered into the **Static Preferred DNS Server** and **Static Alternate DNS Server** fields.
Static Preferred DNS Server	Allows the user to enter or edit a static IP address for the preferred DNS server. To change this setting, first deselect the **Use DHCP to obtain DNS server addresses** checkbox.
Static Alternate DNS Server	Uses the secondary DNS server IP address when **Use DHCP to obtain DNS server addresses** is **not selected**. Enter an IP address of 0.0.0.0 if there is no alternate DNS server.
Register iDRAC on DNS	Registers the iDRAC name on the DNS server. The default is **Disabled**.

Table 5-1. Network Settings *(continued)*

Setting	Description
DNS iDRAC Name	Displays the iDRAC name only when **Register iDRAC on DNS** is selected. The default name is idrac-*service_tag*, where *service_tag* is the service tag number of the Dell server. For example: idrac-00002.
Use DHCP for DNS Domain Name	Uses the default DNS domain name. When the box is not selected and the **Register iDRAC on DNS** option is selected, modify the DNS domain name in the **DNS Domain Name** field. The default is **Disabled**. **NOTE:** To select the **Use DHCP for DNS Domain Name** checkbox, also select the **Use DHCP (For NIC IP Address)** checkbox.
DNS Domain Name	The default **DNS Domain Name** is blank. When the **Use DHCP for DNS Domain Name** checkbox is selected, this option is grayed out and the field cannot be modified.
Community String	Contains the community string to use in **Simple Network Management Protocol (SNMP)** alert traps sent from the iDRAC. SNMP alert traps are transmitted by the iDRAC when a platform event occurs. The default is **public**.
SMTP Server Address	The IP address of the **Simple Mail Transfer Protocol (SMTP)** server that the iDRAC communicates with to send e-mail alerts when a platform event occurs. The default is **127.0.0.1**.

Table 5-2. IPMI LAN Settings

Setting	Description
Enable IPMI Over LAN	When checked, indicates that the IPMI LAN channel is enabled. The default is **off**.
Channel Privilege Level Limit	Configures the maximum privilege level, for the user, that can be accepted on the LAN channel. Select one of the following options: **Administrator**, **Operator**, or **User**. The default is **Administrator**.
Encryption Key	Configures the encryption key: 0 to 20 hexadecimal characters (with no blanks allowed). The default is blank.

Table 5-3. Network Configuration Page Buttons

Button	Description
Advanced Settings	Opens the **Network Security** page, allowing the user to enter IP Range, and IP Blocking attributes.
Print	Prints the **Network Configuration** values that appear on the screen.
Refresh	Reloads the **Network Configuration** page.
Apply	Saves any new settings made to the network configuration page. **NOTE:** Changes to the NIC IP address settings will close all user sessions and require users to reconnect to the iDRAC Web interface using the updated IP address settings. All other changes will require the NIC to be reset, which may cause a brief loss in connectivity.

Configuring IP Filtering and IP Blocking

NOTE: You must have **Configure iDRAC** permission to perform the following steps.

1. Click **System**→ **Remote Access**→ **iDRAC** and then click the **Network/Security** tab to open the **Network Configuration** page.
2. Click **Advanced Settings** to configure the network security settings.

   Table 5-4 describes the **Network Security** page settings.
3. When you have finished configuring the settings, click **Apply**.
4. Click the appropriate button to continue. See Table 5-5.

Table 5-4. Network Security Page Settings

Settings	Description
IP Range Enabled	Enables the IP Range checking feature, which defines a range of IP addresses that can access the iDRAC. The default is **off**.
IP Range Address	Determines the acceptable IP subnet address. The default is **192.168.1.0**.
IP Range Subnet Mask	Defines the significant bit positions in the IP address. The subnet mask should be in the form of a netmask, where the more significant bits are all 1's with a single transition to all zeros in the lower-order bits. The default is **255.255.255.0**.

Table 5-4. Network Security Page Settings *(continued)*

Settings	Description
IP Blocking Enabled	Enables the IP address blocking feature, which limits the number of failed login attempts from a specific IP address for a preselected time span. The default is **off**.
IP Blocking Fail Count	Sets the number of login failures attempted from an IP address before the login attempts are rejected from that address. The default is **10**.
IP Blocking Fail Window	Determines the time span in seconds within which IP Block Fail Count failures must occur to trigger the IP Block Penalty Time. The default is **3600**.
IP Blocking Penalty Time	The time span in seconds that login attempts from an IP address with excessive failures are rejected. The default is **3600.**

Table 5-5. Network Security Page Buttons

Button	Description
Print	Prints the **Network Security** values that appear on the screen.
Refresh	Reloads the **Network Security** page.
Apply	Saves any new settings that you made to the **Network Security** page.
Go Back to Network Page	Returns to the **Network** page.

Configuring Platform Events

Platform event configuration provides a mechanism for configuring the iDRAC to perform selected actions on certain event messages. The actions include no action, reboot system, power cycle system, power off system, and generate an alert (Platform Event Trap [PET] and/or e-mail).

The filterable platform events are listed in Table 5-6.

.

Table 5-6. Filterable Platform Events

Index	Platform Event
1	Battery Warning Assert
2	Battery Critical Assert
3	Discrete Voltage Critical Assert
4	Temperature Warning Assert
5	Temperature Critical Assert
6	Redundancy Degraded
7	Redundancy Lost
8	Processor Warning Assert
9	Processor Critical Assert
10	Processor Absent Assert
11	Event Log Critical Assert
12	Watchdog Critical Assert

When a platform event occurs (for example, a battery warning assert), a system event is generated and recorded in the System Event Log (SEL). If this event matches a platform event filter (PEF) that is enabled and you have configured the filter to generate an alert (PET or e-mail), then a PET or e-mail alert is sent to one or more configured destinations.

If the same platform event filter is also configured to perform an action (such as rebooting the system), the action is performed.

Configuring Platform Event Filters (PEF)

NOTE: Configure platform event filters before you configure the platform event traps or e-mail alert settings.

1. Log in to the iDRAC Web interface. See "Accessing the Web Interface" on page 55.
2. Click **System** and then the **Alert Management** tab.

3 On the Platform Events page, enable **Alert Generation** for an event by clicking the corresponding **Generate Alert** checkbox for that event.

NOTE: You can enable or disable Alert Generation for all events by clicking the checkbox next to the Generate Alert column heading.

4 Click the radio button below the action you would like to enable for each event. Only one action can be set for each event.

5 Click **Apply**.

NOTE: **Generate Alert** must be enabled for an alert to be sent to any valid, configured destination (PET or e-mail).

Configuring Platform Event Traps (PET)

NOTE: You must have **Configure iDRAC** permission to add or enable/disable an SNMP alert. The following options will not be available if you do not have **Configure iDRAC** permission.

1 Log in to the remote system using a supported Web browser. See "Accessing the Web Interface" on page 55.

2 Ensure that you followed the procedures in "Configuring Platform Event Filters (PEF)" on page 62.

3 Configure your PET destination IP address:

a Click the **Enable** checkbox next to the **Destination Number** you would like to activate.

b Enter an IP address in the **Destination IP Address** box.

NOTE: The destination community string must be the same as the iDRAC community string.

c Click **Apply**.

NOTE: To successfully send a trap, configure the **Community String** value on the **Network Configuration** page. The **Community String** value indicates the community string to use in a Simple Network Management Protocol (SNMP) alert trap sent from the iDRAC. SNMP alert traps are transmitted by the iDRAC when a platform event occurs. The default setting for the **Community String** is **Public**.

d Click **Send** to test the configured alert (if desired).

e Repeat step a through step d for any remaining destination numbers.

Configuring E-Mail Alerts

1 Log in to the remote system using a supported Web browser.

2 Ensure that you followed the procedures in "Configuring Platform Event Filters (PEF)" on page 62.

3 Configure your e-mail alert settings.

   a On the **Alert Management** tab, click **Email Alert Settings**.

4 Configure your e-mail alert destination.

   a In the **Email Alert Number** column, click a destination number. There are four possible destinations to receive alerts.

   b Ensure that the **Enabled** checkbox is selected.

   c In the **Destination Email Address** field, type a valid e-mail address.

   d Click **Apply**.

   NOTE: To successfully send a test e-mail, the **SMTP Server Address** must be configured on the **Network Configuration** page. The IP address of the **SMTP Server** communicates with the iDRAC to send e-mail alerts when a platform event occurs.

   e Click **Send** to test the configured e-mail alert (if desired).

   f Repeat step a through step e for any remaining e-mail alert settings.

Configuring IPMI

1 Log in to the remote system using a supported Web browser.

2 Configure IPMI over LAN.

   a Click **System**→ **Remote Access**→ iDRAC, then click the **Network/Security**.

   b In the **Network Configuration** page under **IPMI LAN Settings**, select **Enable IPMI Over LAN**.

   c Update the IPMI LAN channel privileges, if required:

   NOTE: This setting determines the IPMI commands that can be executed from the IPMI over LAN interface. For more information, see the IPMI 2.0 specifications.

Under **IPMI LAN Settings**, click the **Channel Privilege Level Limit** drop-down menu, select **Administrator**, **Operator**, or **User** and click **Apply**.

d Set the IPMI LAN channel encryption key, if required.

NOTE: The iDRAC IPMI supports the RMCP+ protocol.

NOTE: The encryption key must consist of an even number of hexadecimal characters with a maximum length of 20 characters.

Under **IPMI LAN Settings** in the **Encryption Key field**, type the encryption key.

e Click **Apply**.

3 Configure IPMI Serial over LAN (SOL).

a Click **System**→ **Remote Access**→ **iDRAC**.

b Click the **Network Security** tab, then click **Serial Over LAN**.

c On the **Serial Over LAN Configuration** page, click the **Enable Serial Over LAN** checkbox to enable Serial over LAN.

d Update the IPMI SOL baud rate.

NOTE: To redirect the serial console over the LAN, ensure that the SOL baud rate is identical to your managed server's baud rate.

Click the **Baud Rate** drop-down menu to select a data speed of 19.2 kbps, 57.6 kbps or 115.2 kbps.

e Click **Apply**.

Adding and Configuring iDRAC Users

To manage your system with the iDRAC and maintain system security, create unique users with specific administrative permissions (or *role-based authority*).

To add and configure iDRAC users, perform the following steps:

NOTE: You must have **Configure iDRAC** permission to perform the following steps.

1 Click **System**→ **Remote Access**→ **iDRAC** and then click the **Network/Security** tab.

2 Open the **Users** page to configure users.

The **Users** page displays each user's **User ID, State, Username, IPMI LAN Privileges**, **iDRAC Privileges**, and **Serial Over LAN**.

NOTE: User-1 is reserved for the IPMI anonymous user and is not configurable.

3 In the **User ID** column, click a user ID number.

4 On the **User Configuration** page, configure the user's properties and privileges.

Table 5-7 describes the **General** settings for configuring an iDRAC user name and password.

Table 5-8 describes the **IPMI LAN Privileges** for configuring the user's LAN privileges.

Table 5-9 describes the **User Group** permissions for the **IPMI LAN Privileges** and the **iDRAC User Privileges** settings.

Table 5-10 describes the **iDRAC Group** permissions. If you add an **iDRAC User Privilege** to the **Administrator**, **Power User**, or **Guest User**, the **iDRAC Group** will change to the **Custom** group.

5 When completed, click **Apply**.

6 Click the appropriate button to continue. See Table 5-11.

Table 5-7. General Properties

Property	Description
User ID	Contains one of 16 preset User ID numbers. This field cannot be edited.
Enable User	When checked, indicates that the user's access to the iDRAC is enabled. When unchecked, user access is disabled.
Username	Specifies an iDRAC user name with up to 16 characters. Each user must have a unique user name. **NOTE:** User names on the iDRAC cannot include the / (forward slash) or . (period) characters. **NOTE:** If the user name is changed, the new name will not appear in the user interface until the next user login.

Table 5-7. General Properties *(continued)*

Property	Description
Change Password	Enables the **New Password** and **Confirm New Password** fields. When unchecked, the user's Password cannot be changed.
New Password	Enables editing the iDRAC user's password. Enter a **Password** with up to 20 characters. The characters will not display.
Confirm New Password	Retype the iDRAC user's password to confirm.

Table 5-8. IPMI LAN User Privileges

Property	Description
Maximum LAN User Privilege Granted	Specifies the user's maximum privilege on the IPMI LAN channel to one of the following user groups: **None**, **Administrator**, **Operator**, or **User**.
Enable Serial Over LAN	Allows the user to use IPMI Serial Over LAN. When checked, this privilege is enabled.

Table 5-9. iDRAC User Privileges

Property	Description
iDRAC Group	Specifies the user's maximum iDRAC user privilege as one of the following: **Administrator**, **Power User**, **Guest User**, **Custom**, or **None**. See Table 5-10 for **iDRAC Group** permissions.
Login to iDRAC	Enables the user to log in to the iDRAC.
Configure iDRAC	Enables the user to configure the iDRAC.
Configure Users	Enables the user to allow specific users to access the system.
Clear Logs	Enables the user to clear the iDRAC logs.
Execute Server Control Commands	Enables the user to execute RACADM commands.

Table 5-9. iDRAC User Privileges *(continued)*

Property	Description
Access Console Redirection	Enables the user to run Console Redirection.
Access Virtual Media	Enables the user to run and use Virtual Media.
Test Alerts	Enables the user to send test alerts (e-mail and PET) to a specific user.
Execute Diagnostic Commands	Enables the user to run diagnostic commands.

Table 5-10. iDRAC Group Permissions

User Group	Permissions Granted
Administrator	**Login to iDRAC**, **Configure iDRAC**, **Configure Users**, **Clear Logs**, **Execute Server Control Commands**, **Access Console Redirection**, **Access Virtual Media**, **Test Alerts**, **Execute Diagnostic Commands**
Power User	**Login to iDRAC**, **Clear Logs**, **Execute Server Control Commands**, **Access Console Redirection**, **Access Virtual Media**, **Test Alerts**
Guest User	**Login to iDRAC**
Custom	Selects any combination of the following permissions: **Login to iDRAC**, **Configure iDRAC**, **Configure Users**, **Clear Logs**, **Execute Server Action Commands**, **Access Console Redirection**, **Access Virtual Media**, **Test Alerts**, **Execute Diagnostic Commands**
None	No assigned permissions

Table 5-11. User Configuration Page Buttons

Button	Action
Print	Prints the **User Configuration** values that appear on the screen.
Refresh	Reloads the **User Configuration** page.

Table 5-11. User Configuration Page Buttons *(continued)*

Button	Action
Apply	Saves any new settings made to the user configuration.
Go Back To Users Page	Returns to the **Users Page**.

Securing iDRAC Communications Using SSL and Digital Certificates

This section provides information about the following data security features that are incorporated in your iDRAC:

- Secure Sockets Layer (SSL)
- Certificate Signing Request (CSR)
- Accessing the SSL main menu
- Generating a new CSR
- Uploading a server certificate
- Viewing a server certificate

Secure Sockets Layer (SSL)

The iDRAC includes a Web server that is configured to use the industry-standard SSL security protocol to transfer encrypted data over a network. Built upon public-key and private-key encryption technology, SSL is a widely accepted technology for providing authenticated and encrypted communication between clients and servers to prevent eavesdropping across a network.

An SSL-enabled system can perform the following tasks:

- Authenticate itself to an SSL-enabled client
- Allow the client to authenticate itself to the server
- Allow both systems to establish an encrypted connection

The encryption process provides a high level of data protection. The iDRAC employs the 128-bit SSL encryption standard, the most secure form of encryption generally available for Internet browsers in North America.

The iDRAC Web server has a Dell self-signed SSL digital certificate (Server ID) by default. To ensure high security over the Internet, replace the Web server SSL certificate with a certificate signed by a well-known certificate authority. To initiate the process of obtaining a signed certificate, you can use the iDRAC Web interface to generate a Certificate Signing Request (CSR) with your company's information. You can then submit the generated CSR to a CA such as VeriSign or Thawte.

Certificate Signing Request (CSR)

A CSR is a digital request to a Certificate Authority (CA) for a secure server certificate. Secure server certificates allow clients of the server to trust the identity of the server they have connected to and to negotiate an encrypted session with the server.

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 a CSR, they review and verify the information the CSR contains. If the applicant meets the CA's security standards, the CA issues a digitally-signed certificate that uniquely identifies that applicant for transactions over networks and on the Internet.

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

Accessing the SSL Main Menu

1. Click **System**→ **Remote Access**→ **iDRAC**, then click the **Network/Security** tab.
2. Click **SSL** to open the **SSL Main Menu** page.

Use the **SSL Main Menu** page to generate a CSR to send to a CA. The CSR information is stored on the iDRAC firmware.

Table 5-12 describes the options available when generating a CSR.

Table 5-13 describes the available buttons on the **SSL Main Menu** page.

Table 5-12. SSL Main Menu Options

Field	Description
Generate a New Certificate Signing Request (CSR)	Select the option and click **Next** to open the **Generate Certificate Signing Request** (CSR) page. **NOTE:** Each new CSR overwrites any previous CSR on the firmware. For a CA to accept your CSR, the CSR in the firmware must match the certificate returned from the CA.
Upload Server Certificate	Select the option and click **Next** to open the **Certificate Upload** page and upload the certificate sent to you by the CA. **NOTE:** Only X509, Base 64-encoded certificates are accepted by the iDRAC. DER-encoded certificates are not accepted.
View Server Certificate	Select the option and click **Next** to open the **View Server Certificate** page and view an existing server certificate.

Table 5-13. SSL Main Menu Buttons

Button	Description
Print	Prints the **SSL Main Menu** values that appear on the screen.
Refresh	Reloads the **SSL Main Menu** page.
Next	Processes the information on the **SSL Main Menu** page and continues to the next step.

Generating a New Certificate Signing Request

NOTE: Each new CSR overwrites any previous CSR data stored in the firmware. The CSR in the firmware must match the certificate returned from the CA. Otherwise, the iDRAC will not accept the certificate.

1 On the **SSL Main Menu** page, select **Generate a New Certificate Signing Request (CSR)** and click **Next**.

2 On the **Generate Certificate Signing Request (CSR)** page, enter a value for each CSR attribute.

Table 5-14 describes the **Generate Certificate Signing Request (CSR)** page options.

3 Click **Generate** to create the CSR.

4 Click **Download** to save the CSR file to your local computer.

5 Click the appropriate button to continue. See Table 5-15.

Table 5-14. Generate Certificate Signing Request (CSR) Page Options

Field	Description
Common Name	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 Name	The name associated with this organization (for example, XYZ Corporation). Only alphanumeric characters, hyphens, underscores, periods and spaces are valid.
Organization Unit	The name associated with an organizational unit, such as a department (for example, Information Technology). Only alphanumeric characters, hyphens, underscores, periods, and spaces are valid.
Locality	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 other character.
State Name	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.
Country Code	The name of the country where the entity applying for certification is located.
Email	The e-mail address associated with the CSR. Type the company’s e-mail address, or any e-mail address associated with the CSR. This field is optional.

Table 5-15. Generate Certificate Signing Request (CSR) Page Buttons

Button	Description
Print	Prints the **Generate Certificate Signing Request** values that appear on the screen.
Refresh	Reloads the **Generate Certificate Signing Request** page.
Generate	Generates a CSR and then prompts the user to save it to a specified directory.
Download	Downloads the certificate to the local computer.
Go Back to SSL Main Menu	Returns the user to the **SSL Main Menu** page.

Uploading a Server Certificate

1 In the **SSL Main Menu** page, select **Upload Server Certificate** and click **Next**.

The **Certificate Upload** page appears.

2 In the **File Path** field, type the path to the certificate or click **Browse** to navigate to the certificate file.

NOTE: The **File Path** value displays the relative file path of the certificate you are uploading. You must type the absolute file path, which includes the full path and the complete file name and file extension.

3 Click **Apply**.

4 Click the appropriate button to continue. See Table 5-16.

Table 5-16. Certificate Upload Page Buttons

Button	Description
Print	Prints the values that appear on the **Certificate Upload** page.
Refresh	Reloads the **Certificate Upload** page.
Apply	Applies the certificate to the iDRAC firmware.
Go Back to SSL Main Menu	Returns the user to the **SSL Main Menu** page.

Viewing a Server Certificate

1 On the **SSL Main Menu** page, select **View Server Certificate** and click **Next**.

Table 5-17 describes the fields and associated descriptions listed in the **Certificate** window.

2 Click the appropriate button to continue. See Table 5-18.

Table 5-17. Certificate Information

Field	Description
Serial Number	Certificate serial number
Subject Information	Certificate attributes entered by the subject
Issuer Information	Certificate attributes returned by the issuer
Valid From	Issue date of the certificate
Valid To	Expiration date of the certificate

Table 5-18. View Server Certificate Page Buttons

Button	Description
Print	Prints the **View Server Certificate** values that appear on the screen.
Refresh	Reloads the **View Server Certificate** page.
Go Back to SSL Main Menu	Return to the **SSL Main Menu** page.

Configuring and Managing Active Directory Certificates

NOTE: You must have **Configure iDRAC** permission to configure Active Directory and upload, download, and view an Active Directory certificate.

NOTE: For more information about Active Directory configuration and how to configure Active Directory with the standard schema or an extended schema, see "Using the iDRAC with Microsoft Active Directory" on page 89.

To access the **Active Directory Main Menu**:

1. Click **System**→ **Remote Access**→ **iDRAC,** and then click the **Network/Security** tab.
2. Click **Active Directory** to open the **Active Directory Main Menu** page.

   Table 5-19 lists the **Active Directory Main Menu** page options.
3. Click the appropriate button to continue. See Table 5-20.

Table 5-19. Active Directory Main Menu Page Options

Field	Description
Configure Active Directory	Configures the Active Directory **ROOT Domain Name**, **Active Directory Authentication Timeout**, **Active Directory Schema Selection**, **iDRAC Name**, **iDRAC Domain Name**, **Role Groups**, **Group Name**, **and Group Domain** settings.
Upload Active Directory CA Certificate	Uploads an Active Directory certificate to the iDRAC.
Download iDRAC Server Certificate	The **Windows Download Manager** downloads an iDRAC server certificate to the system.
View Active Directory CA Certificate	Displays an Active Directory Certificate that has been uploaded to the iDRAC.

Table 5-20. Active Directory Main Menu Page Buttons

Button	Definition
Print	Prints the **Active Directory Main Menu** values that appear on the screen.
Refresh	Reloads the **Active Directory Main Menu** page.
Next	Processes the information on the **Active Directory Main Menu** page and continues to the next step.

Configuring Active Directory (Standard Schema and Extended Schema)

1. On the **Active Directory Main Menu** page, select **Configure Active Directory** and click **Next**.

2 On the **Active Directory Configuration** page, enter the Active Directory settings.

Table 5-21 describes the **Active Directory Configuration and Management** page settings.

3 Click **Apply** to save the settings.

4 Click the appropriate button to continue. See Table 5-22.

5 To configure the Role Groups for Active Directory Standard Schema, click on the individual Role Group (1-5). See Table 5-23 and Table 5-24.

NOTE: To save the settings on the **Active Directory Configuration** page, click **Apply** before proceeding to the **Custom Role Group** page.

Table 5-21. Active Directory Configuration Page Settings

Setting	Description
Enable Active Directory	When checked, enables Active Directory. The default is **disabled**.
ROOT Domain Name	The Active Directory ROOT domain name. This default is blank. The name must be a valid domain name consisting of *x.y*, where *x* is a 1-254 character ASCII string with no spaces between characters, and *y* is a valid domain type such as com, edu, gov, int, mil, net, or org. The default is blank.
Timeout	The time, in seconds, to wait for Active Directory queries to complete. Minimum value is equal to or greater than 15 seconds. The default value is **120**.
Use Standard Schema	Uses standard schema with Active Directory.
Use Extended Schema	Uses the extended schema with Active Directory.
iDRAC Name	The name that uniquely identifies the iDRAC in Active Directory. This default is blank. The name must be a 1-254 character ASCII string with no spaces between characters.

Table 5-21. Active Directory Configuration Page Settings *(continued)*

Setting	Description
iDRAC Domain Name	The DNS name of the domain, where the Active Directory iDRAC object resides. This default is blank. The name must be a valid domain name consisting of *x.y*, where *x* is a 1-254 character ASCII string with no spaces between characters, and *y* is a valid domain type such as com, edu, gov, int, mil, net, or org.
Role Groups	The list of role groups associated with the iDRAC. To change the settings for a role group, click their role group number, in the role groups list.
Group Name	The name that identifies the role group in the Active Directory associated with the iDRAC. This default is blank.
Group Domain	The domain type where the Role Group resides.

Table 5-22. Active Directory Configuration Page Buttons

Button	Description
Print	Prints the **Active Directory Configuration** values that appear on the screen.
Refresh	Reloads the **Active Directory Configuration** page.
Apply	Saves any new settings made to the **Active Directory Configuration** page.
Go Back to Active Directory Main Menu	Returns to the **Active Directory Main Menu** page.

Table 5-23. Role Group Privileges

Setting	Description
Role Group Privilege Level	Specifies the user's maximum iDRAC user privilege as one of the following: **Administrator**, **Power User**, **Guest User**, **None**, or **Custom**. See Table 5-24 for **Role Group** permissions.

Table 5-23. Role Group Privileges *(continued)*

Setting	Description
Login to iDRAC	Allows the group log in access to the iDRAC.
Configure iDRAC	Allows the group permission to configure the iDRAC.
Configure Users	Allows the group permission to configure users.
Clear Logs	Allows the group permission to clear logs.
Execute Server Control Commands	Allows the group permission to execute server control commands.
Access Console Redirection	Allows the group access to Console Redirection.
Access Virtual Media	Allows the group access to Virtual Media.
Test Alerts	Allows the group to send test alerts (e-mail and PET) to a specific user.
Execute Diagnostic Commands	Allows the group permission to execute diagnostic commands.

Table 5-24. Role Group Permissions

Property	Description
Administrator	**Login to iDRAC**, **Configure iDRAC**, **Configure Users**, **Clear Logs**, **Execute Server Control Commands**, **Access Console Redirection**, **Access Virtual Media**, **Test Alerts**, **Execute Diagnostic Commands**
Power User	**Login to iDRAC**, **Clear Logs**, **Execute Server Control Commands**, **Access Console Redirection**, **Access Virtual Media**, **Test Alerts**
Guest User	**Login to iDRAC**

Table 5-24. Role Group Permissions *(continued)*

Property	Description
Custom	Selects any combination of the following permissions: **Login to iDRAC**, **Configure iDRAC**, **Configure Users**, **Clear Logs**, **Execute Server Action Commands**, **Access Console Redirection**, **Access Virtual Media**, **Test Alerts**, **Execute Diagnostic Commands**
None	No assigned permissions

Uploading an Active Directory CA Certificate

1 On the **Active Directory Main Menu** page, select **Upload Active Directory CA Certificate** and click **Next**.

2 On the **Certificate Upload page,** type the file path of the certificate in the **File Path** field, or click **Browse** to navigate to the certificate file.

NOTE: The **File Path** value displays the relative file path of the certificate you are uploading. You must type the absolute file path, which includes the full path and the complete file name and file extension.

Ensure that the domain controller's SSL certificates have been signed by the same Certificate Authority and that this Certificate is available on the management station accessing the iDRAC.

3 Click **Apply**.

4 Click the appropriate button to continue. See Table 5-25.

Table 5-25. Certificate Upload Page Buttons

Button	Description
Print	Prints the **Certificate Upload** values that appear on the screen.
Refresh	Reloads the **Certificate Upload** page.
Apply	Applies the certificate to the iDRAC firmware.
Go Back to Active Directory Main Menu	Returns to the **Active Directory Main Menu** page.

Downloading an iDRAC Server Certificate

1. On the **Active Directory Main Menu** page, select **Download iDRAC Server Certificate** and click **Next**.
2. Save the file to a directory on your system.
3. In the **Download Complete** window, click **Close**.

Viewing an Active Directory CA Certificate

Use the **Active Directory Main Menu** page to view a CA server certificate for your iDRAC.

1. On the **Active Directory Main Menu** page, select **View Active Directory CA Certificate** and click **Next**.

   Table 5-26 describes the fields and associated descriptions listed in the **Certificate** window.

2. Click the appropriate button to continue. See Table 5-27.

Table 5-26. Active Directory CA Certificate Information

Field	Description
Serial Number	Certificate serial number.
Subject Information	Certificate attributes entered by the subject.
Issuer Information	Certificate attributes returned by the issuer.
Valid From	Certificate issue date.
Valid To	Certificate expiration date.

Table 5-27. View Active Directory CA Certificate Page Buttons

Button	Description
Print	Prints the **Active Directory CA Certificate values that appear on the screen**.
Refresh	Reloads the **Active Directory CA Certificate** page.
Go Back to Active Directory Main Menu	Returns the user to the **Active Directory Main Menu** page.

Configuring Serial Over LAN

1. Click **System**→ **Remote Access**→ **iDRAC**→ **Network/Security**.
2. Click **Serial Over LAN** to open the **Serial Over LAN Configuration** page.

   Table 5-28 provides information about the **Serial Over LAN Configuration** page settings.
3. Click **Apply**.
4. Configure the advanced settings, if required. Otherwise, click the appropriate button to continue. See Table 5-29.

   To configure the advanced settings, perform the following steps:

   a. Click **Advanced Settings**.

   b. On the **Serial Over LAN Configuration Advanced Settings** page, configure the advanced settings as required. See Table 5-30.

   c. Click **Apply**.

   d. Click the appropriate button to continue. See Table 5-31.

Table 5-28. Serial Over LAN Configuration Page Settings

Setting	Description
Enable Serial Over LAN	When checked, the checkbox indicates that Serial Over LAN is enabled.
Baud Rate	Indicates the data speed. Select a data speed of **19.2 kbps**, **57.6 kbps**, or **115.2 kbps**.

Table 5-29. Serial Over LAN Configuration Page Buttons

Button	Description
Print	Prints the **Serial Over LAN Configuration** values that appear on the screen.
Refresh	Reloads the **Serial Over LAN Configuration** page.
Advanced Settings	Opens the **Serial Over LAN Configuration Advanced Settings** page.
Apply	Supplies any new settings that you make while viewing the **Serial Over LAN Configuration** page.

Table 5-30. Serial Over LAN Configuration Advanced Settings Page Settings

Setting	Description
Character Accumulate Interval	The amount of time that the iDRAC will wait before transmitting a partial SOL character data package. The time is measured in seconds.
Character Send Threshold	The iDRAC will send an SOL character data package containing the characters as soon as this number of characters (or greater) has been accepted. The threshold is measured in characters.

Table 5-31. Serial Over LAN Configuration Advanced Settings Page Buttons

Button	Description
Print	Prints the **Serial Over LAN Configuration Advanced Settings** values that appear on the screen.
Refresh	Reloads the **Serial Over LAN Configuration Advanced Settings** page.
Apply	Saves any new settings that you make while viewing the **Serial Over LAN Configuration Advanced Settings** page.
Go Back To Serial Over LAN Configuration Page	Returns the user to the **Serial Over LAN Configuration** page.

Configuring iDRAC Services

NOTE: To modify these settings, you must have **Configure iDRAC** permission.

NOTE: When you apply changes to services, the changes take effect immediately. Existing connections may be terminated without warning.

1 Click **System**→ **Remote Access**→ **iDRAC**, and then click the **Network/Security** tab.

2 Click **Services** to open the **Services** configuration page.

3 Configure the following services, as required:

- Web server — see Table 5-32 for Web server settings
- SSH — see Table 5-33 for SSH settings

- Telnet — see Table 5-34 for telnet settings
- Automated System Recovery Agent — see Table 5-35 for Automated System Recovery Agent settings

4 Click **Apply**.

5 Click the appropriate button to continue. See Table 5-36.

Table 5-32. Web Server Settings

Setting	Description
Enabled	Enables or disables the iDRAC web server. When checked, the checkbox indicates that the web server is enabled. The default is **enabled**.
Max Sessions	The maximum number of simultaneous sessions allowed for this system. This field is not editable. There can be four simultaneous sessions.
Current Sessions	The number of current sessions on the system, less than or equal to the **Max Sessions**. This field is not editable.
Timeout	The time, in seconds, that a connection is allowed to remain idle. The session is cancelled when the timeout is reached. Changes to the timeout setting take affect immediately and will reset the web server. Timeout range is 60 to 1920 seconds. The default is **300** seconds.
HTTP Port Number	The port on which the iDRAC listens for a browser connection. The default is **80**.
HTTPS Port Number	The port on which the iDRAC listens for a secure browser connection. The default is **443**.

Table 5-33. SSH Settings

Setting	Description
Enabled	Enables or disables SSH. When checked, the checkbox indicates that SSH is enabled.
Max Sessions	The maximum number of simultaneous sessions allowed for this system. Only one session is supported.
Active Sessions	The number of current sessions on the system.

