Integrated Dell™ Remote Access Controller 6 (iDRAC6) Version 1.2

User Guide

DELL™

Notes and Cautions

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

CAUTION: A CAUTION indicates potential damage to hardware or loss of data if instructions are not followed.

_____

Contents

Contents | **13**

1

iDRAC6 Overview

The Integrated Dell™ Remote Access Controller6 (iDRAC6) 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 iDRAC6 uses an integrated System-on-Chip microprocessor for the remote monitor/control system. The iDRAC6 co-exists on the system board with the managed PowerEdge server. The server operating system is concerned with executing applications; the iDRAC6 is concerned with monitoring and managing the server's environment and state outside of the operating system.

You can configure the iDRAC6 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, iDRAC6 can log event data and capture an image of the screen when it detects that the system has crashed.

The iDRAC6 network interface is enabled with a static IP address of 192.168.0.120 by default. It must be configured before the iDRAC6 is accessible. After the iDRAC6 is configured on the network, it can be accessed at its assigned IP address with the iDRAC6 Web interface, Telnet, or Secure Shell (SSH), and supported network management protocols, such as Intelligent Platform Management Interface (IPMI).

iDRAC6 Express Management Features

The iDRAC6 Express provides the following management features:

- Dynamic Domain Name System (DDNS) registration
- Remote system management and monitoring using a Web interface and the SM-CLP command line over a serial, Telnet, or SSH connection
- Support for Microsoft® Active Directory® authentication — Centralizes iDRAC6 user IDs and passwords in Active Directory using an extended schema or a standard schema

- Monitoring — Provides access to system information and status of components

- Access to system logs — Provides access to the system event log, the iDRAC6 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 iDRAC6 Web interface from Dell OpenManage Server Administrator or Dell OpenManage IT Assistant

- iDRAC6 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

- IPv6 support — Adds IPv6 support such as providing access to the iDRAC6 Web interface using an IPv6 address, specifies iDRAC6 NIC IPv6 address, and specifies a destination number to configure an IPv6 SNMP alert destination.

- WS-MAN support — Provides network accessible management using the Web Services for Management (WS-MAN) protocol.

- SM-CLP support — Adds Server Management-Command Line Protocol (SM-CLP) support, which provides standards for systems management CLI implementations.

- Firmware rollback and recovery — Allows you to boot from (or rollback to) the firmware image of your choice.

For more information about iDRAC6 Express, see your *Hardware Owner's Manual* at **support.dell.com\manuals**.

iDRAC6 Enterprise and vFlash Media

Adds support for RACADM, virtual KVM, Virtual Media features, a dedicated NIC, and Virtual Flash (with an optional Dell vFlash Media card). Virtual Flash allows you to store emergency boot images and diagnostic tools on the vFlash Media. For more information about iDRAC6 Enterprise and vFlash Media, see your *Hardware Owner's Manual* at **support.dell.com\manuals**.

Table 1-1 lists the features available for BMC, iDRAC6 Express, iDRAC6 Enterprise, and vFlash Media.

Table 1-1.   iDRAC6 Feature List

Feature	BMC	iDRAC6 Express	iDRAC6 Enterprise	vFlash Media
Interface and Standards Support				
IPMI 2.0	✔	✔	✔	✔
Web-based GUI	✖	✔	✔	✔
SNMP	✖	✔	✔	✔
WSMAN	✖	✔	✔	✔
SMASH-CLP	✖	✔	✔	✔
RACADM Command Line	✖	✖	✔	✔
Connectivity				
Shared/Failover Network Modes	✔	✔	✔	✔
IPv4	✔	✔	✔	✔
VLAN Tagging	✔	✔	✔	✔
IPv6	✖	✔	✔	✔
Dynamic DNS	✖	✔	✔	✔
Dedicated NIC	✖	✖	✔	✔

Table 1-1. iDRAC6 Feature List *(continued)*

Feature	BMC	iDRAC6 Express	iDRAC6 Enterprise	vFlash Media
Security and Authentication				
Role-based Authority	✓	✓	✓	✓
Local Users	✓	✓	✓	✓
Active Directory	✗	✓	✓	✓
Two-factor Authentication	✗	✓	✓	✓
Single sign-on	✗	✓	✓	✓
SSL Encryption	✓	✓	✓	✓
Remote Management and Remediation				
Remote Firmware Update	✓[1]	✓	✓	✓
Remote operating system installation	✗	✓	✓	✓
Server Power Control	✓[1]	✓	✓	✓
Serial-over-LAN (with proxy)	✓	✓	✓	✓
Serial-over-LAN (no proxy)	✗	✓	✓	✓
Power Capping	✗	✓	✓	✓
Last Crash Screen Capture	✗	✓	✓	✓
Boot Capture	✗	✓	✓	✓
Virtual Media	✗	✗	✓	✓

Table 1-1.   iDRAC6 Feature List *(continued)*

Feature	BMC	iDRAC6 Express	iDRAC6 Enterprise	vFlash Media
Virtual Console	✖	✖	✔	✔
Virtual Console Sharing	✖	✖	✔	✔
Virtual Flash	✖	✖	✖	✔
Monitoring				
Sensor Monitoring and Alerting	✔[1]	✔	✔	✔
Real-time Power Monitoring	✖	✔	✔	✔
Real-time Power Graphing	✖	✔	✔	✔
Historical Power Counters	✖	✔	✔	✔
Logging				
System Event Log (SEL)	✔	✔	✔	✔
RAC Log	✖	✔	✔	✔
Trace Log	✖	✔	✔	✔

[1]–Feature is available only through IPMI and not through a web GUI

✔ = Supported; ✖ =Not Supported

The iDRAC6 provides the following security features:

- User authentication through 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-based interface or SM-CLP

- SM-CLP and Web interfaces, which support 128-bit and 40-bit encryption (for countries where 128 bit is not acceptable), using the SSL 3.0 standard

- 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.

- 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

- Ability to limit the IP address range for clients connecting to the iDRAC6

- Smart Card Authentication

Supported Platforms

For the latest supported platforms, see the iDRAC6 Readme file and the *Dell Systems Software Support Matrix* available at **support.dell.com/manuals** and on the *Dell Systems Management Tools and Documentation* DVD that was shipped with your system.

Supported Operating Systems

For the latest information, see the iDRAC6 Readme file and the *Dell Systems Software Support Matrix* available at **support.dell.com/manuals** and on the *Dell Systems Management Tools and Documentation* DVD that was shipped with your system.

Supported Web Browsers

For the latest information, see the iDRAC6 Readme file and the *Dell Systems Software Support Matrix* available at **support.dell.com/manuals** and on the *Dell Systems Management Tools and Documentation* DVD that was shipped with your system.

NOTE: Due to serious security flaws, support for SSL 2.0 has been discontinued. Your browser must be configured to enable SSL 3.0 in order to work properly.

Supported Remote Access Connections

Table 1-2 lists the connection features.

Table 1-2.   Supported Remote Access Connections

Connection	Features
iDRAC6 NIC	• 10Mbps/100Mbs/Ethernet
	• DHCP support
	• SNMP traps and e-mail event notification
	• Support for SM-CLP (Telnet or SSH) command shell, for operations such as iDRAC6 configuration, system boot, reset, power-on, and shutdown commands
	• Support for IPMI utilities, such as IPMItool and ipmish

iDRAC6 Ports

Table 1-3 lists the ports iDRAC6 listens on for connections. Table 1-4 identifies the ports that the iDRAC6 uses as a client. This information is required when opening firewalls for remote access to an iDRAC6.

Table 1-3.   iDRAC6 Server Listening Ports

Port Number	Function
22*	SSH
23*	Telnet
80*	HTTP
443*	HTTPS

Table 1-3. iDRAC6 Server Listening Ports _(continued)_

Port Number	Function
623	RMCP/RMCP+
5900*	Console Redirection keyboard/mouse, Virtual Media Service, Virtual Media Secure Service, Console Redirection video

* Configurable port

Table 1-4. iDRAC6 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 guide, the following documents provide additional information about the setup and operation of the iDRAC6 in your system. The documents are available on the Dell Support website at **support.dell.com/manuals**.

- The iDRAC6 online help provides detailed information about using the Web-based interface.

- The _Dell Lifecycle Controller User Guide_ provides information on the Unified Server Configurator (USC), the Unified Server Configurator – Lifecycle Controller Enabled (USC – LCE), and Remote Services.

- The _Dell Systems Software Support Matrix_ provides information about the various Dell systems, the operating systems supported by these systems, and the Dell OpenManage components that can be installed on these systems.

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

- The *Dell OpenManage Software Quick Installation Guide* provides an overview of applications that you can install on your management station (console) and on your managed systems and procedures for installing your console and managed system applications on systems running supported operating systems.

- See the *Dell OpenManage IT Assistant User's Guide* for information about using IT Assistant.

- For installing an iDRAC6, see your *Hardware Owner's Manual*.

- See the *Dell OpenManage Server Administrator User's Guide* for information about installing and using Server Administrator.

- See the *Dell Update Packages User's Guide* for information about obtaining and using Dell Update Packages as part of your system update strategy.

- See the *Dell OpenManage Baseboard Management Controller Utilities User's Guide* for information about the iDRAC6 and the IPMI interface.

The following system documents are also available to provide more information about the system in which your iDRAC6 is installed:

- The safety instructions that came with your system provide important safety and regulatory information. For additional regulatory information, see the Regulatory Compliance home page at **www.dell.com/regulatory_compliance**. Warranty information may be included within this document or as a separate document.

- The *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

Getting Started With the iDRAC6

The iDRAC6 enables you to remotely monitor, troubleshoot, and repair a Dell system even when the system is down. The iDRAC6 offers a rich set of features like console redirection, virtual media, virtual KVM, Smart Card authentication, and single sign-on.

The *management station* is the system from which an administrator remotely manages a Dell system that has an iDRAC6. The systems that are monitored in this way are called *managed systems*.

Optionally, you can install Dell™ OpenManage™ software on the management station as well as the managed system. Without the managed system software, you cannot use the RACADM locally, and the iDRAC6 cannot capture the last crash screen.

To set up iDRAC6, follow these general steps:

NOTE: This procedure may differ for various systems. See your specific system's *Hardware Owner's Manual* on the Dell Support Website at **support.dell.com/manuals** for precise instructions on how to perform this procedure.

1 Configure the iDRAC6 properties, network settings, and users — You can configure the iDRAC6 by using either the iDRAC6 Configuration Utility, the Web-based interface, or the RACADM.

2 If using a Windows system, configure the Microsoft® Active Directory® to provide access to the iDRAC6, allowing you to add and control iDRAC6 user privileges to your existing users in your Active Directory software.

3 Configure Smart Card authentication — Smart Card provides an added level of security to your enterprise.

4 Configure remote access points, such as console redirection and virtual media.

5 Configure the security settings.

6 Configure alerts for efficient systems management capability.

7 Configure the iDRAC6 Intelligent Platform Management Interface (IPMI) settings to use the standards-based IPMI tools to manage the systems on your network.

3

Basic Installation of the iDRAC6

This section provides information about how to install and set up your iDRAC6 hardware and software.

Before You Begin

Gather the following items that were included with your system, prior to installing and configuring the iDRAC6 software:

- iDRAC6 hardware (currently installed or in the optional kit)
- iDRAC6 installation procedures (located in this chapter)
- *Dell Systems Management Tools and Documentation* DVD

Installing the iDRAC6 Express/Enterprise Hardware

NOTE: The iDRAC6 connection emulates a USB keyboard connection. As a result, when you restart the system, the system will not notify you if your keyboard is not attached.

The iDRAC6 Express/Enterprise may be preinstalled on your system, or available separately. To get started with the iDRAC6 that is installed on your system, see "Software Installation and Configuration Overview."

If an iDRAC6 Express/Enterprise is not installed on your system, see your platform *Hardware Owner's Manual* for hardware installation instructions.

Configuring Your System to Use an iDRAC6

To configure your system to use an iDRAC6, use the iDRAC6 Configuration Utility.

To run the iDRAC6 Configuration Utility:

1 Turn on or restart your system.

2 Press <Ctrl><E> when prompted during POST.

If your operating system begins to load before you press <Ctrl><E>, allow the system to finish booting, and then restart your system and try again.

3 Configure the LOM.

   a Use the arrow keys to select **LAN Parameters** and press <Enter>. **NIC Selection** is displayed.

   b Use the arrow keys to select one of the following NIC modes:

   • **Dedicated** — Select this option to enable the remote access device to utilize the dedicated network interface available on the iDRAC6 Enterprise. This interface is not shared with the host operating system and routes the management traffic to a separate physical network, enabling it to be separated from the application traffic. This option is available only if an iDRAC6 Enterprise is installed in the system. After you install the iDRAC6 Enterprise card, ensure that you change the **NIC Selection** to **Dedicated**. This can be done either through the iDRAC6 Configuration Utility, the iDRAC6 Web Interface, or through RACADM.

   • **Shared** — Select this option to share the network interface with the host operating system. The remote access device network interface is fully functional when the host operating system is configured for NIC teaming. The remote access device receives data through NIC 1 and NIC 2, but transmits data only through NIC 1. If NIC 1 fails, the remote access device will not be accessible.

- **Shared with Failover LOM2** — Select this option to share the network interface with the host operating system. The remote access device network interface is fully functional when the host operating system is configured for NIC teaming. The remote access device receives data through NIC 1 and NIC 2, but transmits data only through NIC 1. If NIC 1 fails, the remote access device fails over to NIC 2 for all data transmission. The remote access device continues to use NIC 2 for data transmission. If NIC 2 fails, the remote access device fails over all data transmission back to NIC 1 if the failure in NIC1 has been corrected.

- **Shared with Failover All LOMs** — Select this option to share the network interface with the host operating system. The remote access device network interface is fully functional when the host operating system is configured for NIC teaming. The remote access device receives data through NIC 1, NIC 2, NIC 3, and NIC 4; but it transmits data only through NIC 1. If NIC 1 fails, the remote access device fails over all data transmission to NIC 2. If NIC 2 fails, the remote access device fails over all data transmission to NIC 3. If NIC 3 fails, the remote access device fails over all data transmission to NIC 4. If NIC 4 fails the remote access device fails over all data transmission back to NIC 1, but only if the original NIC 1 failure has been corrected. This option may not be available on iDRAC6 Enterprise.

4 Configure the network controller LAN parameters to use DHCP or a Static IP address source.

   a Using the down-arrow key, select **LAN Parameters**, and press <Enter>.

   b Using the up-arrow and down-arrow keys, select **IP Address Source**.

   c Using the right-arrow and left-arrow keys, select **DHCP**, **Auto Config** or **Static**.

   d If you selected **Static**, configure the **Ethernet IP Address**, **Subnet Mask**, and **Default Gateway** settings.

   e Press <Esc>.

5 Press <Esc>.

6 Select **Save Changes and Exit**.

Software Installation and Configuration Overview

This section provides a high-level overview of the iDRAC6 software installation and configuration process. For more information about the iDRAC6 software components, see "Installing the Software on the Managed System."

Installing Your iDRAC6 Software

To install your iDRAC6 software:

1   Install the software on the managed system. See "Installing the Software on the Managed System."

2   Install the software on the management station. See "Installing the Software on the Managed System."

Configuring Your iDRAC6

To configure your iDRAC6:

1   Use one of the following configuration tools:

  • Web-based interface (see "Configuring the iDRAC6 Using the Web Interface")

  • RACADM CLI (see "Using the iDRAC6 SM-CLP Command Line Interface")

  • Telnet console (see "Using a Telnet Console")

  📝 **NOTE:** Using more than one iDRAC6 configuration tool at the same time may generate unexpected results.

2   Configure the iDRAC6 network settings. See "Configuring the iDRAC6 Network Settings."

3   Add and configure iDRAC6 users. See "Adding and Configuring iDRAC6 Users."

4   Configure the Web browser to access the Web-based interface. See "Configuring a Supported Web Browser."

5   Disable the Microsoft® Windows® Automatic Reboot Option. See "Disabling the Windows Automatic Reboot Option."

6   Update the iDRAC6 Firmware. See "Updating the iDRAC6 Firmware."

Installing the Software on the Managed System

Installing software on the managed system is optional. Without the managed system software, you cannot use the RACADM locally, and the iDRAC6 cannot capture the last crash screen.

To install the managed system software, install the software on the managed system using the *Dell Systems Management Tools and Documentation* DVD. For instructions about how to install this software, see your *Software Quick Installation Guide* available on the Dell Support website at **support.dell.com\manuals**.

Managed system software installs your choices from the appropriate version of Dell™ OpenManage™ Server Administrator on the managed system.

NOTE: Do not install the iDRAC6 management station software and the iDRAC6 managed system software on the same system.

If Server Administrator is not installed on the managed system, you cannot view the system's last crash screen or use the **Auto Recovery** feature.

For more information about the last crash screen, see "Viewing the Last System Crash Screen."

Installing the Software on the Management Station

Your system includes the *Dell Systems Management Tools and Documentation* DVD. This DVD includes the following components:

- DVD root - Contains the Dell Systems Build and Update Utility, which provides server setup and system installation information

- SYSMGMT - Contains the systems management software products including Dell OpenManage Server Administrator

- Docs - Contains documentation for systems management software products, peripherals, and RAID controllers

- SERVICE - Contains the tools you need to configure your system, and delivers the latest diagnostics and Dell-optimized drivers for your system

For information about Server Administrator, IT Assistant, and Unified Server Configurator, see the *Server Administrator User's Guide*, the *IT Assistant User's Guide*, and the *Lifecycle Controller User's Guide* available on the Dell Support website at **support.dell.com\manuals**.

Installing and Removing RACADM on a Linux Management Station

To use the remote RACADM functions, install RACADM on a management station running Linux.

NOTE: When you run **Setup** on the *Dell Systems Management Tools and Documentation* DVD, the RACADM utility for all supported operating systems is installed on your management station.

Installing RACADM

1 Log on as root to the system where you want to install the management station components.

2 If necessary, mount the *Dell Systems Management Tools and Documentation* DVD using the following command or a similar command:

   ```
   mount /media/cdrom
   ```

3 Navigate to the **/linux/rac** directory and execute the following command:

   ```
   rpm -ivh *.rpm
   ```

For help with the RACADM command, type **racadm help** after issuing the previous commands.

Uninstalling RACADM

To uninstall RACADM, open a command prompt and type:

```
rpm -e <racadm_package_name>
```

where *<racadm_package_name>* is the rpm package that was used to install the RAC software.

For example, if the rpm package name is **srvadmin-racadm5**, then type:

```
rpm -e srvadmin-racadm5
```

Updating the iDRAC6 Firmware

Use one of the following methods to update your iDRAC6 firmware.

- Web-based Interface (see "Updating the iDRAC6 Firmware Using the Web-Based Interface")
- RACADM CLI (see "Updating the iDRAC6 Firmware Using RACADM")
- Dell Update Packages (see "Updating the iDRAC6 Firmware Using Dell Update Packages for Supported Windows and Linux Operating Systems")

Before You Begin

Before you update your iDRAC6 firmware using local RACADM or the Dell Update Packages, perform the following procedures. Otherwise, the firmware update operation may fail.

1 Install and enable the appropriate IPMI and managed node drivers.

2 If your system is running a Windows operating system, enable and start the **Windows Management Instrumentation** (WMI) service.

3 If you are using iDRAC6 Enterprise and your system is running SUSE® Linux Enterprise Server (version 10) for Intel® EM64T, start the **Raw** service.

4 Disconnect and unmount Virtual Media.

   NOTE: If iDRAC6 firmware update is interrupted for any reason, a wait of up to 30 minutes may be required before a firmware update will be allowed again.

5 Ensure that the USB is enabled.

Downloading the iDRAC6 Firmware

To update your iDRAC6 firmware, download the latest firmware from the Dell Support website located at **support.dell.com** and save the file to your local system.

The following software components are included with your iDRAC6 firmware package:

- Compiled iDRAC6 firmware code and data
- Web-based interface, JPEG, and other user interface data files
- Default configuration files

Updating the iDRAC6 Firmware Using the Web-Based Interface

For detailed information, see "Updating the iDRAC6 Firmware/System Services Recovery Image."

Updating the iDRAC6 Firmware Using RACADM

You can update the iDRAC6 firmware using the CLI-based RACADM tool. If you have installed Server Administrator on the managed system, use local RACADM to update the firmware.

1   Download the iDRAC6 firmware image from the Dell Support website at **support.dell.com** to the managed system.

For example:

```
C:\downloads\firmimg.d6
```

2   Run the following RACADM command:

```
racadm fwupdate -pud c:\downloads\
```

You can also update the firmware using remote RACADM and a TFTP server.

For example:

```
racadm -r <iDRAC6 IP address> -u <username> -p
<password> fwupdate -g -u -a <path>
```

where *path* is the location on the TFTP server where the **firmimg.d6** is stored.

Updating the iDRAC6 Firmware Using Dell Update Packages for Supported Windows and Linux Operating Systems

Download and run the Dell Update Packages for supported Windows and Linux operating systems from Dell Support website at **support.dell.com**. For more information, see the *Dell Update Package User's Guide* available on the Dell Support website at **support.dell.com\manuals**.

NOTE: When updating the iDRAC6 firmware using the Dell Update Package utility in Linux, you may see these messages displayed on the console:

```
usb 5-2: device descriptor read/64, error -71

usb 5-2: device descriptor not accepting
address 2, error -71
```

These errors are cosmetic in nature and should be ignored. These messages are caused due to reset of the USB devices during the firmware update process and are harmless.

Clearing the Browser Cache

After the firmware upgrade, clear the Web browser cache.

See your Web browser's online help for more information.

Configuring a Supported Web Browser

The following sections provide instructions for configuring the supported Web browsers.

Configuring Your Web Browser to Connect to the iDRAC6 Web-Based Interface

If you are connecting to the iDRAC6 Web-based 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 your Internet Explorer Web browser to access a proxy server:

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.

List of Trusted Domains

When you access the iDRAC6 Web-based interface through the Web browser, you are prompted to add the iDRAC6 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 reestablish a connection to the iDRAC6 Web-based interface.

32-bit and 64-bit Web Browsers

The iDRAC6 Web-based 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 iDRAC6.

Viewing Localized Versions of the Web-Based Interface

Windows

The iDRAC6 Web-based interface is supported on the following Windows operating system languages:

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

To view a localized version of the iDRAC6 Web-based interface in Internet Explorer:

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 Click **OK**.