Table 5-33. SSH Settings *(continued)*

Setting	Description
Timeout	The secure shell idle timeout, in seconds. Timeout range is 60 to 1920 seconds. Enter 0 seconds to disable the Timeout feature. The default is **300**.
Port Number	The port on which the iDRAC listens for an SSH connection. The default is **22**.

Table 5-34. Telnet Settings

Setting	Description
Enabled	Enables or disables telnet. When checked, telnet is enabled.
Max Sessions	The maximum number of simultaneous sessions allowed for this system. Only one session is supported.
Active Sessions	The number of current sessions on the system.
Timeout	The telnet idle timeout, in seconds. Timeout range is 60 to 1920 seconds. Enter 0 seconds to disable the Timeout feature. The default is **0**.
Port Number	The port on which the iDRAC listens for a telnet connection. The default is **23**.

Table 5-35. Automated System Recovery Agent Setting

Setting	Description
Enabled	Enables the Automated System Recovery Agent.

Table 5-36. Services Page Buttons

Button	Description
Print	Prints the **Services** page.
Refresh	Refreshes the **Services** page.
Apply Changes	Applies the **Services** page settings.

Updating the iDRAC Firmware

NOTICE: If the iDRAC firmware becomes corrupted, as could occur if the iDRAC firmware update progress is interrupted before it completes, you can recover the iDRAC using the CMC. See your *CMC Firmware User's Guide* for instructions.

NOTE: The firmware update, by default, retains the current iDRAC settings. During the update process, you have the option to reset the iDRAC configuration to the factory defaults. If you set the configuration to the factory defaults external network access will be disabled when the update completes. You must enable and configure the network using the iDRAC Configuration Utility or the CMC Web interface.

1 Start the iDRAC Web interface.

2 Click **System**→ **Remote Access**→ **iDRAC**, then click the **Update** tab.

   NOTE: To update the firmware, the iDRAC must be placed in an update mode. Once in this mode, the iDRAC will automatically reset, even if you cancel the update process.

3 On the **Firmware Update** page, click **Next** to start the update process.

4 In the **Firmware Update - Upload (page 1 of 4)** window, click **Browse**, or type the path to the firmware image that you downloaded.

   For example:

   `C:\Updates\V1.0\<image_name>`.

   The default firmware image name is **firmimg.imc**.

5 Click **Next**.

   - The file will be uploaded to the iDRAC. This may take several minutes to complete.

     OR

   - You can click **Cancel** at this time, if you would like to end the firmware upgrade process. Clicking **Cancel** will reset the iDRAC to normal operating mode.

6 In the **Firmware Update - Validation (page 2 of 4)** window, you will see the results of the validation performed on the image file you uploaded.

   - If the image file uploaded successfully and passed all verification checks, a message will appear indicating that the firmware image has been verified.

OR

- If the image did not upload successfully, or it did not pass the verification checks, the firmware update will return to the **Firmware Update - Upload (page 1 of 4)** window. You can attempt to upgrade the iDRAC again or click **Cancel** to reset the iDRAC to normal operating mode.

NOTE: If you deselect the **Preserve Configuration** checkbox, the iDRAC will be reset to its default settings. In the default settings, the LAN is disabled. You will not be able to log in to the iDRAC Web interface. You will have to reconfigure the LAN settings using the CMC Web interface or iKVM using the iDRAC Configuration Utility during BIOS POST.

7 By default the **Preserve Configuration** checkbox is checked, to preserve the current settings on the iDRAC after an upgrade. If you do not want the settings to be preserved, deselect the **Preserve Configuration** checkbox.

8 Click **Begin Update** to start the upgrade process. Do not interrupt the upgrade process.

9 In the **Firmware Update - Updating (page 3 of 4)** window, you will see the status of the upgrade. The progress of the firmware upgrade operation, measured in percentages, will appear in the **Progress** column.

10 Once the firmware update is complete, the **Firmware Update - Update Results (page 4 of 4)** window will appear and the iDRAC will reset automatically. You must close the current browser window and reconnect to the iDRAC using a new browser window.

Recovering iDRAC Firmware Using the CMC

Typically, the iDRAC firmware is updated using iDRAC facilities such as the iDRAC Web interface, the SM-CLP command line interface, or operating system specific update packages downloaded from **support.dell.com**.

If the iDRAC firmware becomes corrupted, as could occur if the iDRAC firmware update progress is interrupted before it completes, you can use the CMC Web interface to update its firmware.

If the CMC detects the corrupted iDRAC firmware, the iDRAC is listed on the **Updatable Components** page in the CMC Web interface.

NOTE: See the *CMC Firmware User's Guide* for instructions for using the CMC Web interface.

To update the iDRAC firmware, perform the following steps:

1. Download the latest iDRAC firmware to your management computer from **support.dell.com**.
2. Log in to the CMC Web-based interface.
3. Click **Chassis** in the system tree.
4. Click the **Update** tab. The **Updatable Components** page appears. The server with the recoverable iDRAC is included in the list if it is able to be recovered from the CMC.
5. Click **server-*n***, where ***n*** is the number of the server whose iDRAC you want to recover.
6. Click **Browse**, to browse to the iDRAC firmware image you downloaded, and click **Open**.
7. Click **Begin Firmware Update**.

After the firmware image file has been uploaded to the CMC, the iDRAC will update itself with the image.

6

Using the iDRAC with Microsoft Active Directory

A directory service maintains a common database of all information needed for controlling users, computers, printers, and other devices on a network. If your company uses the Microsoft® Active Directory® service software, you can configure the software to provide access to the iDRAC, allowing you to add and control iDRAC user privileges to your existing users in your Active Directory software.

NOTE: Using Active Directory to recognize iDRAC users is supported on the Microsoft Windows® 2000 and Windows Server® 2003 operating systems.

You can use Active Directory to define user access on iDRAC through an extended schema solution which uses Dell-defined Active Directory objects or a standard schema solution which uses Active Directory group objects only.

Advantages and Disadvantages of Extended Schema and Standard Schema

When using Active Directory to configure access to the iDRAC, you must choose either the extended schema or the standard schema solution.

The advantages of using the extended schema solution are:

- All of the access control objects are maintained in Active Directory.
- Maximum flexibility in configuring user access on different iDRACs with different privilege levels.

The advantages of using the standard schema solution are:

- No schema extension is required because standard schema uses Active Directory objects only.
- Configuration on the Active Directory side is simple.

Extended Schema Active Directory Overview

There are three ways to enable Active Directory with the extended schema:

- With the iDRAC Web interface. See "Configuring the iDRAC With Extended Schema Active Directory Using the Web Interface" on page 104.
- With the RACADM CLI tool. See "Configuring the iDRAC With Extended Schema Active Directory Using RACADM" on page 106.
- With the SM-CLP command line. See "Configuring the iDRAC With Extended Schema Active Directory and SM-CLP" on page 107.

Active Directory Schema Extensions

The Active Directory data is a distributed database of Attributes and Classes. The Active Directory schema includes the rules that determine the type of data that can be added or included in the database. The user class is one example of a Class that is stored in the database. Some example user class attributes can include 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 Attributes and Classes to support remote management Authentication and Authorization.

Each 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 Microsoft Active Directory, Dell received unique OIDs, unique name extensions, and uniquely linked attribute IDs for the attributes and classes we added to the directory service, as shown in Table 6-1.

Table 6-1. Dell Active Directory Object Identifiers

Active Directory Service Class	Active Directory OID
Dell extension	`dell`
Dell base OID	`1.2.840.113556.1.8000.1280`
RAC LinkID range	`12070` to `12079`

Overview of the RAC Schema Extensions

To provide the greatest flexibility in the multitude of customer environments, Dell provides a group of properties that can be configured by the user depending on the desired results. Dell has extended the schema to include an Association, Device, and Privilege property. The Association property 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

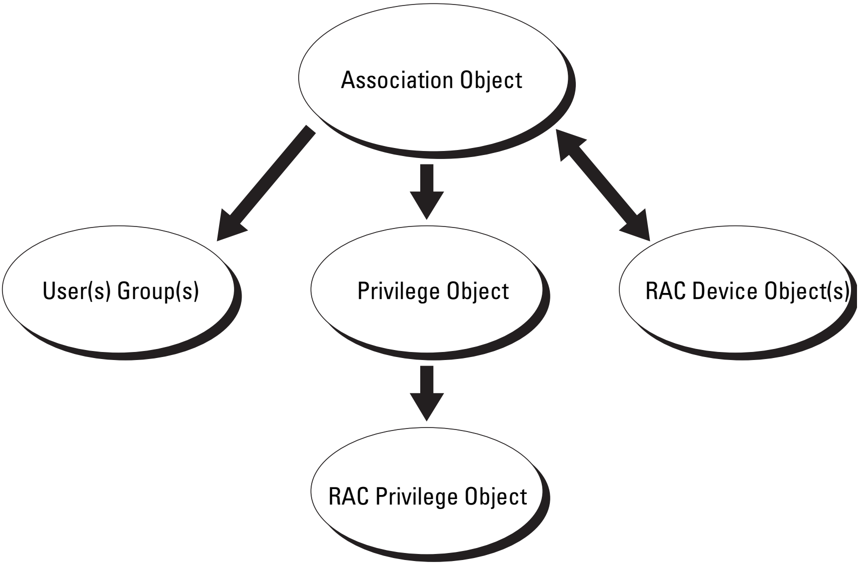
For each of the physical RACs on the network that you want to integrate with Active Directory for Authentication and Authorization, create at least one Association Object and one RAC Device Object. You can create multiple Association Objects, and each Association Object can be linked to as many users,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

However, each Association Object can be linked (or, may link users, groups of users, or RAC Device Objects) to only one Privilege Object. This example allows an Administrator to control each user's 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 users can perform authentication and authorization with Active Directory. The Administrator must 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



NOTE: The RAC privilege object applies to both DRAC 4 and iDRAC.

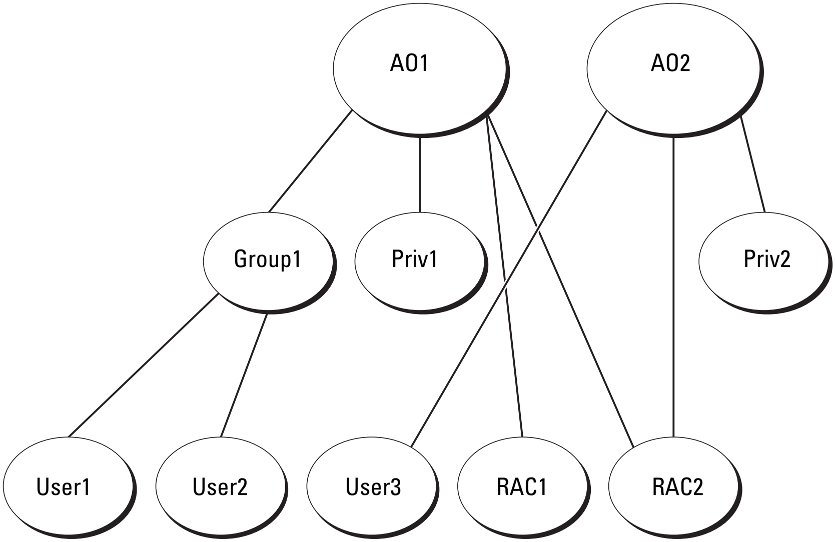
You can create as many or as few association objects as required. However, you must create at least one Association Object, and you must have one RAC Device Object for each RAC (iDRAC) on the network that you want to integrate with Active Directory for Authentication and Authorization with the RAC (iDRAC).

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 includes one Privilege Object per Association Object. The Association Object connects the "Users" who have "Privileges" on the RACs.

You can configure Active Directory objects in a single domain or in multiple domains. For example, you have two iDRACs (RAC1 and RAC2) and three existing Active Directory users (user1, user2, and user3). You want to give user1 and user2 an administrator privilege to both iDRACs and give user3 a login privilege to the RAC2. Figure 6-2 shows how you set up the Active Directory objects in this scenario.

When adding Universal Groups from separate domains, create an Association Object with Universal Scope. The Default Association objects created by the Dell Schema Extender Utility are Domain Local Groups and will not work with Universal Groups from other domains.

Figure 6-2. Setting Up Active Directory Objects in a Single Domain



To configure the objects for the single domain scenario, perform the following tasks:

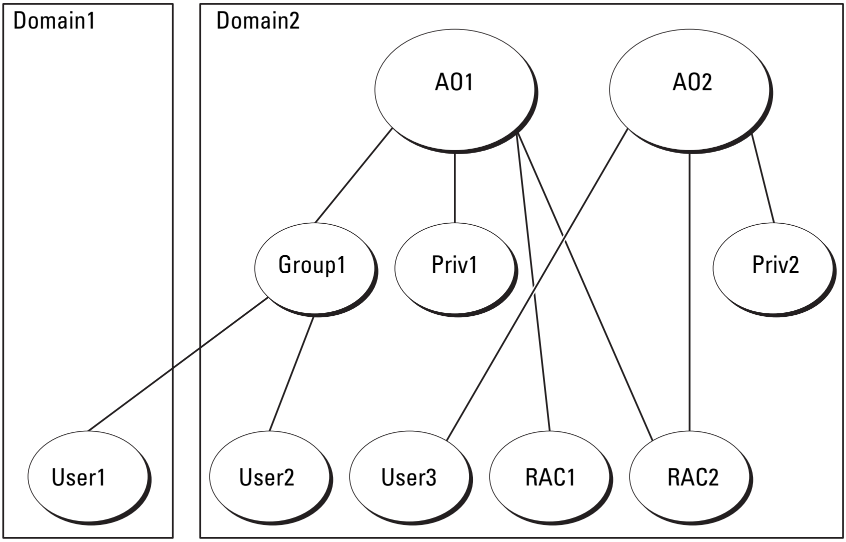
1. Create two Association Objects.
2. Create two RAC Device Objects, RAC1 and RAC2, to represent the two iDRACs.
3. Create two Privilege Objects, Priv1 and Priv2, in which Priv1 has all privileges (administrator) and Priv2 has login privileges.
4. Group user1 and user2 into Group1.
5. Add Group1 as Members 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 iDRAC Users and Privileges to Active Directory" on page 102 for detailed instructions.

Figure 6-3 provides an example of Active Directory objects in multiple domains. In this scenario, you have two iDRACs (RAC1 and RAC2) and three existing Active Directory users (user1, user2, and user3). User1 is in Domain1, and user2 and user 3 are in Domain2. In this scenario, configure user1 and user2 with administrator privileges to both iDRACs and configure user3 with login privileges to the RAC2.

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



To configure 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.

Figure 6-3 shows the objects in Domain2.

3. Create two RAC Device Objects, RAC1 and RAC2, to represent the two iDRACs.
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 Extended Schema Active Directory to Access Your iDRAC

Before using Active Directory to access your iDRAC, configure the Active Directory software and the iDRAC by performing the following steps in order:

1. Extend the Active Directory schema (see "Extending the Active Directory Schema" on page 95).
2. Extend the Active Directory Users and Computers Snap-in (see "Installing the Dell Extension to the Active Directory Users and Computers Snap-In" on page 101).
3. Add iDRAC users and their privileges to Active Directory (see "Adding iDRAC Users and Privileges to Active Directory" on page 102).
4. Enable SSL on each of your domain controllers (see "Enabling SSL on a Domain Controller" on page 115).
5. Configure the iDRAC Active Directory properties using either the iDRAC Web interface or the RACADM (see "Configuring the iDRAC With Extended Schema Active Directory Using the Web Interface" on page 104 or "Configuring the iDRAC With Extended Schema Active Directory Using RACADM" on page 106).

Extending the Active Directory Schema

Extending your Active Directory schema adds a Dell organizational unit, schema classes and attributes, and example privileges and association objects to the Active Directory schema. Before you extend the schema, ensure that you 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 one of the following:

- Dell Schema Extender utility
- LDIF script file

If you use the LDIF script file, the Dell organizational unit will not be added to the schema.

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

- *CD drive*:**\support\OMActiveDirectory Tools\RAC4-5\LDIF_Files**
- *CD drive*:**\support\OMActiveDirectory Tools\RAC4-5\Schema_Extender**

To use the LDIF files, see the instructions in the readme included in the **LDIF_Files** directory. To use the Dell Schema Extender to extend the Active Directory Schema, see "Using the Dell Schema Extender" on page 96.

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 of this file.

1. In the **Welcome** screen, click **Next.**
2. Read and understand the warning and click **Next**.
3. 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) and the Active Directory Schema snap-in to verify that the following exist:

   - Classes (see Table 6-2 through Table 6-7)
   - Attributes (Table 6-8)

   See your Microsoft documentation for more information on how to enable and use the Active Directory Schema snap-in in the MMC.

Table 6-2. 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
dellRACPrivileges	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 6-3. dellRacDevice Class

OID	1.2.840.113556.1.8000.1280.1.1.1.1
Description	Represents the Dell RAC device. The RAC device must be configured as dellRacDevice in Active Directory. This configuration enables the iDRAC to send Lightweight Directory Access Protocol (LDAP) queries to Active Directory.
Class Type	Structural Class
SuperClasses	dellProduct
Attributes	dellSchemaVersion dellRacType

Table 6-4. dellAssociationObject Class

OID	1.2.840.113556.1.8000.1280.1.1.1.2
Description	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 6-5. dellRAC4Privileges Class

OID	1.2.840.113556.1.8000.1280.1.1.1.3
Description	Used to define the privileges (Authorization Rights) for the iDRAC device.
Class Type	Auxiliary Class
SuperClasses	None
Attributes	dellIsLoginUser dellIsCardConfigAdmin dellIsUserConfigAdmin dellIsLogClearAdmin dellIsServerResetUser dellIsConsoleRedirectUser dellIsVirtualMediaUser dellIsTestAlertUser dellIsDebugCommandAdmin

Table 6-6. dellPrivileges Class

OID	1.2.840.113556.1.8000.1280.1.1.1.4
Description	Used as a container Class for the Dell Privileges (Authorization Rights).
Class Type	Structural Class
SuperClasses	User
Attributes	dellRAC4Privileges

Table 6-7. dellProduct Class

OID	1.2.840.113556.1.8000.1280.1.1.1.5
Description	The main class from which all Dell products are derived.
Class Type	Structural Class

Table 6-7. dellProduct Class *(continued)*

OID	1.2.840.113556.1.8000.1280.1.1.1.5
SuperClasses	Computer
Attributes	dellAssociationMembers

Table 6-8. List of Attributes Added to the Active Directory Schema

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

Table 6-8. List of Attributes Added to the Active Directory Schema *(continued)*

Attribute Name/Description	Assigned OID/Syntax Object Identifier	Single Valued
dellIsServerResetUser TRUE if the user has Server Reset rights on the device.	1.2.840.113556.1.8000.1280.1.1.2.7 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsConsoleRedirectUser TRUE if the user has Console Redirection rights on the device.	1.2.840.113556.1.8000.1280.1.1.2.8 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsVirtualMediaUser TRUE if the user has Virtual Media rights on the device.	1.2.840.113556.1.8000.1280.1.1.2.9 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsTestAlertUser TRUE if the user has Test Alert User rights on the device.	1.2.840.113556.1.8000.1280.1.1.2.10 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsDebugCommandAdmin TRUE if the user has Debug Command 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

Table 6-8. List of Attributes Added to the Active Directory Schema *(continued)*

Attribute Name/Description	Assigned OID/Syntax Object Identifier	Single Valued
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 the administrator can manage RAC (iDRAC) devices, Users and User Groups, RAC Associations, and RAC Privileges.

When you install your systems management software using the *Dell Systems Management Consoles* CD, you can extend the snap-in by selecting the **Dell Extension to the Active Directory User's and Computers Snap-In** option during the installation procedure. See the *Dell OpenManage Software Quick Installation Guide* for additional instructions about installing systems management software.

For more information about the Active Directory User's and Computers snap-in, see your Microsoft documentation.

Installing the Administrator Pack

You must install the Administrator Pack on each system that is managing the Active Directory iDRAC Objects. If you do not install the Administrator Pack, you cannot view the Dell RAC Object in the container.

See "Opening the Active Directory Users and Computers Snap-In" on page 102 for more information.

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 logged into the domain controller, click **Start→ Admin Tools→ Active Directory Users and Computers**.

   If you are not logged into the domain controller, you must have the appropriate Microsoft Administrator Pack installed on your local system. To install this Administrator Pack, click **Start→ Run**, type `MMC`, and press **Enter**.

   The Microsoft Management Console (MMC) appears.

2. In the **Console 1** window, click **File** (or **Console** on systems running Windows 2000).
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 iDRAC Users and Privileges to Active Directory

Using the Dell-extended Active Directory Users and Computers snap-in, you can add iDRAC users and privileges by creating RAC, Association, and Privilege objects. To add each object type, perform the following procedures:

- Create a RAC device Object
- Create a Privilege Object
- Create an Association Object
- Add objects to an Association Object

Creating a RAC Device Object

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

   The **New Object** window appears.

3. Type a name for the new object. The name must be identical to the iDRAC Name that you will type in step a of "Configuring the iDRAC With Extended Schema Active Directory Using the Web Interface" on page 104.

4 Select **RAC Device Object**.

5 Click **OK**.

Creating a Privilege Object

NOTE: A Privilege Object must be created in the same domain as the related Association Object.

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

2 Select **New**→ **Dell RAC Object**.

The **New Object** window appears.

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 Privileges** tab and select the privileges that you want the user to have (for more information, see "iDRAC User Privileges" on page 67).

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.

For example, if you select **Universal**, the 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

Using the **Association Object Properties** window, you can associate users or user groups, privilege objects, and RAC devices or RAC device groups. If your system is running Windows 2000 mode or higher, use Universal Groups to span domains with your user or RAC objects.

You can add groups of Users and RAC devices. The procedure for creating Dell-related groups and non-Dell-related groups is identical.

Adding 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. Only one privilege object can be added to an Association Object.

Adding Privileges

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. Multiple RAC devices can be added to an Association Object.

Adding RAC Devices or RAC Device Groups

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 click **OK**.

Configuring the iDRAC With Extended Schema Active Directory Using the Web Interface

1 Open a supported Web browser window.

2 Log in to the iDRAC Web interface.

3 Click **System→ Remote Access**.

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

5 On the **Active Directory Main Menu** page, select **Configure Active Directory** and click **Next**.

6 In the Common Settings section:

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

   b Type the **Root Domain Name**. The **Root Domain Name** is the fully qualified root domain name for the forest.

   c Type the **Timeout** time in seconds.

7 Click **Use Extended Schema** in the Active Directory Schema Selection section.

8 In the Extended Schema Settings section:

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

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

9 Click **Apply** to save the Active Directory settings.

10 Click **Go Back To Active Directory Main Menu**.

11 Upload your domain forest Root CA certificate into the iDRAC.

   a Select the **Upload Active Directory CA Certificat**e radio button and then click **Next**.

   b In the **Certificate Upload** page, type the file path of the certificate or browse to the certificate file.

   NOTE: The **File Path** value displays the relative file path of the certificate you are uploading. You must type the absolute file path, which includes the full path and the complete file name and file extension.

   The domain controllers' SSL certificates should have been signed by the root CA. Have the root CA certificate available on your management station accessing the iDRAC (see "Exporting the Domain Controller Root CA Certificate" on page 116).

c Click **Apply**.

The iDRAC Web server automatically restarts after you click **Apply**.

12 Log out and then log in to the iDRAC to complete the iDRAC Active Directory feature configuration.

13 Click **System**→ **Remote Access**.

14 Click the **Configuration** tab and click **Network**.

15 If **Use DHCP (for NIC IP Address)** is selected under **Network Settings**, then select **Use DHCP to obtain DNS server address**.

To manually input a DNS server IP address, deselect **Use DHCP to obtain DNS server addresses** and type your primary and alternate DNS server IP addresses.

16 Click **Apply Changes**.

The iDRAC Extended Schema Active Directory feature configuration is complete.

Configuring the iDRAC With Extended Schema Active Directory Using RACADM

Use the following commands to configure the iDRAC Active Directory feature with the extended schema using the RACADM CLI tool instead of the Web interface.

1 Open a command prompt and type the following RACADM commands:

```
racadm config -g cfgActiveDirectory -o cfgADEnable
1
```

```
racadm config -g cfgActiveDirectory -o cfgADType 1
```

```
racadm config -g cfgActiveDirectory -o
cfgADRacDomain <rac-FQDN>
```

```
racadm config -g cfgActiveDirectory -o
cfgADRootDomain <root-FQDN>
```

```
racadm config -g cfgActiveDirectory -o
cfgADRacName <RAC-common-name>
```

```
racadm sslcertupload -t 0x2 -f <root-CA-
certificate-TFTP-URI>
```

```
racadm sslcertdownload -t 0x1 -f <RAC-SSL-
certificate>
```

2 If DHCP is enabled on the iDRAC and you want to use the DNS provided by the DHCP server, type the following RACADM command:

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

3 If DHCP is disabled on the iDRAC or you want to manually input your DNS IP addresses, type the following RACADM commands:

```
racadm config -g cfgLanNetworking -o
cfgDNSServersFromDHCP 0
```

```
racadm config -g cfgLanNetworking -o cfgDNSServer1
<primary-DNS-IP-address>
```

```
racadm config -g cfgLanNetworking -o cfgDNSServer2
<secondary-DNS-IP-address>
```

4 Press **Enter** to complete the iDRAC Active Directory feature configuration.

Configuring the iDRAC With Extended Schema Active Directory and SM-CLP

NOTE: You must have a TFTP server running from which you can retrieve the root CA certificate and to which you can save the iDRAC server certificate.

Use the following commands to configure the iDRAC Active Directory feature with the extended schema using SM-CLP.

1 Log in to the iDRAC using telnet or SSH and enter the following SM-CLP commands:

```
cd /system/sp1/oemdell_adservice1

set enablestate=1

set oemdell_schematype=1

set oemdell_adracdomain=<rac-FQDN>

set oemdell_adrootdomain=<root-FQDN>

set oemdell_adracname=<RAC-common-name>
set /system1/sp1/oemdell_ssl1 oemdell_certtype=AD
```

```
load -source <root-CA-certificate-TFTP-URI>
```

```
set /system1/sp1/oemdell_ssl1 oemdell_certtype=SSL
dump -destination <DRAC-server-certificate-TFTP-
URI> /system1/sp1/oemdell_ssl1
```

2 If DHCP is enabled on the iDRAC and you want to use the DNS provided by the DHCP server, type the following SM-CLP command:

```
set /system1/sp1/enetport1/lanendpt1/ipendpt1/\
dnsendpt1 oemdell_serversfromdhcp=1
```

3 If DHCP is disabled on the iDRAC or you want to manually enter your DNS IP address, type the following SM-CLP commands:

```
set /system1/sp1/enetport1/lanendpt1/\
ipendpt1/dnsendpt1 oemdell_serversfromdhcp=0
```

```
set /system1/sp1/enetport1/lanendpt1/ipendpt1/\
dnsendpt1/remotesap1 dnsserveraddress=<primary-
DNS-IP-address>
```

```
set /system1/sp1/enetport1/lanendpt1/ipendpt1/\
dnsendpt1/remotesap1 dnsserveraddress=<secondary-
DNS-IP-address>
```

Active Directory Standard Schema Overview

As shown in Figure 6-4, using standard schema for Active Directory integration requires configuration on both Active Directory and the iDRAC. On the Active Directory side, a standard group object is used as a role group. A user who has iDRAC access will be a member of the role group. To give this user access to a specific iDRAC, the role group name and its domain name need to be configured on the specific iDRAC. Unlike the extended schema solution, the role and the privilege level is defined on each iDRAC, not in the Active Directory. Up to five role groups can be configured and defined in each iDRAC. Table 5-10 on page 68 shows the privileges level of the role groups and Table 6-9 shows the default role group settings.

Figure 6-4. Configuration of iDRAC with Microsoft Active Directory and the Standard Schema

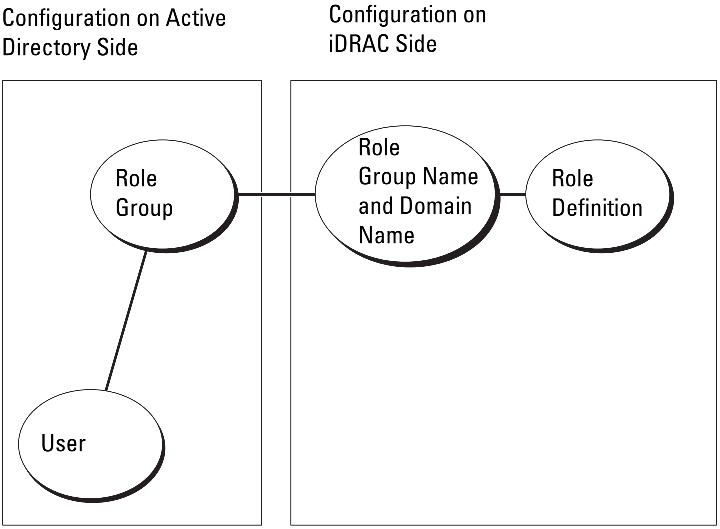

Configuration on Active Directory Side
Configuration on iDRAC Side
Role Group
User
Role Group Name and Domain Name
Role Definition

Table 6-9. Default Role Group Privileges

Default Privilege Level	Permissions Granted	Bit Mask
Administrator	Login to iDRAC, Configure iDRAC, Configure Users, Clear Logs, Execute Server Control Commands, Access Console Redirection, Access Virtual Media, Test Alerts, Execute Diagnostic Commands	0x000001ff
Power User	Login to iDRAC, Clear Logs, Execute Server Control Commands, Access Console Redirection, Access Virtual Media, Test Alerts	0x000000f9
Guest User	Login to iDRAC	0x00000001
None	No assigned permissions	0x00000000
None	No assigned permissions	0x00000000

NOTE: The Bit Mask values are used only when setting up the standard schema with the RACADM.

There are two ways to enable the standard schema in Active Directory:

- With the iDRAC Web user interface. See "Configuring the iDRAC With Standard Schema Active Directory and the Web Interface" on page 110.
- With the RACADM CLI tool. See "Configuring the iDRAC With Standard Schema Active Directory and RACADM" on page 112.

Configuring Standard Schema Active Directory to Access Your iDRAC

You need to perform the following steps to configure the Active Directory before an Active Directory user can access the iDRAC:

1 On an Active Directory server (domain controller), open the Active Directory Users and Computers Snap-in.

2 Create a group or select an existing group. The name of the group and the name of this domain will need to be configured on the iDRAC with the Web interface, RACADM, or SM-CLP (see "Configuring the iDRAC With Standard Schema Active Directory and the Web Interface" on page 110 or "Configuring the iDRAC With Standard Schema Active Directory and RACADM" on page 112).

3 Add the Active Directory user as a member of the Active Directory group to access the iDRAC.

Configuring the iDRAC With Standard Schema Active Directory and the Web Interface

1 Open a supported Web browser window.

2 Log in to the iDRAC Web interface.

3 Click **System**→ **Remote Access**→ **iDRAC**, then click the **Configuration** tab.

4 Select **Active Directory** to open the **Active Directory Main Menu** page.

5 On the **Active Directory Main Menu** page, select **Configure Active Directory** and click **Next**.

6. In the Common Settings section:

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

   b. Type the **Root Domain Name**. The **Root Domain Name** is the fully qualified root domain name for the forest.

   c. Type the **Timeout** time in seconds.

7. Click **Use Standard Schema** in the Active Directory Schema Selection section.

8. Click **Apply** to save the Active Directory settings.

9. In the **Role Groups** column of the Standard Schema settings section, click a **Role Group**.

   The **Configure Role Group** page appears, which includes a role group's **Group Name**, **Group Domain**, and **Role Group Privileges**.

10. Type the **Group Name**. The group name identifies the role group in the Active Directory associated with the iDRAC.

11. Type the **Group Domain**. The **Group Domain** is the fully qualified root domain name for the forest.

12. In the **Role Group Privileges** page, set the group privileges.

    Table 5-10 on page 68 describes the **Role Group Privileges**.

    If you modify any of the permissions, the existing **Role Group Privilege** (**Administrator**, **Power User**, or **Guest User**) will change to either the Custom group or the appropriate **Role Group Privilege** based on the permissions modified.

13. Click **Apply** to save the Role Group settings.

14. Click **Go Back To Active Directory Configuration and Management**.

15. Click **Go Back To Active Directory Main Menu**.

16. Upload your domain forest Root CA certificate into the iDRAC.

    a. Select the **Upload Active Directory CA Certificat**e radio button and then click **Next**.

b In the **Certificate Upload** page, type the file path of the certificate or browse to the certificate file.