7 In the **Language Preference** window, click **OK**.

Linux

If you are running Console Redirection on a Red Hat® Enterprise Linux® (version 4) client with a Simplified Chinese GUI, the viewer menu and title may appear in random characters. This issue is caused by an incorrect encoding in the Red Hat Enterprise Linux (version 4) Simplified Chinese operating system. To fix this issue, access and modify the current encoding settings by performing the following steps:

1 Open a command terminal.

2 Type "locale" and press <Enter>. The following output is displayed.

```
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 Navigate to the **/etc/sysconfig/i18n** file.

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.

7 Relaunch the iDRAC6.

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

For advanced configurations of the iDRAC6, see "Advanced iDRAC6 Configuration."

4

Configuring the iDRAC6 Using the Web Interface

The iDRAC6 provides a Web interface that enables you to configure the iDRAC6 properties and users, perform remote management tasks, and troubleshoot a remote (managed) system for problems. For everyday systems management, use the iDRAC6 Web interface. This chapter provides information about how to perform common systems management tasks with the iDRAC6 Web interface and provides links to related information.

Most Web interface configuration tasks can also be performed with RACADM commands or with Server Management-Command Line Protocol (SM-CLP) commands.

Local RACADM commands are executed from the managed server.

SM-CLP and SSH/Telnet RACADM 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 iDRAC6 SM-CLP Command Line Interface." For more information about RACADM commands see "RACADM Subcommand Overview" and "iDRAC6 Property Database Group and Object Definitions".

Accessing the Web Interface

To access the iDRAC6 Web interface, perform the following steps:

1 Open a supported Web browser window.

   To access the Web interface using an IPv4 address, go to step 2.

   To access the Web interface using an IPv6 address, go to step 3.

2 Access the Web interface using an IPv4 address; you must have IPv4 enabled:

   In the browser **Address** bar, type:

   ```
   https://<iDRAC-IPv4-address>
   ```

   Then, press <Enter>.

3 Access the Web interface using an IPv6 address; you must have IPv6 enabled.

   In the browser **Address** bar, type:

   ```
   https://[<iDRAC-IPv6-address>]
   ```

   Then, press <Enter>.

4 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 iDRAC6 and `port-number` is the HTTPS port number.

5 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 iDRAC6 and `port-number` is the HTTPS port number.

The iDRAC6 **Login** window is displayed.

Logging In

You can log in as either an iDRAC6 user or as a Microsoft® Active Directory® user. The default user name and password for an iDRAC6 user are **root** and **calvin**, respectively.

You must have been granted **Login to iDRAC** privilege by the administrator to log in to iDRAC6.

To log in, perform the following steps:

1 In the **Username** field, type one of the following:

    • Your iDRAC6 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 *<username>*, *<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 iDRAC6 user password or Active Directory user password. Passwords are case sensitive.

3 From the **Domain** drop-down box, select *This iDRAC* for logging in as an iDRAC6 user, or select any of the available domains for logging in as a Active Directory user.

    NOTE: For Active Directory users, if you have specified the domain name as a part of the Username, select *This iDRAC* from the drop down menu.

4 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 iDRAC6 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 iDRAC6 NIC

This section assumes that the iDRAC6 has already been configured and is accessible on the network. See "Configuring Your iDRAC6" for help with the initial iDRAC6 network configuration.

Configuring the Network and IPMI LAN Settings

✍ **NOTE:** You must have Configure iDRAC permission 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 iDRAC6 supplies the client identifier option using a one-byte interface number (0) followed by a six-byte MAC address.

✍ **NOTE:** If you are running with Spanning Tree Protocol (STP) enabled, ensure that you also have PortFast or a similar technology turned on as follows:

- On the ports for the switch connected to iDRAC6

- On the ports connected to the management station running an iDRAC KVM session

> **NOTE:** You may see the following message if the system halts during POST: `Strike the F1 key to continue, F2 to run the system setup program` One possible reason for the error is a network storm event, which causes you to lose communication with the iDRAC6. After the network storm subsides, restart the system.

1 Click **Remote Access→Configuration→Network.**

2 On the **Network** page, you can enter Network Interface Card settings, Common iDRAC settings, IPv4 settings, IPv6 settings, IPMI settings, and VLAN settings. See Table 4-1, Table 4-2, Table 4-3, Table 4-4, Table 4-5, and Table 4-6 for descriptions of these settings.

3 When you have completed entering the required settings, click **Apply Changes**.

4 Click the appropriate button to continue. See Table 4-7.

Table 4-1.   Network Interface Card Settings

Setting	Description
NIC Selection	Configures the current mode out of the four possible modes: • Dedicated (iDRAC NIC) **NOTE:** This option is only available on iDRAC6 Enterprise. • Shared (LOM1) • Shared with Failover LOM2 • Shared with Failover All LOMs **NOTE:** This option may not be available on iDRAC6 Enterprise. **NOTE:** iDRAC6 will not communicate locally through the same physical port if **NIC Selection** is set to either **Shared** or **Shared with Failover** modes. This is because a network switch will not send out packets through the same port it received the packets.
MAC Address	Displays the Media Access Control (MAC) address that uniquely identifies each node in a network.
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 iDRAC6 via the network is blocked. The default is **On**.

Table 4-1.   Network Interface Card Settings *(continued)*

Setting	Description
Auto Negotiation	If set to **On**, displays the Network Speed and Mode by communicating with the nearest router or hub. If set to **Off**, allows you to set the Network Speed and Duplex Mode manually (Off).
	If **NIC Selection** is *not* set to **Dedicated**, Auto Negotiation setting will always be enabled (**On**).
Network Speed	Enables you to set the Network Speed to 100 Mb or 10 Mb to match your network environment. This option is not available if Auto Negotiation is set to **On**.
Duplex Mode	Enables you to set the Duplex Mode to full or half to match your network environment. This option is not available if **Auto Negotiation** is set to **On**.

Table 4-2.   Common iDRAC Settings

Setting	Description
Register iDRAC on DNS	Registers the iDRAC6 name on the DNS server.
	The default is **Disabled**.
DNS iDRAC Name	Displays the iDRAC6 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 checkbox 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.

Table 4-3.   IPv4 Settings

Setting	Description
Enabled	If NIC is enabled, this selects IPv4 protocol support and sets the other fields in this section to be enabled.
Use DHCP (For NIC IP Address)	Prompts the iDRAC6 to obtain an IP address for the NIC from the Dynamic Host Configuration Protocol (DHCP) server. The default is **off**.
IP Address	Specifies the iDRAC6 NIC IP address.
Subnet Mask	Allows you to enter or edit a static IP address for the iDRAC6 NIC. To change this setting, deselect the Use DHCP (For NIC IP Address) checkbox.
Gateway	The address of a router or switch. The value is in the "dot separated" format, such as 192.168.0.1.
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 **Preferred DNS Server** and **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 **Preferred DNS Server** and **Alternate DNS Server** fields.
Preferred DNS Server	DNS Server IP address.
Alternate DNS Server	Alternate IP address.

Table 4-4. IPv6 Settings

Setting	Description
Enabled	If the checkbox is selected, IPv6 is enabled. If the checkbox is not selected, IPv6 is disabled. The default is disabled.
Auto Config	Checking this box allows the iDRAC6 to obtain the IPv6 address for the iDRAC6 NIC from the Dynamic Host Configuration Protocol (DHCPv6) server. Enabling **Auto Config** also deactivates and flushes out the static values for IP Address 1, Prefix Length, and IP Gateway.
IP Address 1	Configures the IPv6 address for the iDRAC NIC. To change this setting, you must first disable **AutoConfig** by deselecting the associated checkbox.
Prefix Length	Configures the prefix length of the IPv6 address. It can be a value between 1 and 128 inclusive. To change this setting, you must first disable **AutoConfig** by deselecting the associated checkbox.
IP Gateway	Configures the static gateway for the iDRAC NIC. To change this setting, you must first disable **AutoConfig** by deselecting the associated checkbox.
Link Local Address	Specifies the iDRAC6 NIC IPv6 address.
IP Address 2	Specifies the additional iDRAC6 NIC IPv6 address if one is available.
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 **Preferred DNS Server** and **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 **Preferred DNS Server** and **Alternate DNS Server** fields.

Table 4-4. IPv6 Settings *(continued)*

Setting	Description
Preferred DNS Server	Configures the static IPv6 address for the preferred DNS server. To change this setting, you must first uncheck Use **DHCP to obtain DNS Server Addresses**.
Alternate DNS Server	Configures the static IPv6 address for the alternate DNS server. To change this setting, you must first uncheck Use **DHCP to obtain DNS Server Addresses**.

Table 4-5. IPMI 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 minimum 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 4-6. VLAN Settings

Setting	Description
Enable VLAN ID	If enabled, only matched Virtual LAN (VLAN) ID traffic will be accepted.
VLAN ID	VLAN ID field of 802.1g fields. Enter a valid value for VLAN ID (must be a number from 1 to 4094).
Priority	Priority field of 802.1g fields. Enter a number from 0 to 7 to set the priority of the VLAN ID.

Table 4-7.   Network Configuration Page Buttons

Button	Description
Print	Prints the **Network Configuration** values that appear on the screen.
Refresh	Reloads the **Network Configuration** page.
Advanced Settings	Opens the **Network Security** page, allowing the user to enter IP Range and IP Blocking attributes.
Apply Changes	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 iDRAC6 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 **Remote Access→Configuration** and then click the **Network** tab to open the **Network** page.

2   Click **Advanced Settings** to configure the network security settings.

Table 4-8 describes the **Network Security Page Settings**. When you have finished configuring the settings, click **Apply**.

3   Click the appropriate button to continue. See Table 4-9.

Table 4-8. 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 address bit pattern, depending on the 1's in the subnet mask. This value is bitwise AND'd with the IP Range Subnet Mask 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 establish an iDRAC6 session. Logins from IP addresses that are outside this range will fail. The default values in each property allow an address range from 192.168.1.0 to 192.168.1.255 to establish an iDRAC6 session.
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**.
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 4-9. Network Security Page Buttons

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

Configuring Platform Events

Platform event configuration provides a mechanism for configuring the iDRAC6 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 4-10.

Table 4-10. Platform Event Filters

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

Table 4-10. Platform Event Filters *(continued)*

Index	Platform Event
12	Processor Absent
13	Power Supply Warning Assert
14	Power Supply Critical Assert
15	Power Supply Absent
16	Event Log Critical Assert
17	Watchdog Critical Assert
18	System Power Warning Assert
19	System Power 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 remote system using a supported Web browser. See "Accessing the Web Interface."

2 Click **System→Alert Management→Platform Events**.

3 In the first table, select the **Enable Platform Event Filter Alerts** checkbox and then click **Apply Changes**.

NOTE: Enable Platform Event Filter Alerts must be enabled for an alert to be sent to any valid, configured destination (PET or e-mail).

4 In the next table, **Platform Event Filters List**, click the filter that you want to configure.

5 In the **Set Platform Events** page, select the appropriate **Shutdown Action** or select **None**.

6 Select or deselect **Generate Alert** to enable or disable this action.

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

7 Click **Apply Changes**.

You are returned to the **Platform Events** page where the changes you applied are displayed in the **Platform Event Filters List**.

8 Repeat steps 4 through 7 to configure additional platform event filters.

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."

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

3 Click **System→Alert Management→Traps Settings**.

4 In either the **IPv4 Destination List** or the **IPv6 Destination List**, click a destination number to configure your IPv4 or IPv6 SNMP alert destination.

5 On the **Set Platform Event Alert Destination** page, select or deselect **Enable Destination**. A checked box indicates that the IP address is enabled to receive the alerts. An unchecked box means that the IP address is disabled for receiving alerts.

6 Enter a valid Platform Event Trap destination IP address and click **Apply Changes**.

7 Click **Send Test Trap** to test the configured alert, or click **Go Back to the Platform Event Destination Page**.

> *NOTE:* Your user account must have **Test Alerts** permission to send a test trap. See Table 6-6, "iDRAC Group Permissions," for more information.

On the **Platform Event Alert Destinations** page, the changes you applied are displayed in either the IPv4 or IPv6 **Destination List**.

8 In the **Community String** field, enter the appropriate iDRAC SNMP community name. Click **Apply Changes**.

   ✏️ **NOTE:** The destination community string must be the same as the iDRAC6 community string.

9 Repeat steps 4 through 7 to configure additional IPv4 or IPv6 destination numbers.

Configuring E-Mail Alerts

✏️ **NOTE:** E-Mail alerts support both IPv4 and IPv6 addresses.

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)."

3 Click **System→Alert Management→Email Alert Settings**.

4 In the table under **Destination Email Addresses**, click the **Email Alert Number** for which you want to configure a destination address.

5 On the **Set Email Alert** page, select or deselect **Enable E-mail Alert**. A checked box indicates that the email address is enabled to receive the alerts. An unchecked box means that the email address is disabled for receiving alert messages.

6 In the **Destination E-mail Address** field, type a valid e-mail address.

7 In the **E-mail Description** field, type a short description to be displayed in the e-mail.

8 Click **Apply Changes**.

9 If you want to test the configured e-mail alert, click **Send Test Email**. If not, click **Go Back to the E-mail Alert Destination Page**.

10 Click **Go Back to the E-mail Alert Destination Page** and enter a valid SMTP IP address in the **SMTP (e-mail) Server IP Address** field.

   ✏️ **NOTE:** To successfully send a test e-mail, the **SMTP (email) Server IP Address** must be configured on the **E-mail Alert Settings** page. The SMTP Server uses the set IP address to communicate with the iDRAC6 to send e-mail alerts when a platform event occurs.

11 Click **Apply Changes**.

12 Repeat steps 4 through 9 to configure additional e-mail alert destinations.

Configuring IPMI

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

2 Configure IPMI over LAN.

    a In the **System** tree, click **Remote Access**.

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

    c In the **Network Configuration** page under **IPMI LAN Settings**, select **Enable IPMI Over LAN** and click **Apply Changes**.

    d 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 Changes**.

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

    ✎ **NOTE:** iDRAC6 IPMI supports the RMCP+ protocol.

    Under **IPMI LAN Settings** in the **Encryption Key field**, type the encryption key and click **Apply Changes**.

    ✎ **NOTE:** The encryption key must consist of an even number of hexadecimal characters with a maximum of 40 characters.

3 Configure IPMI Serial over LAN (SOL).

    a In the **System** tree, click **Remote Access**.

    b In the **Configuration** tab, click **Serial Over LAN**.

    c In the **Serial Over LAN Configuration** page, select **Enable Serial Over LAN**.

    d Update the IPMI SOL baud rate.

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

    e Click the **Baud Rate** drop-down menu, select the appropriate baud rate, and click **Apply Changes**.

f Update the **Minimum Required Privilege**. This property defines the minimum user privilege that is required to use the **Serial Over LAN** feature.

Click the **Channel Privilege Level Limit** drop-down menu, select **User**, **Operator**, or **Administrator**.

g Click **Apply Changes**.

4 Configure IPMI Serial.

a In the **Configuration** tab, click **Serial**.

b In the **Serial Configuration** menu, change the IPMI serial connection mode to the appropriate setting.

Under **IPMI Serial**, click the **Connection Mode Setting** drop-down menu, select the appropriate mode.

c Set the IPMI Serial baud rate.

Click the **Baud Rate** drop-down menu, select the appropriate baud rate, and click **Apply Changes**.

d Set the Channel Privilege Level Limit.

Click the **Channel Privilege Level Limit** drop-down menu, select **Administrator**, **Operator**, or **User**.

e Click **Apply Changes**.

f Ensure that the serial MUX is set correctly in the managed system's BIOS Setup program.

- Restart your system.
- During POST, press <F2> to enter the BIOS Setup program.
- Navigate to **Serial Communication**.
- In the **Serial Connection** menu, ensure that **External Serial Connector** is set to **Remote Access Device**.
- Save and exit the BIOS Setup program.
- Restart your system.

If IPMI serial is in terminal mode, you can configure the following additional settings:

- Delete control
- Echo control
- Line edit
- New line sequences
- Input new line sequences

For more information about these properties, see the IPMI 2.0 specification. For additional information about terminal mode commands, see the *Dell OpenManage Baseboard Management Controller Utilities User's Guide* at **support.dell.com\manuals**.

Configuring iDRAC6 Users

See "Adding and Configuring iDRAC6 Users" for detailed information.

Securing iDRAC6 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 SSL through the Web-based Interface
- Generating a CSR
- Uploading a server certificate
- Viewing a server certificate

Secure Sockets Layer (SSL)

The iDRAC6 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 iDRAC6 employs the 128-bit SSL encryption standard, the most secure form of encryption generally available for Internet browsers in North America.

The iDRAC6 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 iDRAC6 Web interface to generate a Certificate Signing Request (CSR) with your company's information. You can then submit the generated CSR to a Certificate Authority (CA) such as VeriSign or Thawte.

Certificate Signing Request (CSR)

A CSR is a digital request to a 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 iDRAC6 firmware. The CSR information stored on the iDRAC6 firmware must match the information contained in the certificate.

Accessing SSL Through the Web-Based Interface

1 Click **Remote Access→Configuration**.

2 Click **SSL** to open the **SSL** page.

Use the **SSL** page to perform one of the following options:

- Generate a Certificate Signing Request (CSR) to send to a CA. The CSR information is stored on the iDRAC6 firmware.

- Upload a server certificate.

- View a server certificate.

Table 4-11 describes the above **SSL** page options.

Table 4-11. SSL Page Options

Field	Description
Generate Certificate Signing Request (CSR)	This option enables you to generate a CSR to send to a CA to request a secure Web certificate.
	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	This option enables you to upload an existing certificate that your company has title to and uses to control access to the iDRAC6.
	NOTE: Only X509, Base 64 encoded certificates are accepted by theiDRAC6. DER-encoded certificates are not accepted. Upload a new certificate to replace the default certificate you received with your iDRAC6.
View Server Certificate	This option allows you to view an existing server certificate.

Generating a Certificate Signing Request

NOTE: Each new CSR overwrites any previous CSR data stored on the firmware. Before iDRAC can accept your signed CSR, the CSR in the firmware should match the certificate returned from the CA.

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

2 On the **Generate Certificate Signing Request (CSR)** page, enter a value for each CSR attribute. Table 4-12 describes the CSR attributes.

3 Click **Generate** to create the CSR and download it onto to your local computer.

4 Click the appropriate button to continue. See Table 4-13.

Table 4-12. Generate Certificate Signing Request (CSR) Attributes

Field	Description
Common Name	The exact name being certified (usually the iDRAC's domain name, for example, **www.xyzcompany.com**). Alphanumeric characters, hyphens, underscores, spaces, and periods are 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 4-13.   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.
Go Back to SSL Main Menu	Returns the user to the **SSL** page.

Uploading a Server Certificate

1 On the **SSL** page, select **Upload Server Certificate** and click **Next**.

   The **Upload Server Certificate** page is displayed.

2 In the **File Path** field, type the path of the certificate in the **Value** 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

3 Click **Apply**.

4 Click the appropriate page button to continue. See Table 4-14.

Table 4-14.   Certificate Upload Page Buttons

Button	Description
Print	Print the **Certificate Upload** page.
Go Back to SSL Main Menu	Return to the **SSL Main Menu** page.
Apply	Apply the certificate to the iDRAC6 firmware.

Viewing a Server Certificate

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

   The **View Server Certificate** page displays the server certificate that you uploaded to the iDRAC.

   Table 4-15 describes the fields and associated descriptions listed in the **Certificate** table.

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

Table 4-15. 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 4-16. 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	Returns to the **SSL** page.

Configuring and Managing Active Directory Certificates

The page enables you to configure and manage Active Directory settings.

✍ **NOTE:** You must have **Configure iDRAC** permission to use or configure Active Directory.

✍ **NOTE:** Before configuring or using the Active Directory feature, ensure that your Active Directory server is configured to communicate with iDRAC6.

✍ **NOTE:** For detailed information about Active Directory configuration and how to configure Active Directory with Extended Schema or Standard Schema, see "Using the iDRAC6 With Microsoft Active Directory."

To access the **Active Directory Configuration and Management** page:

1 Click **Remote Access→Configuration**.

2 Click **Active Directory** to open the **Active Directory Configuration and Management** page.

   Table 4-17 lists the **Active Directory Configuration and Management** page options.

3 Click the appropriate button to continue. See Table 4-18.

Table 4-17. Active Directory Configuration and Management Page Options

Attribute	Description
Common Settings	
Active Directory Enabled	Specifies whether Active Directory is enabled or disabled.
Single Sign-On Enabled	Specifies whether single sign–on is enabled or disabled. If enabled, you can log into iDRAC6 without entering your domain user authentication credentials, such as user name and password. Values are **Yes** and **No**.
Schema Selection	Specifies whether Standard Schema or Extended Schema is in use with Active Directory.
	NOTE: In this release, the Smart Card based Two Factor Authentication (TFA) and the single sign-on (SSO) features are not supported if the Active directory is configured for Extended schema.

Table 4-17. Active Directory Configuration and Management Page Options *(continued)*

Attribute	Description
User Domain Name	This value holds up to 40 User Domain entries. If configured, the list of user domain names will appear in the login page as a pull-down menu for the login user to choose from. If not configured, Active Directory users are still able to log in by entering the user name in the format of user_name@domain_name, domain_name/user_name, or domain_name\user_name.
Timeout	Specifies the time in seconds to wait for Active Directory queries to complete. The default is 120 seconds.
Domain Controller Server Address 1-3 (FQDN or IP)	Specifies the fully qualified domain name (FQDN) of the Domain Controller or the IP address. At least one of the 3 addresses is required to be configured. iDRAC attempts to connect to each of the configured addresses one-by-one until a successful connection is made. If extended schema is selected, these are the addresses of the domain controllers where the iDRAC device object and the Association objects are located. If standard schema is selected, these are the addresses of the domain controllers where the user accounts and the role groups are located.
Certificate Validation Enabled	iDRAC uses Lightweight Directory Access Protocol (LDAP) over Security Socket Layer (SSL) while connecting Active Directory. By default, iDRAC uses the CA certificate loaded in iDRAC to validate the Security Socket Layer (SSL) server certificate of the domain controllers during Security Socket Layer (SSL) handshake and provides strong security. The certificate validation can be disabled for testing purpose or the system Administrator chooses to trust the domain controllers in the security boundary without validating their Security Socket Layer (SSL) certificates. This option specifies whether Certificate validation is enabled or disabled.

Table 4-17.   Active Directory Configuration and Management Page Options *(continued)*

Attribute	Description
Active Directory CA Certificate	
Certificate	The certificate of the Certificate Authority that signs all the domain controllers' Security Socket Layer (SSL) server certificate.
Extended Schema Settings	**iDRAC Name**: Specifies the name that uniquely identifies the iDRAC in Active Directory. This value is NULL by default.
	iDRAC Domain Name: The DNS name (string) of the domain where the Active Directory iDRAC object resides. This value is NULL by default.
	These settings will be displayed only if the iDRAC has been configured for use with an Extended Active Directory Schema.
Standard Schema Settings	**Global Catalog Server Address 1-3 (FQDN or IP)**: Specifies the fully qualified domain name (FQDN) or the IP address of the Global Catalog server(s). At least one of the 3 addresses is required to be configured. iDRAC attempts to connect to each of the configured addresses one-by-one until a successful connection is made. The Global Catalog server is required for standard schema only in the case that the user accounts and the role groups are in different domains.
	Role Groups: Specifies the list of role groups associated with iDRAC6.
	Group Name: Specifies the name that identifies the role group in the Active Directory associated with iDRAC6.
	Group Domain: Specifies the group domain.
	Group Privilege: Specifies the group privilege level.
	These settings will be displayed only if the iDRAC has been configured for use with a Standard Active Directory Schema.

Table 4-18. Active Directory Configuration and Management Page Buttons

Button	Definition
Print	Prints the values that are displayed on the **Active Directory Configuration and Management** page.
Refresh	Reloads the **Active Directory Configuration and Management** page.
Configure Active Directory	Enables you to configure Active Directory. See "Using the iDRAC6 With Microsoft Active Directory" for detailed configuration information.
Test Settings	Allows you to test the Active Directory configuration using the settings you specified. See "Using the iDRAC6 With Microsoft Active Directory" for details on using the **Test Settings** option.

Configuring iDRAC6 Services

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

1   Click **Remote Access→Configuration**. Then, click the **Services** tab to display the **Services** configuration page.

2   Configure the following services, as required:

- Local Configuration — see Table 4-19

- Web server — see Table 4-20 for Web server settings

- SSH — see Table 4-21 for SSH settings

- Telnet — see Table 4-22 for Telnet settings.

- Remote RACADM — see Table 4-23 for Remote RACADM settings.

- SNMP Agent — see Table 4-24 for SNMP settings.

- Automated System Recovery (ASR) Agent — see Table 4-25 for ASR Agent settings.

3   Click **Apply**.

4   Click the appropriate button to continue. See Table 4-26.

Table 4-19. Local Configuration

Setting	Description
Disable the iDRAC Local Configuration using option ROM	Disables local configuration of iDRAC using option ROM. Option ROM resides in the BIOS and provides a user interface engine that allows BMC and iDRAC configuration. The option ROM prompts you to enter the setup module by pressing <Ctrl+E>.
Disable the iDRAC Local Configuration using RACADM	Disables local configuration of iDRAC using local RACADM.

Table 4-20. Web Server Settings

Setting	Description
Enabled	Enables or disables the iDRAC6 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. The maximum number of simultaneous sessions is five.
Active Sessions	The number of current sessions on the system, less than or equal to the value for **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 terminate the current Web interface session. The web server will also be reset. Please wait for a few minutes before opening a new Web interface session. The timeout range is 60 to 10800 seconds. The default is 1800 seconds.
HTTP Port Number	The port on which the iDRAC6 listens for a browser connection. The default is **80**.
HTTPS Port Number	The port on which the iDRAC6 listens for a secure browser connection. The default is **443**.

Table 4-21. SSH Settings

Setting	Description
Enabled	Enables or disable SSH. When checked, the checkbox indicates that SSH is enabled.
Timeout	The secure shell idle timeout, in seconds. The 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 iDRAC6 listens for an SSH connection. The default is **22**.

Table 4-22. Telnet Settings

Setting	Description
Enabled	Enables or disables telnet. When checked, telnet is enabled.
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 **300**.
Port Number	The port on which the iDRAC6 listens for a telnet connection. The default is **23**.

Table 4-23. Remote RACADM Settings

Setting	Description
Enabled	Enables/disables Remote RACADM. When checked, Remote RACADM is enabled.
Active Sessions	The number of current sessions on the system.

Table 4-24. SNMP Settings

Setting	Description
Enabled	Enables/disables SNMP. When checked, SNMP is enabled.
SNMP Community Name	Enables/disables the SNMP Community Name. When checked, the SNMP Community Name is enabled. The name of the community that contains the IP address for the SNMP Alert destination. The Community Name may be up to 31 nonblank characters in length. The default is **public**.

Table 4-25.   Automated System Recovery Agent Setting

Setting	Description
Enabled	Enables/disables the Automated System Recovery Agent. When checked, the Automated System Recovery Agent is enabled.

Table 4-26.   Services Page Buttons

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

Updating the iDRAC6 Firmware/System Services Recovery Image

> **NOTE:** If the iDRAC6 firmware becomes corrupted, as could occur if the iDRAC6 firmware update progress is interrupted before it completes, you can recover the iDRAC6 using the iDRAC6 Web interface.

> **NOTE:** The firmware update, by default, retains the current iDRAC6 settings. During the update process, you have the option to reset the iDRAC6 configuration to the factory defaults. If you set the configuration to the factory defaults, you must configure the network using the iDRAC6 Configuration Utility.

1   Open the iDRAC6 Web-based interface and log in to the remote system.

2   Click **Remote Access**, and then click the **Update** tab.

3 In the **Upload/Rollback (Step 1 of 3)** page, click **Browse**, or type the path to the firmware image that you downloaded from **support.dell.com** or the System Services recovery image.

> **NOTE:** If you are running Firefox, the text cursor does not appear in the **Firmware Image** field.

For example:

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

OR

`\\192.168.1.10\Updates\V1.0\<image_name>`

The default firmware image name is **firmimg.d6**.

4 Click **Upload**.

The file will be uploaded to the iDRAC6. This process may take several minutes to complete.

The following message will be displayed until the process is complete:

`File upload in progress...`

5 On the **Status (page 2 of 3)** page, 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, the image file name will be displayed. If a firmware image was uploaded, the current and the new firmware versions will be displayed.

  OR

- If the image did not upload successfully, or it did not pass the verification checks, an appropriate error message is displayed, and the update will return to the **Upload/Rollback (Step 1 of 3)** page. You can attempt to update the iDRAC6 again or click **Cancel** to reset the iDRAC6 to normal operating mode.

6 In the case of a firmware image, **Preserve Configuration** provides you with the option to preserve or clear the existing iDRAC6 configuration. This option is selected by default.

> ✐ **NOTE:** If you deselect the **Preserve Configuration** checkbox, the iDRAC6 will be reset to its default settings. In the default settings, the LAN is enabled. You may not be able to log in to the iDRAC6 Web interface. You will have to reconfigure the LAN settings using the iDRAC6 Configuration Utility during BIOS POST.

7 Click **Update** to start the update process.

8 In the **Updating (Step 3 of 3)** page, you will see the status of the update. The progress of the update, measured in percentages, will appear in the **Progress** column.

> ✐ **NOTE:** While in the update mode, the update process will continue in the background even if you navigate away from this page.

If the firmware update is successful, the iDRAC6 will reset automatically. You should close the current browser window and reconnect to the iDRAC6 using a new browser window. An appropriate error message is displayed if an error occurs.

If the System Services Recovery update succeeds/fails, an appropriate status message is displayed.

iDRAC6 Firmware Rollback

iDRAC6 has the provision to maintain two simultaneous firmware images. You can choose to boot from (or rollback to) the firmware image of your choice.

1 Open the iDRAC6 Web-based interface and log in to the remote system.

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

2 In the **Upload/Rollback (Step 1 of 3)** page, click **Rollback**. The current and the rollback firmware versions are displayed on the **Status (Step 2 of 3)** page.

Preserve Configuration provides you with the option to preserve or clear the existing iDRAC6 configuration. This option is selected by default.

NOTE: If you deselect the **Preserve Configuration** checkbox, the iDRAC6 will be reset to its default settings. In the default settings, the LAN is enabled. You may not be able to log in to the iDRAC6 Web interface. You will have to reconfigure the LAN settings using the iDRAC6 Configuration Utility during BIOS POST or the racadm command (available locally on the server).

3 Click **Update** to start the firmware update process.

On the **Updating** (Step 3 of 3) page, you see the status of the rollback operation. The progress, measured in percentages, appear in the **Progress** column.

NOTE: While in the update mode, the update process will continue in the background even if you navigate away from this page.

If the firmware update is successful, the iDRAC6 will reset automatically. You should close the current browser window and reconnect to the iDRAC6 using a new browser window. An appropriate error message is displayed if an error occurs.

5

Advanced iDRAC6 Configuration

This section provides information about advanced iDRAC6 configuration and is recommended for users with advanced knowledge of systems management and who want to customize the iDRAC6 environment to suit their specific needs.

Before You Begin

You should have completed the basic installation and setup of your iDRAC6 hardware and software. See "Basic Installation of the iDRAC6" for more information.

Configuring iDRAC6 for Viewing Serial Output Remotely Over SSH/Telnet

You can configure the iDRAC6 for remote serial console redirection by performing the following steps:

First, configure the BIOS to enable serial console redirection:

  1 Turn on or restart your system.

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

      <F2> = System Setup

  3 Scroll down and select **Serial Communication** by pressing <Enter>.

4 Set the **Serial Communication** screen options as follows:

```
serial communication....On with serial redirection
via com2
```

Ø **NOTE:** You can set serial communication to **On with serial redirection via com1** as long as the serial port address field, serial device2, is set to com1, also.

```
serial port address....Serial device1 = com1,
serial device2 = com2

external serial connector....Serial device 1

failsafe baud rate....115200

remote terminal type....vt100/vt220

redirection after boot....Enabled
```

Then, select **Save Changes**.

5 Press <Esc> to exit the **System Setup** program and complete the System Setup program configuration.

Configuring the iDRAC6 Settings to Enable SSH/Telnet

Next, configure the iDRAC6 settings to enable ssh/telnet, which you can do either through RACADM or the iDRAC6 Web interface.

To configure iDRAC6 settings to enable ssh/telnet using RACADM, run the following commands:

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

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

You can also run RACADM commands remotely; see "Using RACADM Remotely."

To configure iDRAC6 settings to enable ssh/telnet using the iDRAC6 Web interface, follow these steps:

1 Expand the **System** tree and click **Remote Access**.

2 Click the **Configuration** tab and then click **Services**.

3 Select **Enabled** under the **SSH** or **Telnet** sections.

4 Click **Apply Changes**.

The next step is to connect to iDRAC6 through Telnet or SSH.

Starting a Text Console Through Telnet or SSH

After you have logged into the iDRAC6 through your management station terminal software with telnet or SSH, you can redirect the managed system text console by using **console com2**, which is a telnet/SSH command. Only one **console com2** client is supported at a time.

To connect to the managed system text console, open an iDRAC6 command prompt (displayed through a telnet or SSH session) and type:

```
console com2
```

The `console -h com2` command displays the contents of the serial history buffer before waiting for input from the keyboard or new characters from the serial port.

The default (and maximum) size of the history buffer is 8192 characters. You can set this number to a smaller value using the command:

```
racadm config –g cfgSerial -o cfgSerialHistorySize
<number>
```

To configure Linux for console direction during boot, see "Configuring Linux for Serial Console Redirection During Boot."

Using a Telnet Console

Running Telnet Using Microsoft® Windows® XP or Windows 2003

If your management station is running Windows XP or Windows 2003, you may experience an issue with the characters in an iDRAC6 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.

Running Telnet Using Windows 2000

If your management station is running Windows 2000, you cannot access BIOS setup by pressing the <F2> key. To fix this issue, use the telnet client supplied with the Windows Services for UNIX® 3.5—a recommended free download from Microsoft. Go to **www.microsoft.com/downloads/** and search for "*Windows Services for UNIX 3.5*."

Enabling Microsoft Telnet for Telnet Console Redirection

📝 **NOTE:** Some telnet clients on Microsoft operating systems may not display the BIOS setup screen correctly when BIOS console redirection is set for VT100/VT220 emulation. If this issue occurs, update the display by changing BIOS console redirection to ANSI mode. To perform this procedure in the BIOS setup menu, select **Console Redirection** →**Remote Terminal Type** →**ANSI**.

📝 **NOTE:** When you configure the client VT100 emulation window, set the window or application that is displaying the redirected console to 25 rows x 80 columns to ensure proper text display; otherwise, some text screens may be garbled.

1 Enable **Telnet** in **Windows Component Services**.

2 Connect to the iDRAC6 in the management station.

Open a command prompt, type the following, and press <Enter>:

`telnet <IP address>:<port number>`

where `IP address` is the IP address for the iDRAC6 and `port number` is the telnet port number (if you are using a new port).

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:

1 Open a command prompt window (if required).

2 If you are not already 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 is displayed:

`Backspace will be sent as delete.`

To configure a Linux telnet session to use the <Backspace> key:

1 Open a command prompt and type:

```
stty erase ^h
```

2 At the prompt, type:

```
telnet
```

Using the Secure Shell (SSH)

It is critical that your system's devices and device management are secure. Embedded connected devices are the core of many business processes. If these devices are compromised, your business may be at risk, which requires new security demands for command line interface (CLI) device management software.

Secure Shell (SSH) is a command line session that includes the same capabilities as a telnet session, but with improved security. The iDRAC6 supports SSH version 2 with password authentication. SSH is enabled on the iDRAC6 when you install or update your iDRAC6 firmware.

You can use either `PuTTY` or `OpenSSH` on the management station to connect to the managed system's iDRAC6. When an error occurs during the login procedure, the secure shell client issues an error message. The message text is dependent on the client and is not controlled by the iDRAC6.

 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 four SSH sessions are supported at any given time. The session timeout is controlled by the `cfgSsnMgtSshIdleTimeout` property as described in the "iDRAC6 Property Database Group and Object Definitions."

To enable the SSH on the iDRAC6, type:

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

To change the SSH port, type:

```
racadm config -g cfgRacTuning -o cfgRacTuneSshPort
<port number>
```

For more information on `cfgSerialSshEnable` and `cfgRacTuneSshPort` properties, see "iDRAC6 Property Database Group and Object Definitions."

The iDRAC6 SSH implementation supports multiple cryptography schemes, as shown in Table 5-1.

Table 5-1.   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

NOTE: SSHv1 is not supported.

Configuring Linux for Serial Console Redirection During Boot

The following steps are specific to the Linux GRand Unified Bootloader (GRUB). Similar changes would be necessary if you use a different boot loader.

NOTE: When you configure the client VT100 emulation window, set the window or application that is displaying the redirected console to 25 rows x 80 columns to ensure proper text display; otherwise, some text screens may be garbled.

Edit the **/etc/grub.conf** file as follows:

1 Locate the General Setting sections in the file and add the following two new lines:

```
serial --unit=1 --speed=57600
terminal --timeout=10 serial
```

2 Append two options to the kernel line:

```
kernel ............. console=ttyS1,115200n8r
console=tty1
```

3 If the /etc/grub.conf contains a splashimage directive, comment it out.

Table 5-2 provides a sample /etc/grub.conf file that shows the changes described in this procedure.

Table 5-2. Sample File: /etc/grub.conf

```
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after
making changes
# to this file
# NOTICE:  You do not have a /boot partition.  This
means that
#          all kernel and initrd paths are relative
to /, e.g.
#          root (hd0,0)
#          kernel /boot/vmlinuz-version ro root=
/dev/sdal
#          initrd /boot/initrd-version.img
#
#boot=/dev/sda
default=0
timeout=10
#splashimage=(hd0,2)/grub/splash.xpm.gz
```

Table 5-2. Sample File: /etc/grub.conf *(continued)*

```
serial --unit=1 --speed=57600
terminal --timeout=10 serial

title Red Hat Linux Advanced Server (2.4.9-e.3smp)
   root (hd0,0)
   kernel /boot/vmlinuz-2.4.9-e.3smp ro root=
/dev/sda1 hda=ide-scsi console=ttyS0 console=
ttyS1,115200n8r
   initrd /boot/initrd-2.4.9-e.3smp.img
title Red Hat Linux Advanced Server-up (2.4.9-e.3)
   root (hd0,00)
   kernel /boot/vmlinuz-2.4.9-e.3 ro root=/dev/sda1 s
   initrd /boot/initrd-2.4.9-e.3.im
```

When you edit the **/etc/grub.conf** file, use the following guidelines:

1 Disable GRUB's graphical interface and use the text-based interface; otherwise, the GRUB screen will not be displayed in RAC console redirection. To disable the graphical interface, comment out the line starting with `splashimage`.

2 To enable multiple GRUB options to start console sessions through the RAC serial connection, add the following line to all options:

   `console=ttyS1,115200n8r console=tty1`

   Table 5-2 shows `console=ttyS1,57600` added to only the first option.

Enabling Login to the Console After Boot

Edit the file **/etc/inittab** as follows:

   Add a new line to configure `agetty` on the COM2 serial port:

   `co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi`

Table 5-3 shows a sample file with the new line.

Table 5-3. Sample File: /etc/innitab

```
#
# inittab  This file describes how the INIT process
should set up
#         the system in a certain run-level.
#
# Author:  Miquel van Smoorenburg
#          Modified for RHS Linux by Marc Ewing and
Donnie Barnes
#
# Default runlevel. The runlevels used by RHS are:
#   0 - halt (Do NOT set initdefault to this)
#   1 - Single user mode
#   2 - Multiuser, without NFS (The same as 3, if you
do not have
#      networking)
#   3 - Full multiuser mode
#   4 - unused
#   5 - X11
#   6 - reboot (Do NOT set initdefault to this)
#
id:3:initdefault:

# System initialization.
si::sysinit:/etc/rc.d/rc.sysinit

l0:0:wait:/etc/rc.d/rc 0
l1:1:wait:/etc/rc.d/rc 1
l2:2:wait:/etc/rc.d/rc 2
l3:3:wait:/etc/rc.d/rc 3
l4:4:wait:/etc/rc.d/rc 4
l5:5:wait:/etc/rc.d/rc 5
l6:6:wait:/etc/rc.d/rc 6
```

Table 5-3. Sample File: /etc/innitab *(continued)*

```
# Things to run in every runlevel.
ud::once:/sbin/update

# Trap CTRL-ALT-DELETE
ca::ctrlaltdel:/sbin/shutdown -t3 -r now

# When our UPS tells us power has failed, assume we
have a few
# minutes of power left. Schedule a shutdown for 2
minutes from now.
# This does, of course, assume you have power
installed and your
# UPS is connected and working correctly.
pf::powerfail:/sbin/shutdown -f -h +2 "Power Failure;
System Shutting Down"
# If power was restored before the shutdown kicked
in, cancel it.
pr:12345:powerokwait:/sbin/shutdown -c "Power
Restored; Shutdown Cancelled"


# Run gettys in standard runlevels
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
1:2345:respawn:/sbin/mingetty tty1
2:2345:respawn:/sbin/mingetty tty2
3:2345:respawn:/sbin/mingetty tty3
4:2345:respawn:/sbin/mingetty tty4
5:2345:respawn:/sbin/mingetty tty5
6:2345:respawn:/sbin/mingetty tty6

# Run xdm in runlevel 5
# xdm is now a separate service
x:5:respawn:/etc/X11/prefdm -nodaemon
```

Edit the file **/etc/securetty** as follows:

Add a new line with the name of the serial tty for COM2:

```
ttyS1
```

Table 5-4 shows a sample file with the new line.

Table 5-4.   Sample File: /etc/securetty

```
vc/1
vc/2
vc/3
vc/4
vc/5
vc/6
vc/7
vc/8
vc/9
vc/10
vc/11
tty1
tty2
tty3
tty4
tty5
tty6
tty7
tty8
tty9
tty10
tty11
ttyS1
```

Configuring iDRAC6 for Serial Connection

You can use any of the following interfaces for connecting to the iDRAC6 via serial connection:

- iDRAC6 CLI
- Direct Connect Basic mode
- Direct Connect Terminal mode

To set up your system to use any of these interfaces, perform the following steps.

Configure the **BIOS** to enable serial connection:

1 Turn on or restart your system.

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

   <F2> = System Setup

3 Scroll down and select **Serial Communication** by pressing <Enter>.

4 Set the **Serial Communication** screen as follows:

   external serial connector....remote access device

   Then, select **Save Changes**.

5 Press <Esc> to exit the **System Setup** program and complete the System Setup program configuration.

Next, connect your DB-9 or Null Modem cable from the management station to the managed node server. See "Connecting the DB-9 or Null Modem Cable for the Serial Console."

Next, be sure your management terminal emulation software is configured for serial connection. See "Configuring the Management Station Terminal Emulation Software."

Finally, configure the iDRAC6 settings to enable serial connections, which you can do either through RACADM or the iDRAC6 Web interface.

To configure iDRAC6 settings to enable serial connections using RACADM, run the following command:

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

To configure iDRAC6 settings to enable serial connections using the iDRAC6 Web interface, follow these steps:

1 Expand the **System** tree and click **Remote Access**.

2 Click the **Configuration** tab and then click **Serial**.

3 Select **Enabled** under the **RAC Serial** section.

4 Click **Apply Changes**.

When you are connected serially with the previous settings, you should see a login prompt. Enter the iDRAC6 username and password (default values are root, calvin, respectively).

From this interface, you can execute such features as RACADM. For example, to print out the System Event Log, enter the following RACADM command:

```
racadm getsel
```

Configuring iDRAC for Direct Connect Basic Mode and Direct Connect Terminal Mode

Using RACADM, run the following command to disable the iDRAC6 command line interface:

```
racadm config –g cfgSerial –o cfgSerialConsoleEnable 0
```

Then, run the following RACADM command to enable Direct Connect Basic:

```
racadm config –g cfgIpmiSerial –o
cfgIpmiSerialConnectionMode 1
```

Or, run the following RACADM command to enable Direct Connect Terminal:

```
racadm config –g cfgIpmiSerial –o
cfgIpmiSerialConnectionMode 0
```

You can perform the same actions using the iDRAC6 Web interface:

1 Expand the **System** tree and click **Remote Access**.

2 Click the **Configuration** tab and then click **Serial**.

3 Deselect **Enabled** under the **RAC Serial** section.

  For Direct Connect Basic:

  Under the **IPMI Serial** section change the **Connection Mode Settings** dropdown menu to **Direct Connect Basic Mode**.

  For Direct Connect Terminal mode:

  Under the **IPMI Serial** section change the **Connection Mode Settings** dropdown menu to **Direct Connect Terminal Mode**.

4 Click **Apply Changes**. For more information about Direct Connect Basic and Direct Connect Terminal modes see "Configuring Serial and Terminal Modes."

Direct Connect Basic mode will enable you to use such tools as ipmish directly through the serial connection. For example, to print the System Event Log using ipmish via IPMI Basic mode, run the following command:

```
ipmish –com 1 –baud 57600  –flow cts –u root –p calvin
sel get
```

Direct Connect Terminal mode will enable you to issue ASCII commands to the iDRAC6. For example, to power on/off the server via Direct Connect Terminal mode:

1 Connect to iDRAC6 via terminal emulation software

2 Type the following command to login:

```
[SYS PWD -U root calvin]
```

You will see the following in response:

```
[SYS]
```

```
[OK]
```

3 Type the following command to verify a successful login:

```
[SYS TMODE]
```

You will see the following in response:

```
[OK TMODE]
```

4 To power off the server (server will immediately power off), type the following command:

```
[SYS POWER OFF]
```

5 To power on the server (server will immediately power on):

```
[SYS POWER ON]
```

Switching Between RAC Serial Interface Communication Mode and Serial Console Redirection

iDRAC6 supports Escape key sequences that allow switching between RAC Serial Interface communication and Serial console redirection.

To set your system to allow this behavior, do the following:

1 Turn on or restart your system.

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

    <F2> = System Setup

3 Scroll down and select **Serial Communication** by pressing <Enter>.

4 Set the **Serial Communication** screen as follows:

   serial communication -- On with serial redirection via com2

   📝 **NOTE:** You can set the **serial communication** field to **On with serial redirection via com1** as long as **serial device2** in the **serial port address** field is also set to **com1**.

   serial port address -- Serial device1 = com1, serial device2 = com2

   external serial connector -- Serial device 2

   failsafe baud rate....115200

   remote terminal type ...vt100/vt220

   redirection after boot ... Enabled

   Then, select **Save Changes**.

5 Press <Esc> to exit the **System Setup** program and complete the System Setup program configuration.

Connect the null modem cable between the managed system's external serial connector and the management station's serial port.

Use a terminal emulation program (hyperterminal or teraterm) on the management station and based on where the managed server is in its boot process, you will see either the POST screens or the operating system screens. This is based on the configuration: SAC for windows and Linux text mode screens for Linux. Set the management station's terminal settings as Baud Rate–115200, data–8 bit, parity–none, stop–1 bit, and Flow Control–None.

To switch to RAC Serial Interface Communication Mode when in Serial Console Redirection Mode, use the following key sequence:

```
<Esc> +<Shift> <9>
```

The key sequence above directs you either to the "iDRAC Login" prompt (if the RAC is set to "RAC Serial" mode) or to the "Serial Connection" mode where terminal commands can be issued (if the RAC is set to "IPMI Serial Direct Connect Terminal Mode").

To switch to Serial Console Redirection Mode when in RAC Serial Interface Communication Mode, use the following key sequence:

```
<Esc> +<Shift> <q>
```

Connecting the DB-9 or Null Modem Cable for the Serial Console

To access the managed system using a serial text console, connect a DB-9 null modem cable to the COM port on the managed system. In order for the connection to work with the NULL modem cable, the corresponding serial communications settings should be made in the CMOS setup. Not all DB-9 cables carry the pinout/signals necessary for this connection. The DB-9 cable for this connection must conform to the specification shown in Table 5-5.

NOTE: The DB-9 cable can also be used for BIOS text console redirection.

Table 5-5. Required Pinout for DB-9 Null Modem Cable

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

Configuring the Management Station Terminal Emulation Software

iDRAC6 supports a serial or telnet text console from a management station running one of the following types of terminal emulation software:

- Linux Minicom in an Xterm
- Hilgraeve's HyperTerminal Private Edition (version 6.3)
- Linux Telnet in an Xterm
- Microsoft Telnet

Perform the steps in the following subsections to configure your type of terminal software. If you are using Microsoft Telnet, configuration is not required.

Configuring Linux Minicom for Serial Console Emulation

Minicom is the serial port access utility for Linux. The following steps are valid for configuring Minicom version 2.0. Other Minicom versions may differ slightly but require the same basic settings. Use the information in "Required Minicom Settings for Serial Console Emulation" to configure other versions of Minicom.

Configuring Minicom Version 2.0 for Serial Console Emulation

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

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

2 In the Xterm window, move your mouse arrow to the lower right-hand corner of the window and resize the window to 80 x 25.

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

   If you have a Minicom configuration file, type `minicom <Minicom config file name>` and skip to step 17.

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

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

6 Press <a> and select the appropriate serial device (for example, **/dev/ttyS0**).

7 Press <e> and set the **Bps/Par/Bits** option to **57600 8N1**.

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

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

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

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

12 Press <Enter> to save each blank value.

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

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

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

16 At the command shell prompt, type minicom *<Minicom config file name>*.

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

18 Press <Ctrl+a>, <z>, <x> to exit Minicom.

NOTE: If you are using Minicom for serial text console redirection to configure the managed system BIOS, it is recommended to turn on color in Minicom. To turn on color, type the following command: minicom -c on

Ensure that the Minicom window displays a command prompt. When the command prompt is displayed, your connection is successful and you are ready to connect to the managed system console using the **connect** serial command.

Required Minicom Settings for Serial Console Emulation

Use Table 5-6 to configure any version of Minicom.

Table 5-6. Minicom Settings for Serial Console Emulation

Setting Description	Required Setting
Bps/Par/Bits	57600 8N1
Hardware flow control	Yes
Software flow control	No

Table 5-6.   Minicom Settings for Serial Console Emulation *(continued)*

Setting Description	Required Setting
Terminal emulation	ANSI
Modem dialing and parameter settings	Clear the **init**, **reset**, **connect**, and **hangup** settings so that they are blank
Window size	80 x 25 (to resize, drag the corner of the window)

Configuring HyperTerminal for Serial Console Redirection

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

⚠ **CAUTION: All versions of the Microsoft Windows operating system include Hilgraeve's HyperTerminal terminal emulation software. However, the included version does not provide many functions required during console redirection. Instead, you can use any terminal emulation software that supports VT100/VT220 or ANSI emulation mode. One example of a full VT100/VT220 or ANSI terminal emulator that supports console redirection on your system is Hilgraeve's HyperTerminal Private Edition 6.3. Also, use of the command line window to perform telnet serial console redirection may display garbage characters.**

To configure HyperTerminal for serial console redirection:

1 Start the HyperTerminal program.

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

3 Next to **Connect using:**, select the COM port on the management station (for example, COM2) to which you have connected the DB-9 null modem cable and click **OK**.

4 Configure the COM port settings as shown in Table 5-7.

5 Click **OK**.

6 Click **File** →**Properties**, and then click the **Settings** tab.

7 Set the **Telnet terminal ID:** to **ANSI**.

8 Click **Terminal Setup** and set **Screen Rows** to **26**.

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

Table 5-7. Management Station COM Port Settings

Setting Description	Required Setting
Bits per second	57600
Data bits	8
Parity	None
Stop bits	1
Flow control	Hardware

Configuring Serial and Terminal Modes

Configuring IPMI and iDRAC6 Serial

1 Expand the **System** tree and click **Remote Access**.

2 Click the **Configuration** tab and then click **Serial**.

3 Configure the IPMI serial settings.

   See Table 5-8 for description of the IPMI serial settings.

4 Configure the iDRAC6 serial settings.

   See Table 5-9 for description of the iDRAC6 serial settings.

5 Click **Apply Changes**.

6 Click the appropriate **Serial Configuration** page button to continue.
   See Table 5-10 for description of the serial configuration page settings.

Table 5-8. IPMI Serial Settings

Setting	Description
Connection Mode Settings	• Direct Connect Basic Mode - IPMI Serial Basic Mode • Direct Connect Terminal Mode - IPMI Serial Terminal Mode
Baud Rate	• Sets the data speed rate. Select **9600 bps**, **19.2 kbps**, **57.6 kbps**, or **115.2 kbps**.

Table 5-8.   IPMI Serial Settings *(continued)*

Setting	Description
Flow Control	• None — Hardware Flow Control Off • RTS/CTS — Hardware Flow Control On
Channel Privilege Level Limit	• Administrator • Operator • User

Table 5-9.   iDRAC6 Serial Settings

Setting	Description
Enabled	Enables or disables the iDRAC6 serial console. Checked= Enabled; Unchecked=Disabled
Timeout	The maximum number of seconds of line idle time before the line is disconnected. The range is 60 to 1920 seconds. Default is 300 seconds. Use 0 seconds to disable the Timeout feature.
Redirect Enabled	Enables or disables Console Redirection. Checked=Enabled; Unchecked=Disabled
Baud Rate	The data speed on the external serial port. Values are **9600 bps, 19.2 kbps, 57.6 kbps**, and **115.2 kbps**. Default is **57.6 kbps**.
Escape Key	Specifies the <Esc> key. The default are the ^\ characters.
History Buffer Size	The size of the serial history buffer, which holds the last characters written to the console. The maximum and default = 8192 characters.
Login Command	The iDRAC6 command line to be executed upon valid login.

Table 5-10.   Serial Configuration Page Settings

Button	Description
Print	Print the **Serial Configuration** page.
Refresh	Refresh the **Serial Configuration** page.
Apply Changes	Apply the IPMI and iDRAC6 serial changes.
Terminal Mode Settings	Opens the **Terminal Mode Settings** page.

Configuring Terminal Mode

1 Expand the **System** tree and click **Remote Access**.

2 Click the **Configuration** tab and then click **Serial**.

3 In the **Serial** page, click **Terminal Mode Settings**.

4 Configure the terminal mode settings.

See Table 5-11 for description of the terminal mode settings.

5 Click **Apply Changes**.

6 Click the appropriate **Terminal Mode Settings** page button to continue. See Table 5-12 for description of the terminal mode settings page buttons.

Table 5-11.   Terminal Mode Settings

Setting	Description
Line Editing	Enables or disables line editing.
Delete Control	Select one of the following:
	• iDRAC outputs a <bksp><sp><bksp> character when <bksp> or <del> is received —
	• iDRAC outputs a <del> character when <bksp> or <del> is received —
Echo Control	Enables or disables echo.
Handshaking Control	Enables or disables handshaking.
New Line Sequence	Select **None**, **<CR-LF>**, **<NULL>**, **<CR>**, **<LF-CR>**, or **<LF>**.
Input New Line Sequence	Select **<CR>** or **<NULL>**.

Table 5-12.   Terminal Mode Settings Page Buttons

Button	Description
Print	Print the **Terminal Mode Settings** page.
Refresh	Refresh the **Terminal Mode Settings** page.

Table 5-12.   Terminal Mode Settings Page Buttons *(continued)*

Button	Description
Return to Serial Port Configuration	Return to the **Serial Port Configuration** page.
Apply Changes	Apply the terminal mode settings changes.

Configuring the iDRAC6 Network Settings

⚠️ **CAUTION: Changing your iDRAC6 Network settings may disconnect your current network connection.**

Configure the iDRAC6 network settings using one of the following tools:

- Web-based Interface — See "Configuring the iDRAC6 NIC"
- RACADM CLI — See "cfgLanNetworking"
- iDRAC6 Configuration Utility — See "Configuring Your System to Use an iDRAC6"

✍️ **NOTE:** If you are deploying the iDRAC6 in a Linux environment, see "Installing RACADM."

Accessing the iDRAC6 Through a Network

After you configure the iDRAC6, you can remotely access the managed system using one of the following interfaces:

- Web-based interface
- RACADM
- Telnet Console
- SSH
- IPMI

Table 5-13 describes each iDRAC6 interface.

Table 5-13.   iDRAC6 Interfaces

Interface	Description
Web-based interface	Provides remote access to the iDRAC6 using a graphical user interface. The Web-based interface is built into the iDRAC6 firmware and is accessed through the NIC interface from a supported Web browser on the management station.

RACADM	Provides remote access to the iDRAC6 using a command line interface. RACADM uses the iDRAC6 IP address to execute RACADM commands.
	
	NOTE: The racadm remote capability option is supported only on management stations. For more information, see "Using RACADM Remotely."
	
	NOTE: When using the racadm remote capability, you must have write permission on the folders where you are using the RACADM subcommands involving file operations, for example:
	
	`racadm getconfig -f <file name>`
	
	or:
	
	`racadm sslcertupload -t 1 -f c:\cert\cert.txt subcommands`

Telnet Console	Provides access to the iDRAC6 and support for serial and RACADM commands including **powerdown**, **powerup**, **powercycle**, and **hardreset** commands. **NOTE:** Telnet is an unsecure protocol that transmits all data—including passwords—in plain text. When transmitting sensitive information, use the SSH interface.

Table 5-13.   iDRAC6 Interfaces *(continued)*

Interface	Description
SSH Interface	Provides the same capabilities as the telnet console using an encrypted transport layer for higher security.
IPMI Interface	Provides access through the iDRAC6 to the remote system's basic management features. The interface includes IPMI over LAN, IPMI over Serial, and Serial over LAN. For more information, see the *Dell OpenManage Baseboard Management Controller Utilities User's Guide* at **support.dell.com\manuals**.

NOTE: The iDRAC6 default user name is `root` and the default password is `calvin`.

You can access the iDRAC6 Web-based interface through the iDRAC6 NIC by using a supported Web browser, or through Server Administrator or IT Assistant.

To access the iDRAC6 remote access interface using Server Administrator, do the following:

- Launch Server Administrator.
- From the system tree on the left pane of the Server Administrator home page, click **System→Main System Chassis→Remote Access Controller**.

For more information, see your *Server Administrator User's Guide*.

Using RACADM Remotely

NOTE: Configure the IP address on your iDRAC6 before using the RACADM remote capability. For more information about setting up your iDRAC6 and a list of related documents, see "Basic Installation of the iDRAC6."

RACADM provides a remote capability option (**-r**) that allows you to connect to the managed system and execute RACADM subcommands from a remote console or management station. To use the remote capability, you need a valid user name (**-u** option) and password (**-p** option), and the iDRAC6 IP address.

NOTE: If the system from where you are accessing the remote system does not have an iDRAC6 certificate in its default certificate store, a message is displayed when you type a RACADM command. For more information about iDRAC6 certificates, see "Securing iDRAC6 Communications Using SSL and Digital Certificates."

```
Security Alert: Certificate is invalid - Name on
Certificate is invalid or does not match site name

Continuing execution. Use -S option for racadm to
stop the execution on certificate-related errors.
```

RACADM continues to execute the command. However, if you use the −S option, RACADM stops executing the command and displays the following message:

```
Security Alert: Certificate is invalid - Name on
Certificate is invalid or does not match site name

Racadm not continuing execution of the command.

ERROR: Unable to connect to iDRAC6 at specified
IP address
```

🖉 **NOTE:** The RACADM remote capability is supported only on management stations. For more information, see the *Dell Systems Software Support Matrix* under **Dell OpenManage Software** on the Dell Support website at **support.dell.com\manuals** for more information.

🖉 **NOTE:** When using the RACADM remote capability, you must have write permissions on the folders where you are using the RACADM subcommands involving file operations, for example:

```
racadm getconfig -f <file name>
```

or

```
racadm sslcertupload -t 1 -f c:\cert\cert.txt
subcommands
```

RACADM Synopsis

```
racadm -r <iDRAC6 IP Address> -u <username> -p
<password> <subcommand> <subcommand options>
```

```
racadm -i -r <iDRAC6 IP Address> <subcommand>
<subcommand options>
```

For example:

```
racadm -r 192.168.0.120 -u root -p calvin getsysinfo
racadm -i -r 192.168.0.120 getsysinfo
```

If the HTTPS port number of the iDRAC6 has been changed to a custom port other than the default port (443), the following syntax must be used:

```
racadm -r <iDRAC6 IP Address>:<port> -u <username> -p
<password> <subcommand> <subcommand options>
```

```
racadm -i -r <iDRAC6 IP Address>:<port> <subcommand>
<subcommand options>
```

RACADM Options

Table 5-14 lists the options for the RACADM command.

Table 5-14.   racadm Command Options

Option	Description
-r *<racIpAddr>*	Specifies the controller's remote IP address.
-r *<racIpAddr>*:*<port number>*	Use:*<port number>* if the iDRAC6 port number is not the default port (443)
-i	Instructs RACADM to interactively query the user for user name and password.
-u *<usrName>*	Specifies the user name that is used to authenticate the command transaction. If the -u option is used, the -p option must be used, and the -i option (interactive) is not allowed.
-p *<password>*	Specifies the password used to authenticate the command transaction. If the -p option is used, the -i option is not allowed.
-S	Specifies that RACADM should check for invalid certificate errors. RACADM stops the execution of the command with an error message if it detects an invalid certificate.

Enabling and Disabling the RACADM Remote Capability

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

The **RACADM** remote capability is enabled by default. If disabled, type the following **RACADM** command to enable:

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

To disable the remote capability, type:

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

RACADM Subcommands

Table 5-15 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."

When entering a RACADM subcommand, prefix the command with `racadm`, for example:

```
racadm help
```

Table 5-15.   RACADM Subcommands

Command	Description
help	Lists iDRAC6 subcommands.
help *<subcommand>*	Lists usage statement for the specified subcommand.
arp	Displays the contents of the ARP table. ARP table entries may not be added or deleted.
clearasrscreen	Clears the last ASR (crash) screen (last blue screen).
clrraclog	Clears the iDRAC6 log. A single entry is made to indicate the user and time that the log was cleared.
config	Configures the iDRAC6.
getconfig	Displays the current iDRAC6 configuration properties.
coredump	Displays the last iDRAC6 coredump.

Table 5-15. RACADM Subcommands *(continued)*

Command	Description
coredumpdelete	Deletes the coredump stored in the iDRAC6.
fwupdate	Executes or displays status on iDRAC6 firmware updates.
getssninfo	Displays information about active sessions.
getsysinfo	Displays general iDRAC6 and system information.
getractime	Displays the iDRAC6 time.
ifconfig	Displays the current iDRAC6 IP configuration.
netstat	Displays the routing table and the current connections.
ping	Verifies that the destination IP address is reachable from the iDRAC6 with the current routing-table contents.
setniccfg	Sets the IP configuration for the controller.
getniccfg	Displays the current IP configuration for the controller.
getsvctag	Displays service tags.
racdump	Dumps iDRAC6 status and state information for debug.
racreset	Resets the iDRAC6.
racresetcfg	Resets the iDRAC6 to the default configuration.
serveraction	Performs power management operations on the managed system.
getraclog	Displays the iDRAC6 log.
clrsel	Clears the System Event Log entries.
gettracelog	Displays the iDRAC6 trace log. If used with $-i$, the command displays the number of entries in the iDRAC6 trace log.
sslcsrgen	Generates and downloads the SSL CSR.
sslcertupload	Uploads a CA certificate or server certificate to the iDRAC6.
sslcertdownload	Downloads a CA certificate.
sslcertview	Views a CA certificate or server certificate in the iDRAC6.
sslkeyupload	Forces the iDRAC6 to send a test e-mail over the iDRAC6 NIC to check the e-mail configuration.
testtrap	Forces the iDRAC6 to send a test SNMP trap over the iDRAC6 NIC to check the trap configuration.
vmdisconnect	Forces a virtual media connection to close.
vmkey	Resets the virtual flash size to its default size (256 MB).

Frequently Asked Questions About RACADM Error Messages

After performing an iDRAC6 reset (using the racadm racreset command), I issue a command and the following message is displayed:

```
ERROR: Unable to connect to RAC at specified
IP address
```

What does this message mean?

You must wait until the iDRAC6 completes the reset before issuing another command.

When I use the racadm commands and subcommands, I get errors that I don't understand.

You may encounter one or more of the following errors when using the RACADM commands and subcommands:

- Local RACADM error messages — Problems such as syntax, typographical errors, and incorrect names.
- Remote RACADM error messages—Problems such as incorrect IP Address, incorrect username, or incorrect password.

When I ping the iDRAC6 IP address from my system and then switch my iDRAC6 between Dedicated and Shared modes during the ping response, I do not receive a response.

Clear the ARP table on your system.

Configuring Multiple iDRAC6 Controllers

Using RACADM, you can configure one or more iDRAC6 controllers with identical properties. When you query a specific iDRAC6 controller using its group ID and object ID, RACADM creates the **racadm.cfg** configuration file from the retrieved information. By exporting the file to one or more iDRAC6, you can configure your controllers with identical properties in a minimal amount of time.

NOTE: Some configuration files contain unique iDRAC6 information (such as the static IP address) that must be modified before you export the file to other iDRAC6.

To configure multiple iDRAC6 controllers, perform the following procedures:

1 Use RACADM to query the target iDRAC6 that contains the appropriate configuration.

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

   Open a command prompt and type:

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

   📝 **NOTE:** Redirecting the iDRAC6 configuration to a file using **getconfig -f** is only supported with the local and remote RACADM interfaces.

2 Modify the configuration file using a simple text editor (optional).

3 Use the new configuration file to modify a target iDRAC6.

   In the command prompt, type:

   ```
   racadm config -f myfile.cfg
   ```

4 Reset the target iDRAC6 that was configured.

   In the command prompt, type:

   ```
   racadm racreset
   ```

The **getconfig -f racadm.cfg** subcommand requests the iDRAC6 configuration and generates the **racadm.cfg** file. If required, you can configure the file with another name.

You can use the **getconfig** command to enable you to perform the following actions:

• Display all configuration properties in a group (specified by group name and index)

• Display all configuration properties for a user by user name

The **config** subcommand loads the information into the other iDRAC6. Use **config** to synchronize the user and password database with Server Administrator.

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

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

⚠ **CAUTION: It is recommended that you edit this file with a simple text editor. The RACADM utility uses an ASCII text parser. Any formatting confuses the parser, which may corrupt the RACADM database.**

Creating an iDRAC6 Configuration File

The iDRAC6 configuration file *<filename>*.**cfg** is used with the `racadm config -f <filename>.cfg` command. You can use the configuration file to build a configuration file (similar to an **.ini** file) and configure the iDRAC6 from this file. You may use any file name, and the file does not require a **.cfg** extension (although it is referred to by that extension name in this subsection).

The **.cfg** file can be:

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

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

The **.cfg** file is first parsed to verify that valid group and object names are present and that some simple syntax rules are being followed. Errors are flagged with the line number that detected the error, and a simple message explains the problem. The entire file is parsed for correctness, and all errors are displayed. Write commands are not transmitted to the iDRAC6 if an error is found in the **.cfg** file. The user must correct *all* errors before any configuration can take place. The **-c** option may be used in the **config** subcommand, which verifies syntax only and does *not* perform a write operation to the iDRAC6.

Use the following guidelines when you create a **.cfg** file:

- 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 iDRAC6 for that group. Any objects within that group are simple modifications when the iDRAC6 is configured. If a modified object represents a new index, the index is created on the iDRAC6 during configuration.

- You cannot specify an index of your choice in a **.cfg** file.

  Indexes may be created and deleted, so over time the group may become fragmented with used and unused indexes. If an index is present, it is modified. If an index is not present, the first available index is used. This method allows flexibility when adding indexed entries where 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 **.cfg** file that parses and runs correctly on one iDRAC6 may not run correctly on another if all indexes are full and you must add a new user.

- Use the **racresetcfg** subcommand to configure multiple iDRAC6 with identical properties.

  Use the **racresetcfg** subcommand to reset the iDRAC6 to original defaults, and then run the `racadm config -f <filename>.cfg` command. Ensure that the **.cfg** file includes all required objects, users, indexes, and other parameters.

⚠ **CAUTION: Use the racresetcfg subcommand to reset the database and the iDRAC6 NIC settings to the original default settings and remove all users and user configurations. While the root user is available, other users' settings are also reset to the default settings.**

Parsing Rules

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

  A comment line *must* start in column one. A '#' character in any other column is treated as a '#' character.

  Some modem parameters may include # characters in its string. An escape character is not required. You may want to generate a **.cfg** from a `racadm getconfig -f <filename>.cfg` command, and then perform a `racadm config -f <filename>.cfg` command to a different iDRAC6, without adding escape characters.

  Example:

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

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

  The starting "[" character denoting a group name *must* start in column one. This group name *must* be specified before any of the objects in that group. Objects that do not include an associated group name generate an error. The configuration data is organized into groups as defined in "iDRAC6 Property Database Group and Object Definitions."

  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}
  ```

- All parameters are specified as "object=value" pairs with no white space between the object, =, or value.

  White spaces that are included after the value are ignored. A 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). These characters are valid modem chat script characters.

  See the example in the previous bullet.

- The **.cfg** 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>.cfg` command places a comment in front of index objects, allowing the user to see the included comments.

NOTE: You may create an indexed group manually using the following command: `racadm config -g <groupName> -o <anchored object> -i <index 1-16> <unique anchor name>`

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

  You must remove an indexed object manually using the following command:

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

NOTE: A NULL string (identified by two "" characters) directs the iDRAC6 to delete the index for the specified group.

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

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

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

  `[cfgUserAdmin]`

  `cfgUserAdminUserName=<USER_NAME>`

  If you type `racadm getconfig -f <myexample>.cfg`, the command builds a **.cfg** file for the current iDRAC6 configuration. This configuration file can be used as an example and as a starting point for your unique **.cfg** file.

Modifying the iDRAC6 IP Address

When you modify the iDRAC6 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
```

The command **racadm config -f myfile.cfg** parses the file and identifies any errors by line number. A correct file will update the proper entries. Additionally, you can use the same **getconfig** command from the previous example to confirm the update.

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

✎ **NOTE:** "Anchor" is an internal term and should not be used in the file.

Configuring iDRAC6 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 iDRAC6 Configuration Utility at boot-up when you are prompted to type <Ctrl><E>. For more information about configuring network properties with the iDRAC6 Configuration Utility, see "Configuring Your System to Use an iDRAC6."

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 iDRAC6 LAN is disabled even if DHCP is enabled.

iDRAC6 Modes

The iDRAC6 can be configured in one of four modes:

- Dedicated
- Shared
- Shared with Failover LOM2
- Shared with Failover All LOMs

Table 5-16 provides a description of each mode.

Table 5-16. iDRAC6 NIC Configurations

Mode	Description
Dedicated	The iDRAC6 uses its own NIC (RJ-45 connector) and the iDRAC MAC address for network traffic.
Shared	The iDRAC6 uses LOM1 on the planar.
Shared with Failover LOM2	The iDRAC6 uses LOM1 and LOM2 as a team for failover. The team uses the iDRAC6 MAC address.
Shared with Failover All LOMs	The iDRAC6 uses LOM1, LOM2, LOM3, and LOM4 as a team for failover. The team uses the iDRAC6 MAC address.

Frequently Asked Questions about Network Security

When accessing the iDRAC6 Web-based interface, I get a security warning stating the hostname of the SSL certificate does not match the hostname of the iDRAC6.

The iDRAC6 includes a default iDRAC6 server certificate to ensure network security for the Web-based interface and remote RACADM features. When this certificate is used, the Web browser displays a security warning because the default certificate is issued to **iDRAC6 default certificate** which does not match the host name of the iDRAC6 (for example, the IP address).

To address this security concern, upload a iDRAC6 server certificate issued to the IP address or the iDRAC name of the iDRAC6. When generating the certificate signing request (CSR) to be used for issuing the certificate, ensure that the common name (CN) of the CSR matches the IP address (**if certificate issued to IP**) of the iDRAC6 (for example, 192.168.0.120) or the registered DNS iDRAC6 name (**if certificate issued to iDRAC registered name**).

To ensure that the CSR matches the registered DNS iDRAC6 name:

1 In the **System** tree, click **Remote Access**.

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

3 In the **Common Settings** table:

   a Select the **Register iDRAC on DNS** check box.

   b In the **DNS iDRAC Name** field, enter the iDRAC6 name.

4 Click **Apply Changes**.

See "Securing iDRAC6 Communications Using SSL and Digital Certificates" for more information about generating CSRs and issuing certificates.

Why are the remote RACADM and Web-based services unavailable after a property change?

It may take a while for the remote RACADM services and the Web-based interface to become available after the iDRAC6 Web server resets.

The iDRAC6 Web server is reset after the following occurrences:

- When the network configuration or network security properties are changed using the iDRAC6 Web user interface
- When the **cfgRacTuneHttpsPort** property is changed (including when a config -f <*config file*> changes it)
- When **racresetcfg** is used
- When the iDRAC6 is reset
- When a new SSL server certificate is uploaded

Why doesn't my DNS server register my iDRAC6?

Some DNS servers only register names of 31 characters or fewer.

When accessing the iDRAC6 Web-based interface, I get a security warning stating the SSL certificate was issued by a certificate authority (CA) that is not trusted.

iDRAC6 includes a default iDRAC6 server certificate to ensure network security for the Web-based interface and remote RACADM features. This certificate was not issued by a trusted CA. To address this security concern, upload a iDRAC6 server certificate issued by a trusted CA (for example, Microsoft Certificate Authority, Thawte or Verisign). See "Securing iDRAC6 Communications Using SSL and Digital Certificates" for more information about issuing certificates.

6

Adding and Configuring iDRAC6 Users

To manage your system with the iDRAC6 and maintain system security, create unique users with specific administrative permissions (or *role-based authority*). For additional security, you can also configure alerts that are e-mailed to specific users when a specific system event occurs.

Using the Web Interface to Configure iDRAC6 Users

Adding and Configuring iDRAC6 Users

To manage your system with the iDRAC6 and maintain system security, create unique users with specific administrative permissions (or *role-based authority*).

To add and configure iDRAC6 users, perform the following steps:

NOTE: You must have **Configure Users** permission to configure an iDRAC user.

1 Click **Remote Access→Configuration→Users**.

The **Users** page displays the following information for iDRAC users: **User ID, State** (Enabled/Disabled)**, User Name, RAC Privilege**, **IPMI LAN Privilege**, **IPMI Serial Privilege**, and **Serial Over LAN** state (Enabled/Disabled).

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

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

On the **User Main Menu** page, you can configure a user, view a user certificate, upload a trusted certification authority (CA) certificate, or view a trusted CA certificate.

If you select **Configure User** and click **Next**, the **User Configuration** page is displayed. Continue on to step 4.

3 On the **User Configuration** page, configure the following:

- The username, password, and access permissions for a new or existing iDRAC user. Table describes **General User Settings**.

- The user's IPMI privileges. Table 6-4 describes the **IPMI User Privileges** for configuring the user's LAN privileges.

- The iDRAC user privileges. Table 6-5 describes the **iDRAC User Privileges**.

- The iDRAC Group access permissions. Table 6-6 describes the **iDRAC Group Permissions**.

4 When completed, click **Apply Changes**.

5 Click the appropriate button to continue. See Table 6-7.

Table 6-1. User States and Permissions

Setting	Description
User ID	Displays a sequential list of user ID numbers. Each field under **User ID** contains one of 16 preset User ID numbers. This field cannot be edited.
State	Displays the login state of the user: Enabled or Disabled. (Disabled is the default.)
	NOTE: User 2 is enabled by default.
User Name	Displays the login name of the user. Specifies an iDRAC6 user name with up to 16 characters. Each user must have a unique user name.
	NOTE: User names on the iDRAC6 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.
RAC Privilege	Displays the group (privilege level) to which the user is assigned (Administrator, Operator, Read Only, or None).
IPMI LAN Privilege	Displays the IPMI LAN privilege level to which the user is assigned (Administrator, Operator, Read Only, or None).
IPMI Serial Privilege	Displays the IPMI Serial Port privilege level to which the user is assigned (Administrator, Operator, Read Only, or None).
Serial Over LAN	Allows/Disallows the user to use IPMI Serial Over LAN.

Table 6-2. Smart Card Configuration Options

Option	Description
View User Certificate	Displays the user certificate page that has been uploaded to the iDRAC.
Upload Trusted CA Certificate	Enables you to upload the trusted CA certificate to iDRAC and import it to the user profile.
View Trusted CA Certificate	Displays the trusted CA certificate that has been uploaded to the iDRAC. The trusted CA certificate is issued by the CA who is authorized to issue certificates to users.

Table 6-3. General User Settings

User ID	One of 16 preset User ID numbers.
Enable User	When checked, indicates that the user's access to the iDRAC6 is enabled. When unchecked, user access is disabled.
User Name	A User Name with up to 16 characters.
Change Password	Enables the **New Password** and **Confirm New Password** fields. When unchecked, the user's Password cannot be changed.
New Password	Enter a **Password** with up to 20 characters. The characters will not be displayed.
Confirm New Password	Retype the iDRAC user's password to confirm.

Table 6-4. IPMI 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: **Administrator**, **Operator**, **User**, or **None**.
Maximum Serial Port User Privilege Granted	Specifies the user's maximum privilege on the IPMI Serial channel to one of the following user groups: **Administrator**, **Operator**, **User**, or **None**.
Enable Serial Over LAN	Allows the user to use IPMI Serial Over LAN. When checked, this privilege is enabled.

Table 6-5.   iDRAC User Privileges

Property	Description
Roles	Specifies the user's maximum iDRAC user privilege as one of the following: **Administrator**, **Operator**, **Read Only**, or **None**. See Table 6-6 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 Server Control commands.
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 6-6.   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**
Operator	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**
Read Only	**Login to iDRAC**
None	No assigned permissions

Table 6-7. User Configuration Page Buttons

Button	Action
Print	Prints the **User Configuration** values that appear on the screen.
Refresh	Reloads the **User Configuration** page.
Go Back To Users Page	Returns to the **Users Page**.
Apply Changes	Saves any new settings made to the user configuration.

Using the RACADM Utility to Configure iDRAC6 Users

✍ **NOTE:** You must be logged in as user **root** to execute RACADM commands on a remote Linux system.

Single or multiple iDRAC6 users can be configured using the RACADM command line that is installed with the iDRAC6 agents on the managed system.

To configure multiple iDRAC6 with identical configuration settings, perform one of the following procedures:

- Use the RACADM examples in this section as a guide to create a batch file of RACADM commands and then execute the batch file on each managed system.

- Create the iDRAC6 configuration file as described in "RACADM Subcommand Overview" and execute the **racadm config** subcommand on each managed system using the same configuration file.

Before You Begin

You can configure up to 16 users in the iDRAC6 property database. Before you manually enable an iDRAC6 user, verify if any current users exist. If you are configuring a new iDRAC6 or if you ran the **racadm racresetcfg** command, the only current user is root with the password calvin. The **racresetcfg** subcommand resets the iDRAC6 to the original default values.

⚠ CAUTION: Use caution when using the racresetcfg command, as *all* configuration parameters are reset to their default values. Any previous changes are lost.

✎ NOTE: Users can be enabled and disabled over time. As a result, a user may have a different index number on each iDRAC6.

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 of 1–16:

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

✎ NOTE: You can also type racadm getconfig -f <myfile.cfg> and view or edit the **myfile.cfg** file, which includes all iDRAC6 configuration parameters.

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

```
# cfgUserAdminIndex=XX

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 is displayed after the "=", that index is taken by that user name.

✎ NOTE: When you manually enable or disable a user with the **racadm config** subcommand, you *must* specify the index with the -**i** option. Observe that the **cfgUserAdminIndex** object displayed in the previous example contains a '#' character. Also, if you use the **racadm config** -**f racadm.cfg** command to specify any number of groups/objects to write, the index cannot be specified. A new user is added to the first available index. This behavior allows more flexibility in configuring multiple iDRAC6 with the same settings.

Adding an iDRAC6 User

To add a new user to the RAC configuration, a few basic commands can be used. In general, perform the following procedures:

1 Set the user name.

2 Set the password.

3 Set the following user privileges:

   • iDRAC privilege

   • IPMI LAN privilege

   • IPMI Serial privilege

   • Serial Over LAN 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 RAC.

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

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

```
racadm config -g cfgUserAdmin -i 2 -o
cfgUserAdminPrivilege 0x00000001
```

```
racadm config -g cfgUserAdmin -i 2 -o
cfgUserAdminIpmiLanPrivilege 4
```

```
racadm config -g cfgUserAdmin -i 2 -o
cfgUserAdminIpmiSerialPrivilege 4
```

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

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

To verify, use one of the following commands:

```
racadm getconfig -u john
```

```
racadm getconfig -g cfgUserAdmin -i 2
```

Removing an iDRAC6 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 iDRAC6 to remove the user configuration at the specified index and reset the user configuration to the original factory defaults.

Enabling an iDRAC6 User With Permissions

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

NOTE: See Table B-2 for a list of valid bit mask values for specific user privileges. The default privilege value is 0, which indicates the user has no privileges enabled.

```
racadm config -g cfgUserAdmin -o
cfgUserAdminPrivilege -i <index> <user privilege
bitmask value>
```

7

Using the iDRAC6 With Microsoft Active Directory

A directory service maintains a common database of all information needed for controlling users, computers, printers, etc. on a network. If your company already uses the Microsoft® Active Directory® service software, you can configure the software to provide access to iDRAC6, allowing you to add and control iDRAC6 user privileges to your existing users in your Active Directory software.

NOTE: Using Active Directory to recognize iDRAC6 users is supported on the Microsoft Windows® 2000, Windows Server® 2003, and Windows Server 2008 operating systems.

Table 7-1 shows the iDRAC6 Active Directory user privileges.

Table 7-1. iDRAC6 User Privileges

Privilege	Description
Login to iDRAC	Enables the user to log in to the iDRAC6
Configure iDRAC	Enables the user to configure the iDRAC6
Configure Users	Enables the user to allow specific users to access the system
Clear Logs	Enables the user to clear the iDRAC6 logs
Execute Server Control Commands	Enables the user to execute RACADM commands
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

Prerequisites for Enabling Active Directory Authentication for the iDRAC6

To use the Active Directory authentication feature of the iDRAC6, you must have already deployed an Active Directory infrastructure. See the Microsoft website for information on how to set up an Active Directory infrastructure, if you don't already have one.

iDRAC6 uses the standard Public Key Infrastructure (PKI) mechanism to authenticate securely into the Active Directory; therefore, you would also require an integrated PKI into the Active Directory infrastructure. See the Microsoft website for more information on the PKI setup.

To correctly authenticate to all the domain controllers, you also need to enable the Secure Socket Layer (SSL) on all domain controllers that iDRAC6 connects to. See "Enabling SSL on a Domain Controller" for more specific information.

Supported Active Directory Authentication Mechanisms

You can use Active Directory to define user access on the iDRAC6 through two methods: you can use the *extended schema* solution, which Dell has customized to add Dell-defined Active Directory objects. Or, you can use the *standard schema* solution, which uses Active Directory group objects only. See the sections that follow for more information about these solutions.

When using Active Directory to configure access to iDRAC6, 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.
- Configuring user access on different iDRAC6 with varying privilege levels is provided.

The advantage of using the standard schema solution is that no schema extension is required because all of the necessary object classes are provided by Microsoft's default configuration of the Active Directory schema.

Extended Schema Active Directory Overview

Using the extended schema solution requires the Active Directory schema extension, as described in the following section.

Extending the Active Directory Schema

Important: The schema extension for this product is different from the previous generations of Dell Remote Management products. You must extend the new schema and install the new Active Directory Users and Computers Microsoft Management Console (MMC) Snap-in on your directory. The old schema does not work with this product.

NOTE: Extending the new schema or installing the new extension to Active Directory User and Computer Snap-in has no impact on previous products.

The schema extender and Active Directory Users and Computers MMC Snap-in extension are on the *Dell Systems Management Tools and Documentation* DVD. For more information, see "Extending the Active Directory Schema" and "Installing the Dell Extension to the Active Directory Users and Computers Snap-In." For further details on extending the schema for iDRAC6 and installing the Active Directory Users and Computers MMC Snap-in, see the *Dell OpenManage Installation and Security User's Guide* available on **support.dell.com/manuals**.

NOTE: When you create iDRAC Association Objects or iDRAC Device Objects, ensure that you select **Dell Remote Management Object Advanced**.

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 necessary changes 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's Active Directory, Dell received unique OIDs, unique name extensions, and uniquely linked attribute IDs for our attributes and classes that are added into the directory service.

Dell extension is: dell

Dell base OID is: 1.2.840.113556.1.8000.1280

RAC LinkID range is:12070 to 12079

Overview of the iDRAC 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 iDRAC devices. This model provides an Administrator maximum flexibility over the different combinations of users, iDRAC privileges, and iDRAC devices on the network without adding too much complexity.

Active Directory Object Overview

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

However, each Association Object can be linked (or, may link users, groups of users, or iDRAC Device Objects) to only one Privilege Object. This example allows an Administrator to control each user's privileges on specific iDRACs.

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

Figure 7-1 illustrates that the Association Object provides the connection that is needed for all of the Authentication and Authorization.

Figure 7-1.   Typical Setup for Active Directory Objects
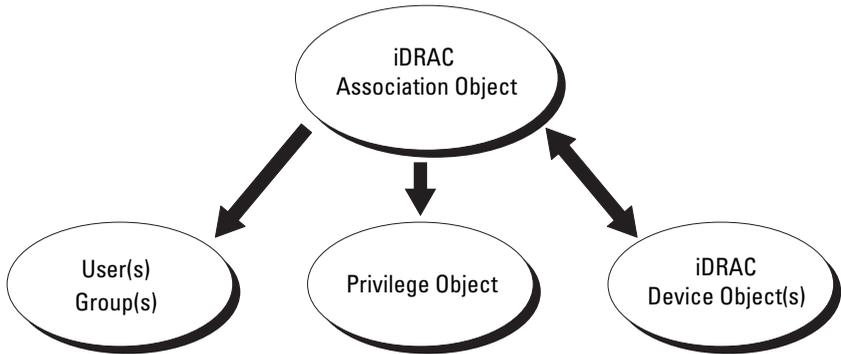
You can create as many or as few association objects as required. However, you must create at least one Association Object, and you must have one iDRAC Device Object for each iDRAC on the network that you want to integrate with Active Directory for Authentication and Authorization with the iDRAC.

The Association Object allows for as many or as few users and/or groups as well as iDRAC 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 iDRACs.

The Dell extension to the Active Directory Users and Computers MMC Snap-in only allows associating the Privilege Object and iDRAC Objects from the same domain with the Association Object. The Dell extension does not allow a group or an iDRAC object from other domains to be added as a product member of the Association Object.

Users, user groups, or nested user groups from any domain can be added into the Association Object. Extended Schema solutions support any user group type and any user group nesting across multiple domains allowed by Microsoft Active Directory.

Accumulating Privileges Using Extended Schema

The Extended Schema Authentication mechanism supports Privilege
Accumulation from different privilege objects associated with the same user
through different Association Objects. In other words, Extended Schema
Authentication accumulates privileges to allow the user the super set of all
assigned privileges corresponding to the different privilege objects associated
with the same user.

Figure 7-2 provides an example of accumulating privileges using
Extended Schema.

Figure 7-2.   Privilege Accumulation for a User
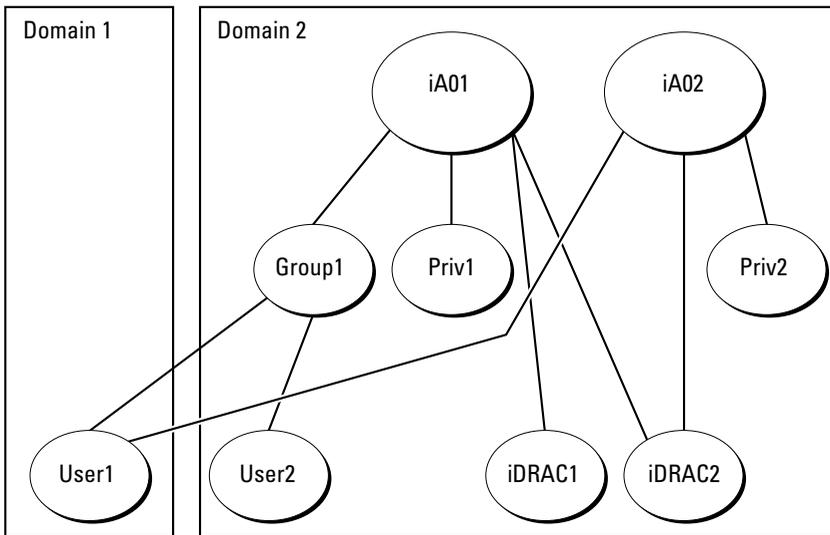
The figure shows two Association Objects—iA01 and iA02. User1 is
associated to iDRAC2 through both association objects. Therefore, User1 has
accumulated privileges that are the result of combining the privileges set for
objects Priv1 and Priv2 on iDRAC2.

For example, Priv1 has these privileges: Login, Virtual Media, and Clear Logs and Priv2 has these privileges: Login to iDRAC, Configure iDRAC, and Test Alerts. As a result, User1 now has the privilege set: Login to iDRAC, Virtual Media, Clear Logs, Configure iDRAC, and Test Alerts, which is the combined privilege set of Priv1 and Priv2.

Extended Schema Authentication accumulates privileges to allow the user the maximum set of privileges possible considering the assigned privileges of the different privilege objects associated to the same user.

In this configuration, User1 has both Priv1 and Priv2 privileges on iDRAC2. User1 has Priv1 privileges on iDRAC1 only. User2 has Priv1 privileges on both iDRAC1 and iDRAC2. In addition, this figure shows that User1 can be in a different domain and can be associated by a nested group.

Configuring Extended Schema Active Directory to Access Your iDRAC

Before using Active Directory to access your iDRAC6, configure the Active Directory software and the iDRAC6 by performing the following steps in order:

1 Extend the Active Directory schema (see "Extending the Active Directory Schema").

2 Extend the Active Directory Users and Computers Snap-in (see "Installing the Dell Extension to the Active Directory Users and Computers Snap-In").

3 Add iDRAC6 users and their privileges to Active Directory (see "Adding iDRAC Users and Privileges to Active Directory").

4 Enable SSL on each of your domain controllers (see "Enabling SSL on a Domain Controller").

5 Configure the iDRAC6 Active Directory properties using either the iDRAC6 Web-based interface or the RACADM (see "Configuring Active Directory With Extended Schema Using the iDRAC6 Web-Based Interface" or "Configuring Active Directory With Extended Schema Using RACADM").

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 methods:

- 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 Tools and Documentation* DVD in the following respective directories:

- *DVD drive*:**\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\LDIF_Files**
- **<DVD *drive*>:\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\Schema_Extender**

> *NOTE:* The **Remote_Management** folder is for extending the Schema on older remote access products like DRAC 4 and DRAC 5, and the **Remote_Management_Advanced** folder is for extending the Schema on iDRAC6.

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."

You can copy and run the Schema Extender or LDIF files from any location.

Using the Dell Schema Extender

> *NOTE:* 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 MMC and the Active Directory Schema Snap-in to verify that the following exist:

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

See your Microsoft documentation for details about using the MMC and the Active Directory Schema Snap-in.

Table 7-2.   Class Definitions for Classes Added to the Active Directory Schema

Class Name	Assigned Object Identification Number (OID)
delliDRACDevice	1.2.840.113556.1.8000.1280.1.7.1.1
delliDRACAssociation	1.2.840.113556.1.8000.1280.1.7.1.2
dellRAC4Privileges	1.2.840.113556.1.8000.1280.1.1.1.3
dellPrivileges	1.2.840.113556.1.8000.1280.1.1.1.4
dellProduct	1.2.840.113556.1.8000.1280.1.1.1.5

Table 7-3.   dellRacDevice Class

OID	1.2.840.113556.1.8000.1280.1.7.1.1
Description	Represents the Dell iDRAC device. The iDRAC device must be configured as delliDRACDevice 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 7-4.   delliDRACAssociationObject Class

OID	1.2.840.113556.1.8000.1280.1.7.1.2
Description	Represents the Dell Association Object. The Association Object provides the connection between the users and the devices.