NOTE: The **File Path** value displays the relative file path of the certificate you are uploading. You must type the absolute file path, which includes the full path and the complete file name and file extension.

The domain controllers' SSL certificates should have been signed by the root CA. Have the root CA certificate available on your management station accessing the iDRAC (see "Exporting the Domain Controller Root CA Certificate" on page 116).

c Click **Apply**.

The iDRAC Web server automatically restarts after you click **Apply**.

17 Log out and then log in to the iDRAC to complete the iDRAC Active Directory feature configuration.

18 Click **System**→ **Remote Access**.

19 Click the **Configuration** tab and then click **Network**.

20 If **Use DHCP (for NIC IP Address)** is selected under **Network Settings**, select **Use DHCP to obtain DNS server address**.

To manually input a DNS server IP address, deselect **Use DHCP to obtain DNS server addresses** and type your primary and alternate DNS server IP addresses.

21 Click **Apply Changes**.

The iDRAC standard schema Active Directory feature configuration is complete.

Configuring the iDRAC With Standard Schema Active Directory and RACADM

Using the following commands to configure the iDRAC Active Directory feature with the standard schema using the RACADM CLI instead of the Web interface.

1 Open a command prompt and type the following RACADM commands:

```
racadm config -g cfgActiveDirectory -o cfgADEnable
1
```

```
racadm config -g cfgActiveDirectory -o cfgADType 2
racadm config -g cfgActiveDirectory -o
cfgADRootDomain <root-FQDN>

racadm config -g cfgStandardSchema -i <index> -o
cfgSSADRoleGroupName <role-group-common-name>

racadm config -g cfgStandardSchema -i <index> -o
cfgSSADRoleGroupDomain <RAC-FQDN>

racadm config -g cfgStandardSchema -i <index> -o
cfgSSADRoleGroupPrivilege <permissions-bit-mask>

racadm sslcertupload -t 0x2 -f <root-CA-
certificate-TFTP-URI>

racadm sslcertdownload -t 0x1 -f <RAC-SSL-
certificate-TFTP-URI>
```

NOTE: For bit mask values, see Table B-1.

2 If DHCP is enabled on the iDRAC and you want to use the DNS provided by the DHCP server, type the following RACADM commands:

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

3 If DHCP is disabled on the iDRAC or you want to input your DNS IP addresses manually, type the following RACADM 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>
```

Configuring the iDRAC With Standard Schema Active Directory and SM-CLP

NOTE: You cannot upload certificates using SM-CLP. Instead, use the iDRAC Web interface or local RACADM commands.

Use the following commands to configure the iDRAC Active Directory Feature with the standard schema using SM-CLP.

1 Log in to the iDRAC using telnet or SSH and enter the following SM-CLP commands:

```
cd /system/sp1/oemdell_adservice1
```

```
set enablestate=1
```

```
set oemdell_schematype=2
```

```
set oemdell_adracdomain=<RAC-FQDN>
```

2 Enter the following commands for each of the five Active Directory role groups:

```
set /system1/sp1/groupN oemdell_groupname=<role-
groupN-common-name>
```

```
set /system1/sp1/groupN oemdell_groupdomain=<rac-
FQDN>
```

```
set /system1/sp1/groupN oemdell_groupprivilege=
<user-permission-bit-mask>
```

where *N* is a number from 1 to 5.

3 Enter the following commands to set up the Active Directory SSL certifications.

```
set /system1/sp1/oemdell_ssl1 oemdell_certtype=AD
load -source <root-CA-certificate-TFTP-URI>
```

```
set /system1/sp1/oemdell_ssl1 oemdell_certtype=SSL
```

```
dump -destination <iDRAC-server-certificate-TFTP-
URI> /system1/sp1/oemdell_ssl1
```

4 If DHCP is enabled on the iDRAC and you want to use the DNS provided by the DHCP server, type the following SM-CLP command:

```
set /system1/sp1/enetport1/lanendpt1/\
ipendpt1/dnsendpt1 oemdell_serversfromdhcp=1
```

5 If DHCP is disabled on the iDRAC or you want to manually enter your DNS IP addresses, type the following SM-CLP commands:

```
set /system1/sp1/enetport1/lanendpt1/\
ipendpt1/dnsendpt1 oemdell_serversfromdhcp=0
```

```
set /system1/sp1/enetport1/lanendpt1/ipendpt1/\
dnsendpt1/remotesap1 dnsserveraddress=<primary-
DNS-IP-address>
```

```
set /system1/sp1/enetport1/lanendpt1/ipendpt1/\
dnsendpt1/remotesap1 dnsserveraddress=<secondary-
DNS-IP-address>
```

Enabling SSL on a Domain Controller

If you are using Microsoft Enterprise Root CA to automatically assign all your domain controllers to an SSL certificate, perform the following steps to enable SSL on each domain controller.

1 Install a Microsoft Enterprise Root CA on a Domain Controller.

 a Select **Start**→ **Control Panel**→ **Add or Remove Programs**.

 b Select **Add/Remove Windows Components**.

 c In the **Windows Components Wizard**, select the **Certificate Services** check box.

 d Select **Enterprise root CA** as **CA Type** and click **Next**.

 e Enter **Common name for this CA**, click **Next**, and click **Finish**.

2 Enable SSL on each of your domain controllers by installing the SSL certificate for each controller.

 a Click **Start**→ **Administrative Tools**→ **Domain Security Policy**.

 b Expand the **Public Key Policies** folder, right-click **Automatic Certificate Request Settings** and click **Automatic Certificate Request**.

 c In the **Automatic Certificate Request Setup Wizard**, click **Next** and select **Domain Controller**.

 d Click **Next** and click **Finish**.

Exporting the Domain Controller Root CA Certificate

NOTE: If your system is running Windows 2000, the following steps may vary.

1 Locate the domain controller that is running the Microsoft Enterprise CA service.

2 Click **Start**→ **Run**.

3 In the **Run** field, type `mmc` and click **OK**.

4 In the **Console 1** (MMC) window, click **File** (or **Console** on Windows 2000 machines) 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 directory on your system.

15 Upload the certificate you saved in step 14 to the iDRAC.

To upload the certificate using RACADM, see "Configuring the iDRAC With Extended Schema Active Directory Using the Web Interface" on page 104.

To upload the certificate using the Web interface, perform the following procedure:

a Open a supported Web browser window.

b Log in to the iDRAC Web interface.

c Click **System**→ **Remote Access**, then click the **Configuration** tab.

d Click **Security** to open the **Security Certificate Main Menu** page.

e In the **Security Certificate Main Menu** page, select **Upload Server Certificate** and click **Apply**.

f In the **Certificate Upload** screen, perform one of the following procedures:

- Click **Browse** and select the certificate.
- In the **Value** field, type the path to the certificate.

g Click **Apply**.

Importing the iDRAC Firmware SSL Certificate

Use the following procedure to import the iDRAC firmware SSL certificate to all domain controller trusted certificate lists.

NOTE: If your system is running Windows 2000, the following steps may vary.

NOTE: If the iDRAC firmware SSL certificate is signed by a well-known CA, you are not required to perform the steps in this section.

The iDRAC SSL certificate is the identical certificate used for the iDRAC Web server. All iDRACs are shipped with a default self-signed certificate.

To access the certificate using the iDRAC Web interface, select **Configuration**→ **Active Directory**→ **Download iDRAC Server Certificate**.

1. On the domain controller, open an **MMC Console** window and select **Certificates**→ **Trusted Root Certification Authorities**.
2. Right-click **Certificates**, select **All Tasks** and click **Import**.
3. Click **Next** and browse to the SSL certificate file.
4. 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, you must install it on all your Domain Controllers.

5. 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.
6. Click **Finish** and click **OK**.

Using Active Directory to Log In To the iDRAC

You can use Active Directory to log in to the iDRAC using the Web interface. Use one of the following formats to enter your username:

<username@domain>

or

<domain>\<username>

or

<domain>/<username>

where *username* is an ASCII string of 1–256 bytes.

White space and special characters (such as \, /, or @) cannot be used in the user name or the domain name.

NOTE: You cannot specify NetBIOS domain names, such as Americas, as these names cannot be resolved.

Frequently Asked Questions

Table 6-10 lists frequently asked questions and answers.

Table 6-10. Using iDRAC With Active Directory: Frequently Asked Questions

Question	Answer
Can I log into the iDRAC using Active Directory across multiple trees?	Yes. The iDRAC's Active Directory querying algorithm supports multiple trees in a single forest.
Does the log in to the iDRAC 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 iDRAC 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.

Table 6-10. Using iDRAC With Active Directory: Frequently Asked Questions *(continued)*

Question	Answer
Does using the iDRAC 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.
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 iDRAC only allows uploading one trusted CA SSL certificate.

I created and uploaded a new RAC certificate and now the Web 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, generate a CSR and then create a new web certificate from Microsoft Certificate Services and load it using the RACADM CLI from the managed server by using the following RACADM commands:
	`racadm sslcsrgen [-g] [-u] [-f {filename}]`
	`racadm sslcertupload -t 1 -f {web_sslcert}`

Table 6-10. Using iDRAC With Active Directory: Frequently Asked Questions *(continued)*

Question	Answer
What can I do if I cannot log into the iDRAC using Active Directory authentication? How do I troubleshoot the issue?	**1** Ensure that you use the correct user domain name during a login and not the NetBIOS name. **2** If you have a local iDRAC user account, log into the iDRAC using your local credentials. After you are logged in, perform the following steps: **a** Ensure that you have checked the **Enable Active Directory** box on the iDRAC **Active Directory Configuration** page. **b** Ensure that the DNS setting is correct on the iDRAC **Networking Configuration** page. **c** Ensure that you have uploaded the Active Directory certificate from your Active Directory root CA to the iDRAC. **d** Check the Domain Controller SSL certificates to ensure that they have not expired. **e** Ensure that your **DRAC Name**, **Root Domain Name**, and **DRAC Domain Name** match your Active Directory environment configuration. **f** Ensure that the iDRAC password has a maximum of 127 characters. While the iDRAC can support passwords of up to 256 characters, Active Directory only supports passwords that have a maximum length of 127 characters.

7

Using GUI Console Redirection

This section provides information about using the iDRAC console redirection feature.

Overview

The iDRAC console redirection feature enables you to access the local console remotely in either graphic or text mode. Using console redirection, you can control one or more iDRAC-enabled systems from one location.

You do not have to sit in front of each server to perform all the routine maintenance. You can instead manage the servers from wherever you are, from your desktop or laptop computer. You can also share the information with others—remotely and instantly.

Using Console Redirection

NOTE: When you open a console redirection session, the managed server does not indicate that the console has been redirected.

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 server. 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:

- A maximum of two simultaneous console redirection sessions are supported. Both sessions view the same managed server console simultaneously.
- A console redirection session should not be launched from a web browser on the managed system.
- A minimum available network bandwidth of 1 MB/sec is required.

Supported Screen Resolutions and Refresh Rates

Table 7-1 lists the supported screen resolutions and corresponding refresh rates for a console redirection session that is running on the managed server.

Table 7-1. Supported Screen Resolutions and Refresh Rates

Screen Resolution	Refresh Rate (Hz)
720x400	70
640x480	60, 72, 75, 85
800x600	60, 70, 72, 75, 85
1024x768	60, 70, 72, 75, 85
1280x1024	60

Configuring Your Management Station

To use Console Redirection on your management station, perform the following procedures:

1 Install and configure a supported Web browser. See the following sections for more information:

- "Supported Web Browsers" on page 23

  NOTICE: Console Redirection and Virtual Media only support 32-bit Web browsers. Using 64-bit Web browsers may generate unexpected results or failure of operations.

- "Configuring a Supported Web Browser" on page 42

2 If you are using Firefox or want to use the Java Viewer with Internet Explorer, install a Java Runtime Environment (JRE). See "Installing a Java Runtime Environment (JRE)" on page 46.

3 It is recommended that you configure your monitor display resolution to 1280x1024 pixels or higher.

NOTICE: If you have an active console redirection session and a lower resolution monitor is connected to the iKVM, the server console resolution may reset if the server is selected on the local console. If the server is running a Linux operating system, an X11 console may not be viewable on the local monitor. Pressing <Ctrl><Alt><F1> at the iKVM will switch Linux to a text console.

Configuring Console Redirection in the iDRAC Web Interface

To configure console redirection in the iDRAC Web interface, perform the following steps:

1. Click **System** and then click the **Console** tab.
2. Click **Configuration** to open the **Console Redirection Configuration** page.
3. Configure the console redirection properties. Table 7-2 describes the settings for console redirection.
4. When completed, click **Apply**.
5. Click the appropriate button to continue. See Table 7-3.

Table 7-2. Console Redirection Configuration Properties

Property	Description
Enabled	Click to enable or disable Console Redirection. **Checked** indicates that Console Redirection is enabled. **Unchecked** indicates that Console Redirection is disabled. The default is **enabled**.
Max Sessions	Displays the maximum number of Console Redirection sessions that are possible, **1** or **2**. Use the drop-down menu to change the maximum number of Console Redirection sessions allowed. The default is **2**.
Active Sessions	Displays the number of Active Console sessions. This field is read-only.
Keyboard and Mouse Port Number	The network port number used for connecting to the Console Redirection Keyboard/Mouse option. This traffic is always encrypted. You may need to change this number if another program is using the default port. The default is **5900**.
Video Port Number	The network port number used for connecting to the Console Redirection Screen service. You may need to change this setting if another program is using the default port. The default is **5901**.

Table 7-2. Console Redirection Configuration Properties *(continued)*

Property	Description
Video Encryption Enabled	**Checked** indicates that video encryption is enabled. All traffic going to the video port is encrypted. **Unchecked** indicates that video encryption is disabled. Traffic going to the video port is not encrypted. The default is **Encrypted**. Disabling encryption can improve performance on slower networks.
Mouse Mode	Choose **Windows** if the managed server is running on a Windows operating system. Choose **Linux** if your server is running on Linux. Choose **None** if your server is not running on a Windows or Linux operating system. The default is **Windows**.
Console Plug-In Type for IE	When using Internet Explorer on a Windows operating system, you can choose from the following viewers: *ActiveX* - The *ActiveX Console Redirection* viewer Java - *Java Console Redirection* viewer. **NOTE:** You must have the Java runtime environment installed on your client system to use the Java viewer.
Disable Local Console	Checked indicates that output to the iKVM monitor is disabled during console redirection. This ensures that the tasks you perform using **Console Redirection** will not be visible on the managed server’s local monitor.

NOTE: For information about using Virtual Media with Console Redirection, see "Configuring and Using Virtual Media" on page 137.

The buttons in Table 7-5 are available on the **Console Redirection Configuration** page.

Table 7-3. Console Redirection Configuration Page Buttons

Button	Definition
Print	Prints the **Console Redirection Configuration** page
Refresh	Reloads the **Console Redirection Configuration** page
Apply	Saves any new settings made to the console redirection.

Configuring Console Redirection in the SM-CLP Command Line Interface

Opening a Console Redirection Session

When you open a console redirection session, the Dell Virtual KVM Viewer Application starts and the remote system's desktop appears in the viewer. Using the Virtual KVM Viewer Application, you can control the remote system's mouse and keyboard functions from your local management station.

To open a console redirection session in the Web interface, perform the following steps:

1. Click **System** and then click the **Console** tab.
2. In the **Console Redirection** page, use the information in Table 7-4 to ensure that a console redirection session is available.

   If you wish to reconfigure any of the property values displayed, see "Configuring Console Redirection in the iDRAC Web Interface" on page 123.

Table 7-4. Console Redirection Page Information

Property	Description
Console Redirection Enabled	Yes/No
Video Encryption Enabled	Yes/No
Max Sessions	Displays the maximum number of supported console redirection sessions
Current Sessions	Displays the current number of active console redirection sessions

Table 7-4. Console Redirection Page Information *(continued)*

Property	Description
Mouse Mode	Displays the mouse acceleration currently in effect. **Mouse Acceleration** mode should be chosen based on the type of operating system installed on the managed server.
Console Plug-in Type	Shows the plug-in type currently configured. **ActiveX** — An Active-X viewer will be launched. Active-X viewer will only work on Internet Explorer while running on a Windows Operating System. **Java** — A Java viewer will be launched. The Java viewer can be used on any browser including Internet Explorer. If your client runs on an operating system other than Windows, then you must use the Java Viewer. If you are accessing the iDRAC using Internet Explorer while running on a Windows operating system, you may choose either Active-X or Java as the plug-in type.
Local Console	Unchecked if the local console has not been disabled. If checked the console cannot be accessed by anyone using the iKVM connection on the chassis.

NOTE: For information about using Virtual Media with Console Redirection, see "Configuring and Using Virtual Media" on page 137.

The buttons in Table 7-5 are available on the **Console Redirection** page.

Table 7-5. Console Redirection Page Buttons

Button	Definition
Refresh	Reloads the **Console Redirection Configuration** page
Launch Viewer	Opens a console redirection session on the targeted remote system
Print	Prints the **Console Redirection Configuration** page

3. If a console redirection session is available, click **Launch Viewer**.

   NOTE: Multiple message boxes may appear after you launch the application. To prevent unauthorized access to the application, you must navigate through these message boxes within three minutes. Otherwise, you will be prompted to relaunch the application.

   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 management station connects to the iDRAC and the remote system's desktop appears in the Dell Digital KVM Viewer Application.

4. Two mouse pointers appear in the viewer window: one for the remote system and one for your local system. You must synchronize the two mouse pointers so that the remote mouse pointer follows your local mouse pointer. See "Synchronizing the Mouse Pointers" on page 130.

Using the Video Viewer

The Video Viewer provides a user interface between the management station and the managed server, allowing you to see the managed server's desktop and control its mouse and keyboard functions from your management station. When you connect to the remote system, the Video Viewer starts in a separate window.

The Video Viewer provides various control adjustments such as color mode, mouse synchronization, snapshots, keyboard macros, and access to Virtual Media. Click **Help** for more information on these functions.

When you start a console redirection session and the Video Viewer appears, you may need to adjust the color mode and synchronize the mouse pointers.

Table 7-6 describes the menu options that are available for use in the viewer.

Table 7-6. Viewer Menu Bar Selections

Menu Item	Item	Description
Video	Pause	Temporarily pauses console redirection.
	Resume	Resumes console redirection.
	Refresh	Redraws the viewer screen image.
	Capture Current Screen	Captures the current remote system screen to a **.bmp** file on Windows or a **.png** file on Linux. A dialog box is displayed that allows you to save the file to a specified location.
	Full Screen	To make the Video Viewer expand into full screen mode, select **Full Screen** from the **Video** menu.
	Exit	When you have finished using the Console and have logged out (using the remote system's logout procedure), select **Exit** from the **Video** menu to close the **Video Viewer** window.

Table 7-6. Viewer Menu Bar Selections *(continued)*

Menu Item	Item	Description
Keyboard	Hold Right Alt Key	Select this item before typing keys you want to combine with the right <Alt> key.
	Hold Left Alt Key	Select this item before typing keys you want to combine with the left <Alt> key.
	Left Windows Key	Select **Hold Down** before typing characters you want to combine with the left Windows key. Select **Press and Release** to send a left Windows key keystroke.
	Right Windows Key	Select **Hold Down** before typing characters you want to combine with the right Windows key. Select **Press and Release** to send a right Windows key keystroke.
	Macros	When you select a macro, or type the hotkey specified for the macro, the action is executed on the remote system. The Video Viewer provides the following macros: • Ctrl-Alt-Del • Alt-Tab • Alt-Esc • Ctrl-Esc • Alt-Space • Alt-Enter • Alt-Hyphen • Alt-F4 • PrtScn • Alt-PrtScn • F1 • Pause • Alt+m
	Keyboard Pass-through	The Keyboard pass-through mode allows all keyboard functions on the client to be redirected to the server.

Table 7-6. Viewer Menu Bar Selections *(continued)*

Menu Item	Item	Description
Mouse	Synchronize Cursor	The **Mouse** menu enables you to synchronize the cursor so that the mouse on the client is redirected to the mouse on the server.
Options	Color Mode	Allows you to select a color depth to improve performance over the network. For example, if you are installing software from virtual media, you can choose the lowest color depth (3-bit gray), so that less network bandwidth is used by the console viewer leaving more bandwidth for transferring data from the media. The color mode can be set to 15-bit color, 7-bit color, 4-bit color, 4-bit gray, and 3-bit gray.
Media	Virtual Media Wizard	The **Media** menu provides access to the Virtual Media Wizard, which allows you to redirect to a device or image such as a: • Floppy drive • CD • DVD • Image in ISO format • USB Flash drive For information about the Virtual Media feature, see "Configuring and Using Virtual Media" on page 137. You must keep the Console Viewer window active when using Virtual Media.
Help	N/A	Activates the **Help** menu.

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 Video Viewer window.

To synchronize the mouse pointers click **Mouse→ Synchronize cursor** or press <Alt><M>.

The Synchronize cursor menu item is a toggle. Ensure that there is a check mark next to the item in the menu so that the mouse synchronization is active.

When using Red Hat® Linux® or Novell® SUSE® Linux, be sure to configure the mouse mode for Linux before you launch the viewer. See "Configuring Console Redirection in the iDRAC Web Interface" on page 123 for help with configuration. The operating system's default mouse settings are used to control the mouse arrow in the iDRAC Console Redirection screen.

Disabling or Enabling Local Console

You can configure the iDRAC to disallow iKVM connections using the iDRAC Web interface. When the local console is disabled, a yellow status dot appears in the list of servers (OSCAR) to indicate that the console is locked in the iDRAC. When the local console is enabled, the status dot is green.

If you want to have ensure that you have exclusive access to the managed server console, you must disable the local console *and* reconfigure the **Max Sessions** to `1` on the **Console Redirection Page**.

NOTE: The local console feature is supported on all x9xx PowerEdge systems except PowerEdge SC1435 and 6950.

NOTE: By disabling (turning off) the local video on the server, the monitor, keyboard, and mouse connected to the iKVM are disabled.

To disable or enable the local console, perform the following procedure:

1 On your management station, open a supported Web browser and log into the iDRAC. See "Accessing the Web Interface" on page 55 for more information.

2 Click **System**, click the **Console** tab, and then click **Configuration**.

3 If you want to disable (turn off) local video on the server, in the **Console Redirect Configuration** page, select the **Disable Local Console** checkbox and then click **Apply**. The default value is **OFF**.

4 If you want to enable (turn on) local video on the server, in the **Console Redirect Configuration** page, deselect the **Disable Local Console** checkbox and then click **Apply**.

The **Console Redirection** page displays the status of the Local Server Video.

Frequently Asked Questions

Table 7-7 lists frequently asked questions and answers.

Table 7-7. Using Console Redirection: Frequently Asked Questions

Question	Answer
Can a new remote console video session be started when the local video on the server is turned off?	Yes.
Why does it take 15 seconds to turn off the local video on the server after requesting to turn off the local video?	It gives a local user an opportunity to take any action before the video is switched off.
Is there a time delay when turning on the local video?	No, once a local video turn **ON** request is received by iDRAC the video is turned on instantly.
Can the local user also turn off the video?	Yes, a local user can use the local RACADM CLI to turn off the video.
Can the local user also turn on the video?	No. Once the local console is disabled, the local user's keyboard and mouse are disabled and they are unable to change any settings.
Does switching off the local video also switch off the local keyboard and mouse?	Yes.
Does turning off the local console turn off the video on the remote console session?	No, turning the local video on or off is independent of the remote console session.

Table 7-7. Using Console Redirection: Frequently Asked Questions *(continued)*

Question	Answer
What privileges are needed for an iDRAC user to turn on or off the local server video?	Any user with iDRAC configuration privileges can turn the local console on or off.
How can I get the current status of the local server video?	The status is displayed on the **Console Redirection Configuration** page of the iDRAC Web interface. The RACADM CLI command **racadm getconfig –g cfgRacTuning** displays the status in the object **cfgRacTuneLocalServerVideo**. The status is also seen on the iKVM OSCAR display. When the local console is enabled, a green status appears next to the server name. When disabled, a yellow dot indicates that the local console is locked by the iDRAC.
I cannot see the bottom of the system screen from the Console Redirection window.	Ensure that the management station’s monitor resolution is set to 1280x1024.
The console window is garbled.	The console viewer on Linux requires a UTF-8 character set. Check your locale and reset the character set if needed. See "Setting the Locale in Linux" on page 44 for more information.
Why do I get a blank screen on the managed server when loading the Windows 2000 operating system?	The managed server does not have the correct ATI video driver. You must update the video driver by using the *Dell PowerEdge Installation and Server Management* CD.

Table 7-7. Using Console Redirection: Frequently Asked Questions *(continued)*

Question	Answer
Why doesn’t the mouse sync in DOS when performing Console Redirection?	The Dell BIOS is emulating the mouse driver as a PS/2 mouse. By design, the PS/2 mouse uses relative position for the mouse pointer, which causes the lag in syncing. iDRAC has a USB mouse driver, which allows absolute position and closer tracking of the mouse pointer. Even if iDRAC passes the USB absolute mouse position to the Dell BIOS, the BIOS emulation would convert it back to relative position and the behavior would remain. To fix this problem, set the mouse mode to **NONE** in the Console Redirection configuration.
Why doesn’t the mouse sync under the Linux text console?	Virtual KVM requires the USB mouse driver, but the USB mouse driver is available only under the X-Window operating system.
I am still having issues with mouse synchronization.	Ensure that the correct mouse is selected for your operating system before starting a console redirection session. Ensure that **Synchronize Mouse** is checked in the **Mouse** menu. Press <Alt><M> or select **Mouse→ Synchronize mouse** to toggle mouse synchronization. When synchronization is enabled, a check mark appears next to the selection in the **Mouse** menu.
Why can't I use a keyboard or mouse while installing a Microsoft® operating system remotely by using iDRAC Console Redirection?	When you remotely install a supported Microsoft operating system on a system with Console Redirection enabled in the BIOS, you receive an EMS Connection Message that requires that you select **OK** before you can continue. You cannot use the mouse to select **OK** remotely. You must either select **OK** on the local system or restart the remotely managed server, reinstall, and then turn Console Redirection off in the BIOS. This message is generated by Microsoft to alert the user that Console Redirection is enabled. To ensure that this message does not appear, always turn off Console Redirection in the BIOS before installing an operating system remotely.

Table 7-7. Using Console Redirection: Frequently Asked Questions *(continued)*

Question	Answer
Why doesn't the Num Lock indicator on my management station reflect the status of the Num Lock on the remote server?	When accessed through the iDRAC, the Num Lock indicator on the management station does not necessarily coincide with the state of the Num Lock on the remote server. The state of the Num Lock is dependent on the setting on the remote server when the remote session is connected, regardless of the state of the Num Lock on the management station.
Why do multiple Session Viewer windows appear when I establish a console redirection session from the local host?	You are configuring a console redirection session from the local system. This is not supported.
If I am running a console redirection session and a local user accesses the managed server, do I receive a warning message?	No. If a local user accesses the system, you both have control of the system.
How much bandwidth do I need to run a console redirection session?	Dell recommends a 5 MB/sec connection for good performance. A 1 MB/sec connection is required for minimal performance.
What are the minimum system requirements for my management station to run console redirection?	The management station requires an Intel Pentium III 500 MHz processor with at least 256 MB of RAM.

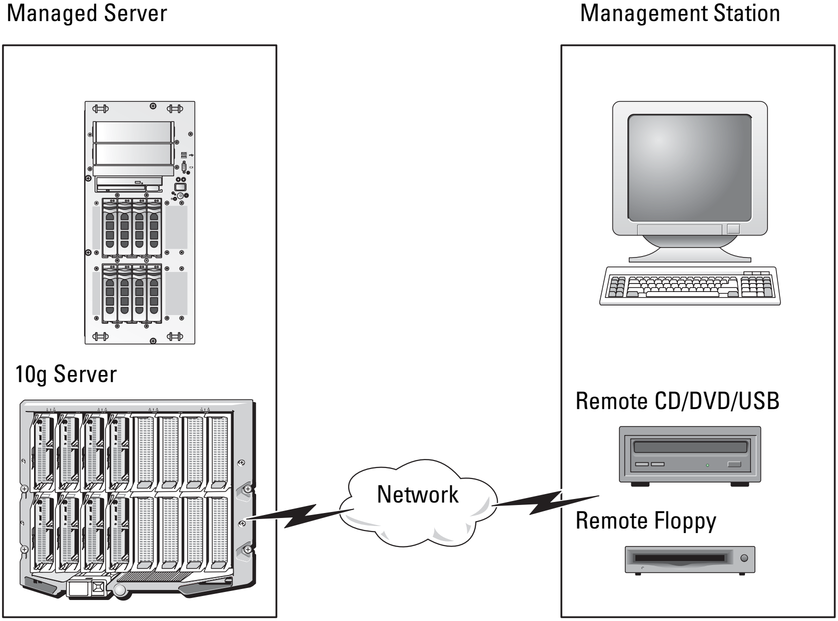
8

Configuring and Using Virtual Media

Overview

The **Virtual Media** feature, accessed through the console redirection viewer, provides the managed server access to media connected to a remote system on the network. Figure 8-1 shows the overall architecture of **Virtual Media**.

Figure 8-1. Overall Architecture of Virtual Media



Using **Virtual Media**, administrators can remotely boot their managed servers, 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.

Virtual media defines two devices for the managed server's operating system and BIOS: a floppy disk device and an optical disk device.

The management station provides the physical media or image file across the network. When **Virtual Media** is connected, all virtual CD/floppy drive access requests from the managed server are directed to the management station across the network. Connecting **Virtual Media** appears the same as inserting media into physical devices. When virtual media is not connected, virtual devices on the managed server appear as two drives without media installed in the drives.

Table 8-1 lists the supported drive connections for virtual floppy and virtual optical drives.

NOTE: Changing **Virtual Media** while connected could stop the system boot sequence.

Table 8-1. Supported Drive Connections

Supported Virtual Floppy Drive Connections	Supported Virtual Optical Drive Connections
Legacy 1.44 floppy drive with a 1.44 floppy diskette	CD-ROM, DVD, CDRW, combination drive with CD-ROM media
USB floppy drive with a 1.44 floppy diskette	CD-ROM/DVD image file in the ISO9660 format
1.44 floppy image	USB CD-ROM drive with CD-ROM media
USB removable disk	

Windows-Based Management Station

To run the **Virtual Media** feature on a management station running the Microsoft® Windows® operating system, install a supported version of Internet Explorer with the ActiveX Control plug-in. Set the browser security to **Medium** or a lower setting to enable Internet Explorer to download and install signed ActiveX controls.

See "Supported Web Browsers" on page 23 for more information.

You must have administrator rights to install ActiveX. Before installing the ActiveX control, Internet Explorer may display a security warning. To complete the ActiveX control installation procedure, accept the ActiveX control when Internet Explorer prompts you with a security warning.

Linux-Based Management Station

To run the virtual media feature on a management station running the Linux operating system, install a supported version of Firefox. See "Supported Web Browsers" on page 23 for more information.

A Java Runtime Environment (JRE) is required is required to run the console redirection plugin. You can download a JRE from **java.sun.com**. JRE version 1.6 or above is recommended.

Configuring Virtual Media

1. Log in to the iDRAC Web interface.
2. Select **System** in the navigation tree and click the **Console** tab.
3. Click **Configuration→ Virtual Media** to configure the Virtual Media settings.

   Table 8-2 describes the **Virtual Media** configuration values.
4. When you have finished configuring the settings, click **Apply**.
5. Click the appropriate button to continue. See Table 8-3.

Table 8-2. Virtual Media Configuration Values

Attribute	Value
Attach Virtual Media	**Attach** - Immediately attaches **Virtual Media** to the server. **Detach** - Immediately detaches **Virtual Media** from the server. **Auto-Attach** - Attaches **Virtual Media** to the server only when a virtual media session is started.

Table 8-2. Virtual Media Configuration Values *(continued)*

Attribute	Value
Maximum Sessions	Displays the maximum number of **Virtual Media** sessions allowed. This is always 1.
Active Sessions	Displays the current number of Virtual Media sessions.
Virtual Media Encryption Enabled	Click the checkbox to enable or disable encryption on **Virtual Media** connections. Checked enables encryption; unchecked disables encryption.
Virtual Media Port Number	The network port number used for connecting to the **Virtual Media** service without encryption. Two consecutive ports starting from the port number specified are used to connect to the **Virtual Media** service. The port number following the specified port must not be configured for any other iDRAC service. The default is **3668**.
Virtual Media SSL Port Number	The network port number used for encrypted connections to the **Virtual Media** service. Two consecutive ports starting from the port number specified are used to connect to the **Virtual Media** service. The port number following the specified port must not be configured for any other iDRAC service. The default is **3670**.
Floppy Emulation	Indicates whether the **Virtual Media** appears as a floppy drive or as a USB key to the server. If **Floppy Emulation** is checked, the **Virtual Media** device appears as a floppy device on the server. If it is unchecked, it appears as a USB Key drive.
Enable Boot Once	Check this box to enable the boot once option. This option automatically terminates the **Virtual Media** session after the server has booted once. This option is useful for automated deployments.

Table 8-3. Virtual Media Configuration Page Buttons

Button	Description
Print	Prints the **Console Configuration** values that appear on the screen.
Refresh	Reloads the **Console Configuration** page.
Apply	Saves any new settings made to the **Console Configuration** page.

Running Virtual Media

NOTICE: Do not issue a **racreset** command when running a **Virtual Media** session. Otherwise, undesirable results may occur, including loss of data.

NOTICE: The Console Viewer window application must remain active while you access the virtual media.

1 Open a supported Web browser on your management station. See "Supported Web Browsers" on page 23.

NOTICE: Console Redirection and **Virtual Media** only support 32-bit Web browsers. Using 64-bit Web browsers may generate unexpected results or failures.

2 Start the iDRAC Web interface. "Accessing the Web Interface" on page 55.

3 Select **System** in the navigation tree and click the **Console** tab.

The **Console Redirection** page appears. If you want to change the values of any of the displayed attributes, see "Configuring Virtual Media" on page 139.

NOTE: The **Floppy Image File** under **Floppy Drive** (if applicable) may appear, as this device can be virtualized as a virtual floppy. You can select one optical drive and one floppy at the same time, or a single drive.

NOTE: The virtual device drive letters on the managed server do not coincide with the physical drive letters on the management station.

NOTE: **Virtual Media** may not function properly on Windows operating system clients that are configured with Internet Explorer Enhanced Security. To resolve this issue, see your Microsoft operating system documentation or contact your administrator.

4 Click **Launch Viewer**.

> **NOTE:** On Linux, the file **jviewer.jnlp** is downloaded to your desktop and a dialog box will ask what to do with the file. Choose the option to **Open with program** and then select the **javaws** application, which is located in the **bin** subdirectory of your JRE installation directory.

The **iDRACView** application launches in a separate window.

5 Click **Media→ Virtual Media Wizard…**.

The Media Redirection wizard appears.

6 View the Status window. If media is connected, you must disconnect it before connecting a different media source. Click the **Disconnect** button to the right of the media you wish to disconnect.

7 Select the radio button next to the media types you wish to connect.

You can select one radio button in the **Floppy/USB Drive** section and one in the **CD/DVD Drive** section.

If you want to connect a Floppy image or ISO image, enter the path (on your local computer) to the image, or click the **Browse** button and browse to the image.

8 Click the **Connect button next to each selected media type.**

The media is connected and the Status window is updated.

9 Click the **Close button.**

Disconnecting Virtual Media

1 Click **Media→ Virtual Media Wizard…**.

2 Click **Disconnect** next to the media you wish to disconnect.

The media is disconnected and the Status window is updated.

3 Click **Close**.

Booting From Virtual Media

The system BIOS enables you to boot from virtual optical drives or virtual floppy drives. During POST, enter the BIOS setup window and verify that the virtual drives are enabled and listed in the correct order.

To change the BIOS setting, perform the following steps:

1. Boot the managed server.
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 optical drives and virtual floppy drives are listed with the standard boot devices.
4. Ensure that the virtual drive is enabled and listed as the first device with bootable media. If required, follow the on-screen instructions to modify the boot order.
5. Save the changes and exit.

   The managed server reboots.

   The managed server 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 the virtual device. Otherwise, the system overlooks the device—similar to a physical device without bootable media.

Installing Operating Systems Using Virtual Media

This section describes a manual, interactive method to install the operating system on your management station that may take several hours to complete. A scripted operating system installation procedure using **Virtual Media** may take less than 15 minutes to complete. See "Deploying the Operating System" on page 189 for more information.

1. Verify the following:
   - The operating system installation CD is inserted in the management station’s CD drive.
   - The local CD drive is selected.
   - You are connected to the virtual drives.
2. Follow the steps for booting from the virtual media in the "Booting From Virtual Media" section to ensure that the BIOS is set to boot from the CD drive that you are installing from.
3. Follow the on-screen instructions to complete the installation.

Using Virtual Media When the Server's Operating System Is Running

Windows-Based Systems

On Windows systems, the virtual media drives are automounted if they are attached and configured with a drive letter.

Using the virtual drives from within Windows is similar to using your physical drives. When you connect to the media using the Virtual Media wizard, the media is available at the system by clicking the drive and browsing its content.

Linux-Based Systems

Depending on the configuration of the software on your system, the virtual media drives may not be automounted. If your drives are not automounted, manually mount the drives using the Linux **mount** command.

Frequently Asked Questions

Table 8-4 lists frequently asked questions and answers.

Table 8-4. Using Virtual Media: Frequently Asked Questions

Question	Answer
Sometimes, I notice my Virtual Media client connection drop. Why?	When a network time-out occurs, the iDRAC firmware drops the connection, disconnecting the link between the server and the Virtual Drive. If the Virtual Media configuration settings are changed in the iDRAC Web interface or by local RACADM commands, any connected media is disconnected when the configuration change is applied. To reconnect to the Virtual Drive, use the Virtual Media wizard.
Which operating systems support the iDRAC?	See "Supported Operating Systems" on page 22 for a list of supported operating systems.
Which Web browsers support the iDRAC?	See "Supported Web Browsers" on page 23 for a list of supported Web browsers.

Table 8-4. Using Virtual Media: Frequently Asked Questions *(continued)*

Question	Answer
Why do I sometimes lose my client connection?	• You can sometimes lose your client connection if the network is slow or if you change the CD in the client system CD drive. For example, if you change the CD in the client system's CD drive, the new CD might have an autostart feature. If this is the case, the firmware can time out and the connection can be lost if the client system takes too long before it is ready to read the CD. If a connection is lost, reconnect from the GUI and continue the previous operation. • When a network timeout occurs, the iDRAC firmware drops the connection, disconnecting the link between the server and the Virtual Drive. Also, someone may have altered the Virtual Media configuration settings in the Web interface or by entering RADACM commands. To reconnect to the Virtual Drive, use the **Virtual Media** feature.
An installation of the Windows operating system seems to take too long. Why?	If you are installing the Windows operating system using the *Dell PowerEdge Installation and Server Management* CD and a slow network connection, the installation procedure may require an extended amount of time to access the iDRAC Web interface due to network latency. While the installation window does not indicate the installation progress, the installation procedure is in progress.
I am viewing the contents of a floppy drive or USB memory key. If I try to establish a Virtual Media connection using the same drive, I receive a connection failure message and am asked to retry. Why?	Simultaneous access to Virtual Floppy drives is not allowed. Close the application used to view the drive contents before you attempt to virtualize the drive.

Table 8-4. Using Virtual Media: Frequently Asked Questions *(continued)*

Question	Answer
How do I configure my virtual device as a bootable device?	On the managed server, access the BIOS Setup and navigate to the boot menu. Locate the virtual CD, Virtual Floppy, or Virtual Flash and change the device boot order as needed. For example, to boot from a CD drive, configure the CD drive as the first drive in the boot order.
What types of media can I boot from?	The iDRAC allows you to boot from the following bootable media: • CDROM/DVD Data media • ISO 9660 image • 1.44 Floppy disk or floppy image • A USB key that is recognized by the operating system as a removable disk • A USB key image
How can I make my USB key bootable?	Search **support.dell.com** for the Dell Boot Utility, a Windows program you can use to make your Dell USB key bootable. You can also boot with a Windows 98 startup disk and copy system files from the startup disk to your USB key. For example, from the DOS prompt, type the following command: `sys a: x: /s` where *x*: is the USB key you want to make bootable. You can also use the Dell boot utility to create a bootable USB key. This utility is only compatible with Dell-branded USB keys. To download the utility, open a Web browser, navigate to the Dell Support website located at **support.dell.com**, and search for R122672.exe.

Table 8-4. Using Virtual Media: Frequently Asked Questions *(continued)*

Question	Answer

I cannot locate my Virtual Floppy device on a system running Red Hat® Enterprise Linux® or the SUSE® Linux operating system. My Virtual Media is attached and I am connected to my remote floppy. What should I do?	Some Linux versions do not automount the Virtual Floppy Drive and the Virtual CD drive in a similar manner. To mount the Virtual Floppy Drive, locate the device node that Linux assigns to the Virtual Floppy Drive. Perform the following steps to correctly find and mount the Virtual Floppy Drive:
	1 Open a Linux command prompt and run the following command:
	`grep "Virtual Floppy" /var/log/messages`
	2 Locate the last entry to that message and note the time.
	3 At the Linux prompt, run the following command:
	`grep "`*`hh:mm:ss`*`" /var/log/messages`
	where:
	`hh:mm:ss` is the time stamp of the message returned by grep in step 1.
	4 In step 3, read the result of the grep command and locate the device name that is given to the Dell Virtual Floppy.
	5 Ensure that you are attached and connected to the Virtual Floppy Drive.
	6 At the Linux prompt, run the following command:
	mount */dev/sdx* /mnt/floppy
	where:
	`/dev/sdx` is the device name found in step 4
	`/mnt/floppy` is the mount point.

What file system types are supported on my Virtual Floppy Drive?	Your Virtual Floppy Drive supports FAT16 or FAT32 file systems.

Table 8-4. Using Virtual Media: Frequently Asked Questions *(continued)*

Question	Answer
When I performed a firmware update remotely using the iDRAC Web interface, my virtual drives at the server were removed. Why?	Firmware updates cause the iDRAC to reset, drop the remote connection, and unmount the virtual drives. The drives will reappear when the iDRAC reset is complete.

Using the Local RACADM Command Line Interface

The local RACADM command line interface (CLI) provides access to the iDRAC management features from the managed server. RACADM provides access to the same features as the iDRAC Web interface. However, RACADM can be used in scripts to ease configuration of multiple servers and iDRACs, where the Web interface is more useful for interactive management.

Local RACADM commands do not use network connections to access the iDRAC from the managed server. This means that you can use local RACADM commands to configure the initial iDRAC networking.

For more information about configuring multiple iDRACs, see "Configuring Multiple iDRACs" on page 170.

This section provides the following information:

- Using RACADM from a command prompt
- Configuring your iDRAC using the **racadm** command
- Using the RACADM configuration file to configure multiple iDRACs

Using the RACADM Command

You run RACADM commands locally (on the managed server) from a command prompt or shell prompt.

Log into the managed server, start a command shell, and enter local RACADM commands in the following format:

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

Without options, the RACADM command displays general use information. To display the RACADM subcommand list, type:

```
racadm help
```

The subcommand list includes all commands that are supported by the iDRAC.

To get help for a subcommand, type:

```
racadm help <subcommand>
```

The command displays the syntax and command-line options for the subcommand.

RACADM Subcommands

Table 9-1 provides a description of each RACADM subcommand that you can run in RACADM. For a detailed listing of RACADM subcommands including syntax and valid entries, see "RACADM Subcommand Overview" on page 223.

Table 9-1. RACADM Subcommands

Command	Description
clrraclog	Clears the iDRAC log. After clearing, a single entry is made to indicate the user and time that the log was cleared.
clrsel	Clears the managed server's System Event Log entries.
config	Configures the iDRAC.
getconfig	Displays the current iDRAC configuration properties.
getniccfg	Displays the current IP configuration for the controller.
getraclog	Displays the iDRAC log.
getractime	Displays the iDRAC time.
getssninfo	Displays information about active sessions.
getsvctag	Displays service tags.
getsysinfo	Displays information about the iDRAC and managed server, including IP configuration, hardware model, firmware versions, and operating system information.
gettracelog	Displays the iDRAC trace log. If used with `-i`, the command displays the number of entries in the iDRAC trace log.
help	Lists iDRAC subcommands.
help <*subcommand*>	Lists usage statement for the specified subcommand.

Table 9-1. RACADM Subcommands *(continued)*

Command	Description
racreset	Resets the iDRAC.
racresetcfg	Resets the iDRAC to the default configuration.
serveraction	Performs power management operations on the managed server.
setniccfg	Sets the IP configuration for the controller.
sslcertdownload	Downloads a CA certificate.
sslcertupload	Uploads a CA certificate or server certificate to the iDRAC.
sslcertview	Views a CA certificate or server certificate in the iDRAC.
sslcsrgen	Generates and downloads the SSL CSR.
testemail	Forces the iDRAC to send an e-mail over the iDRAC NIC.
testtrap	Forces the iDRAC to send an SNMP alert over the iDRAC NIC.
vmdisconnect	Forces a virtual media connection to close.

Using the RACADM Utility to Configure the iDRAC

This section describes how to use RACADM to perform various iDRAC configuration tasks.

Displaying Current iDRAC Settings

The RACADM **getconfig** subcommand retrieves current configuration settings from the iDRAC. The configuration values are organized into *groups* containing one or more *objects*, and the objects have *values*.

See "iDRAC Property Database Group and Object Definitions" on page 253 for a complete description of the groups and objects.

To display a list of all of the iDRAC groups, enter this command:

```
racadm getconfig -h
```

To display the objects and values for a particular group, enter this command:

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

For example, to display a list of all **cfgLanNetworking** group object settings, type the following command:

```
racadm getconfig -g cfgLanNetworking
```

Managing iDRAC Users with RACADM

NOTICE: Use caution when using the **racresetcfg** command, as *all* configuration parameters are reset to the original defaults. Any previous changes are lost.

NOTE: If you are configuring a new iDRAC or if you ran the **racadm racresetcfg** command, the only current user is **root** with the password **calvin**.

NOTE: Users can be enabled and disabled over time. As a result, a user may have a different index number on each iDRAC.

You can configure up to 15 users in the iDRAC property database. (A sixteenth user is reserved for the IPMI LAN user.) Before you manually enable an iDRAC user, verify if any current users exist.

To verify if a user exists, type the following command at the command prompt:

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

OR

type the following command once for each index from 1 to 16:

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

NOTE: You can also type `racadm getconfig -f <filename>` and view the generated *<filename>* file, which includes all users, as well as all other iDRAC configuration parameters.

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

```
# cfgUserAdminIndex=nn

cfgUserAdminUserName=
```

If the **cfgUserAdminUserName** object has no value, that index number, which is indicated by the **cfgUserAdminIndex** object, is available for use. If a name appears after the =, that index is assigned to that user name.

Adding an iDRAC User

To add a new user to the iDRAC, perform the following steps:

1. Set the user name.
2. Set the password.
3. Set the Login to iDRAC user privilege.
4. Enable the user.

Example

The following example describes how to add a new user named "John" with a "123456" password and login privileges to the iDRAC:

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

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

```
racadm config -g cfgUserAdmin -o cfgUserPrivilege -i 2
0x00000001
```

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

To verify the new user, use one of the following commands:

```
racadm getconfig -u john
```

```
racadm getconfig –g cfgUserAdmin –i 2
```

Enabling an iDRAC User With Permissions

To grant a user a specific administrative (role-based) permissions, set the **cfgUserAdminPrivilege** property to a bitmask constructed from the values show in Table 9-2:

Table 9-2. Bit Masks for User Privileges

User Privilege	Privilege Bit Mask
Login to iDRAC	0x0000001
Configure iDRAC	0x0000002
Configure Users	0x0000004

Table 9-2. Bit Masks for User Privileges *(continued)*

User Privilege	Privilege Bit Mask
Clear Logs	0x0000008
Execute Server Control Commands	0x0000010
Access Console Redirection	0x0000020
Access Virtual Media	0x0000040
Test Alerts	0x0000080
Execute Debug Commands	0x0000100

For example, to allow the user **Configure iDRAC**, **Configure Users**, **Clear Logs,** and **Access Console Redirection** privileges, add the values 0x00000002, 0x00000004, 0x00000008, and 0x00000010 to construct the bitmap 0x0000002E. Then enter the following command to set the privilege:

```
racadm config -g cfgUserAdmin -o
cfgUserAdminPrivilege -i 2 0x0000002E
```

Removing an iDRAC User

When using RACADM, users must be disabled manually and on an individual basis. Users cannot be deleted by using a configuration file.

The following example illustrates the command syntax that can be used to delete a RAC user:

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

A null string of double quote characters ("") instructs the iDRAC to remove the user configuration at the specified index and reset the user configuration to the original factory defaults.

Testing E-mail Alerting

The iDRAC e-mail alert feature allows users to receive e-mail alerts when a critical event occurs on the managed server. The following example shows how to test the e-mail alert feature to ensure that the iDRAC can properly send e-mail alerts across the network.

```
racadm testemail -i 2
```

NOTE: Ensure that the SMTP and E-mail Alert settings are configured before testing the e-mail alert feature. See "Configuring E-Mail Alerts" on page 64 for more information.

Testing the iDRAC SNMP Trap Alert Feature

The iDRAC SNMP trap alerting feature allows SNMP trap listener configurations to receive traps for system events that occur on the managed server.

The following example shows how a user can test the SNMP trap alert feature.

```
racadm testtrap -i 2
```

NOTE: Before you test the iDRAC SNMP trap alerting feature, ensure that the SNMP and trap settings are configured correctly. See the **testtrap** and **testemail** subcommand descriptions to configure these settings.

Configuring iDRAC Network Properties

To generate a list of available network properties, type the following:

```
racadm getconfig -g cfgLanNetworking
```

To use DHCP to obtain an IP address, use the following command to write the object **cfgNicUseDhcp** and enable this feature:

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

The commands provide the same configuration functionality as the iDRAC configuration utility when you are prompted to type <Ctrl><E>. For more information about configuring network properties with the iDRAC configuration utility, see "LAN" on page 199.

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
```

```
racadm config -g cfgLanNetworking -o
cfgDNSServersFromDHCP 0
```

```
racadm config -g cfgLanNetworking -o cfgDNSServer1
192.168.0.5
```

```
racadm config -g cfgLanNetworking -o cfgDNSServer2
192.168.0.6
```

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

```
racadm config -g cfgLanNetworking -o cfgDNSRacName
RAC-EK00002
```

```
racadm config -g cfgLanNetworking -o
cfgDNSDomainNameFromDHCP 0
```

```
racadm config -g cfgLanNetworking -o cfgDNSDomainName
MYDOMAIN
```

NOTE: If **cfgNicEnable** is set to **0**, the iDRAC LAN is disabled even if DHCP is enabled.

Configuring IPMI

1 Configure IPMI over LAN by entering the following command:

```
racadm config -g cfgIpmiLan -o cfgIpmiLanEnable 1
```

NOTE: This setting determines the IPMI commands that can be executed from the IPMI over LAN interface. For more information, see the IPMI 2.0 specifications.

a Update the IPMI channel privileges by entering the following command:

```
racadm config -g cfgIpmiLan -o
cfgIpmiLanPrivilegeLimit <level>
```

where *<level>* is one of the following:

- 2 (**User**)
- 3 (**Operator**)
- 4 (**Administrator**)

For example, to set the IPMI LAN channel privilege to 2 (User), type the following command:

```
racadm config -g cfgIpmiLan -o
cfgIpmiLanPrivilegeLimit 2
```

b Set the IPMI LAN channel encryption key, if required, using a command such as the following:

NOTE: The iDRAC IPMI supports the RMCP+ protocol. See the IPMI 2.0 specifications for more information.

```
racadm config -g cfgIpmiLan -o
cfgIpmiEncryptionKey <key>
```

where *<key>* is a 20-character encryption key in a valid hexadecimal format.

2 Configure IPMI Serial over LAN (SOL) using the following command:

```
racadm config -g cfgIpmiSol -o cfgIpmiSolEnable 1
```

NOTE: The IPMI SOL minimum privilege level determines the minimum privilege required to activate IPMI SOL. For more information, see the IPMI 2.0 specification.

a Update the IPMI SOL minimum privilege level using the following command:

```
racadm config -g cfgIpmiSol -o
cfgIpmiSolMinPrivilege <level>
```

where *<level>* is one of the following:

- 2 (**User**)
- 3 (**Operator**)
- 4 (**Administrator**)

For example, to configure the IPMI privileges to 2 (User), enter the following command:

```
racadm config -g cfgIpmiSol -o
cfgIpmiSolMinPrivilege 2
```

NOTE: To redirect the serial console over LAN, ensure that the SOL baud rate is identical to your managed server's baud rate.

b Update the IPMI SOL baud rate using the following command:

```
racadm config -g cfgIpmiSol -o
cfgIpmiSolBaudRate <baud-rate>
```

where *<baud-rate>* is 19200, 57600, or 115200 bps.

For example:

```
racadm config -g cfgIpmiSol -o
cfgIpmiSolBaudRate 57600
```

c Enable SOL by typing the following command at the command prompt.

NOTE: SOL can be enabled or disabled for each individual user.

```
racadm config -g cfgUserAdmin -o
cfgUserAdminSolEnable -i <id> 2
```

where *<id>* is the user's unique ID.

Configuring PEF

You can configure the action you wish the iDRAC to take for each platform alert. Table 9-3 lists the possible actions and the value to identify them in RACADM.

Table 9-3. Platform Event Action

Action	Value
No action	0
Power off	1
Reboot	2
Power Cycle	3

1 Configure PEF actions using the following command:

```
racadm config -g cfgIpmiPef -o cfgIpmiPefAction
-i <index> <action-value>
```

where <*index*> is the PEF index (see Table 5-6 on page 62), and <*action-value*> is a value from Table 9-3.

For example, to enable PEF to reboot the system and send an IPMI alert when a processor critical event is detected, type the following command:

```
racadm config -g cfgIpmiPef -o cfgIpmiPefAction
-i 9 2
```

Configuring PET

1 Enable global alerts using the following command:

```
racadm config -g cfgIpmiLan -o
cfgIpmiLanAlertEnable 1
```

2 Enable PET using the following command:

```
racadm config -g cfgIpmiPet -o
cfgIpmiPetAlertEnable -i <index> <0|1>
```

where <`index`> is the PET destination index and `0` or `1` disable PET or enable PET, respectively.

For example, to enable PET with index 4, type the following command:

```
racadm config -g cfgIpmiPet -o
cfgIpmiPetAlertEnable -i 4 1
```

3 Configure your PET policy using the following command:

```
racadm config -g cfgIpmiPet -o
cfgIpmiPetAlertDestIPAddr -i <index> <IP-address>
```

where <*index*> is the PET destination index and <*IP-address*> is the destination IP address of the system that receives the platform event alerts.

4 Configure the Community Name string.

At the command prompt, type:

```
racadm config -g cfgIpmiLan -o
cfgIpmiPetCommunityName <name>
```

where <*name*> is the PET Community Name.

Configuring E-mail Alerts

1 Enable global alerts by entering the following command:

```
racadm config -g cfgIpmiLan -o
cfgIpmiLanAlertEnable 1
```

2 Enable e-mail alerts by entering the following commands:

```
racadm config -g cfgEmailAlert -o
cfgEmailAlertEnable -i <index> <0|1>
```

where <*index*> is the e-mail destination index and 0 disables the e-mail alert or 1 enables the alert. The e-mail destination index can be a value from 1 through 4.

For example, to enable e-mail with index 4, type the following command:

```
racadm config -g cfgEmailAlert -o
cfgEmailAlertEnable -i 4 1
```

3 Configure your e-mail settings by entering the following command:

```
racadm config -g cfgEmailAlert -o
cfgEmailAlertAddress -i 1 <email-address>
```

where 1 is the e-mail destination index and <*email-address*> is the destination e-mail address that receives the platform event alerts.

4 To configure a custom message, enter the following command:

```
racadm config -g cfgEmailAlert -o
cfgEmailAlertCustomMsg -i <index> <custom-message>
```

where <*index*> is the e-mail destination index and <*custom-message*> is the custom message.

5 Test the configured e-mail alert, if desired, by entering the following command:

```
racadm testemail -i <index>
```

where <*index*> is the e-mail destination index to test.

Configuring IP Filtering (IpRange)

IP address filtering (or *IP Range Checking*) allows iDRAC access only from clients or management workstations whose IP addresses are within a user-specified range. All other login requests are denied.

IP filtering compares the IP address of an incoming login to the IP address range that is specified in the following **cfgRacTuning** properties:

- **cfgRacTuneIpRangeAddr**
- **cfgRacTuneIpRangeMask**

The **cfgRacTuneIpRangeMask** property is applied to both the incoming IP address and to the **cfgRacTuneIpRangeAddr** properties. If the results are identical, the incoming login request is allowed to access the iDRAC. Logins from IP addresses outside this range receive an error.

The login proceeds if the following expression equals zero:

```
cfgRacTuneIpRangeMask & (<incoming-IP-address> ^
cfgRacTuneIpRangeAddr)
```

where & is the bitwise AND of the quantities and ^ is the bitwise exclusive-OR.

See "cfgRacTuning" on page 269 for a complete list of **cfgRacTuning** properties.

Table 9-4. IP Address Filtering (IpRange) Properties

Property	Description
cfgRacTuneIpRangeEnable	Enables the IP range checking feature.
cfgRacTuneIpRangeAddr	Determines the acceptable IP address bit pattern, depending on the 1's in the subnet mask. This property is bitwise *and*ed with **cfgRacTuneIpRangeMask** to determine the upper portion of the allowed IP address. Any IP address that contains this bit pattern in its upper bits is allowed to log in. Logins from IP addresses that are outside this range fail. The default values in each property allow an address range from 192.168.1.0 to 192.168.1.255 to log in.
cfgRacTuneIpRangeMask	Defines the significant bit positions in the IP address. The mask should be in the form of a netmask, where the more significant bits are all 1's with a single transition to all zeros in the lower-order bits.

Configuring IP Filtering

To configure IP filtering in the Web interface, follow these steps:

1. Click **System**→ **Remote Access**→ **iDRAC**→ **Network/Security**.
2. On the **Network Configuration** page, click **Advanced Settings**.
3. Check the **IP Range Enabled** checkbox and enter the **IP Range Address** and **IP Range Subnet Mask**.
4. Click **Apply**.

Following are examples using local RACADM to set up IP filtering.

NOTE: See "Using the Local RACADM Command Line Interface" on page 149 for more information about RACADM and RACADM commands.

1. The following RACADM commands block all IP addresses except 192.168.0.57:

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

```
racadm config -g cfgRacTuning -o
cfgRacTuneIpRangeAddr 192.168.0.57
```

```
racadm config -g cfgRacTuning -o
cfgRacTuneIpRangeMask 255.255.255.255
```

2 To restrict logins to a small set of four adjacent IP addresses (for example, 192.168.0.212 through 192.168.0.215), select all but the lowest two bits in the mask, as shown below:

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

```
racadm config -g cfgRacTuning -o
cfgRacTuneIpRangeAddr 192.168.0.212
```

```
racadm config -g cfgRacTuning -o
cfgRacTuneIpRangeMask 255.255.255.252
```

The last byte of the range mask is set to 252, the decimal equivalent of 11111100b.

IP Filtering Guidelines

Use the following guidelines when enabling IP filtering:

- Ensure that **cfgRacTuneIpRangeMask** is configured in the form of a netmask, where all most significant bits are 1's (which defines the subnet in the mask) with a transition to all 0's in the low-order bits.
- Use the desired range's base address as the value of **cfgRacTuneIpRangeAddr**. The 32-bit binary value of this address should have zeros in all the low-order bits where there are zeros in the mask.

Configuring IP Blocking

IP blocking dynamically determines when excessive login failures occur from a particular IP address and blocks (or prevents) the address from logging into the iDRAC for a preselected time span.

The IP blocking features include:

- The number of allowed login failures (**cfgRacTuneIpBlkFailcount**)
- The time frame in seconds during which these failures must occur (**cfgRacTuneIpBlkFailWindow**)

- The amount of time in seconds that the blocked IP address is prevented from establishing a session after the allowed number of failures is exceeded (**cfgRacTuneIpBlkPenaltyTime**)

As login failures accumulate from a specific IP address, they are registered by an internal counter. When the user logs in successfully, the failure history is cleared and the internal counter is reset.

NOTE: When login attempts are refused from the client IP address, some SSH clients may display the following message: `ssh exchange identification: Connection closed by remote host`.

See "iDRAC Property Database Group and Object Definitions" on page 253 for a complete list of **cfgRacTune** properties.

"Login Retry Restriction Properties" on page 164 lists the user-defined parameters.

Table 9-5. Login Retry Restriction Properties

Property	Definition
cfgRacTuneIpBlkEnable	Enables the IP blocking feature. When consecutive failures (**cfgRacTuneIpBlkFailCount**) from a single IP address are encountered within a specific amount of time (**cfgRacTuneIpBlkFailWindow**), all further attempts to establish a session from that address are rejected for a certain time span (**cfgRacTuneIpBlkPenaltyTime**).
cfgRacTuneIpBlkFailCount	Sets the number of login failures from an IP address before the login attempts are rejected.
cfgRacTuneIpBlkFailWindow	The time frame in seconds during which the failure attempts are counted. When the failures exceed this limit, they are dropped from the counter.
cfgRacTuneIpBlkPenaltyTime	Defines the time span in seconds that login attempts from an IP address with excessive failures are rejected.

Enabling IP Blocking

The following example prevents a client IP address from establishing a session for five minutes if that client has failed five login attempts in a one-minute period of time.

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

```
racadm config -g cfgRacTuning -o
cfgRacTuneIpBlkFailCount 5
```

```
racadm config -g cfgRacTuning -o
cfgRacTuneIpBlkFailWindow 60
```

```
racadm config -g cfgRacTuning -o
cfgRacTuneIpBlkPenaltyTime 300
```

The following example prevents more than three failed attempts within one minute, and prevents additional login attempts for an hour.

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

```
racadm config -g cfgRacTuning -o
cfgRacTuneIpBlkFailCount 3
```

```
racadm config -g cfgRacTuning -o
cfgRacTuneIpBlkFailWindow 60
```

```
racadm config -g cfgRacTuning -o
cfgRacTuneIpBlkPenaltyTime 360
```

Configuring iDRAC Telnet and SSH Services Using Local RACADM

The telnet/SSH console can be configured locally (on the managed server) using RACADM commands.

NOTE: You must have **Configure iDRAC** permission to execute the commands in this section.

NOTE: When you reconfigure telnet or SSH settings in the iDRAC, any current sessions are terminated without warning.

To enable telnet and SSH from the local RACADM, log in to the managed server and type the following commands at a command prompt:

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

To disable the telnet or SSH service, change the value from `1` to `0`:

```
racadm config -g cfgSerial -o cfgSerialTelnetEnable 0
```

```
racadm config -g cfgSerial -o cfgSerialSshEnable 0
```

Type the following command to change the telnet port number on the iDRAC:

```
racadm config -g cfgRacTuning -o cfgRacTuneTelnetPort
<new port number>
```

For example, to change the telnet port from the default 22 to 8022, type this command:

```
racadm config -g cfgRacTuning -o cfgRacTuneTelnetPort
8022
```

For a complete list of available RACADM CLI commands, see "Using the Local RACADM Command Line Interface" on page 149.

Using an iDRAC Configuration File

An iDRAC configuration file is a text file that contains a representation of the values in the iDRAC database. You can use the RACADM **getconfig** subcommand to generate a configuration file containing the current values from the iDRAC. You can then edit the file and use the RACADM **config -f** subcommand to load the file back into the iDRAC, or to copy the configuration to other iDRACs.

Creating an iDRAC Configuration File

The configuration file is a plain (unformatted) text file. You can use any valid file name; the **.cfg** file extension is a recommended convention.

The configuration file can be:

- Created with a text editor
- Obtained from the iDRAC with the RACADM **getconfig** subcommand
- Obtained from the iDRAC with the RACADM **getconfig** subcommand and then edited

To obtain a configuration file, with the RACADM **getconfig** command, enter the following command at a command prompt on the managed server:

```
racadm getconfig -f myconfig.cfg
```

This command creates the file **myconfig.cfg** in the current directory.

Configuration File Syntax

NOTICE: Edit the configuration file with a plain text editor, such as **Notepad** on Windows or **vi** on Linux. The **racadm** utility parses ASCII text only. Any formatting confuses the parser and may corrupt the iDRAC database.

This section describes the format of the configuration file.

- Lines that start with # are comments.

  A comment *must* start in the first column of the line. A # character in any other column is treated as a normal # character.

  Example:

  ```
  #

  # This is a comment

  [cfgUserAdmin]

  cfgUserAdminPrivilege=4
  ```

- 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 include an associated group name generate an error. The configuration data is organized into groups as defined in "iDRAC Property Database Group and Object Definitions" on page 253.

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

  Example:

  `[cfgLanNetworking]` (*group name*)

  `cfgNicIpAddress=143.154.133.121` (*object name*)

- Parameters are specified as *object=value* pairs with no white space between the object, =, and value.

  White space that is included after the value is ignored. White space inside a value string remains unmodified. Any character to the right of the = is taken as is (for example, a second =, or a #, *[*, *]*, and so forth).