Table 7-4.   delliDRACAssociationObject Class *(continued)*

OID	1.2.840.113556.1.8000.1280.1.7.1.2
Class Type	Structural Class
SuperClasses	Group
Attributes	dellProductMembers
	dellPrivilegeMember

Table 7-5.   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 7-6.   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 7-7. 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
SuperClasses	Computer
Attributes	**dellAssociationMembers**

Table 7-8. List of Attributes Added to the Active Directory Schema

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

Table 7-8. List of Attributes Added to the Active Directory Schema *(continued)*

Attribute Name/Description	Assigned OID/Syntax Object Identifier	Single Valued
dellIsLogClearAdmin	1.2.840.113556.1.8000.1280.1.1.2.6	TRUE
TRUE if the user has Log Clearing rights on the device.	Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
dellIsServerResetUser	1.2.840.113556.1.8000.1280.1.1.2.7	TRUE
TRUE if the user has Server Reset rights on the device.	Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
dellIsConsoleRedirectUser	1.2.840.113556.1.8000.1280.1.1.2.8	TRUE
TRUE if the user has Console Redirection rights on the device.	Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
dellIsVirtualMediaUser	1.2.840.113556.1.8000.1280.1.1.2.9	TRUE
TRUE if the user has Virtual Media rights on the device.	Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
dellIsTestAlertUser	1.2.840.113556.1.8000.1280.1.1.2.10	TRUE
TRUE if the user has Test Alert User rights on the device.	Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
dellIsDebugCommandAdmin	1.2.840.113556.1.8000.1280.1.1.2.11	TRUE
TRUE if the user has Debug Command Admin rights on the device.	Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
dellSchemaVersion	1.2.840.113556.1.8000.1280.1.1.2.12	TRUE
The Current Schema Version is used to update the schema.	Case Ignore String (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	
dellRacType	1.2.840.113556.1.8000.1280.1.1.2.13	TRUE
This attribute is the Current RAC Type for the delliDRACDevice object and the backward link to the dellAssociationObjectMembers forward link.	Case Ignore String (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	

Table 7-8. List of Attributes Added to the Active Directory Schema *(continued)*

Attribute Name/Description	Assigned OID/Syntax Object Identifier	Single Valued
dellAssociationMembers	1.2.840.113556.1.8000.1280.1.1.2.14	FALSE
List of dellAssociationObjectMembers that belong to this Product. This attribute is the backward link to the dellProductMembers linked attribute.	Distinguished Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	
Link ID: 12071		

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 iDRAC devices, Users and User Groups, iDRAC Associations, and iDRAC Privileges.

When you install your systems management software using the *Dell Systems Management Tools and Documentation* DVD, you can install the Snap-in by selecting the **Active Directory Users 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 x64-bit Windows Operating Systems, the Snap-in installer is located under **<DVD drive>:\SYSMGMT\ManagementStation\ support\OMActiveDirectory_SnapIn64**

For more information about the Active Directory Users 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 iDRAC Object in the container.

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

Opening the Active Directory Users and Computers Snap-In

To open the Active Directory Users and Computers Snap-in:

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 MMC is displayed.

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 iDRAC, Association, and Privilege objects. To add each object type, perform the following procedures:

• Create an iDRAC device Object

• Create a Privilege Object

• Create an Association Object

• Configuring an Association Object

Creating an iDRAC Device Object

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

2   Select **New→Dell Remote Management Object Advanced**.

    The **New Object** window is displayed.

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 Active Directory With Extended Schema Using the iDRAC6 Web-Based Interface."

4 Select **iDRAC 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 Remote Management Object Advanced**.

The **New Object** window is displayed.

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 **Remote Management Privileges** tab and select the privileges that you want the user to have.

Creating an Association Object

✐ **NOTE:** The iDRAC Association Object is derived from Group and its scope is set to Domain Local.

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

2 Select **New→Dell Remote Management Object Advanced**.

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**.

Configuring an Association Object

Using the **Association Object Properties** window, you can associate users or user groups, privilege objects, and iDRAC devices.

You can add groups of Users. 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 an iDRAC 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 iDRAC device connected to the network that is available for the defined users or user groups. Multiple iDRAC devices can be added to an Association Object.

Adding iDRAC Devices

To add iDRAC devices:

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

2 Type the iDRAC device name and click **OK**.

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

Configuring Active Directory With Extended Schema Using the iDRAC6 Web-Based Interface

1 Open a supported Web browser window.

2 Log in to the iDRAC6 Web-based interface.

3 Expand the **System** tree and click **Remote Access**.

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

5 Scroll to the bottom of the **Active Directory Configuration and Management** page, and click **Configure Active Directory**.

The **Step 1 of 4 Active Directory Configuration and Management** page is displayed.

6 Under **Certificate Settings**, check **Enable Certificate Validation** if you want to validate the SSL certificate of your Active Directory servers; otherwise, go to step 9.

7 Under **Upload Active Directory CA Certificate**, type the file path of the certificate or browse to find the certificate file.

> *NOTE:* You must type the absolute file path, which includes the full path and the complete file name and file extension.

8 Click **Upload**.

The certificate information for the Active Directory CA certificate that you uploaded is displayed.

9 Under **Upload Kerberos Keytab**, type the path of the keytab file or browse to locate the file. Click **Upload**. The Kerberos keytab will be uploaded into the iDRAC6.

10 Click **Next** to go to the **Step 2 of 4 Active Directory Configuration and Management**.

11 Click **Enable Active Directory**.

> ⚠ **CAUTION: In this release, the Smart Card based Two Factor Authentication (TFA) and the single sign-on (SSO) features are not supported if the Active Directory is configured for Extended Schema.**

12 Click **Add** to enter the user domain name.

13 Type the user domain name in the prompt and click **OK**. Note that this step is optional. If you configure a list of user domains, the list will be available in the Web-based interface login screen. You can choose from the list, and then you only need to type the user name.

14 Type the **Timeout** time in seconds to specify the time the iDRAC6 will wait for Active Directory responses. The default is 120 seconds.

15 Type the Domain Controller Server Address. You can enter up to three Active Directory servers for login processing, but you are required to configure at least one server by entering the IP address or the fully qualified domain name (FQDN). iDRAC6 tries to connect to each configured server until a connection is established.

> *NOTE:* The FQDN or IP address that you specify in this field should match the Subject or Subject Alternative Name field of your domain controller certificate if you have certificate validation enabled.

16 Click **Next** to go to the **Step 3 of 4 Active Directory Configuration and Management**.

17 Under **Schema Selection**, click **Extended Schema.**

18 Click **Next** to go to the **Step 4 of 4 Active Directory Configuration and Management.**

19 Under **Extended Schema Settings**, type the iDRAC name and domain name to configure the iDRAC device object. The iDRAC domain name is the Domain in which iDRAC Object is created.

20 Click **Finish** to save Active Directory Extended Schema settings.

The iDRAC6 Web server automatically returns you to the **Active Directory Configuration and Management** page.

21 Click **Test Settings** to check the Active Directory Extended Schema settings.

22 Type your Active Directory user name and password.

The test results and the test log are displayed. For additional information, see "Testing Your Configurations."

> **NOTE:** You must have a DNS server configured properly on iDRAC to support Active Directory login. Click **Remote Access**→**Configuration**→**Network** page to configure DNS server(s) manually or use DHCP to get DNS server(s).

You have completed the Active Directory configuration with Extended Schema.

Configuring Active Directory With Extended Schema Using RACADM

Use the following commands to configure the iDRAC Active Directory feature with Extended Schema using the RACADM CLI tool instead of the Web-based interface.

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

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

racadm config -g cfgActiveDirectory -o cfgADType 1

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

racadm config -g cfgActiveDirectory -o
cfgADRacDomain <fully qualified rac domain name>
```

```
racadm config -g cfgActiveDirectory -o
cfgDomainController1 <fully qualified domain name
or IP Address of the domain controller>

racadm config -g cfgActiveDirectory -o
cfgDomainController2 <fully qualified domain name
or IP Address of the domain controller>

racadm config -g cfgActiveDirectory -o
cfgDomainController3 <fully qualified domain name
or IP Address of the domain controller>
```

NOTE: At least one of the three addresses is required to be configured. iDRAC attempts to connect to each of the configured addresses one-by-one until a successful connection is made. When the extended schema option is selected, these are the FQDN or IP addresses of the domain controllers where this iDRAC device is located. Global catalog servers are not used in extended schema mode at all.

NOTE: The FQDN or IP address that you specify in this field should match the Subject or Subject Alternative Name field of your domain controller certificate if you have certificate validation enabled.

⚠ **CAUTION: In this release, the Smart Card based Two Factor Authentication (TFA) and the single sign-on (SSO) features are not supported if the Active Directory is configured for Extended Schema.**

If you want to disable the certificate validation during SSL handshake, type the following RACADM command:

```
racadm config -g cfgActiveDirectory -o
cfgADCertValidationEnable 0
```

In this case, you do not have to upload a CA certificate.

If you want to enforce the certificate validation during SSL handshake, type the following RACADM command:

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

In this case, you must upload a CA certificate using the following RACADM command:

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

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

Using the following RACADM command may be optional. See "Importing the iDRAC6 Firmware SSL Certificate" for additional information.

```
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 address, type 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 If you want to configure a list of user domains so that you only need to enter the user name during login to the iDRAC6 Web-based interface, type the following command:

```
racadm config -g cfgUserDomain -o
cfgUserDomainName -i <index>
```

You can configure up to 40 user domains with index numbers between 1 and 40.

See "Using Active Directory to Log In to the iDRAC6" for details about user domains.

5 Press **Enter** to complete the Active Directory configuration with Extended Schema.

Standard Schema Active Directory Overview

As shown in Figure 7-3, using standard schema for Active Directory integration requires configuration on both Active Directory and the iDRAC6.

Figure 7-3.   Configuration of iDRAC with Microsoft Active Directory and Standard Schema
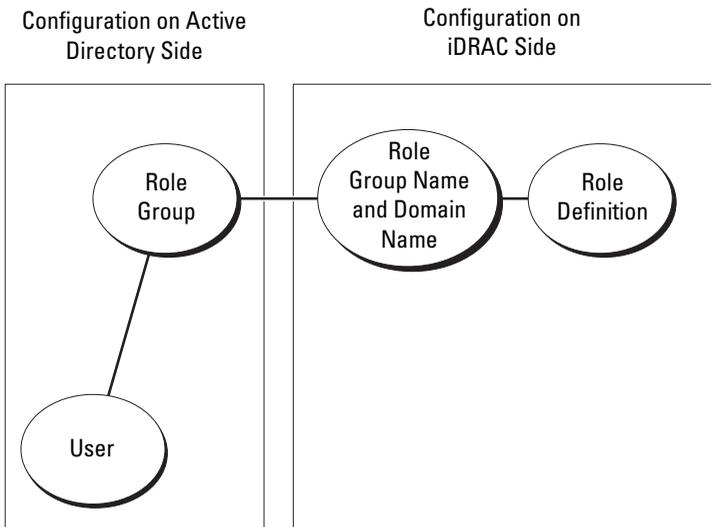
On the Active Directory side, a standard group object is used as a role group. A user who has iDRAC6 access will be a member of the role group. To give this user access to a specific iDRAC6, the role group name and its domain name need to be configured on the specific iDRAC6. Unlike the extended schema solution, the role and the privilege level is defined on each iDRAC6, not in the Active Directory. Up to five role groups can be configured and defined in each iDRAC. Table 7-9 shows the default role group privileges.

Table 7-9.   Default Role Group Privileges

Role Groups	Default Privilege Level	Permissions Granted	Bit Mask
Role Group 1	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
Role Group 2	Operator	Login to iDRAC, Configure iDRAC, Execute Server Control Commands, Access Console Redirection, Access Virtual Media, Test Alerts, Execute Diagnostic Commands	0x000000f9
Role Group 3	Read Only	Login to iDRAC	0x00000001
Role Group 4	None	No assigned permissions	0x00000000
Role Group 5	None	No assigned permissions	0x00000000

NOTE: The Bit Mask values are used only when setting Standard Schema with the RACADM.

Single Domain Versus Multiple Domain Scenarios

If all of the login users and role groups, as well as the nested groups, are in the same domain, then only the domain controllers' addresses must be configured on iDRAC6. In this single domain scenario, any group type is supported.

If all of the login users and role groups, or any of the nested groups, are from multiple domains, then Global Catalog server addresses are required to be configured on iDRAC6. In this multiple domain scenario, all of the role groups and nested groups, if any, must be Universal Group type.

Configuring Standard Schema Active Directory to Access Your iDRAC

You must perform the following steps to configure Active Directory before an Active Directory user can access iDRAC6:

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 must be configured on the iDRAC6 by using either the Web-based interface or RACADM (see "Configuring Active Directory With Standard Schema Using the iDRAC6 Web-Based Interface" or "Configuring Active Directory With Standard Schema Using RACADM").

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

Configuring Active Directory With Standard Schema Using the iDRAC6 Web-Based Interface

1 Open a supported Web browser window.

2 Log in to the iDRAC6 Web-based interface.

3 Expand the **System** tree and click **Remote Access**.

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

5 Scroll to the bottom of the **Active Directory Configuration and Management** page, and click **Configure Active Directory**.

The **Step 1 of 4 Active Directory Configuration and Management** page is displayed.

6 Under **Certificate Settings**, check **Enable Certificate Validation** if you want to validate the SSL certificate of your Active Directory servers; otherwise, go to step 9.

7 Under **Upload Active Directory CA Certificate**, type the file path of the certificate or browse to find the certificate file.

   NOTE: You must type the absolute file path, which includes the full path and the complete file name and file extension.

8 Click **Upload**.

The certificate information for the valid Active Directory CA certificate is displayed.

9 Under **Upload Kerberos Keytab**, type the path of the keytab file or browse to locate the file. Click **Upload**. The Kerberos keytab is uploaded into the iDRAC6.

10 Click **Next** to go to the **Step 2 of 4 Active Directory Configuration and Management**.

11 Select **Enable Active Directory**.

12 Select **Enable Single Sign-On** if you want to log into iDRAC6 without entering your domain user authentication credentials, such as user name and password.

13 Click **Add** to enter the user domain name.

14 Type the user domain name in the prompt and click **OK**.

15 Type the **Timeout** time in seconds to specify the time the iDRAC6 will wait for Active Directory responses. The default is 120 seconds.

16 Type the Domain Controller Server Address. You can enter up to three Active Directory servers for login processing, but you are required to configure at least one server by entering the IP address or the FQDN. iDRAC6 tries to connect to each configured server until a connection is established.

> **NOTE:** The FQDN or IP address that you specify in this field should match the Subject or Subject Alternative Name field of your domain controller certificate if you have certificate validation enabled.

17 Click **Next** to go to the **Step 3 of 4 Active Directory Configuration and Management**.

18 Under **Schema Selection**, click **Standard Schema.**

19 Click **Next** to go to the **Step 4a of 4 Active Directory Configuration and Management** page.

20 Under **Standard Schema Settings**, type the Global Catalog server address to specify its location in Active Directory. You must configure the location of at least one Global Catalog server.

> **NOTE:** The FQDN or IP address that you specify in this field should match the Subject or Subject Alternative Name field of your domain controller certificate if you have certificate validation enabled.

NOTE: The Global Catalog server is only required for standard schema in the case that the user accounts and the role groups are in different domains. And, in this multiple domain case, only the Universal Group can be used.

21 Under **Role Groups**, click a **Role Group**.

The **Step 4b of 4** page is displayed.

22 Specify the **Role Group Name**.

The **Role Group Name** identifies the role group in Active Directory associated with the iDRAC.

23 Specify the **Role Group Domain**, which is the domain of the Role Group.

24 Specify the **Role Group Privileges** by selecting the **Role Group Privilege Level**. For example, if you select **Administrator**, all of the privileges are selected for that level of permission.

25 Click **Apply** to save Role Group settings.

The iDRAC6 Web server automatically returns you to the **Step 4a of 4 Active Directory Configuration and Management** page where your settings are displayed.

26 Repeat step 20 through step 25 to configure additional Role Groups

27 Click **Finish** to return to the **Active Directory Configuration and Management** page.

28 Click **Test Settings** to check the Active Directory Standard Schema settings.

29 Type your iDRAC6 user name and password.

The test results and the test log are displayed. For additional information, see "Testing Your Configurations."

NOTE: You must have a DNS server configured properly on iDRAC to support Active Directory login. Click **Remote Access→Configuration→Network** page to configure DNS server(s) manually or use DHCP to get DNS server(s).

You have completed the Active Directory configuration with Standard Schema.

Configuring Active Directory With Standard Schema Using RACADM

Use the following commands to configure the iDRAC Active Directory Feature with Standard Schema using the RACADM CLI instead of the Web-based interface.

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

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

```
racadm config -g cfgActiveDirectory -o cfgADType 2
```

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

```
racadm config -g cfgStandardSchema -i <index> -o
cfgSSADRoleGroupDomain <fully qualified domain
name>
```

```
racadm config -g cfgStandardSchema -i <index> -o
cfgSSADRoleGroupPrivilege <Bit Mask Number for
specific user permissions>
```

NOTE: For Bit Mask Number values, see Table B-2.

```
racadm config -g cfgActiveDirectory -o
cfgDomainController1 <fully qualified domain name
or IP address of the domain controller>
```

```
racadm config -g cfgActiveDirectory -o
cfgDomainController2 <fully qualified domain name
or IP address of the domain controller>
```

```
racadm config -g cfgActiveDirectory -o
cfgDomainController3 <fully qualified domain name
or IP address of the domain controller>
```

NOTE: The FQDN or IP address that you specify in this field should match the Subject or Subject Alternative Name field of your domain controller certificate if you have certificate validation enabled.

NOTE: Enter the FQDN of the domain controller, *not* just the FQDN of the domain. For example, enter servername.dell.com instead of dell.com.

 NOTE: At least one of the 3 addresses is required to be configured. iDRAC6 attempts to connect to each of the configured addresses one-by-one until a successful connection is made. With Standard Schema, these are the addresses of the domain controllers where the user accounts and the role groups are located.

```
racadm config -g cfgActiveDirectory -o cfgGlobal
Catalog1 <fully qualified domain name or IP
address of the domain controller>
racadm config -g cfgActiveDirectory -o cfgGlobal
Catalog2 <fully qualified domain name or IP
address of the domain controller>
racadm config -g cfgActiveDirectory -o cfgGlobal
Catalog3 <fully qualified domain name or IP
address of the domain controller>
```

 NOTE: The Global Catalog server is only required for standard schema in the case that the user accounts and the role groups are in different domains. And, in this multiple domain case, only the Universal Group can be used.

 NOTE: The FQDN or IP address that you specify in this field should match the Subject or Subject Alternative Name field of your domain controller certificate if you have certificate validation enabled.

If you want to disable the certificate validation during SSL handshake, type the following RACADM command:

```
racadm config -g cfgActiveDirectory -o
cfgADCertValidationEnable 0
```

In this case, no Certificate Authority (CA) certificate needs to be uploaded.

If you want to enforce the certificate validation during SSL handshake, type the following RACADM command:

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

In this case, you must also upload the CA certificate using the following RACADM command:

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

Using the following RACADM command may be optional. See "Importing the iDRAC6 Firmware SSL Certificate" for additional information.

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

2 If DHCP is enabled on the iDRAC6 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 iDRAC6 or you want manually to input your DNS IP address, 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 If you want to configure a list of user domains so that you only need to enter the user name during login to the Web-based interface, type the following command:

```
racadm config -g cfgUserDomain -o
cfgUserDomainName -i <index>
```

Up to 40 user domains can be configured with index numbers between 1 and 40.

See "Using Active Directory to Log In to the iDRAC6" for details about user domains.

Testing Your Configurations

If you want to verify whether your configuration works, or if you need to diagnose the problem with your failed Active Directory login, you can test your settings from the iDRAC6 Web-based interface.

After you finish configuring settings in the iDRAC6 Web-based interface, click **Test Settings** at the bottom of the page. You will be required to enter a test user's name (for example, username@domain.com) and password to run the test. Depending on your configuration, it may take some time for all of the test steps to complete and display the results of each step. A detailed test log will display at the bottom of the results page.

If there is a failure in any step, examine the details in the test log to identify the problem and a possible solution. For most common errors, see "Frequently Asked Questions about Active Directory."

If you need to make changes to your settings, click the **Active Directory** tab and change the configuration step-by-step.

Enabling SSL on a Domain Controller

When the iDRAC authenticates users against an Active Directory domain controller, it starts an SSL session with the domain controller. At this time, the domain controller should publish a certificate signed by the Certificate Authority (CA)—the root certificate of which is also uploaded into the iDRAC. In other words, for iDRAC to be able to authenticate to *any* domain controller—whether it is the root or the child domain controller—that domain controller should have an SSL-enabled certificate signed by the domain's CA.

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. 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 to the iDRAC

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

✐ **NOTE:** If you are using a standalone CA, 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 systems) and select **Add/Remove Snap-in**.

5 In the **Add/Remove Snap-In** window, click **Add**.

6 In the **Standalone Snap-In** window, select **Certificates** and click **Add**.

7 Select **Computer account** and click **Next**.

8 Select **Local Computer** and click **Finish**.

9 Click **OK**.

10 In the **Console 1** window, expand the **Certificates** folder, expand the **Personal** folder, and click the **Certificates** folder.

11 Locate and right-click the root CA certificate, select **All Tasks**, and click **Export...** .

12 In the **Certificate Export Wizard**, click **Next**, and select **No do not export the private key**.

13 Click **Next** and select **Base-64 encoded X.509 (.cer)** as the format.

14 Click **Next** and save the certificate to a directory on your system.

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

    To upload the certificate using RACADM, see "Configuring Active Directory With Extended Schema Using the iDRAC6 Web-Based Interface" or "Configuring Active Directory With Standard Schema Using RACADM."

To upload the certificate using the Web-based interface, see "Configuring Active Directory With Extended Schema Using the iDRAC6 Web-Based Interface" or "Configuring Active Directory With Standard Schema Using the iDRAC6 Web-Based Interface."

Importing the iDRAC6 Firmware SSL Certificate

NOTE: If the Active Directory Server is set to authenticate the client during an SSL session initialization phase, you need to upload the iDRAC Server certificate to the Active Directory Domain controller as well. This additional step is not required if the Active Directory does not perform a client authentication during an SSL session's initialization phase.

Use the following procedure to import the iDRAC6 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 iDRAC6 firmware SSL certificate is signed by a well-known CA and the certificate of that CA is already in the domain controller's Trusted Root Certificate Authority list, 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 iDRAC controllers are shipped with a default self-signed certificate.