- The parser ignores an index object entry.

  You *cannot* specify which index is used. If the index already exists, it is either used or the new entry is created in the first available index for that group.

  The `racadm getconfig -f <filename>` command places a comment in front of index objects, allowing you to see the included comments.

NOTE: You can create an indexed group manually using the following command: racadm config -g <*groupName*> -o <*anchored-object*> -i <*index*> <*unique-anchor-name*>

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

  You must remove an indexed object manually using the following command:

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

NOTE: A NULL string (identified by two "" characters) directs the iDRAC 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>
```

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

  ```
  [cfgUserAdmin]
  ```

  ```
  cfgUserAdminUserName=<username>
  ```

- 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 iDRAC for that group. Any objects within that group are simple modifications when the iDRAC is configured. If a modified object represents a new index, the index is created on the iDRAC during configuration.

- You cannot specify a desired index in a configuration 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 you do not need to make exact index matches between all the RACs being managed. New users are added to the first available index. A configuration file that parses and runs correctly on one iDRAC may not run correctly on another if all indexes are full and you must add a new user.

Modifying the iDRAC IP Address in a Configuration File

When you modify the iDRAC IP address in the configuration file, remove all unnecessary <*variable*>=<*value*> entries. Only the actual variable group's label with "[" and "]" remains, including the two <*variable*>=<*value*> entries pertaining to the IP address change.

For example:

```
#
#   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
```

Loading the Configuration File Into the iDRAC

The command `racadm config -f <filename>` parses the configuration file to verify that valid group and object names are present and that syntax rules are followed. If the file is error-free the command then updates the iDRAC database with the contents of the file.

NOTE: To verify the syntax only and not update the iDRAC database, add the **-c** option to the **config** subcommand.

Errors in the configuration file are flagged with the line number and a message that explains the problem. You must correct all errors before the configuration file can update the iDRAC.

NOTICE: Use the **racresetcfg** subcommand to reset the database and the iDRAC 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.

Before you execute the `racadm config -f <filename>` command, you can run the **racreset** subcommand to reset the iDRAC to its default settings. Ensure that the configuration file you will load includes all desired objects, users, indexes, and other parameters.

To update the iDRAC with the configuration file, execute the following command at the managed server's command prompt:

```
racadm config -f <filename>
```

After the command has completed, you can execute the RACADM **getconfig** subcommand to confirm that the update succeeded.

Configuring Multiple iDRACs

Using a configuration file, you can configure other iDRACs with identical properties. Follow these steps to configure multiple iDRACS:

1 Create the configuration file from the iDRAC whose settings you want to replicate to the others. At a command prompt on the managed server, enter the following command:

```
racadm getconfig -f <filename>
```

where <*filename*> is the name of a file to save the iDRAC properties, such a **myconfig.cfg**.

See "Creating an iDRAC Configuration File" on page 166 for more information.

NOTE: Some configuration files contain unique iDRAC information (such as the static IP address) that must be modified before you export the file to other iDRACs.

2 Edit the configuration file you created in the previous step and remove or comment-out any settings you *do not* want to replicate.

3 Copy the edited configuration file to a network drive where it is accessible to each managed server whose iDRAC you want to configure.

4 For each iDRAC you want to configure:

   a Log in to the managed server and start a command prompt.

   b If you want to reconfigure the iDRAC from the default settings, enter the following command:

   ```
   racadm racreset
   ```

   c Load the configuration file into the iDRAC with the following command:

   ```
   racadm config -f <filename>
   ```

   where <*filename*> is the name of the configuration file you created. Include the full path if the file is not in the working directory.

   d Reset the iDRAC that was configured by entering the following command:

   ```
   racadm reset
   ```

10

Using the iDRAC SM-CLP Command Line Interface

This section provides information about the Server Management Workgroup (SMWG) Server Management-Command Line Protocol (SM-CLP) that is incorporated in the iDRAC.

NOTE: This section assumes that you are familiar with the Systems Management Architecture for Server Hardware (SMASH) Initiative and the SMWG SM-CLP specifications. For more information on these specifications, see the Distributed Management Task Force (DMTF) website at **www.dmtf.org**.

The iDRAC SM-CLP is a protocol driven by the DMTF and SMWG to provide standards for systems management CLI implementations. Many efforts are driven by a defined SMASH architecture that is targeted as a foundation for more standardized systems management set of components. The SMWG SM-CLP is a subcomponent of the overall SMASH efforts driven by DMTF.

SM-CLP provides a subset of the functionality provided by the local RACADM command line interface, but with a different access path. SM-CLP executes within the iDRAC, while RACADM executes on the managed server. Also, RACADM is a Dell proprietary interface, where SM-CLP is an industry standard interface. See "RACADM and SM-CLP Equivalencies" on page 295 for a mapping of the RACADM and SM-CLP commands.

System Management With SM-CLP

The iDRAC SM-CLP enables you to manage the following system features from a command line or script:

- Server Power Management — Turn on, shutdown, or reboot the system
- System Event Log (SEL) Management — Display or clear the SEL records
- iDRAC user account management

- Active Directory configuration
- iDRAC LAN configuration
- SSL Certificate Signature Request (CSR) generation
- Virtual media configuration
- Serial over LAN (SOL) redirection over Telnet or SSH

iDRAC SM-CLP Support

SM-CLP is hosted from the iDRAC firmware and supports telnet and SSH connections. The iDRAC SM-CLP interface is based on the SM-CLP Specification Version 1.0 provided by the DMTF organization.

The following sections provide an overview of the SM-CLP feature that is hosted from the iDRAC.

SM-CLP Features

The SM-CLP specification provides a common set of standard SM-CLP verbs that can be used for simple systems management through the CLI.

SM-CLP promotes the concept of verbs and targets to provide system configuration capabilities through the CLI. The verb indicates the operation to perform and the target determines the entity (or object) that runs the operation.

The following is the syntax of the SM-CLP command line:

```
<verb> [<options>] [<target>] [<properties>]
```

Table 10-1 provides a list of the verbs the iDRAC CLI supports, the syntax of each command, and a list of the options the verb supports.

Table 10-1. Supported SM-CLP CLI Verbs

Verb	Description	Options
cd	Navigates through the managed system address space using the shell. Syntax: `cd [options] [target]`	–default, –examine, –help, –output, –version

Table 10-1. Supported SM-CLP CLI Verbs *(continued)*

Verb	Description	Options
delete	Deletes an object instance. Syntax: `delete [options] target`	–examine, –help, –output, –version
dump	Moves a binary image from the MAP to a URI. `dump -destination <URI> [options] [target]`	–destination, –examine, –help, –output, –version
exit	Exits from the SM-CLP shell session. Syntax: `exit [options]`	–help, –output, –version
help	Displays help for SM-CLP commands. `help`	-examine, -help, -output, -version
load	Moves a binary image to the MAP from a URI. Syntax: `load -source <URI> [options] [target]`	–examine, –help, –output, –source, –version
reset	Resets the target. Syntax: `reset [options] [target]`	–examine, –help, –output, –version
set	Sets the properties of a target Syntax: `set [options] [target] <property name>=<value>`	–examine, –help, –output, –version
show	Displays the target properties, verbs, and subtargets. Syntax: `show [options] [target] <property name>=<value>`	-all, -default, –display, –examine, –help, –level, –output, –version

Table 10-1. Supported SM-CLP CLI Verbs *(continued)*

Verb	Description	Options
start	Starts a target. Syntax: `start [options] [target]`	–examine, –force, –help, –output, –version
stop	Shuts down a target. Syntax: `stop [options] [target]`	–examine, –force, –help, –output, –state, –version, –wait
version	Displays the version attributes of a target. Syntax: `version [options]`	–examine, –help, –output, –version

Table 10-2 describes the SM-CLP options. Some options have abbreviated forms, as shown in the table.

Table 10-2. Supported SM-CLP Options

SM-CLP Option	Description
–all, –a	Instructs the verb to perform all possible functions.
-destination	Specifies the location to store an image in the dump command. Syntax: -destination <URI>
-display, -d	Filters the command output. Syntax: `-display <properties | targets | verbs>[, <properties | targets | verbs>]*`
-examine, -x	Instructs the command processor to validate the command syntax without executing the command.
–help, –h	Displays help for the verb.

Table 10-2. Supported SM-CLP Options

SM-CLP Option	Description
–level, -l	Instructs the verb to operate on targets at additional levels beneath the specified target. Syntax: `-level <n	all>`
–output, –o	Specifies the format for the output. Syntax: `-output <text	clpcsv	clpxml>`
-source	Specifies the location of an image in a load command. Syntax: -source <URI>
–version, –v	Displays the SMASH-CLP version number.

Navigating the MAP Address Space

NOTE: The slash (/) and backslash (\) are interchangeable in SM-CLP address paths. However, a backslash at the end of a command line continues the command on the next line and is ignored when the command is parsed.

Objects that can be managed with SM-CLP are represented by targets arranged in a hierarchical space called the Manageability Access Point (MAP) address space. An address path specifies the path from the root of the address space to an object in the address space.

The root target is represented by a slash (/) or a backslash (\). It is the default starting point when you log in to the iDRAC. Navigate down from the root using the `cd` verb. For example to navigate to the third record in the System Event Log (SEL), enter the following command:

```
->cd /system1/sp1/logs1/record3
```

Enter the `cd` verb with no target to find your current location in the address space. The `..` and `.` abbreviations work as they do in Windows and Linux: `..` refers to the parent level and `.` refers to the current level.

Targets

Table 10-3 provides a list of targets available through the SM-CLP.

Table 10-3. SM-CLP Targets

Target	Definition
/system1/	The managed system target.
/system1/sp1	The service processor.
/system1/sol1	Serial over LAN target.
/system1/sp1/account1 through /system1/sp1/account16	The sixteen local iDRAC user accounts. `account1` is the root account.
/system1/sp1/enetport1	The iDRAC NIC MAC address.
/system1/sp1/enetport1/lanendpt1/ ipendpt1	The iDRAC IP, gateway, and netmask settings.
/system1/sp1/enetport1/lanendpt1/ ipendpt1/dnsendpt1	The iDRAC DNS server settings.
/system1/sp1/group1 through /system1/sp1/group5	The Active Directory standard schema groups.
/system1/sp1/logs1	The log collections target.
/system1/sp1/logs1/record1	An individual SEL record instance on the managed system.
/system1/sp1/logs1/records	The SEL target on the managed system.
/system1/sp1/oemdell_racsecurity1	Storage for parameters used to generate a Certificate Signing Request.
/system1/sp1/oemdell_ssl1	SSL certificate request state.
/system1/sp1/oemdell_vmservice1	The virtual media configuration and state.

Using the Show Verb

To learn more about a target use the `show` verb. This verb displays the target's properties, sub-targets, and a list of the SM-CLP verbs that are allowed at that location.

Using the -display Option

The **show –display** option allows you to limit the output of the command to one or more of properties, targets, and verbs. For example, to display just the properties and targets at the current location, use the following command:

```
show -d properties,targets /system1/sp1/account1
```

To list only certain properties, qualify them, as in the following command:

```
show -d properties=(userid,username)
/system1/sp1/account1
```

If you only want to show one property, you can omit the parentheses.

Using the -level Option

The **show -level** option executes **show** over additional levels beneath the specified target. For example, if you want to see the **username** and **userid** properties of the **account1** through **account16** targets beneath **/system1/sp1**, you could enter the following command:

```
show -l 1 -d properties=(userid,username)
/system1/sp1/account*
```

To see all targets and properties in the address space, use the **-l all** option, as in the following command:

```
show -l all -d properties /
```

Using the -output Option

The **-output** option specifies one of four formats for the output of SM-CLP verbs: **text**, **clpcsv**, **keyword**, and **clpxml**.

The default format is **text**, and is the most readable output. The **clpcsv** format is a comma-separated values format suitable for loading into a spreadsheet program. The **keyword** format outputs information as a list of keyword=value pairs one per line. The **clpxml** format is an XML document containing a **response** XML element. The DMTF has specified the **clpcsv** and **clpxml** formats and their specifications can be found on the DMTF website at **www.dmtf.org**.

The following example shows how to output the contents of the SEL in XML:

```
show -l all -output format=clpxml /system1/sp1/logs1
```

iDRAC SM-CLP Examples

The following subsections provide examples for using the SM-CLP to perform the following operations:

- Server power management
- SEL management
- MAP target navigation
- Display system properties
- Setting the iDRAC IP address, subnet mask, and gateway address

Server Power Management

Table 10-4 provides examples of using SM-CLP to perform power management operations on a managed server.

Table 10-4. Server Power Management Operations

Operation	Syntax

Logging into the iDRAC using the SSH interface	`>ssh 192.168.0.120`
	`>login: root`
	`>password:`

Power down the server	`->stop /system1`
	`system1 has been stopped successfully`

Power up the server from a powered-off state	`->start /system1`
	`system1 has been started successfully`

Reboot the server	`->reset /system1`
	`system1 has been reset successfully`

SEL Management

Table 10-5 provides examples of using the SM-CLP to perform SEL-related operations on the managed system.

Table 10-5. SEL Management Operations

Operation	Syntax

Viewing the SEL	`->show /system1/sp1/logs1`
	
	`Targets:`
	`  record1`
	`  record2`
	`  record3`
	`  record4`
	`  record5`
	
	`Properties:`
	`  Description=IPMI SEL`
	`  MaxNumberOfRecords=512`
	`  CurrentNumberOfRecords=5`
	
	`Verbs:`
	`  cd`
	`  delete`
	`  exit`
	`  help`
	`  show`
	`  version`

Table 10-5. SEL Management Operations *(continued)*

Operation	Syntax

Viewing the SEL record	`->show /system1/sp1/logs1/record4`
	`ufip=/system1/sp1/logs1/log1/record4`
	
	`Properties:`
	` Caption=Not defined`
	` Description=Backplane Drive 0: drive slot sensor for Backplane, drive presence was asserted`
	` ElementName=Not Supported`
	` LogCreationClassName=CIM_RecordLog LogName=IPMI SEL`
	` CreationClassName=CIM_LogRecord`
	` RecordID=4`
	` MessageTimeStamp=16:37:10,January 13,2007`
	
	`Verbs:`
	` cd`
	` exit`
	` help`
	` show`
	` version`

Clearing the SEL	`->delete /system1/sp1/logs1`
	`All records deleted successfully`

MAP Target Navigation

Table 10-6 provides examples of using the **cd** verb to navigate the MAP. In all examples, the initial default target is assumed to be /.

Table 10-6. Map Target Navigation Operations

Operation	Syntax

Navigate to the system target and reboot	`->cd system1`
	`->reset`
	
	NOTE: The current default target is /.

Table 10-6. Map Target Navigation Operations *(continued)*

Operation	Syntax

Navigate to the SEL target and display the log records	`->cd system1`
	`->cd sp1`
	`->cd logs1`
	`->show`

	`->cd system1/sp1/logs1`
	`->show`

Display current target	`->cd .`
Move up one level	`->cd ..`
Exiting the shell	`->exit`

Setting the iDRAC IP Address, Subnet Mask, and Gateway Address

Using SM-CLP to update the iDRAC network properties is a two-part process:

1 Set new values for the NIC properties at location **/system1/sp1/enetport1/lanendpt1/ipendpt1**:

- **oemdell_nicenable** — set to 1 to enable iDRAC networking, 0 to disable
- **ipaddress** — the IP address
- **subnetmask** — the subnet mask
- **oemdell_usedhcp** — set to 1 to enable using DHCP to set the **ipaddress** and **subnetmask** properties, 0 to set static values

2 Commit the new values by setting the **committed** property to 1.

Whenever the **commit** property has the value of 1, the current settings of the properties are active. When you change any of the properties, the **commit** property is reset to 0 to indicate that the values have not been committed.

NOTE: The **commit** property only affects the properties at the **/system1/sp1/enetport1/lanendpt1/ipendpt1** MAP location. All other SM-CLP commands take effect immediately.

NOTE: If you use local RACADM to set the iDRAC network properties, your changes take affect immediately because local RACADM does not depend upon a network connection.

When you commit the changes, the new network settings take effect, which causes your telnet or ssh session to be terminated. By introducing the commit step, you can delay the termination of your session until you have completed all of your SM-CLP commands.

Table 10-7 provides examples of setting the iDRAC properties using SM-CLP.

Table 10-7. Setting iDRAC Networking Properties with SM-CLP

Operation	Syntax
Navigate to the iDRAC NIC properties location	`->cd /system1/sp1/enetport1/lanendpt1/ipendpt1`
Set the new IP address	`->set ipaddress=10.10.10.10`
Set the subnet mask	`->set subnetmask=255.255.255.255`
Turn on the DHCP flag	`->set oemdell_usedhcp=1`
Enable the NIC	`->set oemdell_nicenable=1`
Commit the changes	`->set committed=1`

Updating the iDRAC Firmware Using SM-CLP

To update the iDRAC firmware using SM-CLP, you must know the TFTP URI for the Dell update package.

Follow these steps to update the firmware using SM-CLP:

1 Log in to the iDRAC using telnet or SSH.

2 Check the current firmware version by entering the following command:

```
version
```

3 Enter the following command:

```
load -source tftp://<tftp-server>/<update-path>
/system1/sp1
```

where <*tftp-server*> is the DNS name or IP address of your TFTP server and <*update-path*> is the path to the update package on the TFTP server.

Your telnet or SSH session will be terminated. You may need to wait several minutes for the firmware update to complete.

4 To verify that the new firmware was written, start a new telnet or SSH session and re-enter the version command again.

Using Serial Over LAN (SOL) With Telnet or SSH

Use a Telnet or SSH console on your management station to connect to the iDRAC and then redirect the serial port of the managed server into your console. This feature is an alternative to IPMI SOL, which requires a utility such as **solproxy** to translate the serial stream to and from network packets. The iDRAC SOL implementation eliminates the need for an additional utility because the serial to network translation happens within the iDRAC.

The Telnet or SSH console that you use should be able to interpret and respond to the data arriving from the managed server's serial port. The serial port usually attaches to a shell that emulates an ANSI- or VT100- terminal.

Using Telnet, you connect to the IPMI LAN SOL port—port 2100. The serial console is automatically redirected to your Telnet console.

With SSH or Telnet, you connect to the iDRAC the same way you connect to SM-CLP. The SOL redirection can then be started from the **/system1/sol1** target.

See "Installing Telnet or SSH Clients" on page 46 for more information about using Telnet and SSH clients with iDRAC.

Using SOL Over Telnet With HyperTerminal on Microsoft Windows

1 Select **Start**→ **All Programs**→ **Accessories**→ **Communications**→ **HyperTerminal**.

2 Enter a name for the connection, choose an Icon, and click **OK**.

3 Choose **TCP/IP (Winsock)** from the list in the **Connect using** field.

4. Enter the DNS name or IP address of the iDRAC in the **Host address** field.
5. Enter the Telnet port number in the **Port number** field.
6. Click **OK**.

To end the SOL session, click the HyperTerminal disconnect icon.

Using SOL Over Telnet With Linux

To start SOL from Telnet on a Linux management station, follow these steps:

1. Start a shell.
2. Connect to the iDRAC with the following command:

   ```
   telnet <iDRAC-ip-address>
   ```

   NOTE: If you have changed the port number for the Telnet service from the default, port 23, add the port number to the end of the **telnet** command.

3. Enter the following command to start SOL:

   ```
   start /system1/sol1
   ```

   This connects you to the managed server's serial port.

When you are ready to quit SOL, type `<Ctrl>+]` (hold down control and type a right square bracket, and then release). A Telnet prompt displays. Type `quit` to exit Telnet.

Using SOL Over SSH

The **/system1/sol1** target allows you to redirect the managed server's serial port into your SSH console.

1. Connect to the iDRAC using OpenSSH or PuTTY.
2. Enter the following command to start SOL:

   ```
   start /system1/sol1
   ```

This connects you to the managed server's serial port. The SM-CLP commands are no longer available to you.

When you are ready to quit SOL redirection, type `<Ctrl>+.` (hold down control, type a period, and then release).The SSH session will be closed.

You cannot return to SM-CLP once you have started SOL. You must quit the SSH session and start a new one to use SM-CLP.

11

Deploying Your Operating System Using iVM-CLI

The Virtual Media Command Line Interface (iVM-CLI) utility is a command-line interface that provides virtual media features from the management station to the iDRAC in the remote system. Using iVM-CLI and scripted methods, you can deploy your operating system on multiple remote systems in your network.

This section provides information on integrating the iVM-CLI utility into your corporate network.

Before You Begin

Before using the iVM-CLI utility, ensure that your targeted remote systems and corporate network meet the requirements listed in the following sections.

Remote System Requirements

- The iDRAC is configured in each remote system.

Network Requirements

A network share must contain the following components:

- Operating system files
- Required drivers
- Operating system boot image file(s)

  The image file must be an operating system CD or a CD/DVD ISO image with an industry-standard, bootable format.

Creating a Bootable Image File

Before you deploy your image file to the remote systems, ensure that a supported system can boot from the file. To test the image file, transfer the image file to a test system using the iDRAC Web user interface and then reboot the system.

The following sections provide specific information for creating image files for Linux and Windows systems.

Creating an Image File for Linux Systems

Use the Data Duplicator (dd) utility to create a bootable image file for your Linux system.

To run the utility, open a command prompt and type the following:

```
dd if=<input-device> of=<output-file>
```

For example:

```
dd if=/dev/sdc0 of=mycd.img
```

Creating an Image File for Windows Systems

When choosing a data replicator utility for Windows image files, select a utility that copies the image file and the CD/DVD boot sectors.

Preparing for Deployment

Configuring the Remote Systems

1. Create a network share that can be accessed by the management station.
2. Copy the operating system files to the network share.
3. If you have a bootable, preconfigured deployment image file to deploy the operating system to the remote systems, skip this step.

   If you do not have a bootable, preconfigured deployment image file, create the file. Include any programs and/or scripts used for the operating system deployment procedures.

   For example, to deploy a Microsoft® Windows® operating system, the image file may include programs that are similar to deployment methods used by Microsoft Systems Management Server (SMS).

When you create the image file, do the following:

- Follow standard network-based installation procedures
- Mark the deployment image as "read only" to ensure that each target system boots and executes the same deployment procedure

4 Perform one of the following procedures:

- Integrate **ipmitool** and the Virtual Media command line interface (iVM-CLI) into your existing operating system deployment application. Use the sample **ivmdeploy** script as a guide to using the utility.
- Use the existing **ivmdeploy** script to deploy your operating system.

Deploying the Operating System

Use the iVM-CLI utility and the **ivmdeploy** script included with the utility to deploy the operating system to your remote systems.

Before you begin, review the sample **ivmdeploy** script included with the iVM-CLI utility. The script shows the detailed steps needed to deploy the operating system to remote systems in your network.

The following procedure provides a high-level overview for deploying the operating system on targeted remote systems.

1 List the iDRAC IP addresses of the remote systems that will be deployed in the **ip.txt** text file, one IP address per line.

2 Insert a bootable operating system CD or DVD into the client media drive.

3 Run **ivmdeploy** at the command line.

To run the ivmdeploy script, enter the following command at the command prompt:

```
ivmdeploy -r ip.txt -u <idrac-user> -p <idrac-passwd>
-c {<iso9660-img> | <path>}
```

where:

- *<idrac-user>* is the iDRAC user name, for example **root**
- *<idrac-passwd>* is the password for the iDRAC user, for example **calvin**
- *<iso9660-img>* is the path to an ISO9660 image of the operating system installation CD or DVD

- *<path>* is the path to the device containing the operating system installation CD or DVD

The **ivmdeploy** script passes its command line options to the **ivmcli** utility. See "Command Line Options" on page 191 for details about these options. The script processes the **-r** option slightly differently than the **ivmcli -r** option. If the argument to the **-r** option is the name of an existing file, the script reads iDRAC IP addresses from the specified file and runs the **ivmcli** utility once for each line. If the argument to the **-r** option is not a filename, then it should be the address of a single iDRAC. In this case, the **-r** works as described for the **ivmcli** utility.

The ivmdeploy script supports installation only from a CD/DVD or a CD/DVD ISO9660 image. If you need to install from a floppy disk or a floppy disk image, you can modify the script to use the **ivmcli -f** option.

Using the Virtual Media Command Line Interface Utility

The Virtual Media Command Line Interface (iVM-CLI) utility is a scriptable command-line interface that provides virtual media features from the management station to the iDRAC.

The iVM-CLI utility provides the following features:

NOTE: When virtualizing read-only image files, multiple sessions may share the same image media. When virtualizing physical drives, only one session can access a given physical drive at a time.

- Removable media devices or image files that are consistent with the Virtual Media plug-ins
- Automatic termination when the iDRAC firmware boot once option is enabled
- Secure communications to the iDRAC using Secure Sockets Layer (SSL)

Before you run the utility, ensure that you have Virtual Media user privilege to the iDRAC.

If your operating system supports administrator privileges or an operating system-specific privilege or group membership, administrator privileges are also required to run the iVM-CLI command.

The client system's administrator controls user groups and privileges, thereby controlling the users who can run the utility.

For Windows systems, you must have Power User privileges to run the iVM-CLI utility.

For Linux systems, you can access the iVM-CLI utility without administrator privileges by using the **sudo** command. This command provides a centralized means of providing non-administrator access and logs all user commands. To add or edit users in the iVM-CLI group, the administrator uses the **visudo** command. Users without administrator privileges can add the **sudo** command as a prefix to the iVM-CLI command line (or to the iVM-CLI script) to obtain access to the iDRAC in the remote system and run the utility.

Installing the iVM-CLI Utility

The iVM-CLI utility is located on the *Dell OpenManage™ Systems Management Consoles CD*, which is included with your Dell OpenManage System Management Software Kit. To install the utility, insert the *System Management Consoles* CD into your system's CD drive and follow the on-screen instructions.

The *Systems Management Consoles* CD contains the latest systems management software products, including diagnostics, storage management, remote access service, and the RACADM utility. This CD also contains readme files, which provide the latest systems management software product information.

The *Systems Management Consoles* CD includes **ivmdeploy**—a sample script that illustrates how to use the iVM-CLI and RACADM utilities to deploy software to multiple remote systems.

NOTE: The ivmdeploy script is dependent upon the other files that are present in its directory when it is installed. If want to use the script from another directory, you must copy all of the files with it.

Command Line Options

The iVM-CLI interface is identical on both Windows and Linux systems. The utility uses options that are consistent with the RACADM utility options. For example, an option to specify the iDRAC IP address requires the same syntax for both RACADM and iVM-CLI utilities.

The iVM-CLI command format is as follows:

```
ivmcli [parameter] [operating_system_shell_options]
```

Command-line syntax is case sensitive. See "iVM-CLI Parameters" for more information.

If the remote system accepts the commands and the iDRAC authorizes the connection, the command continues to run until either of the following occurs:

- The iVM-CLI connection terminates for any reason.
- The process is manually terminated using an operating system control. For example, in Windows, you can use the Task Manager to terminate the process.

iVM-CLI Parameters

iDRAC IP Address

```
-r <iDRAC-IP-address>[:<iDRAC-SSL-port>]
```

This parameter provides the iDRAC IP address and SSL port, which the utility needs to establish a Virtual Media connection with the target iDRAC. If you enter an invalid IP address or DDNS name, an error message appears and the command is terminated.

<iDRAC-IP-address> is a valid, unique IP address or the iDRAC Dynamic Domain Naming System (DDNS) name (if supported). If *<iDRAC-SSL-port>* is omitted, port 443 (the default port) is used. The optional SSL port is not required unless you change the iDRAC default SSL port.

iDRAC User Name

```
-u <iDRAC-user-name>
```

This parameter provides the iDRAC user name that will run Virtual Media.

The *<iDRAC-user-name>* must have the following attributes:

- Valid user name
- iDRAC Virtual Media User permission

If iDRAC authentication fails, an error message appears and the command is terminated.

iDRAC User Password

`-p` *`<iDRAC-user-password>`*

This parameter provides the password for the specified iDRAC user.

If iDRAC authentication fails, an error message displays and the command terminates.

Floppy/Disk Device or Image File

`-f {`*`<device-name>`*` | `*`<image-file>`*`}`

where *<device-name>* is a valid drive letter (for Windows systems) or a valid device file name, including the mountable file system partition number, if applicable (for Linux systems); and *<image-file>* is the filename and path of a valid image file.

This parameter specifies the device or file to supply the virtual floppy/disk media.

For example, an image file is specified as:

`-f c:\temp\myfloppy.img` (Windows system)

`-f /tmp/myfloppy.img` (Linux system)

If the file is not write-protected, Virtual Media may write to the image file. Configure the operating system to write-protect a floppy image file that should not be overwritten.

For example, a device is specified as:

`-f a:\` (Windows system)

`-f /dev/sdb4 # 4th partition on device /dev/sdb` (Linux system)

If the device provides a write-protection capability, use this capability to ensure that Virtual Media will not write to the media.

Omit this parameter from the command line if you are not virtualizing floppy media. If an invalid value is detected, an error message displays and the command terminates.

CD/DVD Device or Image File

`-c {<device-name> | <image-file>}`

where <*device-name*> is a valid CD/DVD drive letter (Windows systems) or a valid CD/DVD device file name (Linux systems) and <*image-file*> is the file name and path of a valid ISO-9660 image file.

This parameter specifies the device or file that will supply the virtual CD/DVD-ROM media:

For example, an image file is specified as:

`-c c:\temp\mydvd.img` (Windows systems)

`-c /tmp/mydvd.img` (Linux systems)

For example, a device is specified as:

`-c d:\` (Windows systems)

`-c /dev/cdrom` (Linux systems)

Omit this parameter from the command line if you are not virtualizing CD/DVD media. If an invalid value is detected, an error message is listed and the command terminates.

Specify at least one media type (floppy or CD/DVD drive) with the command, unless only switch options are provided. Otherwise, an error message displays and the command terminates and generates an error.

Version Display

`-v`

This parameter is used to display the iVM-CLI utility version. If no other non-switch options are provided, the command terminates without an error message.

Help Display

`-h`

This parameter displays a summary of the iVM-CLI utility parameters. If no other non-switch options are provided, the command terminates without error.

Manual Display

`-m`

This parameter displays a detailed "man page" for the iVM-CLI utility, including descriptions of all of the possible options.

Encrypted Data

`-e`

When this parameter is included in the command line, iVM-CLI will use an SSL-encrypted channel to transfer data between the management station and the iDRAC in the remote system. If this parameter is not included in the command line, the data transfer is not encrypted.

iVM-CLI Operating System Shell Options

The following operating system features can be used in the iVM-CLI command line:

- stderr/stdout redirection — Redirects any printed utility output to a file.

  For example, using the greater-than character (>) followed by a filename overwrites the specified file with the printed output of the iVM-CLI utility.

  NOTE: The iVM-CLI utility does not read from standard input (**stdin**). As a result, **stdin** redirection is not required.

- Background execution — By default, the iVM-CLI utility runs in the foreground. Use the operating system's command shell features to cause the utility to run in the background. For example, under a Linux operating system, the ampersand character (&) following the command causes the program to be spawned as a new background process.

The latter technique is useful in script programs, as it allows the script to proceed after a new process is started for the iVM-CLI command (otherwise, the script would block until the iVM-CLI program is terminated). When multiple iVM-CLI instances are started in this way, and one or more of the command instances must be manually terminated, use the operating system-specific facilities for listing and terminating processes.

iVM-CLI Return Codes

0 = No error

1 = Unable to connect

2 = iVM-CLI command line error

3 = RAC firmware connection dropped

English-only text messages are also issued to standard error output whenever errors are encountered.

12

Using the iDRAC Configuration Utility

Overview

The iDRAC Configuration Utility is a pre-boot configuration environment that allows you to view and set parameters for the iDRAC and for the managed server. Specifically, you can:

- View the firmware revision numbers for the iDRAC and Primary Backplane firmware
- Configure, enable, or disable the iDRAC local area network
- Enable or disable IPMI over LAN
- Enable a LAN Platform Event Trap (PET) destination
- Attach or detach the Virtual Media devices
- Change the administrative username and password
- Reset the iDRAC configuration to the factory defaults
- View System Event Log (SEL) messages or clear messages from the log

The tasks you can perform using iDRAC configuration utility can also be performed using other utilities provided by the iDRAC or OpenManage software, including the Web interface, the SM-CLP command line interface, the local RACADM command line interface and, in the case of basic network configuration, at the CMC LCD during initial CMC configuration.

Starting the iDRAC Configuration Utility

You must use an iKVM-connected console to access the iDRAC Configuration Utility initially or after a resetting the iDRAC to the default settings.

1. At the keyboard connected to the iKVM console, press <Print Screen> to display the iKVM On Screen Configuration and Reporting (OSCAR) menu. Use <Up Arrow> and <Down Arrow> to highlight the slot containing your server, then press <Enter>.
2. Turn on or restart the server by pressing the power button on the front of the server.
3. When you see the **Press <Ctrl-E> for Remote Access Setup within 5 sec.....** message, immediately press <Ctrl><E>.

NOTE: If your operating system begins to load before you press <Ctrl><E>, allow the system to finish booting, then restart your server and try again.

The iDRAC Configuration Utility displays. The first two lines provide information about the iDRAC firmware and primary backplane firmware revisions. The revision levels can be useful in determining whether a firmware upgrade is needed.

The iDRAC firmware is the portion of the firmware concerned with external interfaces, such as the Web interface, SM-CLP, and Web interfaces. The primary backplane firmware is the portion of the firmware that interfaces with and monitors the server hardware environment.

Using the iDRAC Configuration Utility

Beneath the firmware revision messages, the remainder of the iDRAC Configuration Utility is a menu of items that you can access by using <Up Arrow> and <Down Arrow>.

- If a menu item leads to a submenu or an editable text field, press <Enter> to access the item and <Esc> to leave it when you have finished configuring it.
- If an item has selectable values, such as Yes/No or Enabled/Disabled, press <Left Arrow>, <Right Arrow>, or <Spacebar> to choose a value.
- If an item is not editable, it appears in blue. Some items become editable depending upon other selections you make.

- The bottom line of the screen displays instructions for the current item. You can press <F1> to display help for the current item.
- When you have finished using the iDRAC Configuration Utility, press <Esc> to view the exit menu, where you can choose to save or discard your changes or return to the utility.

The following sections describe the iDRAC Configuration Utility menu items.

LAN

Use <Left Arrow>, <Right Arrow>, and the spacebar to select between **Enabled** and **Disabled**.

The iDRAC LAN is disabled in the default configuration. The LAN must be enabled to permit use of iDRAC facilities, such as the Web interface, telnet/SSH access to the SM-CLP command line interface, console redirection, and virtual media.

If you choose to disable the LAN the following warning is displayed:

```
iDRAC Out-of-Band interface will be disabled if the
LAN Channel is OFF.
```

Press any key to clear the message and continue.

The message informs you that in addition to facilities that you access by connecting to the iDRAC HTTP, HTTPS, telnet or SSH ports directly, out-of-band management network traffic, such as IPMI messages sent to the iDRAC from a management station, are not received when the LAN is disabled. The local RACADM interface remains available and can be used to reconfigure the iDRAC LAN.

IPMI Over LAN (On/Off)

Press <Left Arrow>, <Right Arrow> and the spacebar to choose between **On** and **Off**. When **Off** is selected, the iDRAC will not accept IPMI messages arriving over the LAN interface.

If you choose **Off**, the following warning is displayed:

```
iDRAC Out-of-Band interface will be disabled if the
LAN Channel is OFF.
```

Press any key to clear the message and continue. See "LAN" on page 199 for an explanation of the message.

LAN Parameters

Press <Enter> to display the LAN Parameters submenu. When you have finished configuring the LAN parameters, press <Esc> to return to the previous menu.

Table 12-1. LAN Parameters

Item	Description
RMCP+ Encryption Key	Press <Enter> to edit the value, <Esc> when finished. The RMCP+ Encryption key is a 40-character hexadecimal string (characters 0-9, a-f, and A-F). RMCP+ is an IPMI extension that adds authentication and encryption to IPMI. The default value is a string of 40 0s.
IP Address Source	Select between **DHCP** and **Static**. When DHCP is selected, the **Ethernet IP Address**, **Subnet Mask**, and **Default Gateway** fields are obtained from a DHCP server. If no DHCP server is found on the network, the fields are set to zeros. When **Static** is selected, the **Ethernet IP Address**, **Subnet Mask**, and **Default Gateway** items become editable**.**
Ethernet IP Address	If the **IP Address Source** is set to **DHCP**, this field displays the IP address obtained from DHCP. If the **IP Address Source** is set to **Static**, enter the IP address you wish to assign to the iDRAC. The default is **192.168.0.120** plus the number of the slot containing the server.
MAC Address	This is the non-editable MAC address of the iDRAC network interface.
Subnet Mask	If the **IP Address Source** is set to **DHCP**, this field displays the subnet mask address obtained from DHCP. If the **IP Address Source** is set to **Static**, enter the subnet mask for the iDRAC. The default is **255.255.255.0**.

Table 12-1. LAN Parameters *(continued)*

Item	Description
Default Gateway	If the **IP Address Source** is set to **DHCP**, this field displays the IP address of the default gateway obtained from DHCP. If the **IP Address Source** is set to **Static**, enter the IP address of the default gateway. The default is **192.168.0.1**.
LAN Alert Enabled	Select **On** to enable the Platform Event Trap (PET) LAN alert.
Alert Policy Entry 1	Select Enable or Disable to activate the first alert destination.
Alert Destination 1	Enter the IP address where PET LAN alerts will be forwarded.
Host Name String	Press <Enter> to edit. Enter the name of the host for PET alerts.
DNS Servers from DHCP	Select **On** to retrieve DNS server addresses from a DHCP service on the network. Select **Off** to specify the DNS server addresses below.
DNS Server 1	If **DNS Servers from DHCP** is **Off**, enter the IP address of the first DNS server.
DNS Server 2	If **DNS Servers from DHCP** is **Off**, enter the IP address of the second DNS server.
Register iDRAC Name	Select **On** to register the iDRAC name in the DNS service. Select **Off** if you do not want users to be able to find the iDRAC name in DNS.
iDRAC Name	If **Register iDRAC Name** is set to **On**, press <Enter> to edit the **Current DNS iDRAC Name** text field. Press <Enter> when you have finished editing the iDRAC name. Press <Esc> to return to the previous menu. The iDRAC name must be a valid DNS host name.
Domain Name from DHCP	Select **On** if you want to obtain the domain name from a DHCP service on the network. Select **Off** if you want to specify the domain name.
Domain Name	If **Domain Name from DHCP** is **Off**, press <Enter> to edit the **Current Domain Name** text field. Press <Enter> when you have finished editing. Press <Esc> to return to the previous menu. The domain name must be a valid DNS domain, for example `mycompany.com`.

Virtual Media

Use <Left Arrow> and <Right Arrow> to select **Attached** or **Detached**. When you select **Attached**, the virtual media devices are attached to the USB bus, making them available for use during **Console Redirection** sessions.

If you select **Detached,** users cannot access virtual media devices during **Console Redirection** sessions.

NOTE: To use a USB Flash Drive with the **Virtual Media** feature, the **USB Flash Drive Emulation Type** must be set to **Hard disk** in the BIOS Setup Utility. The BIOS Setup Utility is accessed by pressing <F2> during server start-up. If the **USB Flash Drive Emulation Type** is set to **Auto**, the Flash Drive will appear as a floppy drive to the system.

LAN User Configuration

The LAN user is the iDRAC administrator account, which is **root** by default. Press <Enter> to display the LAN User Configuration submenu. When you have finished configuring the LAN user, press <Esc> to return to the previous menu.

Table 12-2. Lan User Configuration Page

Item	Description
Account Access	Select **Enabled** to enable the administrator account. Select **Disabled** to disable the administrator account.
Account Privilege	Select between **Admin**, **User**, **Operator**, and **No Access**.
Account User Name	Press <Enter> to edit the user name and press <Esc> when you have finished. The default user name is **root**.
Enter Password	Type the new password for the administrator account. The characters are not echoed on the display as you type them.
Confirm Password	Retype the new password for the administrator account. If the characters you enter do not match the characters you entered in the **Enter Password** field, a message is displayed and you must re-enter the password.

Reset to Default

Use the **Reset to Default** menu item to reset all of the iDRAC configuration items to the factory defaults. This may be required, for example, if you have forgotten the administrative user password or if you want to reconfigure the iDRAC from the default settings.

NOTE: In the default configuration, the iDRAC networking is disabled. You cannot reconfigure the iDRAC over the network until you have enabled the iDRAC network in the iDRAC Configuration Utility.

Press <Enter> to select the item. The following warning message appears:

```
Resetting to factory defaults will restore remote Non-
Volatile user settings. Continue?

< NO (Cancel)    >

< YES (Continue) >
```

Select **YES** and press <Enter> to reset the iDRAC to the defaults.

System Event Log Menu

The **System Event Log** Menu allows you to view System Event Log (SEL) messages and to clear the log messages. Press <Enter> to display the **System Event Log Menu**. The system counts the log entries and then displays the total number of records and the most recent message. The SEL retains a maximum of 512 messages.

To view SEL messages, select **View System Event Log** and press <Enter>. Use <Left Arrow> to move to the previous (older) message and <Right Arrow> to move to the next (newer) message. Enter a record number to jump to that record. Press <Esc> when you are through viewing SEL messages.

NOTE: You can only clear the SEL in the iDRAC Configuration Utility or in the iDRAC Web interface.

To clear the SEL, select **Clear the System Event Log** and press <Enter>.

When you have finished with the SEL menu, press <Esc> to return to the previous menu.

Exiting the iDRAC Configuration Utility

When you have finished making changes to the iDRAC configuration, press the <Esc> key to display the Exit menu.

Select Save **Changes and Exit** and press <Enter> to retain your changes.

Select **Discard Changes and Exit** and press <Enter> to ignore any changes you made.

Select **Return to Setup** and press <Enter> to return to the iDRAC Configuration Utility.

13

Recovering and Troubleshooting the Managed Server

This section explains how to perform tasks related to diagnosing and troubleshooting a remote managed server using the iDRAC facilities. It contains the following subsections:

- Trouble Indications — helps you to find messages and other system indications that can lead to a diagnosis of the problem
- Problem-solving tools — describes iDRAC tools that you can use to troubleshoot your system
- Troubleshooting and frequently asked questions — answers to typical situations you may encounter

Safety First–For You and Your System

To perform certain procedures in this section, you must work with the chassis, the PowerEdge server, or other hardware modules. Do not attempt to service the system hardware except as explained in this guide and elsewhere in your system documentation.

⚠ **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 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.**

Trouble Indicators

This section describes indications that there may be a problem with your system.

LED Indicators

The initial indication of system trouble may be the LEDs on the chassis or components installed in the chassis. The following components and modules have status LEDs:

- Chassis LCD display
- Servers
- Fans
- CMCs
- I/O modules
- Power supplies

The single LED on the chassis LCD summarizes the status of all of the components in the system. A solid blue LED on the LCD indicates that no fault conditions have been detected in the system. A blinking amber LED on the LCD indicates that one or more fault conditions have been detected.

If the chassis LCD has a blinking amber LED, you can use the LCD menu to locate the component that has a fault. See the *Dell CMC Firmware Version 1.0 User's Guide* for help using the LCD.

Table 13-1 describes the meanings of the LED on the PowerEdge Server:

Table 13-1. Server LED Indicators

LED indicator	Meaning
solid green	The server is powered on. Absence of the green LED means the server is not powered on.
solid blue	The iDRAC is healthy.
flashing amber	The iDRAC has detected a fault condition or may be in the process of updating firmware.
flashing blue	A user has activated the locator ID for this server.

Hardware Trouble Indicators

Indications that a module has a hardware problem include the following:

- Failure to power up
- Noisy fans

- Loss of network connectivity
- Battery, temperature, voltage, or power monitoring sensor alerts
- Hard drive failures
- USB media failure
- Physical damage caused by dropping, water, or other external stress

When these kinds of problems occur, you can try to correct the problem using these strategies:

- Reseat the module and restart it
- Try inserting the module into a different bay in the chassis
- Try replacing hard drives or USB keys
- Reconnect or replace the power and network cables

If these steps do not correct the problem, consult the *Hardware Owner's Manual* for specific troubleshooting information for the hardware device.

Other Trouble Indicators

Table 13-2. Trouble Indicators

Look for:	Action:
Alert messages from the systems management software	See the systems management software documentation.
Messages in the system Event Log	See "Checking the System Event Log (SEL)" on page 209.
Messages in the start-up POST codes	See "Checking the Post Codes" on page 209.
Messages on the last crash screen	See "Viewing the Last System Crash Screen" on page 210.
Messages in the iDRAC Log	See "Viewing the iDRAC Log" on page 211.

Problem Solving Tools

This section describes iDRAC facilities you can use to diagnose problems with your system, especially when you are trying to solve problems remotely.

- Checking the system health
- Checking the System Event Log for error messages
- Checking the POST codes
- Viewing the last crash screen
- Viewing the iDRAC log
- Accessing system information
- Identifying the managed server in the chassis
- Using the diagnostics console
- Managing power on a remote system

Checking the System Health

When you log in to the iDRAC Web interface, the first page displayed describes the health of the system components. Table 13-3 describes the meaning of the system health indicators.

Table 13-3. System Health Indicators

Indicator	Description
✓	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 question mark icon indicates that the status is unknown.

Click any component on the **Health** page to see information about the component. Sensor readings are displayed for batteries, temperatures, voltages, and power monitoring, helping to diagnose some types of problems. The iDRAC and CMC information pages provide useful current status and configuration information.

Checking the System Event Log (SEL)

The **SEL Log** page displays messages for events that occur on the managed server.

To view the **System Event Log**, perform the following steps:

1. Click **System** and then click the **Logs** tab.
2. Click **System Event Log** to display the **System Event Log** page.

   The **System Event Log** page displays a system health indicator (see Table 13-3), a time stamp, and a description of the event.

3. Click the appropriate **System Event Log** page button to continue (see Table 13-4).

Table 13-4. SEL Page Buttons

Button	Action
Print	Prints the SEL in the sort order that it appears in the window.
Clear Log	Clears the SEL. **NOTE:** The **Clear Log** button appears only if you have **Clear Logs** permission.
Save As	Opens a pop-up window that enables you to save the SEL to a directory of your choice. **NOTE:** If you are using Internet Explorer and encounter a problem when saving, be sure to download the Cumulative Security Update for Internet Explorer, located on the Microsoft® Support website at support.microsoft.com.
Refresh	Reloads the SEL page.

Checking the Post Codes

The **Post Codes** page displays the last system post code prior to booting the operating system. Post codes are progress indicators from the system BIOS, indicating various stages of the boot sequence from Power on Reset, and allow you to diagnose any faults related to system boot-up.

NOTE: View the text for POST code message numbers in the LCD display or in the *Hardware Owner's Manual.*

To view the Post Codes, perform the following steps:

1 Click **System**, the **Logs** tab, and then **Post Codes**.

  The **Post Codes** page displays a system health indicator (see Table 13-3), a hexadecimal code, and a description of the code.

2 Click the appropriate **Post Code** page button to continue (see Table 13-5).

Table 13-5. Post Code Buttons

Button	Action
Print	Prints the **Post Codes** page.
Refresh	Reloads the **Post Codes** page.

Viewing the Last System Crash Screen

NOTICE: The last crash screen feature must be configured in the Server Administrator and in the iDRAC Web interface. See "Configuring the Managed Server to Capture the Last Crash Screen" on page 52 for instructions on configuring this feature.

The **Last Crash Screen** page displays the most recent crash screen, which includes information about the events that occurred before the system crash. The last system crash image is saved in the iDRAC persistent store and is remotely accessible.

To view the **Last Crash Screen** page, perform the following steps:

- Click **System**, the **Logs** tab, and then **Last Crash**.

The **Last Crash Screen** page provides the buttons shown in Table 13-6:

NOTE: The **Save** and **Delete** buttons do not appear if there is no saved crash screen.

Table 13-6. Last Crash Screen Page Buttons

Button	Action
Print	Prints the **Last Crash Screen** page.

Table 13-6. Last Crash Screen Page Buttons

Button	Action
Save	Opens a pop-up window that enables you to save the **Last Crash Screen** page to a directory of your choice.
Delete	Deletes the **Last Crash Screen** page.
Refresh	Reloads the **Last Crash Screen** page.

NOTE: Due to fluctuations in the Auto Recovery timer, the **Last Crash Screen** may not be captured when the System Reset Timer is configured with a value that is too high. The default setting is 480 seconds. Use Server Administrator or IT Assistant to set the System Reset Timer to 60 seconds and ensure that the **Last Crash Screen** functions properly. See "Configuring the Managed Server to Capture the Last Crash Screen" on page 52 for additional information.

Viewing the iDRAC Log

The **iDRAC Log** is a persistent log maintained in the iDRAC firmware. The log contains a list of user actions (such as log in, log out, and security policy changes) and alerts issued by the iDRAC. The oldest entries are overwritten when the log becomes full.

Where the **System Event Log** (SEL) contains records of events that occur in the managed server, the **iDRAC log** contains records of events that occur in the iDRAC.

To access the **iDRAC** Log, perform the following steps:

- Click **System**→ **Remote Access**→ **iDRAC** and then click **iDRAC Log**.

The **iDRAC Log** provides the information in Table 13-7.

Table 13-7. iDRAC Log Page Information

Field	Description
Date/Time	The date and time (for example, `Dec 19 16:55:47`). The iDRAC sets its clock from the managed server's clock. When the iDRAC initially starts and is unable to communicate with the managed server, the time is displayed as the string `System Boot`.
Source	The interface that caused the event.

Table 13-7. iDRAC Log Page Information *(continued)*

Field	Description
Description	A brief description of the event and the user name that logged into the iDRAC.

Using the iDRAC Log Page Buttons

The **iDRAC Log** page provides the following buttons (see Table 13-8).

Table 13-8. iDRAC Log Buttons

Button	Action
Print	Prints the **iDRAC Log** page.
Clear Log	Clears the **iDRAC 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 **iDRAC Log** to a directory of your choice. **NOTE:** If you are using Internet Explorer and encounter a problem when saving, be sure to download the Cumulative Security Update for Internet Explorer, located on the Microsoft Support website at **support.microsoft.com**.
Refresh	Reloads the **iDRAC Log** page.

Viewing System Information

The **System Summary** page displays information about the following system components:

- Main System enclosure
- Integrated Dell Remote Access Controller

To access the system information, click **System→ Properties**.

Main System enclosure

Table 13-9 and Table 13-10 describe the main system enclosure properties.

Table 13-9. System Information Fields

Field	Description
Description	Provides a system description.
BIOS Version	Lists the system BIOS version.
Service Tag	Lists the system Service Tag number.
Host Name	Provides the host system's name.
OS Name	Lists the operating system running on the system.

Table 13-10. Auto Recovery Fields

Field	Description
Recovery Action	When a *system hang* is detected, the iDRAC can be configured to perform one of the following actions: **No Action**, **Hard Reset**, **Power Down**, or **Power Cycle**.
Initial Countdown	The number of seconds after a *system hang* is detected at which the iDRAC will perform a Recovery Action.
Present Countdown	The current value, in seconds, of the countdown timer.

Integrated Dell Remote Access Controller

Table 13-11 describes the iDRAC properties.

Table 13-11. iDRAC Information Fields

Field	Description
Date/Time	Provides the current date and time on the iDRAC in GMT.
Firmware Version	Lists the version of the iDRAC firmware.
Firmware Updated	Lists the date the firmware was last updated. The date is displayed in UTC format, for example: Tue, 8 May 2007, 22:18:21 UTC.

Table 13-11. iDRAC Information Fields *(continued)*

Field	Description
IP Address	The 32-bit address that identifies the network interface. The value is displayed in a *dot separated* format, such as 143.166.154.127.
Gateway	The IP Address of the gateway that acts as a bridge to other networks. This value is in a *dot separated* format, such as 143.166.150.5.
Subnet Mask	The subnet mask identifies the parts of the IP Address that make up the Extended Network Prefix and the Host Number. The value is displayed in a *dot separated* format, such as 255.255.0.0.
MAC Address	The Media Access Control (MAC) Address that uniquely identifies each NIC in a network, for example 00-00-0c-ac-08. This is a Dell-assigned ID and cannot be edited.
DHCP Enabled	**Enabled** indicates that the Dynamic Host Configuration Protocol (DHCP) is enabled. **Disabled** indicates that DHCP is *not* enabled.

Identifying the Managed Server in the Chassis

The PowerEdge M1000-e chassis holds up to sixteen servers. To locate a specific server in the chassis, you can use the iDRAC Web interface to turn on a blue flashing LED on the server. When you turn on the LED, you can specify the number of seconds that you want the LED to flash to ensure that you can reach the chassis while the LED is still flashing. Entering 0 leaves the LED flashing until you disable it.

To identify the server:

1 Click **System**→ **Remote Access**→ **iDRAC**→ **Troubleshooting**.

2 On the **Identify** page, check the value box next to **Identify Server**.

3 In the **Identify Server Timeout** field, enter the number of seconds that you want the LED to blink. Enter 0 if you want the LED to remain flashing until you disable it.

4 Click **Apply.**

A blue LED on the server will flash for the number of seconds you specified.

If you entered 0 leave the LED flashing, follow these steps to disable it:

1. Click **System→ Remote Access→ iDRAC→ Troubleshooting**.
2. On the **Identify** page, uncheck the value box next to **Identify Server**.
3. Click **Apply**.

Using the Diagnostics Console

The iDRAC provides a standard set of network diagnostic tools (see Table 13-12) that are similar to the tools included with Microsoft® Windows® or Linux-based systems. Using the iDRAC Web interface, you can access the network debugging tools.

To access the **Diagnostics Console** page, perform the following steps:

1. Click **System→ iDRAC→ Troubleshooting**.
2. Click the **Diagnostics** tab.

Table 13-12 describes the commands that can be entered on the **Diagnostics Console** page. Type a command and click **Submit**. The debugging results appear in the **Diagnostics Console** page.

Click the **Clear** button to clear the results displayed by the previous command.

To refresh the **Diagnostics Console** page, click **Refresh**.

Table 13-12. 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 content of the routing table.
ping <*IP Address*>	Verifies that the destination IP address is reachable from the iDRAC with the current routing-table contents. A destination IP address must be entered in the field to the right of this option. An Internet control message protocol (ICMP) echo packet is sent to the destination IP address based on the current routing-table contents.

Table 13-12. Diagnostic Commands *(continued)*

Command	Description
gettracelog	Displays the iDRAC trace log. See "gettracelog" on page 242 for more information.

Managing Power on a Remote System

The iDRAC enables you to remotely perform several power management actions on the managed server. Use the Power Management page to perform an orderly shutdown through the operating system when rebooting and powering on and off.

NOTE: You must have **Execute Server Action Commands** permission to perform power management actions. See "Adding and Configuring iDRAC Users" on page 65 for help configuring user permissions.

1 Click **System**, then click the **Power Management** tab.

2 Select a **Power Control Action**, for example **Reset System (warm boot)**. Table 13-13 provides information about Power Control Actions.

3 Click **Apply** to perform the selected action.

4 Click the appropriate button to continue. See Table 13-14.

Table 13-13. Power Control Actions

Power On System	Turns on the system power (equivalent to pressing the power button when the system power is off).
Powers Off System	Turns off the system power (equivalent to pressing the power button when the system power is on).
NMI (Non-Masking Interrupt)	Sends a high-level interrupt to the operating system, which causes the system to halt operation to allow for critical diagnostic or troubleshooting activities.
Graceful Shutdown	Attempts to cleanly shut down the operating system, then powers off the system. It requires an ACPI (Advanced Configuration and Power Interface) aware operating system, which allows for system directed power management.

Table 13-13. Power Control Actions *(continued)*

Reset System (warm boot)	Reboots the system without powering off (warm boot).
Power Cycle System	Powers off, then reboots the system (cold boot).

Table 13-14. Power Management Page Buttons

Button	Action
Print	Prints the **Power Management** values that appear on the screen.
Refresh	Reloads the **Power Management** page.
Apply	Saves any new settings that you make while viewing the Power Management page.

Troubleshooting and Frequently Asked Questions

Table 13-15 contains frequently asked questions about troubleshooting issues.

Table 13-15. Frequently Asked Questions/Troubleshooting

Question	Answer
The LED on the server is blinking amber.	Check the SEL for messages and then clear the SEL to stop the blinking LED. From the iDRAC Web interface: • See "Checking the System Event Log (SEL)" on page 209 From SM-CLP: • See "SEL Management" on page 180 From the iDRAC Configuration Utility: • See "System Event Log Menu" on page 203
There is a blinking blue LED on the server.	A user has activated the locator ID for the server. This is a signal to help them identify the server in the chassis. See "Identifying the Managed Server in the Chassis" on page 214 for information about this feature.

Table 13-15. Frequently Asked Questions/Troubleshooting *(continued)*

Question	Answer
How can I find the IP address of the iDRAC?	From the CMC Web interface: 1 Click **Chassis**→ **Servers**, then click the **Setup** tab. 2 Click **Deploy**. 3 Read the IP address for your server from the table that is displayed. From the iKVM: • Reboot the server and enter the iDRAC Configuration Utility by pressing <Ctrl><E> OR • Watch for the IP address to display during BIOS POST. OR • Select the "Dell CMC" console in the OSCAR to log into the CMC through a local serial connection. CMC RACADM commands can be issued from this connection. Refer to the CMC *Firmware Version 1.0 User's Guide* for a complete list of the CMC RACADM subcommands.

How can I find the IP address of the iDRAC? *(continued)*	For example:
	`$ racadm getniccfg -m server-1`
	`DHCP Enabled        = 1`
	`IP Address          = 192.168.0.1`
	`Subnet Mask         = 255.255.255.0`
	`Gateway             = 192.168.0.1`
	From local RACADM:
	1 Enter the following command at a command prompt:
	`racadm getsysinfo`
	From the LCD:
	1 On the Main Menu, highlight **Server** and press the check button.
	2 Select the server whose IP address you seek and press the check button.

Table 13-15. Frequently Asked Questions/Troubleshooting *(continued)*

Question	Answer

How can I find the IP address of the CMC?	From the iDRAC Web interface:
	• Click **System→ Remote Access→ CMC**.
	The CMC IP address is displayed on the **Summary** page.
	OR
	• Select the "Dell CMC" console in the OSCAR to log into the CMC through a local serial connection. CMC RACADM commands can be issued from this connection. Refer to the CMC *Firmware Version 1.0 User's Guide* for a complete list of the CMC RACADM subcommands.
	`$ racadm getniccfg -m chassis`
	`NIC Enabled          = 1`
	`DHCP Enabled         = 1`
	`Static IP Address    = 192.168.0.120`
	`Static Subnet Mask   = 255.255.255.0`
	`Static Gateway       = 192.168.0.1`
	`Current IP Address   = 10.35.155.151`
	`Current Subnet Mask  = 255.255.255.0`
	`Current Gateway      = 10.35.155.1`
	`Speed                = Autonegotiate`
	`Duplex               = Autonegotiate`

The iDRAC network connection is not working.	• Ensure the LAN cable is connected to the CMC. • Ensure the iDRAC LAN is enabled.
I inserted the server into the chassis and pressed the power button, but nothing happened.	• The iDRAC requires about 30 seconds to initialize before the server can power up. Wait for 30 seconds and then press the power button again. • Check the CMC power budget. The chassis power budget may be exceeded.

Table 13-15. Frequently Asked Questions/Troubleshooting *(continued)*

Question	Answer
I have forgotten the iDRAC administrative user name and password.	You must restore the iDRAC to its default settings. 1 Reboot the server and press <Ctrl><E> when prompted to enter the iDRAC Configuration Utility. 2 On the configuration utility menu, highlight **Reset to Default** and press <Enter>. For more information, see "Reset to Default" on page 203.
How can I change the name of the slot for my server?	1 Log in to the CMC Web interface. 2 Open the **Chassis** tree and click **Servers**. 3 Click the **Setup** tab. 4 Type the new name for the slot in the row for your server. 5 Click **Apply**.
When starting a console redirection session from the iDRAC Web interface, an ActiveX security popup appears.	The iDRAC may not be a trusted site from the client browser. To prevent the security popup from appearing every time you begin a console redirection session, add the iDRAC to the trusted site list: 1 Click **Tools**→ **Internet Options...**→ **Security**→ **Trusted sites**. 2 Click **Sites** and enter the IP address or DNS name of the iDRAC. 3 Click **Add**.
When I start a console redirection session, the viewer screen is blank.	If you have **Virtual Media** privilege but not **Console Redirection** privilege, you are able to start the viewer so that you can access the virtual media feature, but the managed server's console will not display.
The iDRAC does not boot.	Remove and reinsert the server. Check the CMC Web interface to see if the iDRAC appears as an upgradable component. If it does, follow the instructions at "Recovering iDRAC Firmware Using the CMC" on page 86. If this does not correct the problem, contact Technical Support.

Table 13-15. Frequently Asked Questions/Troubleshooting *(continued)*

Question	Answer
When attempting to boot the managed server, the power indicator is green, but there is no POST or no video at all.	This can happen if any of the following conditions is true: • Memory is not installed or is inaccessible. • The CPU is not installed or is inaccessible. • The video riser card is missing or improperly connected. Also, look for error messages in the iDRAC log from the iDRAC Web interface or from the LCD.

A

RACADM Subcommand Overview

This section provides descriptions of the subcommands that are available in the RACADM command line interface.

help

Table A-1 describes the **help** command.

Table A-1. Help Command

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 <subcommand>
```

Description

The **help** subcommand lists all of the subcommands that are available when using the **racadm** command along with a one-line description. You may also type a subcommand after **help** to get the syntax for a specific subcommand.

Output

The **racadm help** command displays a complete list of subcommands.

The **racadm help** <*subcommand*> command displays information for the specified subcommand only.

Supported Interfaces

- Local RACADM

config

Table A-2 describes the **config** and **getconfig** subcommands.

Table A-2. config/getconfig

Subcommand	Definition
config	Configures the iDRAC.
getconfig	Gets the iDRAC configuration data.

Synopsis

```
racadm config [-c|-p] -f <filename>
```

```
racadm config -g <groupName> -o <objectName> [-i
<index>] <value>
```

Supported Interfaces

- Local RACADM

Description

The **config** subcommand allows you to set iDRAC configuration parameters individually or to batch them as part of a configuration file. If the data is different, that iDRAC object is written with the new value.

Input

Table A-3 describes the **config** subcommand options.

Table A-3. config Subcommand Options and Descriptions

Option	Description
-f	The **-f** <*filename*> option causes **config** to read the contents of the file specified by <*filename*> and configure the iDRAC. The file must contain data in the format specified in "Configuration File Syntax" on page 167.

Table A-3. config Subcommand Options and Descriptions *(continued)*

Option	Description
-p	The **-p**, or password, option directs **config** to delete the password entries contained in the config file **-f** <*filename*> after the configuration is complete.
-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*>.
-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 specified here by the index value, not a "named" value.
-c	The **-c**, or check, option is used with the **config** subcommand and allows you to parse the **.cfg** file to find syntax errors. If errors are found, the line number and a short description of what is incorrect are displayed. Writes do not occur to the iDRAC. This option is a check only.

Output

This subcommand generates error output upon encountering either of the following:

- Invalid syntax, group name, object name, index, or other invalid database members
- RACADM CLI failures

This subcommand returns an indication of how many configuration objects that were written out of how many total objects were in the **.cfg** file.

Examples

-
  ```
  racadm config -g cfgLanNetworking -o
  cfgNicIpAddress 10.35.10.110
  ```

  Sets the **cfgNicIpAddress** configuration parameter (object) to the value 10.35.10.110. This IP address object is contained in the group **cfgLanNetworking**.

- `racadm config -f myrac.cfg`

  Configures or reconfigures the iDRAC. The **myrac.cfg** file may be created with the **getconfig** command. The **myrac.cfg** file may also be edited manually as long as the parsing rules are followed.

  NOTE: The **myrac.cfg** file does not contain passwords. To include passwords in the file, you must enter them manually. If you want to remove passwords from the **myrac.cfg** file during configuration, use the **-p** option.

getconfig

The **getconfig** subcommand allows you to retrieve iDRAC configuration parameters individually, or all the iDRAC configuration groups may be retrieved and saved into a file.

Input

Table A-4 describes the **getconfig** subcommand options.

NOTE: The **-f** option without a file specification will output the contents of the file to the terminal screen.

Table A-4. getconfig Subcommand Options

Option	Description
-f	The **-f** <*filename*> option directs **getconfig** to write the entire iDRAC configuration to a configuration file. This file can then be used for batch configuration operations using the **config** subcommand. **NOTE:** The **-f** option does not create entries for the **cfgIpmiPet** and **cfgIpmiPef** groups. You must set at least one trap destination to capture the **cfgIpmiPet** group to the file.
-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.

Table A-4. getconfig Subcommand Options

Option	Description
-i	The **-i** <*index*>, or index, option is valid only for indexed groups and can be used to specify a unique group. 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.
-o	The -o <*objectname*>, or object, option specifies the object name that is used in the query. This option can be used with the **-g** option.
-u	The **-u** <*username*>, or user name, option can be used to display the configuration for the specified user. The <*username*> option is the login name for the user.
-v	The **-v**, or verbose, option displays additional details with the display of the properties and is used with the **-g** option.

Output

This subcommand generates error output upon encountering either of the following:

- Invalid syntax, group name, object name, index, or other invalid database members
- RACADM CLI 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 properties (objects) that are contained in the group **cfgLanNetworking**.

- `racadm getconfig -f myrac.cfg`

  Saves all group configuration objects from the iDRAC to **myrac.cfg**.

- `racadm getconfig -h`

  Displays a list of the available configuration groups on the iDRAC.

- `racadm getconfig -u root`

  Displays the configuration properties for the user named **root**.

- `racadm getconfig -g cfgUserAdmin -i 2 -v`

  Displays the user group instance at index 2 with extensive information for the property values.

Synopsis

```
racadm getconfig -f <filename>

racadm getconfig -g <groupName> [-i <index>]

racadm getconfig -u <username>

racadm getconfig -h
```

Supported Interfaces

- Local RACADM

getssninfo

Table A-5 describes the **getssninfo** subcommand.

Table A-5. 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** command returns a list of users that are connected to the iDRAC. The summary information provides the following information:

- Username
- IP address (if applicable)
- Session type (for example, SSH or telnet)
- Consoles in use (for example, Virtual Media or Virtual KVM)

Supported Interfaces

- Local RACADM

Input

Table A-6 describes the **getssninfo** subcommand options.

Table A-6. getssninfo Subcommand Options

Option	Description
-A	The **-A** option eliminates the printing of data headers.
-u	The **-u** <*username*> user name option limits the printed output to only the detail session records for the given user name. If an asterisk (*) symbol is given as the user name, all users are listed. Summary information is not printed when this option is specified.

Examples

- `racadm getssninfo`

Table A-7 provides an example of output from the **racadm getssninfo** command.

Table A-7. getssninfo Subcommand Output Example

User	IP Address	Type	Consoles
root	192.168.0.10	Telnet	Virtual KVM

- `racadm getssninfo -A`

  ```
  "root" 143.166.174.19 "Telnet" "NONE"
  ```

- `racadm getssninfo -A -u *`

  ```
  "root" "143.166.174.19" "Telnet" "NONE"
  ```

- "bob" "143.166.174.19" "GUI" "NONE"

getsysinfo

Table A-8 describes the **racadm getsysinfo** subcommand.

Table A-8. getsysinfo

Command	Definition
getsysinfo	Displays iDRAC information, system information, and watchdog status information.

Synopsis

```
racadm getsysinfo [-d] [-s] [-w] [-A]
```

Description

The **getsysinfo** subcommand displays information related to the iDRAC, managed server, and watchdog configuration.

Supported Interfaces

- Local RACADM

Input

Table A-9 describes the **getsysinfo** subcommand options.

Table A-9. getsysinfo Subcommand Options

Option	Description
-d	Displays iDRAC information.
-s	Displays system information
-w	Displays watchdog information
-A	Eliminates the printing of headers/labels.

Output

The **getsysinfo** subcommand displays information related to the iDRAC, managed server, and watchdog configuration.

Sample Output

```
RAC Information:
RAC Date/Time            = Wed Aug 22 20:01:33 2007
Firmware Version         = 0.32
Firmware Build           = 13661
Last Firmware Update     = Mon Aug 20 08:09:36 2007

Hardware Version         = NA
Current IP Address       = 192.168.0.120
Current IP Gateway       = 192.168.0.1
Current IP Netmask       = 255.255.255.0
DHCP Enabled             = 1
MAC Address              = 00:14:22:18:cd:f9
Current DNS Server 1     = 10.32.60.4
Current DNS Server 2     = 10.32.60.5
DNS Servers from DHCP    = 1
Register DNS RAC Name    = 1
DNS RAC Name             = iDRAC-783932693338
Current DNS Domain       = us.dell.com

System Information:
System Model             = PowerEdge M600
System BIOS Version      = 0.2.1
BMC Firmware Version     = 0.32
Service Tag              = 48192
Host Name                = dell-x92i38xc2n
OS Name                  =
Power Status             = OFF

Watchdog Information:
Recovery Action          = None
Present countdown value  = 0 seconds
Initial countdown value  = 0 seconds
```

Examples

- `racadm getsysinfo -A -s`

  ```
  "System Information:" "PowerEdge M600" "0.2.1"
  "0.32" "48192" "dell-x92i38xc2n" "" "ON"
  ```

- `racadm getsysinfo -w -s`

```
System Information:
System Model             = PowerEdge M600
System BIOS Version      = 0.2.1
BMC Firmware Version     = 0.32
Service Tag              = 48192
Host Name                = dell-x92i38xc2n
OS Name                  =
Power Status            = ON

Watchdog Information:
Recovery Action          = None
Present countdown value  = 0 seconds
Initial countdown value  = 0 seconds
```

Restrictions

The **Hostname** and **OS Name** fields in the **getsysinfo** output display accurate information only if Dell OpenManage is installed on the managed server. If OpenManage is not installed on the managed server, these fields may be blank or inaccurate.

getractime

Table A-10 describes the **getractime** subcommand.

Table A-10. getractime

Subcommand	Definition
getractime	Displays the current time from the remote access controller.

Synopsis

```
racadm getractime [-d]
```

Description

With no options, the **getractime** subcommand displays the time in a common readable format.

With the **-d** option, **getractime** displays the time in the format, *yyyymmddhhmmss.mmmmmms*, which is the same format returned by the UNIX **date** command.

Output

The **getractime** subcommand displays the output on one line.

Sample Output

```
racadm getractime

Thu Dec  8 20:15:26 2005


racadm getractime -d

20071208201542.000000
```

Supported Interfaces

- Local RACADM

setniccfg

Table A-11 describes the **setniccfg** subcommand.

Table A-11. setniccfg

Subcommand	Definition
setniccfg	Sets the IP configuration for the controller.

Synopsis

```
racadm setniccfg -d
racadm setniccfg -s [<ipAddress> <netmask> <gateway>]
racadm setniccfg -o [<ipAddress> <netmask> <gateway>]
```

Description

The **setniccfg** subcommand sets the iDRAC IP address.

- The **-d** option enables DHCP for the NIC (default is DHCP enabled).
- The **-s** option enables static IP settings. The IP address, netmask, and gateway can be specified. Otherwise, the existing static settings are used. <*ipAddress*>, <*netmask*>, and <*gateway*> must be typed as dot-separated strings.

  ```
  racadm setniccfg -s 192.168.0.120 255.255.255.0
  192.168.0.1
  ```

- The **-o** option disables the NIC completely. <*ipAddress*>, <*netmask*>, and <*gateway*> must be typed as dot-separated strings.

  ```
  racadm setniccfg -o 192.168.0.120 255.255.255.0
  192.168.0.1
  ```

Output

The **setniccfg** subcommand displays an appropriate error message if the operation is not successful. If successful, a message is displayed.

Supported Interfaces

- Local RACADM

getniccfg

Table A-12 describes the **getniccfg** subcommand.

Table A-12. getniccfg

Subcommand	Definition
getniccfg	Displays the current IP configuration for the iDRAC.

Synopsis

```
racadm getniccfg
```

Description

The **getniccfg** subcommand displays the current NIC settings.

Sample Output

The **getniccfg** subcommand will display an appropriate error message if the operation is not successful. Otherwise, on success, the output is displayed in the following format:

```
NIC Enabled      = 1
DHCP Enabled     = 1
IP Address       = 192.168.0.1
Subnet Mask      = 255.255.255.0
Gateway          = 192.168.0.1
```

Supported Interfaces

- Local RACADM

getsvctag

Table A-13 describes the **getsvctag** subcommand.

Table A-13. getsvctag

Subcommand	Definition
getsvctag	Displays a service tag.

Synopsis

```
racadm getsvctag
```

Description

The **getsvctag** subcommand displays the service tag of the host system.

Example

Type `getsvctag` at the command prompt. The output is displayed as follows:

```
Y76TP0G
```

The command returns *0* on success and nonzero on errors.

Supported Interfaces

- Local RACADM

racreset

Table A-14 describes the **racreset** subcommand.

Table A-14. racreset

Subcommand	Definition
racreset	Resets the iDRAC.

NOTICE: When you issue a racreset subcommand, the iDRAC may require up to one minute to return to a usable state.

Synopsis

```
racadm racreset
```

Description

The **racreset** subcommand issues a reset to the iDRAC. The reset event is written into the iDRAC log.

Examples

- `racadm racreset`

  Start the iDRAC soft reset sequence.

Supported Interfaces

- Local RACADM

racresetcfg

Table A-15 describes the **racresetcfg** subcommand.

Table A-15. racresetcfg

Subcommand	Definition
racresetcfg	Resets the entire RAC configuration to factory default values.

Synopsis

```
racadm racresetcfg
```

Supported Interfaces

- Local RACADM

Description

The **racresetcfg** command removes all user-configured database property entries. The database has default properties for all entries that are used to restore the iDRAC back to the default settings.

NOTICE: This command deletes your current iDRAC configuration and resets the iDRAC configuration to the default settings. After reset, the default name and password are **root** and **calvin**, respectively, and the IP address is **192.168.0.120** plus the number of the slot the server inhabits in the chassis.

serveraction

Table A-16 describes the **serveraction** subcommand.

Table A-16. serveraction

Subcommand	Definition
serveraction	Executes a managed server reset or power-on/off/cycle.

Synopsis

```
racadm serveraction <action>
```

Description

The **serveraction** subcommand enables users to perform power management operations on the host system. Table A-17 describes the **serveraction** power control options.

Table A-17. serveraction Subcommand Options

String	Definition
<*action*>	Specifies the action. The <*action*> string options are: • **powerdown** — Powers down the managed server. • **powerup** — Powers up the managed server. • **powercycle** — Issues a power-cycle operation on the managed server. This action is similar to pressing the power button on the system's front panel to power down and then power up the system. • **powerstatus** — Displays the current power status of the server (**ON**, or **OFF**). • **hardreset** — Performs a reset (reboot) operation on the managed server.

Output

The **serveraction** subcommand displays an error message if the requested operation could not be performed, or a success message if the operation completed successfully.

Supported Interfaces

- Local RACADM

getraclog

Table A-18 describes the **racadm getraclog** command.

Table A-18. getraclog

Command	Definition
getraclog -i	Displays the number of entries in the iDRAC log.
getraclog	Displays the iDRAC log entries.

Synopsis

```
racadm getraclog -i
```

```
racadm getraclog [-A] [-o] [-c count] [-s start-
record] [-m]
```

Description

The **getraclog -i** command displays the number of entries in the iDRAC log.

NOTE: If no options are provided, the entire log is displayed.

The following options allow the **getraclog** command to read entries:

Table A-19. getraclog Subcommand Options

Option	Description
-A	Displays the output with no headers or labels.
-c	Provides the maximum count of entries to be returned.
-m	Displays one screen of information at a time and prompts the user to continue (similar to the UNIX **more** command).

Table A-19. getraclog Subcommand Options *(continued)*

Option	Description
-o	Displays the output in a single line.
-s	Specifies the starting record used for the display.

Output

The default output display shows the record number, time stamp, source, and description. The timestamp begins at midnight, January 1 and increases until the managed server boots. After the managed server boots, the managed server's system time is used for the timestamp.

Sample Output

```
Record:       1
Date/Time:    Dec  8 08:10:11
Source:       login[433]
Description:  root login from 143.166.157.103
```

Supported Interfaces

- Local RACADM

clrraclog

Synopsis

```
racadm clrraclog
```

Description

The **clrraclog** subcommand removes all existing records from the iDRAC log. A new single record is created to record the date and time when the log was cleared.

getsel

Table A-20 describes the **getsel** command.

Table A-20. getsel

Command	Definition
getsel -i	Displays the number of entries in the **System Event Log**.
getsel	Displays SEL entries.

Synopsis

```
racadm getsel -i
```

```
racadm getsel [-E] [-R] [-A] [-o] [-c count] [-s
count] [-m]
```

Description

The **getsel -i** command displays the number of entries in the SEL.

The following **getsel** options (without the **-i** option) are used to read entries.

NOTE: If no arguments are specified, the entire log is displayed.

Table A-21. getsel Subcommand Options

Option	Description
-A	Specifies output with no display headers or labels.
-c	Provides the maximum count of entries to be returned.
-o	Displays the output in a single line.
-s	Specifies the starting record used for the display.
-E	Places the 16 bytes of raw SEL at the end of each line of output as a sequence of hex values.
-R	Only the raw data is printed.
-m	Displays one screen at a time and prompts the user to continue (similar to the UNIX **more** command).

Output

The default output display shows the record number, timestamp, severity, and description.

For example:

```
Record:       1
Date/Time:    11/16/2005 22:40:43
Severity:     Ok
Description: System Board SEL: event log sensor for
System Board, log cleared was asserted
```

Supported Interfaces

- Local RACADM

clrsel

Synopsis

```
racadm clrsel
```

Description

The **clrsel** command removes all existing records from the **System Event Log** (SEL).

Supported Interfaces

- Local RACADM

gettracelog

Table A-22 describes the **gettracelog** subcommand.

Table A-22. gettracelog

Command	Definition
gettracelog -i	Displays the number of entries in the **iDRAC trace log**.
gettracelog	Displays the **iDRAC trace log**.

Synopsis

```
racadm gettracelog -i
```

```
racadm gettracelog [-A] [-o] [-c count] [-s
startrecord] [-m]
```

Description

The **gettracelog** (without the **-i** option) command reads entries. The following **gettracelog** entries are used to read entries:

Table A-23. gettracelog Subcommand options

Option	Description
-i	Displays the number of entries in the **iDRAC trace log**.
-m	Displays one screen at a time and prompts the user to continue (similar to the UNIX **more** command).
-o	Displays the output in a single line.
-c	specifies the number of records to display.
-s	specifies the starting record to display.
-A	do not display headers or labels.

Output

The default output display shows the record number, timestamp, source, and description. The timestamp begins at midnight, January 1 and increases until the managed system boots. After the managed system boots, the managed system's system time is used for the timestamp.

For example:

```
Record:      1
Date/Time:   Dec  8 08:21:30
Source:      ssnmgrd[175]
Description: root from 143.166.157.103: session
timeout sid 0be0aef4
```

Supported Interfaces

- Local RACADM

sslcsrgen

Table A-24 describes the **sslcsrgen** subcommand.

Table A-24. sslcsrgen

Subcommand	Description
sslcsrgen	Generates and downloads an SSL certificate signing request (CSR) from the RAC.

Synopsis

```
racadm sslcsrgen [-g] [-f <filename>]
```

```
racadm sslcsrgen -s
```

Description

The **sslcsrgen** subcommand can be used to generate a CSR and download the file to the client's local file system. The CSR can be used for creating a custom SSL certificate that can be used for SSL transactions on the RAC.

Options

Table A-25 describes the **sslcsrgen** subcommand options.

Table A-25. sslcsrgen Subcommand Options

Option	Description
-g	Generates a new CSR.
-s	Returns the status of a CSR generation process (generation in progress, active, or none).
-f	Specifies the filename of the location, <*filename*>, where the CSR will be downloaded.

NOTE: If the **-f** option is not specified, the filename defaults to **sslcsr** in your current directory.

If no options are specified, a CSR is generated and downloaded to the local file system as **sslcsr** by default. The **-g** option cannot be used with the **-s** option, and the **-f** option can only be used with the **-g** option.

The **sslcsrgen -s** subcommand returns one of the following status codes:

- CSR was generated successfully.
- CSR does not exist.
- CSR generation in progress.

NOTE: Before a CSR can be generated, the CSR fields must be configured in the RACADM **cfgRacSecurity** group. For example: `racadm config -g cfgRacSecurity -o cfgRacSecCsrCommonName MyCompany`

Examples

```
racadm sslcsrgen -s
```

or

```
racadm sslcsrgen -g -f c:\csr\csrtest.txt
```

Supported Interfaces

- Local RACADM

sslcertupload

Table A-26 describes the **sslcertupload** subcommand.

Table A-26. sslcertupload

Subcommand	Description
sslcertupload	Uploads a custom SSL server or CA certificate from the client to the iDRAC.

Synopsis

```
racadm sslcertupload -t <type> [-f <filename>]
```

Options

Table A-27 describes the **sslcertupload** subcommand options.

Table A-27. sslcertupload Subcommand Options

Option	Description
-t	Specifies the type of certificate to upload, either the CA certificate or server certificate. 1 = server certificate 2 = CA certificate
-f	Specifies the file name of the certificate to be uploaded. If the file is not specified, the **sslcert** file in the current directory is selected.

The **sslcertupload** command returns `0` when successful and returns a nonzero number when unsuccessful.

Example

```
racadm sslcertupload -t 1 -f c:\cert\cert.txt
```

Supported Interfaces

- Local RACADM

sslcertdownload

Table A-28 describes the **sslcertdownload** subcommand.

Table A-28. sslcertdownload

Subcommand	Description
sslcertdownload	Downloads an SSL certificate from the RAC to the client's file system.

Synopsis

```
racadm sslcertdownload -t <type> [-f <filename>]
```

Options

Table A-29 describes the **sslcertdownload** subcommand options.

Table A-29. sslcertdownload Subcommand Options

Option	Description
-t	Specifies the type of certificate to download, either the Microsoft® Active Directory® certificate or server certificate. 1 = server certificate 2 = Microsoft Active Directory certificate
-f	Specifies the file name of the certificate to be uploaded. If the **-f** option or the filename is not specified, the **sslcert** file in the current directory is selected.

The **sslcertdownload** command returns `0` when successful and returns a nonzero number when unsuccessful.

Example

```
racadm sslcertdownload -t 1 -f c:\cert\cert.txt
```

Supported Interfaces

- Local RACADM

sslcertview

Table A-30 describes the **sslcertview** subcommand.

Table A-30. sslcertview

Subcommand	Description
sslcertview	Displays the SSL server or CA certificate that exists on the iDRAC.

Synopsis

```
racadm sslcertview -t <type> [-A]
```

Options

Table A-31 describes the **sslcertview** subcommand options.

Table A-31. sslcertview Subcommand Options

Option	Description
-t	Specifies the type of certificate to view, either the Microsoft Active Directory certificate or server certificate. 1 = server certificate 2 = Microsoft Active Directory certificate
-A	Prevents printing headers/labels.

Output Example

```
racadm sslcertview -t 1

Serial Number                : 00

Subject Information:
Country Code (CC)            : US
State (S)                    : Texas
Locality (L)                 : Round Rock
Organization (O)             : Dell Inc.
Organizational Unit (OU)     : Remote Access Group
Common Name (CN)             : iDRAC default certificate

Issuer Information:
Country Code (CC)            : US
State (S)                    : Texas
Locality (L)                 : Round Rock
Organization (O)             : Dell Inc.
Organizational Unit (OU)     : Remote Access Group
Common Name (CN)             : iDRAC default certificate
```

```
Valid From                   : Jul  8 16:21:56 2005 GMT
Valid To                     : Jul  7 16:21:56 2010 GMT

racadm sslcertview -t 1 -A


00
US
Texas
Round Rock
Dell Inc.
Remote Access Group
iDRAC default certificate
US
Texas
Round Rock
Dell Inc.
Remote Access Group
iDRAC default certificate
Jul 8 16:21:56 2005 GMT
Jul 7 16:21:56 2010 GMT
```

Supported Interfaces

- Local RACADM

testemail

Table A-32 describes the **testemail** subcommand.

Table A-32. testemail configuration

Subcommand	Description
testemail	Tests the iDRAC's e-mail alerting feature.

Synopsis

```
racadm testemail -i <index>
```

Description

Sends a test e-mail from the iDRAC to a specified destination.

Prior to executing the testemail command, ensure that the specified index in the RACADM **cfgEmailAlert** group is enabled and configured properly. Table A-33 provides an example of commands for the **cfgEmailAlert** group.

Table A-33. testemail Configuration

Action	Command
Enable the alert	`racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 1 1`
Set the destination e-mail address	`racadm config -g cfgEmailAlert -o cfgEmailAlertAddress -i 1 user1@mycompany.com`
Set the custom message that is sent to the destination e-mail address	`racadm config -g cfgEmailAlert -o cfgEmailAlertCustomMsg -i 1 "This is a test!"`
Ensure the SNMP IP address is configured properly	`racadm config -g cfgRemoteHosts -o cfgRhostsSmtpServerIpAddr -i 192.168.0.152`
View the current e-mail alert settings	`racadm getconfig -g cfgEmailAlert -i <index>` where <*index*> is a number from 1 to 4

Options

Table A-34 describes the **testemail** subcommand options.

Table A-34. testemail Subcommand Option

Option	Description
-i	Specifies the index of the e-mail alert to test.

Output

None.

Supported Interfaces

- Local RACADM

testtrap

Table A-35 describes the **testtrap** subcommand.

Table A-35. testtrap

Subcommand	Description
testtrap	Tests the iDRAC's SNMP trap alerting feature.

Synopsis

```
racadm testtrap -i <index>
```

Description

The **testtrap** subcommand tests the iDRAC's SNMP trap alerting feature by sending a test trap from the iDRAC to a specified destination trap listener on the network.

Before you execute the **testtrap** subcommand, ensure that the specified index in the RACADM **cfgIpmiPet** group is configured properly.

Table A-36 provides a list and associated commands for the **cfgIpmiPet** group.

Table A-36. cfg e-mail Alert Commands

Action	Command
Enable the alert	`racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 1 1`
Set the destination e-mail IP address	`racadm config -g cfgIpmiPet -o cfgIpmiPetAlertDestIpAddr -i 1 192.168.0.110`
View the current test trap settings	`racadm getconfig -g cfgIpmiPet -i <index>` where <*index*> is a number from 1 to 4

Input

Table A-37 describes the **testtrap** subcommand options.

Table A-37. testtrap Subcommand Options

Option	Description
-i	Specifies the index of the trap configuration to use for the test Valid values are from 1 to 4.

Supported Interfaces

- Local RACADM

vmdisconnect

Table A-38 describes the **vmdisconnect** subcommand.

Table A-38. vmdisconnect

Subcommand	Description
vmdisconnect	Closes all open iDRAC virtual media connections from remote clients.

Synopsis

```
racadm vmdisconnect
```

Description

The **vmdisconnect** subcommand allows a user to disconnect another user's virtual media session. Once disconnected, the Web interface will reflect the correct connection status. This is available only through the use of local RACADM.

The **vmdisconnect** subcommand enables an iDRAC user to disconnect all active virtual media sessions. The active virtual media sessions can be displayed in the RAC Web interface or by using the RACADM **getsysinfo** subcommand.

Supported Interfaces

- Local RACADM

B

iDRAC Property Database Group and Object Definitions

The iDRAC property database contains the configuration information for the iDRAC. 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 iDRAC. The following sections describe each object and indicate whether the object is readable, writable, or both.

All string values are limited to displayable ASCII characters, except where otherwise noted.

Displayable Characters

Displayable characters include the following set:

```
abcdefghijklmnopqrstuvwxwz

ABCDEFGHIJKLMNOPQRSTUVWXYZ

0123456789~`!@#$%^&*()_+-={}[]|\:";'<>,.?/
```

idRacInfo

This group contains display parameters to provide information about the specifics of the iDRAC being queried.

One instance of the group is allowed. The following subsections describe the objects in this group.

idRacProductInfo (Read Only)

Legal Values

String of up to 63 ASCII characters.

Default

Integrated Dell Remote Access Controller

Description

A text string that identifies 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 Dell PowerEdge servers.

Description

A text description of the RAC type.

idRacVersionInfo (Read Only)

Legal Values

String of up to 63 ASCII characters.

Default

1.0

Description

A string containing the current product firmware version.

idRacBuildInfo (Read Only)

Legal Values

String of up to 16 ASCII characters.

Default

The current RAC firmware build version. For example, "05.12.06".

Description

A string containing the current product build version.

idRacName (Read Only)

Legal Values

String of up to 15 ASCII characters.

Default

iDRAC

Description

A user assigned name to identify this controller.

idRacType (Read Only)

Default

8

Description

Identifies the remote access controller type as the iDRAC.

cfgLanNetworking

This group contains parameters to configure the iDRAC NIC.

One instance of the group is allowed. All objects in this group will require the iDRAC NIC to be reset, which may cause a brief loss in connectivity. Objects that change the iDRAC NIC IP address settings will close all active user sessions and require users to reconnect using the updated IP address settings.

cfgDNSDomainNameFromDHCP (Read/Write)

Legal Values

1 (TRUE)

0 (FALSE)

Default

0

Description

Specifies that the iDRAC DNS domain name should be assigned from the network DHCP server.

cfgDNSDomainName (Read/Write)

Legal Values

String of up to 254 ASCII characters. At least one of the characters must be alphabetic. Characters are restricted to alphanumeric, '-' and '.'.

NOTE: Microsoft® Active Directory® only supports Fully Qualified Domain Names (FQDN) of 64 bytes or fewer.

Default

""

Description

The DNS domain name. This parameter is only valid if **cfgDNSDomainNameFromDHCP** is set to 0 (FALSE).

cfgDNSRacName (Read/Write)

Legal Values

String of up to 63 ASCII characters. At least one character must be alphabetic.

NOTE: Some DNS servers only register names of 31 characters or fewer.

Default

rac-*service tag*

Description

Displays the RAC name, which is rac-*service tag* by default. This parameter is only valid if **cfgDNSRegisterRac** is set to 1 (TRUE).

cfgDNSRegisterRac (Read/Write)

Legal Values

1 (TRUE)

0 (FALSE)

Default

0

Description

Registers the iDRAC name on the DNS server.

cfgDNSServersFromDHCP (Read/Write)

Legal Values

1 (TRUE)

0 (FALSE)

Default

0

Description

Specifies that the DNS server IP addresses should be assigned from the DHCP server on the network.

cfgDNSServer1 (Read/Write)

Legal Values

A string representing a valid IP address. For example: 192.168.0.20.

Description

Specifies the IP address for DNS server 1. This property is only valid if **cfgDNSServersFromDHCP** is set to **0** (FALSE).

NOTE: **cfgDNSServer1** and **cfgDNSServer2** may be set to identical values while swapping addresses.

cfgDNSServer2 (Read/Write)

Legal Values

A string representing a valid IP address. For example: 192.168.0.20.

Default

0.0.0.0

Description

Retrieves the IP address for DNS server 2. This parameter is only valid if **cfgDNSServersFromDHCP** is set to 0 (FALSE).

NOTE: **cfgDNSServer1** and **cfgDNSServer2** may be set to identical values while swapping addresses.

cfgNicEnable (Read/Write)

Legal Values

1 (TRUE)

0 (FALSE)

Default

0

Description

Enables or disables the iDRAC network interface controller. If the NIC is disabled, the remote network interfaces to the iDRAC will no longer be accessible, and the iDRAC will only be available through the local RACADM interface.

cfgNicIpAddress (Read/Write)

NOTE: This parameter is only configurable if the **cfgNicUseDhcp** parameter is set to 0 (FALSE).

Legal Values

A string representing a valid IP address. For example: 192.168.0.20.

Default

192.168.0.*n*

where *n* is 120 plus the server slot number.

Description

Specifies the static IP address to assign to the RAC. This property is only valid if **cfgNicUseDhcp** is set to **0** (FALSE).

cfgNicNetmask (Read/Write)

NOTE: This parameter is only configurable if the **cfgNicUseDhcp** parameter is set to 0 (FALSE).

Legal Values

A string representing a valid subnet mask. For example: 255.255.255.0.

Default

255.255.255.0

Description

The subnet mask used for static assignment of the iDRAC IP address. This property is only valid if **cfgNicUseDhcp** is set to **0** (FALSE).

cfgNicGateway (Read/Write)

NOTE: This parameter is only configurable if the **cfgNicUseDhcp** parameter is set to 0 (FALSE).

Legal Values

A string representing a valid gateway IP address. For example: 192.168.0.1.

Default

192.168.0.1

Description

The gateway IP address used for static assignment of the RAC IP address. This property is only valid if **cfgNicUseDhcp** is set to **0** (FALSE).

cfgNicUseDhcp (Read/Write)

Legal Values

1 (TRUE)

0 (FALSE)

Default

0

Description

Specifies whether DHCP is used to assign the iDRAC IP address. If this property is set to 1 (TRUE), then the iDRAC IP address, subnet mask, and gateway are assigned from the DHCP server on the network. If this property is set to **0** (FALSE), the static IP address, subnet mask, and gateway is assigned from the **cfgNicIpAddress**, **cfgNicNetmask**, and **cfgNicGateway** properties.

cfgNicMacAddress (Read Only)

Legal Values

A string representing the RAC NIC MAC address.

Default

The current MAC address of the iDRAC NIC. For example, 00:12:67:52:51:A3.

Description

The iDRAC NIC MAC address.

cfgUserAdmin

This group provides configuration information about the users who are allowed to access the RAC through the available remote interfaces.

Up to 16 instances of the user group are allowed. Each instance represents the configuration for an individual user.

cfgUserAdminIpmiLanPrivilege (Read/Write)

Legal Values

2 (**User**)

3 (Operator)

4 (**Administrator**)

15 (**No access**)

Default

4 (User 2)

15 (All others)

Description

The maximum privilege on the IPMI LAN channel.

cfgUserAdminPrivilege (Read/Write)

Legal Values

0x00000000 to 0x000001ff

Default

0x00000000

Description

This property specifies the role-based authority privileges allowed for the user. The value is represented as a bit mask that allows for any combination of privilege values. Table B-1 describes the user privilege bit values that can be combined to create bit masks.

Table B-1. Bit Masks for User Privileges

User Privilege	Privilege Bit Mask
Login to iDRAC	0x0000001
Configure iDRAC	0x0000002
Configure Users	0x0000004
Clear Logs	0x0000008
Execute Server Control Commands	0x0000010
Access Console Redirection	0x0000020
Access Virtual Media	0x0000040
Test Alerts	0x0000080
Execute Debug Commands	0x0000100

Examples

Table B-2 provides sample privilege bit masks for users with one or more privileges.

Table B-2. Sample Bit Masks for User Privileges

User Privilege(s)	Privilege Bit Mask
The user is not allowed to access the iDRAC.	0x00000000
The user may only login to the iDRAC and view iDRAC and server configuration information.	0x00000001
The user may login to the iDRAC and change configuration.	0x00000001 + 0x00000002 = 0x00000003
The user may login to RAC, access virtual media, and access console redirection.	0x00000001 + 0x00000040 + 0x00000080 = 0x000000C1

cfgUserAdminUserName (Read/Write)

Legal Values

String. Maximum length = 16.

Default

""

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 quotation marks.

NOTE: This property value must be unique among user names.

cfgUserAdminPassword (Write Only)

Legal Values

A string of up to 20 ASCII characters.

Default

""

Description

The password for this user. User passwords are encrypted and cannot be seen or displayed after the property is written.

cfgUserAdminEnable

Legal Values

1 (TRUE)

0 (FALSE)

Default

0

Description

Enables or disables an individual user.

cfgUserAdminSolEnable

Legal Values

1 (TRUE)

0 (FALSE)

Default

0

Description

Enables or disables Serial Over LAN (SOL) user access.

cfgEmailAlert

This group contains parameters to configure the RAC e-mail alerting capabilities.

The following subsections describe the objects in this group. Up to four instances of this group are allowed.

cfgEmailAlertIndex (Read Only)

Legal Values

1–4

Default

This parameter is populated based on the existing instances.

Description

The unique index of an alert instance.

cfgEmailAlertEnable (Read/Write)

Legal Values

1 (TRUE)

0 (FALSE)

Default

0

Description

Specifies the destination email address for email alerts. For example, user1@company.com.

cfgEmailAlertAddress

Legal Values

E-mail address format, with a maximum length of 64 ASCII characters.

Default

""

Description

The e-mail address of the alert source.

cfgEmailAlertCustomMsg

Legal Values

String. Maximum Length = 32.

Default

""

Description

Specifies a custom message that is sent with the alert.

cfgSessionManagement

This group contains parameters to configure the number of sessions that can connect to the iDRAC.

One instance of the group is allowed. The following subsections describe the objects in this group.

cfgSsnMgtConsRedirMaxSessions (Read/Write)

Legal Values

1 – 2

Default

2

Description

Specifies the maximum number of console redirection sessions allowed on the iDRAC.

cfgSsnMgtWebserverTimeout (Read/Write)

Legal Values

60 – 1920

Default

300

Description

Defines the web server time-out. This property sets the amount of time in seconds that a connection is allowed to remain idle (there is no user input). The session is cancelled if the time limit set by this property is reached. Changes to this setting do not affect the current session; you must log out and log in again to make the new settings effective.

An expired web server session logs out the current session.

cfgSsnMgtSshIdleTimeout (Read/Write)

Legal Values

0 (No time-out)

60 – 1920

Default

300

Description

Defines the secure shell idle time-out. This property sets the amount of time in seconds that a connection is allowed to remain idle (there is no user input). The session is cancelled if the time limit set by this property is reached. Changes to this setting do not affect the current session; you must log out and log in again to make the new settings effective.

An expired secure shell session displays the following error message only after you press <Enter>:

```
Warning: Session no longer valid, may have timed out
```

After the message appears, the system returns you to the shell that generated the Secure Shell session.

cfgSsnMgtTelnetIdleTimeout (Read/Write)

Legal Values

0 (No timeout)

60 – 1920

Default

300

Description

Defines the telnet idle time-out. This property sets the amount of time in seconds that a connection is allowed to remain idle (there is no user input). The session is cancelled if the time limit set by this property is reached. Changes to this setting do not affect the current session (you must log out and log in again to make the new settings effective).

An expired telnet session displays the following error message only after you press <Enter>:

```
Warning: Session no longer valid, may have timed out
```

After the message appears, the system returns you to the shell that generated the telnet session.

cfgSerial

This group contains configuration parameters for the iDRAC services.

One instance of the group is allowed. The following subsections describe the objects in this group.

cfgSerialSshEnable (Read/Write)

Legal Values

1 (TRUE)

0 (FALSE)

Default

1

Description

Enables or disables the secure shell (SSH) interface on the iDRAC.

cfgSerialTelnetEnable (Read/Write)

Legal Values

1 (TRUE)

0 (FALSE)

Default

0

Description

Enables or disables the telnet console interface on the iDRAC.

cfgRacTuning

This group is used to configure various iDRAC configuration properties, such as valid ports and security port restrictions.

cfgRacTuneHttpPort (Read/Write)

Legal Values

10 – 65535

Default

80

Description

Specifies the port number to use for HTTP network communication with the RAC.

cfgRacTuneHttpsPort (Read/Write)

Legal Values

10 – 65535

Default

443

Description

Specifies the port number to use for HTTPS network communication with the iDRAC.

cfgRacTuneIpRangeEnable

Legal Values

1 (TRUE)

0 (FALSE)

Default

0

Description

Enables or disables the IP Address Range validation feature of the iDRAC.

cfgRacTuneIpRangeAddr

Legal Values

String, IP address formatted. For example, 192.168.0.44.

Default

192.168.1.1

Description

Specifies the acceptable IP address bit pattern in positions determined by the 1's in the range mask property (**cfgRacTuneIpRangeMask**).

cfgRacTuneIpRangeMask

Legal Values

Standard IP mask values with left-justified bits

Default

255.255.255.0

Description

String, IP-address formatted. For example, `255.255.255.0`.

cfgRacTuneIpBlkEnable

Legal Values

1 (TRUE)

0 (FALSE)

Default

0

Description

Enables or disables the IP address blocking feature of the RAC.

cfgRacTuneIpBlkFailCount

Legal Values

2 – 16

Default

5

Description

The maximum number of login failures to occur within the window (cfgRacTuneIpBlkFailWindow) before login attempts from the IP address are rejected.

cfgRacTuneIpBlkFailWindow

Legal Values

10 – 65535

Default

60

Description

Defines the time span in seconds that the failed attempts are counted. When failure attempts age beyond this limit, they are dropped from the count.

cfgRacTuneIpBlkPenaltyTime

Legal Values

10 – 65535

Default

300

Description

Defines the time span in seconds that session requests from an IP address with excessive failures are rejected.

cfgRacTuneSshPort (Read/Write)

Legal Values

1 – 65535

Default

22

Description

Specifies the port number used for the iDRAC SSH interface.

cfgRacTuneTelnetPort (Read/Write)

Legal Values

1 – 65535

Default

23

Description

Specifies the port number used for the iDRAC telnet interface.

cfgRacTuneConRedirEncryptEnable (Read/Write)

Legal Values

1 (TRUE)

0 (FALSE)

Default

1

Description

Encrypts the video in a console redirection session.

cfgRacTuneConRedirPort (Read/Write)

Legal Values

1 – 65535

Default

5900

Description

Specifies the port to be used for keyboard and mouse traffic during console redirection activity with the iDRAC.

cfgRacTuneConRedirVideoPort (Read/Write)

Legal Values

1 – 65535

Default

5901

Description

Specifies the port to be used for video traffic during console redirection activity with the iDRAC.

NOTE: This object requires an iDRAC reset before it becomes active.

cfgRacTuneAsrEnable (Read/Write)

Legal Values

0 (FALSE)

1 (TRUE)

Default

0

Description

Enables or disables the iDRAC last crash screen capture feature.

NOTE: This object requires an iDRAC reset before it becomes active.

cfgRacTuneWebserverEnable (Read/Write)

Legal Values

0 (FALSE)

1 (TRUE)

Default

1

Description

Enables and disables the iDRAC web server. If this property is disabled, the iDRAC will not be accessible using client web browsers. This property has no effect on the telnet/SSH or local RACADM interfaces.

cfgRacTuneLocalServerVideo (Read/Write)

Legal Values

1 (Enables)

0 (Disables)

Default

1

Description

Enables (switches ON) or disables (switches OFF) the local server video.

ifcRacManagedNodeOs

This group contains properties that describe the Managed Server operating system.

One instance of the group is allowed. The following subsections describe the objects in this group.

ifcRacMnOsHostname (Read/Write)

Legal Values

String. Maximum Length = 255.

Default

""

Description

The host name of the managed server.

ifcRacMnOsOsName (Read/Write)

Legal Values

String. Maximum Length = 255.

Default

""

Description

The operating system name of the managed server.

cfgRacSecurity

This group is used to configure settings related to the iDRAC SSL certificate signing request (CSR) feature. The properties in this group must be configured before generating a CSR from the iDRAC.

See the RACADM **sslcsrgen** subcommand details for more information on generating certificate signing requests.

cfgSecCsrCommonName (Read/Write)

Legal Values

String. Maximum Length = 254.

Default

""

Description

Specifies the CSR Common Name (CN).

cfgSecCsrOrganizationName (Read/Write)

Legal Values

String. Maximum Length = 254.

Default

""

Description

Specifies the CSR Organization Name (O).

cfgSecCsrOrganizationUnit (Read/Write)

Legal Values

String. Maximum Length = 254.

Default

""

Description

Specifies the CSR Organization Unit (OU).

cfgSecCsrLocalityName (Read/Write)

Legal Values

String. Maximum Length = 254.

Default

""

Description

Specifies the CSR Locality (L).

cfgSecCsrStateName (Read/Write)

Legal Values

String. Maximum Length = 254.

Default

""

Description

Specifies the CSR State Name (S).

cfgSecCsrCountryCode (Read/Write)

Legal Values

String. Maximum Length = 2.

Default

""

Description

Specifies the CSR Country Code (CC)

cfgSecCsrEmailAddr (Read/Write)

Legal Values

String. Maximum Length = 254.

Default

""

Description

Specifies the CSR Email Address.

cfgSecCsrKeySize (Read/Write)

Legal Values

1024

2048

4096

Default

1024

Description

Specifies the SSL asymmetric key size for the CSR.

cfgRacVirtual

This group contains parameters to configure the iDRAC virtual media feature. One instance of the group is allowed. The following subsections describe the objects in this group.

cfgVirMediaAttached (Read/Write)

Legal Values

1 (TRUE)

0 (FALSE)

Default

1

Description

This object is used to attach virtual devices to the system via the USB bus. When the devices are attached the server will recognize valid USB mass storage devices attached to the system. This is equivalent to attaching a local USB CDROM/floppy drive to a USB port on the system. When the devices are attached you then can connect to the virtual devices remotely using the iDRAC Web interface or the CLI. Setting this object to 0 will cause the devices to detach from the USB bus.

NOTE: You must restart your system to enable all changes.

cfgVirAtapiSrvPort (Read/Write)

Legal Values

1 – 65535

Default

3668

Description

Specifies the port number used for encrypted virtual media connections to the iDRAC.

cfgVirAtapiSrvPortSsl (Read/Write)

Legal Values

Any unused port number between 0 and 65535 decimal.

Default

3670

Description

Sets the port used for SSL virtual media connections.

cfgVirMediaBootOnce (Read/Write)

Legal Values

1 (Enabled)

0 (Disabled)

Default

0

Description

Enables or disables the virtual media boot-once feature of the iDRAC. If this property is enabled when the host server is rebooted, this feature will attempt to boot from the virtual media devices—if the appropriate media is installed in the device.

cfgFloppyEmulation (Read/Write)

Legal Values

1 (TRUE)

0 (FALSE)

Default

0

Description

When set to 0, the virtual floppy drive is recognized as a removable disk by Windows operating systems. Windows operating systems will assign a drive letter that is C: or higher during enumeration. When set to 1, the Virtual Floppy drive will be seen as a floppy drive by Windows operating systems. Windows operating systems will assign a drive letter of A: or B:.

cfgActiveDirectory

This group contains parameters to configure the iDRAC Active Directory feature.

cfgADRacDomain (Read/Write)

Legal Values

Any printable text string with no white space. Length is limited to 254 characters.

Default

""

Description

Active Directory Domain in which the DRAC resides.

cfgADRacName (Read/Write)

Legal Values

Any printable text string with no white space. Length is limited to 254 characters.

Default

""

Description

Name of iDRAC as recorded in the Active Directory forest.

cfgADEnable (Read/Write)

Legal Values

1 (TRUE)

0 (FALSE)

Default

0

Description

Enables or disables Active Directory user authentication on the iDRAC. If this property is disabled, local iDRAC authentication is used for user logins instead.

cfgADAuthTimeout (Read/Write)

NOTE: To modify this property, you must have **Configure iDRAC** permission.

Legal Values

15 – 300

Default

120

Description

Specifies the number of seconds to wait for Active Directory authentication requests to complete before timing out.

cfgADRootDomain (Read/Write)

Legal Values

Any printable text string with no white space. Length is limited to 254 characters.

Default

""

Description

Root domain of the Domain Forest.

cfgADSpecifyServerEnable (Read/Write)

Legal Values

1 or 0 (True or False)

Default

0

Description

1 (True) enables you to specify an LDAP or a Global Catalog server. 0 (False) disables this option.

cfgADDomainController (Read/Write)

Valid IP address or a fully qualified domain name (FQDN)

Default

No default value

Description

The iDRAC uses the value you specify to search the LDAP server for user names.

cfgADGlobalCatalog (Read/Write)

Legal Values

Valid IP address or a fully qualified domain name (FQDN)

Default

No default value

Description

iDRAC uses the value you specify to search the Global Catalog server for user names.

cfgADType (Read/Write)

Legal Values

1 = Enables Active Directory with the extended schema.

2 = Enables Active Directory with the standard schema.

Default

1 = Extended schema

Description

Determines the schema type to use with Active Directory.

cfgStandardSchema

This group contains parameters to configure the Active Directory standard schema settings.

cfgSSADRoleGroupIndex (Read Only)

Legal Values

Integer from 1 to 5.

Description

Index of the Role Group as recorded in the Active Directory.

cfgSSADRoleGroupName (Read/Write)

Legal Values

Any printable text string with no white space. Length is limited to 254 characters.

Default

(blank)

Description

Name of the Role Group as recorded in the Active Directory forest.

cfgSSADRoleGroupDomain (Read/Write)

Legal Values

Any printable text string with no white space. Length is limited to 254 characters.

Default

(blank)

Description

Active Directory Domain in which the Role Group resides.

cfgSSADRoleGroupPrivilege (Read/Write)

Legal Values

0x00000000 to 0x000001ff

Default

(blank)

Description

Use the bit mask numbers in Table B-3 to set role-based authority privileges for a Role Group.

Table B-3. Bit Masks for Role Group Privileges

Role Group Privilege	Bit Mask
Login to iDRAC	0x00000001
Configure iDRAC	0x00000002
Configure Users	0x00000004
Clear Logs	0x00000008
Execute Server Control Commands	0x00000010
Access Console Redirection	0x00000020
Access Virtual Media	0x00000040
Test Alerts	0x00000080
Execute Debug Commands	0x00000100

cfgIpmiSol

This group is used to configure the Serial Over LAN (SOL) capabilities of the system.

cfgIpmiSolEnable (Read/Write)

Legal Values

0 (FALSE)

1 (TRUE)

Default

1

Description

Enables or disables SOL.

cfgIpmiSolBaudRate (Read/Write)

Legal Values

19200, 57600, 115200

Default

115200

Description

The baud rate for serial communication over LAN.

cfgIpmiSolMinPrivilege (Read/Write)

Legal Values

2 (User)

3 (Operator)

4 (Administrator)

Default

4

Description

Specifies the minimum privilege level required for SOL access.

cfgIpmiSolAccumulateInterval (Read/Write)

Legal Values

1 – 255.

Default

10

Description

Specifies the typical amount of time that the iDRAC waits before transmitting a partial SOL character data packet. This value is 1-based 5ms increments.

cfgIpmiSolSendThreshold (Read/Write)

Legal Values

1 – 255

Default

255

Description

The SOL threshold limit value. Specifies the maximum number of bytes to buffer before sending an SOL data packet.

cfgIpmiLan

This group is used to configure the IPMI over LAN capabilities of the system.

cfgIpmiLanEnable (Read/Write)

Legal Values

0 (FALSE)

1 (TRUE)

Default

0

Description

Enables or disables the IPMI over LAN interface.

cfgIpmiLanPrivLimit (Read/Write)

Legal Values

2 (User)

3 (Operator)

4 (Administrator)

Default

4

Description

Specifies the maximum privilege level allowed for IPMI over LAN access.

cfgIpmiLanAlertEnable (Read/Write)

Legal Values

0 (FALSE)

1 (TRUE)

Default

0

Description

Enables or disables global e-mail alerting. This property overrides all individual e-mail alerting enable/disable properties.

cfgIpmiEncryptionKey (Read/Write)

Legal Values

A string of hexadecimal digits from 0 to 20 characters with no spaces.

Default

00000000000000000000

Description

The IPMI encryption key.

cfgIpmiPetCommunityName (Read/Write)

Legal Values

A string up to 18 characters.

Default

public

Description

The SNMP community name for traps.

cfgIpmiPef

This group is used to configure the platform event filters available on the managed server.

The event filters can be used to control policy related to actions that are triggered when critical events occur on the managed server.

cfgIpmiPefName (Read Only)

Legal Values

String. Maximum Length = 255.

Default

The name of the index filter.

Description

Specifies the name of the platform event filter.

cfgIpmiPefIndex (Read Only)

Legal Values

1 – 17

Default

The index value of a platform event filter object.

Description

Specifies the index of a specific platform event filter.

cfgIpmiPefAction (Read/Write)

Legal Values

0 (None)

1 (Power Down)

2 (Reset)

3 (Power Cycle)

Default

0

Description

Specifies the action that is performed on the managed server when the alert is triggered.

cfgIpmiPefEnable (Read/Write)

Legal Values

0 (FALSE)

1 (TRUE)

Default

1

Description

Enables or disables a specific platform event filter.

cfgIpmiPet

This group is used to configure platform event traps on the managed server.

cfgIpmiPetIndex (Read/Write)

Legal Values

1 – 4

Default

The appropriate index value.

Description

Unique identifier for the index corresponding to the trap.

cfgIpmiPetAlertDestIpAddr (Read/Write)

Legal Values

String representing a valid IP address. For example, `192.168.0.67`.

Default

0.0.0.0

Description

Specifies the destination IP address for the trap receiver on the network. The trap receiver receives an SNMP trap when an event is triggered on the managed server.

cfgIpmiPetAlertEnable (Read/Write)

Legal Values

0 (FALSE)

1 (TRUE)

Default

1

Description

Enables or disables a specific trap.

C

RACADM and SM-CLP Equivalencies

Table C-1 lists the RACADM groups and objects and, where they exist, SM-SLP equivalent locations in the SM-CLP MAP.

Table C-1. RACADM and SM-CLP Equivalencies

RACADM Group	SM-CLP	Description
idRacInfo		
idRacName		String of up to 15 ASCII characters. Default: **iDRAC**.
idRacProductInfo		String of up to 63 ASCII characters. Default: **Integrated Dell Remote Access Controller**.
idRacDescriptionInfo		String of up to 255 ASCII characters. Default: **This system component provides a complete set of remote management functions for Dell PowerEdge servers**
idRacVersionInfo		String of up to 63 ASCII characters. Default: **1**
idRacBuildInfo		String of up to 16 ASCII characters.
idRacType		Default: 8
cfgActiveDirectory	**/system1/sp1/ oemdell_adservice1**	

Table C-1. RACADM and SM-CLP Equivalencies *(continued)*

RACADM Group	SM-CLP	Description
cfgADEnable	enablestate	0 to disable, 1 to enable. Default: **0**
cfgADRacName	oemdell_adracname	String of up to 254 characters.
cfgADRacDomain	oemdell_adracdomain	String of up to 254 characters.
cfgADRootDomain	oemdell_adrootdomain	String of up to 254 characters.
cfgADAuthTimeout	oemdell_timeout	15 to 300 seconds. Default: **120**
cfgADType	oemdell_schematype	1 for standard schema, 2 for extended schema. Default: **1**
cfgStandardSchema		
cfgSSADRoleGroupIndex	**/system1/sp1/group1 *through* /system1/sp1/group5**	RACADM — group index ID (1-5). SM-CLP — selected with address path.
cfgSSADRoleGroupName	oemdell_groupname	String of up to 254 characters.
cfgSSADRoleGroupDomain	oemdell_groupdomain	String of up to 254 characters.
cfgSSADRoleGroupPrivilege	oemdell_groupprivilege	Bit mask with values between 0x00000000 and 0x000001ff.
cfgLanNetworking	**/system1/sp1/enetport1**	
cfgNicMacAddress	macaddress	The MAC address of the interface. Not editable.
	/system1/sp1/enetport1/ lanendpt1/ipendpt1	
cfgNicEnable	oemdell_nicenable	0 to disable NIC, 1 to enable NIC. Default: **0**
cfgNicUseDHCP	oemdell_usedhcp	0 to configure static network addresses, 1 to use DHCP. Default: **0**

Table C-1. RACADM and SM-CLP Equivalencies *(continued)*

RACADM Group	SM-CLP	Description
cfgNicIpAddress	ipaddress	The iDRAC IP address. Default: **192.168.0.120** plus the server slot number.
cfgNicNetmask	subnetmask	Subnet mask for the iDRAC network. Default: **255.255.255.0**
	committed	When group values change, **committed** is set to 0 to indicate that the new values have not been saved. Set the value to 1 to save the new configuration. Default: **1**
	/system1/sp1/enetport1/lanendpt1/ipendpt1/dnsendpt1	
cfgDNSDomainName	oemdell_dnsdomainname	String of up to 254 ASCII characters. At least one character must be alphabetic.
cfgDNSDomainNameFromDHCP	oemdell_domainnamefromdhcp	Set to 1 to get domain name from DHCP. Default: **0**
cfgDNSRacName	oemdell_dnsracname	String of up to 63 ASCII characters. At least one character must be alphabetic. Default: **iDRAC-** *plus the Dell service tag*.
cfgDNSRegisterRac	oemdell_dnsregisterrac	Set to 1 to register iDRAC name in DNS. Default: **0**
cfgDNSServersFromDHCP	oemdell_dnsserversfromdhcp	Set to 1 to get DNS server addresses from DHCP. Default: **0**
	/server1/sp1/enetport1/lanendpt1/ipendpt1/dnsendpt1/remotesap1	

Table C-1. RACADM and SM-CLP Equivalencies *(continued)*

RACADM Group	SM-CLP	Description
cfgDNSServer1	dnsserveraddresses1	A string representing the IP address of a DNS Server.
	/server1/sp1/enetport1/lanendpt1/ipendpt1/dnsendpt1/remotesap1	
cfgDNSServer2	dnsserveraddresses2	A string representing the IP address of a DNS Server.
	/server1/sp1/enetport1/lanendpt1/ipendpt1/remotesap1	
cfgNicGateway	defaultgatewayaddress	A string representing the IP address of the default gateway. Default: 192.168.0.1
cfgRacVirtual	**/server1/sp1/oemdell_vmservice1**	
cfgFloppyEmulation	oemdell_floppyemulation	Set to 1 to enable floppy disk emulation. Default: 0
cfgVirMediaAttached	enabledstate	Set to 1 to attach media. Default: 1
cfgVirMediaBootOnce	oemdell_singleboot	Set to 1 to perform next boot from selected media. Default 0.
	/server1/sp1/oemdell_vmservice1/tcpendpt1	
	oemdell_sslenabled	Set to 1 if SSL is enabled for first virtual media device, 0 if not. Not editable.
cfgVirAtapiSvrPort	portnumber	Port to use for first virtual media device. Default: 3668
	/server1/sp1/oemdell_vmservice1/tcendpt2	

Table C-1. RACADM and SM-CLP Equivalencies *(continued)*

RACADM Group	SM-CLP	Description
	oemdell_sslenabled	Set to 1 if SSL is enabled for second virtual media device, 0 if not. Not editable.
cfgVirAtapiSvrPortSsl	portnumber	Port to use for second virtual media device. Default: **3670**
cfgUserAdmin	**/server1/sp1/oemdell_vmservice1/tcpendpt2**	
cfgUserAdminEnable	enabledstate	Set to 1 to enable user. Default: **0**
cfgUserAdminIndex	userid	User index, from 1 to 16.
cfgUserAdminIpmiLanPrivilege	oemdell_ipmilanprivileges	2 (user), 3 (operator), 4 (administrator), or 15 (No access). Default: **4**
cfgUserAdminPassword	password	A string of up to 20 ASCII characters.
cfgUserAdminPrivilege	oemdell_extendedprivileges	Bit mask value between 0x00000000 and 0x000001ff. Default: **0x00000000**
cfgUserAdminSolEnable	solenabled	Set to 1 to allow user to use Serial over LAN. Default: **0**
cfgUserAdminUserName	username	String of up to 16 characters.
cfgEmailAlert		
cfgEmailAlertAddress		E-mail destination address, up to 64 characters.
cfgEmailAlertCustomMsg		Message to send in e-mail, up to 32 characters.
cfgEmailAlertEnable		Set to 1 to enable the e-mail alert. Default: **0**

Table C-1. RACADM and SM-CLP Equivalencies *(continued)*

RACADM Group	SM-CLP	Description
cfgEmailAlertIndex		Index of the e-mail alert instance. Number from 1 to 4.
cfgSessionManagement		
cfgSsnMgtConsRedirMaxSessions		Number of concurrent console redirection sessions allowed (1 or 2). Default: **2**
cfgSsnMgtSshIdleTimeout		Number of seconds idle before a SSH session times out. 0 to disable timeout or 60-1920 seconds. Default: **300**
cfgSsnMgtTelnetIdleTimeout		Number of seconds idle before a telnet session times out. 0 to disable timeout or 60-1920 seconds. Default: **300**
cfgSsnMgtWebserverTimeout		Number of seconds idle before a Web interface session times out. 60-1920 seconds. Default: **300**
cfgRacTuning		
cfgRacTuneConRedirEnable		Set to 1 to enable console redirection, 0 to disable. Default:**1**
cfgRacTuneConRedirEncrypt Enable		Set to 1 to enable encryption of console redirection network traffic, 0 to disable. Default: **1**
cfgRacTuneConRedirPort		Port to use for console redirection. Default: **5900**

Table C-1. RACADM and SM-CLP Equivalencies *(continued)*

RACADM Group	SM-CLP	Description
cfgRacTuneConRedirVideoPort		Port to use for console video redirection. Default: **5901**
cfgRacTuneHttpPort		Port to use for Web interface HTTP. Default: **80**
cfgRacTuneHttpsPort		Port to use for secure Web interface HTTPS. Default: **443**
cfgRacTuneIpBlkEnable		Set to 1 to enable IP blocking. Default: **0**
cfgRacTuneIPBlkFailCount		Number of failed login attempts to count before blocking IP (2 to 16). Default: **5**
cfgRacTuneIpBlkFailWindow		Time span in seconds during which to count failed login attempts (10 to 65535). Default: **60**
cfgRacTuneIpBlkPenaltyTime		Time span in seconds that a blocked IP remains blocked (10 to 65535). Default: **300**
cfgRacTuneIpRangeAddr		Base IP address for IP range filter. Default: **192.168.0.1**
cfgRacTuneIpRangeEnable		Set to 1 to allow IP range filtering. Default: 0
cfgRacTuneIpRangeMask		Bit mask applied to the base address to select valid IP addresses. Default: **255.255.255.0**
cfgRacTuneLocalServerVideo		Set to 1 to enable local iKVM console. Default: **1**
cfgRacTuneSshPort		Port to use for the SSH service. Default: **22**

Table C-1. RACADM and SM-CLP Equivalencies *(continued)*

RACADM Group	SM-CLP	Description
cfgRacTuneTelnetPort		Port to use for the telnet service. Default: **23**
cfgRacTuneWebserverEnable		Set to 1 to enable the iDRAC Web interface. Default: **1**
ifcRacManagedNodeOS		
ifcRacMnOsHostname		Host name of the managed server. String of up to 255 characters.
ifcRacMnOsOsName		Name of the managed server operating system. A string of up to 255 characters.
cfgRacSecurity	**/system1/sp1/oemdell_racsecurity1**	
cfgRacSecCsrCommonName	commonname	Active Directory common name. String of up to 254 characters.
cfgRacSecCsrCountryCode	oemdell_countrycode	Active Directory country code. 2 characters.
cfgRacSecCsrEmailAddr	oemdell_emailaddress	E-mail address to use for Certificate Signing Request. String of up to 254 characters.
cfgRacSecCsrKeySize	oemdell_keysize	Length of encryption key (512, 1024, or 2048). Default: **1024**.
cfgRacSecCsrLocalityName	oemdell_localityname	Active Directory locality name. String of up to 254 characters.
cfgRacSecCsrOrganizationName	organizationname	Active Directory organization name. String of up to 254 characters.
cfgRacSecCsrOrganizationUnit	oemdell_organizationunit	Active Directory organization unit name. String of up to 254 characters.

Table C-1. RACADM and SM-CLP Equivalencies *(continued)*

RACADM Group	SM-CLP	Description
cfgRacSecCsrStateName	oemdell_statename	Activity Directory state name. String of up to 254 characters.
cfgIpmiSol		
cfgIpmiSolAccumulateInterval		Maximum number of milliseconds to wait before sending a partial Serial over LAN packet (1 to 255). Default: **10**
cfgIpmiSolBaudRate		Baud rate to use for Serial over LAN (19200, 57600, 115200). Default: **115200**
cfgIpmiSolEnable		Set to 1 to enable Serial over LAN feature. Default: **0**
cfgIpmiSolSendThreshold		Maximum number of characters to collect before sending SOL data (1 to 255). Default: **255**
cfgIpmiSolMinPrivilege		Minimum privilege required to use SOL. 2 (user), 3 (operator), or 4 (administrator). Default: **4**
cfgIpmiLan		
cfgIpmiEncryptionKey		A string of 0 to 40 hexadecimal digits. Default: **00000000000000000000 00000000000000000000**
cfgIpmiLanAlertEnable		Set to 1 to enable IPMI LAN alerts. Default: **0**
cfgIpmiLanEnable		Set to 1 to enable the IPMI over LAN interface. Default: **0**

Table C-1. RACADM and SM-CLP Equivalencies *(continued)*

RACADM Group	SM-CLP	Description
cfgIpmiPetCommunityName		A string of up to 18 characters. Default: **public**
cfgIpmiPef		
cfgIpmiPefAction		The action to take when event is detected. 0 (none), 1 (power down), 2 (reset), 3 (power cycle). Default: **0**
cfgIpmiPefEnable		Set to 1 to enable platform event filtering. Default: **0**
cfgIpmiPefIndex		The index number of the platform event filter. (1 - 17)
cfgIpmiPefName		The name of the platform event, a string of up to 254 characters. Not editable.
cfgIpmiPet		
cfgIpmiPetAlertDestIpAddr		IP address of the platform event trap receiver. Default: **0.0.0.0**
cfgIpmiPetAlertEnable		Set to 1 to enable the platform event trap. Default: **1**
cfgIpmiPetIndex		Index number (1-4) of the platform event trap.

Glossary

Active Directory

Active Directory is a centralized and standardized system that automates network management of user data, security, and distributed resources, and enables interoperation with other directories. Active Directory is designed especially for distributed networking environments.

AGP

Abbreviation for accelerated graphics port, which is a bus specification that allows graphics cards faster access to main system memory.

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.

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.

CMC

Abbreviation for enclosure Management Controller, which is the controller interface between the iDRAC and the managed system's CMC.

bus

A set of conductors connecting the various functional units in a computer. Busses are named by the type of data they carry, such as data bus, address bus, or PCI bus.

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 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.

CD

Abbreviation for compact disc.

CHAP

Acronym for Challenge-Handshake Authentication Protocol, which is an authentication method used by PPP servers to validate the identity of the originator of the connection.

CIM

Acronym for Common Information Model, which is a protocol designed for managing systems on a network.

CLI

Abbreviation for command-line interface.

CLP

Abbreviation for command-line protocol.

console redirection

Console redirection is a function that directs a managed server'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 server.

CSR

Abbreviation for Certificate Signing Request.

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.

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).

DDNS

Abbreviation for Dynamic Domain Name System.

DMTF

Abbreviation for Distributed Management Task Force.

DNS

Abbreviation for Domain Name System.

iDRAC

Abbreviation for Dell Remote Access Controller 5.

DSU

Abbreviation for disk storage unit.

extended schema

A solution used with Active Directory to determine user access to iDRAC; uses Dell-defined Active Directory objects.

FQDN

Acronym for Fully Qualified Domain Names. Microsoft® Active Directory® only supports FQDN of 64 bytes or fewer.

FSMO

Flexible Single Master Operation. It is Microsoft’s way of guaranteeing atomicity of the extension operation.

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.

GRUB

Acronym for GRand Unified Bootloader, a new and commonly-used Linux loader.

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 iDRAC and the CMC.

iAMT

Intel® Active Management Technology — Delivers more secure systems management capabilities whether or not the computer is powered up or turned off, or the operating system is not responding.

ICMB

Abbreviation for Intelligent enclosure Management Bus.

ICMP

Abbreviation for Internet control message protocol.

ID

Abbreviation for identifier, commonly used when referring to a user identifier (user ID) or object identifier (object ID).

iDRAC

Acronym for integrated Dell Remote Access Controller, the integrated System-on-Chip monitor/control system for the Dell 10G PowerEdge servers.

IP

Abbreviation for Internet Protocol, which is the network layer for TCP/IP. IP provides packet routing, fragmentation, and reassembly.

IPMB

Abbreviation for intelligent platform 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.

Kbps

Abbreviation for kilobits per second, which is a data transfer rate.

LAN

Abbreviation for local area network.

LDAP

Abbreviation for Lightweight Directory Access Protocol.

LED

Abbreviation for light-emitting diode.

LOM

Abbreviation for Local area network On Motherboard.

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 server

The managed server is the system in which the iDRAC is embedded.

management station

The management station is a system that remotely accesses the iDRAC.

MAP

Abbreviation for Manageability Access Point.

Mbps

Abbreviation for megabits per second, which is a data transfer rate.

MIB

Abbreviation for management information base.

MII

Abbreviation for Media Independent Interface.

NAS

Abbreviation for network attached storage.

NIC

Abbreviation for network interface card. An adapter circuit board installed in a computer to provide a physical connection to a network.

OID

Abbreviation for Object Identifiers.

OSCAR

Acronym for On Screen Configuration and Reporting. OSCAR is the menu displayed by the Avocent iKVM when you press <Print Screen>. It allows you to select the CMC console or the iDRAC console for a server installed in the CMC.

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.

RAM

Acronym for random-access memory. RAM is general-purpose readable and writable memory on systems and the iDRAC.

RAM disk

A memory-resident program which emulates a hard drive. The iDRAC maintains a RAM disk in its memory.

RAC

Abbreviation for remote access controller.

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 Microsoft's Special Administration Console.

SAP

Abbreviation for Service Access Point.

SEL

Acronym for system event log.

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.

SMWG

Abbreviation for Systems Management Working Group.

SNMP trap

A notification (event) generated by the iDRAC or the CMC that contains information about state changes on the managed server or about potential hardware problems.

SSH

Abbreviation for Secure Shell.

SSL

Abbreviation for secure sockets layer.

standard schema

A solution used with Active Directory to determine user access to iDRAC; uses Active Directory group objects only.

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.

UPS

Abbreviation for uninterruptible power supply.

USB

Abbreviation for Universal Serial Bus.

UTC

Abbreviation for Universal Coordinated Time. *See* GMT.

VLAN

Abbreviation for Virtual Local Area Network.

VNC

Abbreviation for virtual network computing.

VT-100

Abbreviation for Video Terminal 100, which is used by the most common terminal emulation programs.

WAN

Abbreviation for wide area network.

Index