To download the iDRAC SSL certificate, run the following RACADM command:

```
racadm sslcertdownload -t 0x1 -f <RAC SSL 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 iDRAC 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 iDRAC6

You can use Active Directory to log in to the iDRAC6 using one of the following methods:

- Web-based interface
- Remote RACADM
- Serial or telnet console

The login syntax is the same for all three methods:

`<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, because these names cannot be resolved.

If you log in from the Web-based interface and you have configured user domains, the Web-based interface login page will list all the user domains in the pull-down menu for your to choose. If you select a user domain from the pull-down menu, you should only enter the user name. If you select **This iDRAC**, you can still log in as an Active Directory user if you use the login syntax described above in "Using Active Directory to Log In to the iDRAC6."

You can also log into the iDRAC6 using the Smart Card. For more information, see "Logging Into the iDRAC6 Using the Smart Card."

📝 **NOTE:** The Windows 2008 Active Directory server supports only a <username>@<domain_name> string with a maximum length of 256 characters.

Using Active Directory Single Sign-On

You can enable the iDRAC6 to use Kerberos—a network authentication protocol—to enable single sign-on. For more information on setting up the iDRAC6 to use the Active Directory single sign-on feature, see "Enabling Kerberos Authentication."

Configuring the iDRAC6 to Use Single Sign-On

1   Click **Remote Access→Configuration** tab→**Active Directory** subtab→ select **Configure Active Directory**.

2   On the **Step 2 of 4 Active Directory Configuration and Management** page, select **Enable Single Sign-On**. The **Enable Single Sign-On** option is enabled only if you have selected the **Enable Active Directory** option.

The **Enable Single Sign-On** option enables you to log into the iDRAC6 directly after logging into your workstation without entering your domain user authentication credentials, such as user name and password. To log into the iDRAC6 using this feature, you should have already logged into your system using a valid Active Directory user account. Also you should have already configured the user account to log into the iDRAC6 using the Active Directory credentials. The iDRAC6 uses the cached Active Directory credentials to log you in.

To enable single sign–on using the CLI, run the racadm command:

```
racadm -g cfgActiveDirectory -o cfgADSSOEnable 1
```

Logging Into the iDRAC6 Using Single Sign-On

1 Log into your workstation using your network account.

2 To access the iDRAC6 Web page, type:

   `https://<IP address>`

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

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

   where *IP address* is the IP address for the iDRAC6 and *port number* is the HTTPS port number.

   The iDRAC6 single sign-on page is displayed.

3 Click **Login**.

The iDRAC6 logs you in, using your credentials that were cached in the operating system when you logged in using your valid Active Directory account.

Frequently Asked Questions about Active Directory

My Active Directory login failed. How can I troubleshoot the problem?

iDRAC6 provides a diagnostic tool from the Web-based interface. Log in as a local user with administrator privilege from the Web-based interface. Click **Remote Access→Configuration→Active Directory**. Scroll to the bottom of the **Active Directory Configuration and Management** page and click **Test Settings**. Enter a test user name and password, and click **Start Test**. iDRAC6 runs the tests step-by-step and displays the result for each step. A detailed test result is also logged to help you resolve any problems. Click the **Active Directory** tab to return to the **Active Directory Configuration and Management** page. Scroll to the bottom of the page and click **Configure Active Directory** to change your configuration and run the test again until the test user passes the authorization step.

I enabled certificate validation but my Active Directory login failed.
I ran the diagnostics from the GUI and the test result shows the following
error message:

ERROR: Can't contact LDAP server, error:14090086:SSL
routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed:
Please check the correct Certificate Authority (CA) certificate has been
uploaded to iDRAC. Please also check if the iDRAC date is within the valid
period of the certificates and if the Domain Controller Address configured
in iDRAC matches the subject of the Directory Server Certificate.

What could be the problem and how can I fix it?

If certificate validation is enabled, iDRAC6 uses the uploaded CA certificate
to verify the directory server certificate when iDRAC6 establishes the SSL
connection with the directory server. The most common reasons for failing
certification validation are:

1   The iDRAC6 date is not within the valid period of the server certificate or
    CA certificate. Please check your iDRAC6 time and the valid period of
    your certificate.

2   The Domain Controller Addresses configured in iDRAC6 do not match
    the Subject or Subject Alternative Name of the directory server certificate.
    If you are using an IP address, please read the following question and
    answer. If you are using FQDN, please make sure you are using the FQDN
    of the domain controller, not the domain, for example,
    servername.example.com instead of example.com.

I'm using an IP address for a Domain Controller Address and I failed
certificate validation. What's the problem?

Check the Subject or Subject Alternative Name field of your domain controller certificate. Usually Active Directory uses the hostname, not the IP address, of the domain controller in the Subject or Subject Alternative Name field of the domain controller certificate. You can fix the problem in several ways:

1 Configure the hostname (FQDN) of the domain controller as the *domain controller address(es)* on iDRAC6 to match the Subject or Subject Alternative Name of the server certificate.

2 Re-issue the server certificate to use an IP address in the Subject or Subject Alternative Name field so it matches the IP address configured in iDRAC6.

3 Disable certificate validation if you choose to trust this domain controller without certificate validation during the SSL handshake.

I am using extended schema in a multiple domain environment. How should I configure the domain controller address(es)?

This should be the host name (FQDN) or the IP address of the domain controller(s) that serves the domain in which the iDRAC6 object resides.

When do I need to configure Global Catalog Address(es)?

If you are using extended schema, the Global Catalog Address is not used.

If you are using standard schema and users and role groups are from different domains, Global Catalog Address(es) are required. In this case, only Universal Group can be used.

If you are using standard schema and all the users and all the role groups are in the same domain, Global Catalog Address(es) are not required.

How does standard schema query work?

iDRAC6 connects to the configured domain controller address(es) first, if the user and role groups are in that domain, the privileges will be saved.

If Global Controller Address(es) is configured, iDRAC6 continues to query the Global Catalog. If additional privileges are retrieved from the Global Catalog, these privileges will be accumulated.

Does iDRAC6 always use LDAP over SSL?

Yes. All the transportation is over secure port 636 and/or 3269.

During *test setting*, iDRAC6 does a LDAP CONNECT only to help isolate the problem, but it does not do an LDAP BIND on an insecure connection.

Why does iDRAC6 enable certificate validation by default?

iDRAC6 enforces strong security to ensure the identity of the domain controller that iDRAC6 connects to. Without certificate validation, a hacker could spoof a domain controller and hijack the SSL connection. If you choose to trust all the domain controllers in your security boundary without certificate validation, you can disable it through the GUI or the CLI.

Does iDRAC6 support the NetBIOS name?

Not in this release.

What should I check if I can not log into the iDRAC6 using Active Directory?

You can diagnose the problem by clicking **Test Settings** at the bottom of the **Active Directory Configuration and Management** page in the iDRAC6 Web-based interface. Then, you can fix the specific problem indicated by the test results. For additional information, see "Testing Your Configurations."

Most common issues are explained in this section; however, in general you should check the following:

1 Ensure that you use the correct user domain name during a login and not the NetBIOS name.

2 If you have a local iDRAC6 user account, log into the iDRAC6 using your local credentials.

    After you are logged in:

    a Ensure that you have checked the **Enable Active Directory** box on the iDRAC6 **Active Directory Configuration and Management** page.

    b Ensure that the DNS setting is correct on the iDRAC6 Networking configuration page.

    c Ensure that you have uploaded the right Active Directory root CA certificate to the iDRAC6 if you enabled certificate validation. Ensure that the iDRAC6 time is within the valid period of the CA certificate.

    d If you are using the Extended Schema, ensure that the **iDRAC6 Name** and **iDRAC6 Domain Name** match your Active Directory environment configuration.

    If you are using the Standard Schema, ensure that the **Group Name** and **Group Domain Name** match your Active Directory configuration.

3 Check the Domain Controller SSL certificates to ensure that the iDRAC6 time is within the valid period of the certificate.

8

Configuring Smart Card Authentication

The iDRAC6 supports the two factor authentication (TFA) feature by enabling **Smart Card Logon**.

The traditional authentication schemes use user name and password to authenticate users. This provides minimal security.

TFA, on the other hand, provides a higher-level of security by making the users provide two factors of authentication - what you have and what you know—what you have is the Smart Card, a physical device, and what you know—a secret code like a password or PIN.

The two-factor authentication requires users to verify their identities by providing *both* factors.

Configuring Smart Card Login in iDRAC6

To enable the iDRAC6 Smart Card logon feature from the Web-based interface, go to **Remote Access→Configuration→Smart Card** and select **Enable**.

If you:

- **Enable** or **Enable with Remote Racadm**, you are prompted for a Smart Card logon during any subsequent logon attempts using the Web-based interface.

    When you select **Enable**, all command line interface (CLI) out-of-band interfaces, such as telnet, SSH, serial, remote RACADM, and IPMI over LAN, are disabled because these services support only single-factor authentication.

    When you select **Enable with Remote Racadm**, all CLI out-of-band interfaces, except remote RACADM, are disabled.

> ℹ️ **NOTE:** Dell recommends that the iDRAC6 administrator use the **Enable with Remote Racadm** setting only to access the iDRAC6 Web-based interface to run scripts using the remote RACADM commands. If the administrator does not need to use the remote RACADM, Dell recommends the **Enabled** setting for Smart Card logon. Also, ensure that the iDRAC6 local user configuration and/or Active Directory configuration is complete before enabling **Smart Card Logon**.

- **Disable** Smart Card configuration (default). This selection disables the TFA Smart Card Logon feature and the next time you login to the iDRAC6 GUI, you will be prompted for a Microsoft® Active Directory® or local logon username and password, which occurs as the default login prompt from the Web interface.

- **Enable CRL check for Smart Card Logon**, the user's iDRAC certificate, which is downloaded from the Certificate Revocation List (CRL) distribution server is checked for revocation in the CRL.

> ℹ️ **NOTE:** The CRL distribution servers are listed in the Smart Card certificates of the users.

Configuring Local iDRAC6 Users for Smart Card Logon

You can configure the local iDRAC6 users to log into the iDRAC6 using the Smart Card. Click **Remote Access→Configuration→Users**.

However, before the user can log into the iDRAC6 using the Smart Card, you must upload the user's Smart Card certificate and the trusted Certificate Authority (CA) certificate to the iDRAC6.

Exporting the Smart Card Certificate

You can obtain the user's certificate by exporting the Smart Card certificate using the card management software (CMS) from the Smart Card to a file in the Base64 encoded form. You can usually obtain the CMS from the vendor of the Smart Card. This encoded file should be uploaded as the user's certificate to the iDRAC6. The trusted Certificate Authority that issues the Smart Card user certificates should also export the CA certificate to a file in the Base64 encoded form. You should upload this file as the

trusted CA certificate for the user. Configure the user with the username that forms the user's User Principal Name (UPN) in the Smart Card certificate.

📝 **NOTE:** To log into the iDRAC6, the user name that you configure in the iDRAC6 should have the same case as the User Principal Name (UPN) in the Smart Card certificate.

For example, in case the Smart Card certificate has been issued to the user, "sampleuser@domain.com," the username should be configured as "sampleuser."

Configuring Active Directory Users for Smart Card Logon

To configure the Active Directory users to log into the iDRAC6 using the Smart Card, the iDRAC6 administrator should configure the DNS server, upload the Active Directory CA certificate to the iDRAC6, and enable the Active Directory logon. See "Using the iDRAC6 With Microsoft Active Directory" for more information on how to set up Active Directory users.

📝 **NOTE:** If the Smart Card user is present in Active Directory, an Active Directory password is required along with the Smart Card PIN.

You can configure the Active Directory from **Remote Access→ Configuration→Active Directory**.

Configuring Smart Card

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

1 Expand the **System** tree and click **Remote Access**.

2 Click the **Configuration** tab and then click **Smart Card**.

3 Configure the Smart Card logon settings.

   Table 8-1 provides information about the **Smart Card** page settings.

4 Click **Apply Changes**.

Table 8-1. Smart Card Settings

Setting	Description
Configure Smart Card Logon	• **Disabled** — Disables Smart Card logon. Subsequent logins from the graphical user interface (GUI) display the regular login page. All command line out-of-band interfaces including secure shell (SSH), Telnet, Serial, and remote RACADM are set to their default state.
	• **Enabled** — Enables Smart Card logon. After applying the changes, logout, insert your Smart Card and then click **Login** to enter your Smart Card PIN. Enabling Smart Card logon disables all CLI out-of-band interfaces including SSH, Telnet, Serial, remote RACADM, and IPMI over LAN.
	• **Enabled with Remote Racadm** — Enables Smart Card logon along with remote RACADM. All other CLI out-of-band interfaces are disabled.
	NOTE: The Smart Card logon requires you to configure the local iDRAC6 users with the appropriate certificates. If the Smart Card logon is used to log in a Microsoft Active Directory user, then you must ensure that you configure the Active Directory user certificate for that user. You can configure the user certificate in the **Users→User Main Menu** page.
Enable CRL check for Smart Card Logon	This check is available only for Smart Card local users. Select this option if you want iDRAC6 to check the Certificate Revocation List (CRL) for revocation of the user's Smart Card certificate. For the CRL feature to work, the iDRAC6 must have a valid DNS IP address configured as part of its network configuration. You can configure the DNS IP address in iDRAC6 under **Remote Access→Configuration→ Network**.
	The user will not be able to login if:
	• The user certificate is listed as revoked in the CRL file.
	• iDRAC6 is not able to communicate with the CRL distribution server.
	• iDRAC6 is not able to download the CRL.
	NOTE: You must correctly configure the IP address of the DNS server in the **Configuration→Network** page for this check to succeed.

Logging Into the iDRAC6 Using the Smart Card

The iDRAC6 Web interface displays the Smart Card logon page for all users who are configured to use the Smart Card.

NOTE: Ensure that the iDRAC6 local user and/or Active Directory configuration is complete before enabling the Smart Card Logon for the user.

NOTE: Depending on your browser settings, you may be prompted to download and install the Smart Card reader ActiveX plug-in when using this feature for the first time.

1 Access the iDRAC6 Web page using https.

    `https://<IP address>`

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

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

    where `IP address` is the IP address for the iDRAC6 and `port number` is the HTTPS port number.

    The iDRAC6 Login page is displayed prompting you to insert the Smart Card.

2 Insert the Smart Card into the reader and click **Login**.

    The iDRAC6 prompts you for the Smart Card's PIN.

3 Enter the Smart Card PIN for local Smart Card users and if the user is not created locally, iDRAC6 will prompt to enter the password for the user's Active Directory account.

NOTE: If you are an Active Directory user for whom the **Enable CRL check for Smart Card Logon** is selected, iDRAC6 attempts to download the CRL and checks the CRL for the user's certificate. The login through Active Directory fails if the certificate is listed as revoked in the CRL or if the CRL cannot be downloaded for any reason.

You are logged into the iDRAC6.

Logging Into the iDRAC6 Using Active Directory Smart Card Authentication

1 Log into the iDRAC6 using https.

   `https://<IP address>`

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

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

   where *IP address* is the IP address for the iDRAC6 and *port number* is the HTTPS port number.

   The iDRAC6 Login page is displayed prompting you to insert the Smart Card.

2 Insert the Smart Card and click **Login**.

   The PIN pop-up dialog box is displayed.

3 Enter the PIN and click **OK**.

4 Enter the user's Active Directory password to authenticate the user and click **OK**.

   You are logged into the iDRAC6 with your credentials as set in Active Directory.

   NOTE: If the Smart Card user is present in Active Directory, an Active Directory password is required along with the SC PIN. In future releases, the Active Directory password may not be required.

Troubleshooting the Smart Card Logon in iDRAC6

Use the following tips to debug an inaccessible Smart Card:

ActiveX plug-in unable to detect the Smart Card reader

Ensure that the Smart Card is supported on the Microsoft Windows® operating system. Windows supports a limited number of Smart Card cryptographic service providers (CSPs).

Tip: As a general check to see if the Smart Card CSPs are present on a particular client, insert the Smart Card in the reader at the Windows logon (Ctrl-Alt-Del) screen and check to see if Windows detects the Smart Card and displays the PIN dialog-box.

Incorrect Smart Card PIN

Check to see if the Smart Card has been locked out due to too many attempts with an incorrect PIN. In such cases, the issuer of the Smart Card in the organization will be able to help you get a new Smart Card.

Unable to Log into Local iDRAC6

If a local iDRAC6 user cannot log in, check if the username and the user certificates uploaded to the iDRAC6 have expired. The iDRAC6 trace logs may provide important log messages regarding the errors; although the error messages are sometimes intentionally ambiguous due to security concerns.

Unable to Log into iDRAC6 as an Active Directory User

If you cannot log into the iDRAC6 as an Active Directory user, try to log into the iDRAC6 without enabling the Smart Card logon. If you have enabled the CRL check, try the Active Directory logon without enabling the CRL check. The iDRAC6 trace log should provide important messages in case of CRL failure.

You also have the option of disabling the Smart Card Logon through the local racadm using the following command:

```
racadm config -g cfgActiveDirectory -o
cfgADSmartCardLogonEnable 0
```

9

Enabling Kerberos Authentication

Kerberos is a network authentication protocol that allows systems to communicate securely over a non-secure network. It achieves this by allowing the systems to prove their authenticity. To keep with the higher authentication enforcement standards, iDRAC6 now supports Kerberos based Active Directory® authentication to support Active Directory Smart Card and single sign-on logins.

Microsoft® Windows® 2000, Windows XP, Windows Server® 2003, Windows Vista®, and Windows Server 2008 use Kerberos as their default authentication method.

The iDRAC6 uses Kerberos to support two types of authentication mechanisms—Active Directory single sign-on and Active Directory Smart Card logins. For single-sign on login, iDRAC6 uses the user credentials cached in the operating system after the user has logged in using a valid Active Directory account.

For Active Directory smart card login, iDRAC6 uses smart card-based two factor authentication (TFA) as credentials to enable an Active Directory login. This is the follow on feature to the local Smart Card authentication.

Kerberos authentication on iDRAC6 fails if the iDRAC6 time differs from the Domain Controller time. A maximum offset of 5 minutes is allowed. To enable successful authentication, synchronize the server time with the Domain Controller time and then **reset** the iDRAC6.

You can also use the following RACADM time zone offset command to synchronize the time:

```
racadm config -g cfgRacTuning -o
cfgRacTuneTimeZoneOffset <offset value>
```

Prerequisites for single sign-on and Active Directory Authentication Using Smart Card

- Configure the iDRAC6 for Active Directory login. For more information, see "Using Active Directory to Log In to the iDRAC6."

- Register the iDRAC6 as a computer in the Active Directory root domain.

  a Click **Remote Access**→**Configuration** tab→**Network** subtab.

  b Provide a valid **Preferred/Alternate DNS Server** IP address. This value is the IP address of the DNS that is part of the root domain, which authenticates the Active Directory accounts of the users.

  c Select **Register iDRAC on DNS**.

  d Provide a valid **DNS Domain Name**.

  See the *iDRAC6 Online Help* for more information.

To support the two new types of authentication mechanisms, iDRAC6 supports the configuration to enable itself as a kerberized service on a Windows Kerberos network. The Kerberos configuration on iDRAC6 entails the same steps as configuring a non–Windows Server Kerberos service as a security principal in Windows Server Active Directory.

The Microsoft tool **ktpass** (supplied by Microsoft as part of the server installation CD/DVD) is used to create the Service Principal Name (SPN) bindings to a user account and export the trust information into a MIT–style Kerberos *keytab* file, which enables a trust relation between an external user or system and the Key Distribution Centre (KDC). The keytab file contains a cryptographic key, which is used to encrypt the information between the server and the KDC. The ktpass tool allows UNIX–based services that support Kerberos authentication to use the interoperability features provided by a Windows Server Kerberos KDC service.

The keytab obtained from the ktpass utility is made available to the iDRAC6 as a file upload and is enabled to be a kerberized service on the network.

Since the iDRAC6 is a device with a non-Windows operating system, run the **ktpass** utility—part of Microsoft Windows—on the Domain Controller (Active Directory server) where you want to map the iDRAC6 to a user account in Active Directory.

For example, use the following **ktpass** command to create the Kerberos keytab file:

```
C:\>ktpass -princ
HOST/dracname.domainname.com@DOMAINNAME.COM -
mapuser dracname -crypto DES-CBC-MD5 -ptype
KRB5_NT_PRINCIPAL -pass * -out c:\krbkeytab
```

The encryption type that iDRAC6 uses for Kerberos authentication is DES-CBC-MD5. The principal type is KRB5_NT_PRINCIPAL. The properties of the user account that the Service Principal Name is mapped to should have the following account properties enabled:

- Use DES encryption types for this account
- Do not require Kerberos preauthentication

NOTE: It is recommended that you use the latest **ktpass** utility to create the keytab file.

This procedure will produce a keytab file that you should upload to the iDRAC6.

NOTE: The keytab contains an encryption key and should be kept secure.

For more information on the **ktpass** utility, see the Microsoft website at: **http://technet2.microsoft.com/windowsserver/en/library/64042138-9a5a-4981-84e9-d576a8db0d051033.mspx?mfr=true**

- The iDRAC6 time should be synchronized with the Active Directory domain controller.

Configuring the iDRAC6 for single sign-on and Active Directory Authentication Using Smart Card

Upload the keytab obtained from the Active Directory root domain, to the iDRAC6:

1   Click **Remote Access→Configuration** tab→**Active Directory** subtab→ Click **Configure Active Directory**.

2   Select **Upload Kerberos Keytab** and click **Next**.

3   On the **Kerberos Keytab Upload** page, select the keytab file to upload and click **Apply**.

You can also upload the file to iDRAC6 by using CLI racadm commands. The following command uploads the keytab file to iDRAC6:

```
racadm krbkeytabupload -f <filename>
```

where <filename> is the name of the keytab file. The racadm command is supported by both local and remote racadm.

Configuring Active Directory Users for single sign-on Logon

Before using the Active Directory single sign-on logon feature, ensure that you have already configured the iDRAC6 for Active Directory login and the domain user account that you will use to login into the system has been enabled for iDRAC6 Active Directory login.

Also ensure that you have enabled the Active Directory logon setting. See "Using the iDRAC6 With Microsoft Active Directory" for more information on how to set up Active Directory users. You must also enable the iDRAC6 to be a kerberized service by uploading a valid *keytab* file obtained from the Active Directory root domain, to the iDRAC6.

See "Configuring the iDRAC6 to Use Single Sign-On" for information on how to enable single sign–on using the GUI and the CLI.

Logging Into the iDRAC6 Using single sign-on for Active Directory Users

> **NOTE:** To log into the iDRAC6, ensure that you have the latest runtime components of Microsoft Visual C++ 2005 Libraries. For more information, see the Microsoft website.

1 Log into your system using a valid Active Directory account.

2 Type the web address of the iDRAC6 in the address bar of your browser.

> **NOTE:** Depending on your browser settings, you may be prompted to download and install the single sign-on ActiveX plug-in when using this feature for the first time.

You are logged into the iDRAC6 with appropriate Microsoft Active Directory privileges if:

- You are a Microsoft Active Directory user.
- You are configured in the iDRAC6 for Active Directory login.
- The iDRAC6 is enabled for Kerberos Active Directory authentication.

Configuring Active Directory Users for Smart Card Logon

Before using the Active Directory Smart Card logon feature, ensure that you have already configured the iDRAC6 for Active Directory login and the user account that has been issued the Smart Card has been enabled for iDRAC6 Active Directory login.

Also ensure that you have enabled the Active Directory logon setting. See "Using the iDRAC6 With Microsoft Active Directory" for more information on how to set up Active Directory users. You must also enable the iDRAC6 to be a kerberized service by uploading a valid *keytab* file obtained from the Active Directory root domain, to the iDRAC6.

10

Using GUI Console Redirection

This section provides information about using the iDRAC6 console redirection feature.

Overview

The iDRAC6 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 iDRAC6-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.

NOTE: If a console redirection session is already open from the management station to the iDRAC6, an attempt to open a new session from the same management station to that iDRAC6 will result in the existing session becoming active. A new session will not be generated.

NOTE: Multiple console redirection sessions can be opened from a single management station to multiple iDRAC6 controllers simultaneously.

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 four simultaneous console redirection sessions are supported. All sessions view the same managed server console simultaneously.
- Only one session can be opened to a remote server (iDRAC6) from the same client console (management station). However, multiple sessions to multiple remote servers are possible from the same client.
- 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.

The first console redirection session to the iDRAC is a full access session. If a second user requests a console redirection session, the first user is notified and is given the option to reject, **allow as read-only,** or **approve**. The second user is notified that another user has control. The first user must respond within thirty seconds or access is refused to the second user.

All of the **allow as read-only** sessions automatically terminate when the last full access session is terminated.

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"
- "Configuring a Supported Web Browser"

NOTE: Java Run Time Environment must be installed on the management station for the console redirection feature to work.

2 If you are using Internet Explorer, ensure that the browser is enabled to download encrypted content as follows:

- Go to Internet Explorer Options or Settings and select **Tools→ Internet Options→Advanced**.
- Scroll to **Security** and uncheck this option:

  ```
  Do not save encrypted pages to disk
  ```

3 Dell recommends that you configure your monitor display resolution to 1280x1024 pixels or higher.

NOTE: If your system is running a Linux operating system, an X11 console may not be viewable on the local monitor. Pressing <Ctrl><Alt><F1> at the iDRAC KVM will switch Linux to a text console.

NOTE: Occasionally, you may encounter the following Java Script Compilation Error: "Expected: ;". To resolve this issue, adjust the network settings to use "Direct connection" in JavaWebStart: "Edit->Preferences->General->Network Settings" and choose "Direct Connection" instead of "Use browser settings."

Supported Screen Resolutions and Refresh Rates

Table 10-1 lists the supported screen resolutions and corresponding refresh rates for a console redirection session that is running on the managed server.

Table 10-1.   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 Console Redirection in the iDRAC6 Web Interface

To configure console redirection in the iDRAC6 Web interface, perform the following steps:

1 Click **System→Console/Media→Configuration** to configure iDRAC console redirection settings.

2 Configure the console redirection properties. Table 10-2 describes the settings for console redirection.

3 When completed, click **Apply Changes**.

4 Click the appropriate button to continue. See Table 10-3.

Table 10-2. Console Redirection Configuration Properties

Property	Description
Enabled	Click to enable or disable Console Redirection. If this option is checked, it indicates that Console Redirection is enabled. The default option is **enabled**. **NOTE:** Checking or clearing the **Enabled** option once after the virtual KVM is launched may disconnect all your existing virtual KVM sessions.
Max Sessions	Displays the maximum number of Console Redirection sessions that are possible, 1 to 4. 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.
Remote Presence Port	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**. **NOTE:** Modifying the **Remote Presence Port** value once after the virtual KVM is launched may disconnect all your existing virtual KVM sessions.
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. **NOTE:** Enabling or disabling the **Video Encryption Enabled** option once after the virtual KVM is launched may disconnect all your existing virtual KVM sessions.
Local Server Video Enabled	Checked indicates that output to the iDRAC KVM 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."

The buttons in Table 10-3 are available on the **Configuration** page.

Table 10-3. Configuration Page Buttons

Button	Definition
Print	Prints the page
Refresh	Reloads the **Configuration** page
Apply Changes	Saves any new or changed settings

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 is displayed 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→Console/Media→Console Redirection and Virtual Media**.

2 Use the information in Table 10-4 to ensure that a console redirection session is available.

   If you want to reconfigure any of the property values displayed, see "Configuring Console Redirection in the iDRAC6 Web Interface."

Table 10-4. Console Redirection

Property	Description
Console Redirection Enabled	Yes/No (checked\unchecked)
Video Encryption Enabled	Yes/No (checked\unchecked)
Max Sessions	Displays the maximum number of supported console redirection sessions
Active Sessions	Displays the current number of active console redirection sessions

Table 10-4. Console Redirection *(continued)*

Property	Description
Local Server Video Enabled	Yes = Enabled; No = Disabled.
Remote Presence Port	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.

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

The buttons in Table 10-5 are available on the **Console Redirection** and **Virtual Media** page.

Table 10-5. Console Redirection and Virtual Media Page Buttons

Button	Definition
Refresh	Reloads the **Console Redirection and Virtual Media** page
Launch Viewer	Opens a console redirection session on the targeted remote system
Print	Prints the **Console Redirection and Virtual Media** 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 iDRAC6 and the remote system's desktop is displayed in the iDRAC KVM Viewer Application.

4 Two mouse pointers appear in the viewer window: one for the remote system and one for your local system. You can change to a single cursor by selecting the **Single Cursor** option under **Tools** in the iDRAC KVM menu.

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.

NOTE: If the remote server is powered off, the message, No Signal, will be displayed.

The Video Viewer provides various control adjustments such as mouse synchronization, snapshots, keyboard macros, and access to Virtual Media. For more information about these functions, click **System**→**Console/Media** and click **Help** on the **Console Redirection and Virtual Media** page.

When you start a console redirection session and the Video Viewer is displayed, you may need to synchronize the mouse pointers.

Disabling or Enabling Local Server Video

You can configure the iDRAC6 to disallow iDRAC KVM connections using the iDRAC6 Web interface.

If you want to 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 Configuration** page.

NOTE: By disabling (turning off) the local video on the server, the monitor, keyboard, and mouse connected to the iDRAC KVM are still enabled.

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 iDRAC6. See "Accessing the Web Interface" for more information.

2 Click **System**→**Console/Media**→**Configuration**.

3 To disable (turn off) local video on the server, uncheck the **Local Server Video Enabled** checkbox on the **Configuration** page, and then click **Apply**. The default value is OFF.

   NOTE: If the local server video is turned ON, it will take 15 seconds to turn OFF.

4 To enable (turn on) local video on the server, check the **Local Server Video Enabled** checkbox on the **Configuration** page, and then click **Apply**.

Frequently Asked Questions about Console Redirection

Table 10-6 lists frequently asked questions and answers.

Table 10-6.   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, after a local video turn **ON** request is received by iDRAC6, the video is turned on instantly.
Can the local user also turn off the video?	When the local console is disabled, the local user cannot turn off the video.
Can the local user also turn on the video?	When the local console is disabled, the local user cannot turn on the video.
Does switching off the local video also switch off the local keyboard and mouse?	No.
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.
What privileges are needed for an iDRAC6 user to turn on or off the local server video?	Any user with iDRAC6 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 iDRAC6 Web interface. The RACADM CLI command **racadm getconfig –g cfgRacTuning** displays the status in the object **cfgRacTuneLocalServerVideo**.

Table 10-6. Using Console Redirection: Frequently Asked Questions (continued)

Question	Answer
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. Try using the scroll bars on the iDRAC KVM client, as well.
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.
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 the **Single Cursor** option under **Tools** in the iDRAC KVM menu is selected on the iDRAC KVM client.
Why can't I use a keyboard or mouse while installing a Microsoft operating system remotely by using iDRAC6 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.
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 iDRAC6, 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.

Table 10-6. Using Console Redirection: Frequently Asked Questions *(continued)*

Question	Answer
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, 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.
Why do I see a **No Signal** message within the iDRAC KVM Video Viewer?	You may see this message because the iDRAC Virtual KVM plugin is not receiving the remote server desktop video. Generally, this behavior may occur when the remote server is powered off. Occasionally, the message may be displayed due to a remote server desktop video reception malfunction.
Why do I see an **Out of Range** message within the iDRAC KVM Video Viewer?	You may see this message because a parameter necessary to capture video is beyond the range for which the iDRAC can capture the video. Parameters such as display resolution or refresh rate too high will cause and out of range condition. Usually the maximum range of parameters is set by physical limitations such as video memory size or bandwidth.

11

Using the WS-MAN Interface

Web Services for Management (WS–MAN) is a Simple Object Access Protocol (SOAP)–based protocol used for systems management. WS–MAN provides an interoperable protocol for devices to share and exchange data across networks. iDRAC6 uses WS–MAN to convey Distributed Management Task Force (DMTF) Common Information Model (CIM)–based management information; the CIM information defines the semantics and information types that can be manipulated in a managed system. The Dell™–embedded server platform management interfaces are organized into profiles, where each profile defines the specific interfaces for a particular management domain or area of functionality. Additionally, Dell has defined a number of model and profile extensions that provide interfaces for additional capabilities.

The data available through WS-MAN is provided by the iDRAC6 instrumentation interface mapped to the following DMTF profiles and Dell extension profiles:

Supported CIM Profiles

Table 11-1.   Standard DMTF

Standard DMTF
1 Base Server Defines CIM classes for representing the host server.
2 Service Processor: Contains the definition of CIM classes for representing the iDRAC6.

NOTE: The Base Server profile (above) and the Service Processor profile are autonomous in a sense that the objects they describe aggregate all the other CIM objects defined in component profiles.

Table 11-1.   Standard DMTF *(continued)*

3 Physical Asset:
Defines CIM classes for representing the physical aspect of the managed elements. iDRAC6 uses this profile to represent the host server's and its component's FRU information, as well as the physical topology.

4 SM CLP Admin Domain
Defines CIM classes for representing CLP's configuration. iDRAC6 uses this profile for its own implementation of CLP.

5 Power State Management
Defines CIM classes for power control operations. iDRAC6 uses this profile for the host server's power control operations.

6 Power Supply (version 1.1)
Defines CIM classes for representing power supplies. iDRAC6 uses this profile to represent the host server's power supplies to describe power consumption, such as high and low power consumption watermarks.

7 CLP Service
Defines CIM classes for representing CLP's configuration. iDRAC6 uses this profile for its own implementation of CLP.

8 IP Interface

9 DHCP Client

10 DNS Client

11 Ethernet Port
The above profiles define CIM classes for representing network stacks. iDRAC6 uses these profiles to represent the configuration of the iDRAC6 NIC.

12 Record Log
Defines CIM classes for representing different type of logs. iDRAC6 uses this profile to represent the System Event Log (SEL) and iDRAC6 RAC Log.

13 Software Inventory
Defines CIM classes for inventory of installed or available software. iDRAC6 uses this profile for inventory of currently installed iDRAC6 firmware versions through the TFTP protocol.

14 Role Based Authorization
Defines CIM classes for representing roles. iDRAC6 uses this profile for configuring iDRAC6 account privileges.

Table 11-1. Standard DMTF *(continued)*

15 Software Update
Defines CIM classes for inventory of available software updates. iDRAC6 uses this profile for inventory of updates of the firmware through the TFTP protocol.

16 SMASH Collection
Defines CIM classes for representing CLP's configuration. iDRAC6 uses this profile for its own implementation of CLP.

17 Profile Registration
Defines CIM classes for advertising the profile implementations. iDRAC6 uses this profile to advertise its own implemented profiles, as described in this table.

18 Base Metrics
Defines CIM classes for representing metrics. iDRAC6 uses this profile to represent the host server's metrics to describe power consumption, such as high and low power consumption watermarks.

19 Simple Identity Management
Defines CIM classes for representing identities. iDRAC6 uses this profile for configuring iDRAC6 accounts.

20 USB Redirection
Defines CIM classes for representing the remote redirection of local USB ports. iDRAC6 uses this profile in conjunction with the Virtual Media Profile to configure Virtual Media.

Table 11-1. Standard DMTF *(continued)*

Dell Extensions

1 Dell™ Active Directory Client Version 2.0.0
Defines CIM and Dell extension classes for configuring iDRAC6 Active Directory
client and the local privileges for Active Directory groups.

2 Dell Virtual Media
Defines CIM and Dell extension classes for configuring iDRAC6 Virtual Media.
Extends USB Redirection Profile.

3 Dell Ethernet Port
Defines CIM and Dell extension classes for configuring NIC Side-Band interface for
the iDRAC6 NIC. Extends Ethernet Port Profile.

4 Dell Power Utilization Management
Defines CIM and Dell extension classes for representing the host server's power
budget and for configuring/monitoring the host server's power budget.

5 Dell OS Deployment
Defines CIM and Dell extension classes for representing the configuration of OS
Deployment features. It extends the management capability of referencing profiles
by adding the capability to support OS deployment activities by manipulating OS
Deployment features provided by the service processor.

The iDRAC6 WS–MAN implementation uses SSL on port 443 for transport
security, and supports basic and digest authentication. Web services
interfaces can be utilized by leveraging client infrastructure such as
Windows® WinRM and Powershell CLI, open source utilities like
WSMANCLI, and application programming environments like Microsoft®
.NET®.

There are additional implementation guides, white papers, profile, and code
samples available in the Dell Enterprise Technology Center at
www.delltechcenter.com. For more information, also see the following:

- DTMF Web site: **www.dmtf.org/standards/profiles/**
- WS–MAN release notes or Readme file.

12

Using the iDRAC6 SM-CLP Command Line Interface

This section provides information about the Distributed Management Task Force (DMTF) Server Management-Command Line Protocol (SM-CLP) that is incorporated in the iDRAC6.

✍ **NOTE:** This section assumes that you are familiar with the Systems Management Architecture for Server Hardware (SMASH) Initiative and the SM-CLP specifications. For more information on these specifications, see the DMTF website at **www.dmtf.org**.

The iDRAC6 SM-CLP is a protocol that provides standards for systems management CLI implementations. The SM-CLP is a subcomponent of the DMTF SMASH initiative to streamline server management across multiple platforms. The SM-CLP specification, in conjunction with the Managed Element Addressing Specification and numerous profiles to SM-CLP mapping specifications, describes the standardized verbs and targets for various management task executions.

iDRAC6 SM-CLP Support

The SM-CLP is hosted from the iDRAC6 controller firmware and supports telnet, SSH, and serial-based interfaces. The iDRAC6 SM-CLP interface is based on the SM-CLP Specification Version 1.0 provided by the DMTF organization. iDRAC6 SM-CLP supports all profiles described in Table 11-1 "Supported CIM Profiles."

The following sections provide an overview of the SM-CLP feature that is hosted from the iDRAC6.

SM-CLP Features

The SM-CLP promotes the concept of verbs and targets to provide system management capabilities through the CLI. The verb indicates the operation to perform, and the target determines the entity (or object) that runs the operation.

Below is an example of the SM-CLP command line syntax.

```
<verb> [<options>] [<target>] [<properties>]
```

During a typical SM-CLP session, you can perform operations using the verbs listed in Table 12-1.

Table 12-1.   Supported CLI Verbs for System

Verb	Definition
cd	Navigates through the MAP using the shell
set	Sets a property to a specific value
help	Displays help for a specific target
reset	Resets the target
show	Displays the target properties, verbs, and subtargets
start	Turns on a target
stop	Shuts down a target
exit	Exits from the SM-CLP shell session
version	Displays the version attributes of a target
load	Moves a binary image to a specified target address from a URL

Using SM-CLP

SSH (or telnet) in to the iDRAC6 with correct credentials.

The SMCLP prompt (/admin1–>) is displayed.

SM-CLP Targets

Table 12-2 provides a list of targets provided through the SM-CLP to support the operations described in Table 12-1 above.

Table 12-2. SM-CLP Targets

Target	Definitions
`admin1`	admin domain
`admin1/profiles1`	Registered profiles in iDRAC6
`admin1/hdwr1`	Hardware
`admin1/system1`	Managed system target
`admin1/system1/redundancyset1`	Power supply
`admin1/system1/redundancyset1/` `pwrsupply*`	Managed system power supply
`admin1/system1/sensors1`	Managed system sensors
`admin1/system1/capabilities1`	Managed system SMASH collection capabilities
`admin1/system1/capabilities1/` `pwrcap1`	Managed system power utilization capabilities
`admin1/system1/capabilities1/` `elecap1`	Managed system target capabilities
`admin1/system1/logs1`	Record Log collections target
`admin1/system1/logs1/log1`	System Event Log (SEL) record entry
`admin1/system1/logs1/log1/` `record*`	An individual SEL record instance on the managed system
`admin1/system1/settings1`	Managed system SMASH collection settings
`admin1/system1/settings1/` `pwrmaxsetting1`	Managed system maximum power allocation setting
`admin1/system1/settings1/` `pwrminsetting1`	Managed system minimum power allocation setting
`admin1/system1/capacities1`	Managed system capacities SMASH collection
`admin1/system1/consoles1`	Managed system consoles SMASH collection
`admin1/system1/usbredirectsap1`	Virtual Media USB redirection SAP

Table 12-2. SM-CLP Targets *(continued)*

Target	Definitions
`admin1/system1/usbredirectsap1/remotesap1`	Virtual Media destination USB redirection SAP
`admin1/system1/sp1`	Service Processor
`admin1/system1/sp1/timesvc1`	Service Processor time service
`admin1/system1/sp1/capabilities1`	Service processor capabilities SMASH collection
`admin1/system1/sp1/capabilities1/clpcap1`	CLP service capabilities
`admin1/system1/sp1/capabilities1/pwrmgtcap1`	Power state management service capabilities on the system
`admin1/system1/sp1/capabilities1/ipcap1`	IP interface capabilities
`admin1/system1/sp1/capabilities1/dhcpcap1`	DHCP client capabilities
`admin1/system1/sp1/capabilities1/NetPortCfgcap1`	Network port configuration capabilities
`admin1/system1/sp1/capabilities1/usbredirectcap1`	Virtual Media capabilities USB redirection SAP
`admin1/system1/sp1/capabilities1/vmsapcap1`	Virtual Media SAP capabilities
`admin1/system1/sp1/capabilities1/swinstallsvccap1`	Software installation service capabilities
`admin1/system1/sp1/capabilities1/acctmgtcap*`	Account management service capabilities
`admin1/system1/sp1/capabilities1/adcap1`	Active Directory capabilities
`admin1/system1/sp1/capabilities1/rolemgtcap*`	Local Role Based Management capabilities
`admin1/system1/sp1/capabilities/PwrutilmgtCap1`	Power utilization management capabilities

Table 12-2. SM-CLP Targets *(continued)*

Target	Definitions
`admin1/system1/sp1/capabilitie s/metriccap1`	Metric service capabilities
`admin1/system1/sp1/capabilitie s1/elecap1`	Multi-factor Authentication capabilities
`admin1/system1/sp1/capabilitie s1/lanendptcap1`	LAN (Ethernet port) endpoint capabilities
`admin1/system1/sp1/logs1`	Service Processor logs collection
`admin1/system1/sp1/logs1/log1`	System record log
`admin1/system1/sp1/logs1/log1/ record*`	System log entry
`admin1/system1/sp1/settings1`	Service Processor settings collection
`admin1/system1/sp1/settings1/ clpsetting1`	CLP service settings data
`admin1/system1/sp1/settings1/ ipsettings1`	IP interface assignment settings data (Static)
`admin1/system1/sp1/settings1/ ipsettings1/staticipsettings1`	Static IP interface assignment settings data
`admin1/system1/sp1/settings1/ ipsettings1/dnssettings1`	DNS client settings data
`admin1/system1/sp1/settings1/ ipsettings2`	IP interface assignment settings data (DHCP)
`admin1/system1/sp1/settings1/ ipsettings2/dhcpsettings1`	DHCP client settings data
`admin1/system1/sp1/clpsvc1`	CLP service protocol service
`admin1/system1/sp1/clpsvc1/ clpendpt*`	CLP service protocol endpoint
`admin1/system1/sp1/clpsvc1/ tcpendpt*`	CLP service protocol TCP endpoint
`admin1/system1/sp1/jobq1`	CLP service protocol job queue
`admin1/system1/sp1/jobq1/job*`	CLP service protocol job
`admin1/system1/sp1/pwrmgtsvc1`	Power state management service

Table 12-2. SM-CLP Targets *(continued)*

Target	Definitions
`admin1/system1/sp1/ipcfgsvc1`	IP interface configuration service
`admin1/system1/sp1/ipendpt1`	IP interface protocol endpoint
`admin1/system1/sp1/ipendpt1/gateway1`	IP interface gateway
`admin1/system1/sp1/ipendpt1/dhcpendpt1`	DHCP client protocol endpoint
`admin1/system1/sp1/ipendpt1/dnsendpt1`	DNS client protocol endpoint
`admin1/system1/sp1/ipendpt1/dnsendpt1/dnsserver*`	DNS client server
`admin1/system1/sp1/NetPortCfgsvc1`	Network port configuration service
`admin1/system1/sp1/lanendpt1`	LAN endpoint
`admin1/system1/sp1/lanendpt1/enetport1`	Ethernet Port
`admin1/system1/sp1/VMediaSvc1`	Virtual Media service
`admin1/system1/sp1/VMediaSvc1/tcpendpt1`	Virtual Media TCP protocol endpoint
`admin1/system1/sp1/swid1`	Software identity
`admin1/system1/sp1/swinstallsvc1`	Software installation service
`admin1/system1/sp1/account1-16`	Multi-factor Authentication (MFA) account
`admin1/sysetm1/sp1/account1-16/identity1`	Local user identity account
`admin1/sysetm1/sp1/account1-16/identity2`	IPMI identity (LAN) account
`admin1/sysetm1/sp1/account1-16/identity3`	IPMI identity (Serial) account
`admin1/sysetm1/sp1/account1-16/identity4`	CLP identity account

Table 12-2. SM-CLP Targets (continued)

Target	Definitions
admin1/system1/sp1/acctsvc1	MFA account management service
admin1/system1/sp1/acctsvc2	IPMI account management service
admin1/system1/sp1/acctsvc3	CLP account management service
admin1/system1/sp1/group1-5	Active Directory group
admin1/system1/sp1/ group1-5/identity1	Active Directory identity
admin1/system1/sp1/ADSvc1	Active Directory service
admin1/system1/sp1/rolesvc1	Local Role Base Authorization (RBA) service
admin1/system1/sp1/rolesvc1/ Role1-16	Local role
admin1/system1/sp1/rolesvc1/ Role1-16/privilege1	Local role privilege
admin1/system1/sp1/rolesvc1/ Role17-21/	Active Directory role
admin1/system1/sp1/rolesvc1/ Role17-21/privilege1	Active Directory privilege
admin1/system1/sp1/rolesvc2	IPMI RBA service
admin1/system1/sp1/rolesvc2/ Role1-3	IPMI role
admin1/system1/sp1/rolesvc2/ Role4	IPMI Serial Over LAN (SOL) role
admin1/system1/sp1/rolesvc3	CLP RBA Service
admin1/system1/sp1/rolesvc3/ Role1-3	CLP role
admin1/system1/sp1/rolesvc3/ Role1-3/privilege1	CLP role privilege
admin1/system1/sp1/ pwrutilmgtsvc1	Power utilization management service
admin1/system1/sp1/ pwrutilmgtsvc1/pwrcurr1	Power utilization management service current power allocation setting data

Table 12-2. SM-CLP Targets *(continued)*

Target	Definitions
`admin1/system1/sp1/metricsvc1`	Metric service
`/admin1/system1/sp1/metricsvc1` `/cumbmd1`	Cumulative base metric definition
`/admin1/system1/sp1/metricsvc1` `/cumbmd1/cumbmv1`	Cumulative base metric value
`/admin1/system1/sp1/metricsvc1` `/cumwattamd1`	Cumulative watt aggregation metric definition
`/admin1/system1/sp1/metricsvc1` `/cumwattamd1/cumwattamv1`	Cumulative watt aggregation metric value
`/admin1/system1/sp1/metricsvc1` `/cumampamd1`	Cumulative amp aggregation metric definition
`/admin1/system1/sp1/metricsvc1` `/cumampamd1/cumampamv1`	Cumulative amp aggregation metric value
`/admin1/system1/sp1/metricsvc1` `/loamd1`	Low aggregation metric definition
`/admin1/system1/sp1/metricsvc1` `/loamd1/loamv*`	Low aggregation metric value
`/admin1/system1/sp1/metricsvc1` `/hiamd1`	High aggregation metric definition
`/admin1/system1/sp1/metricsvc1` `/hiamd1/hiamv*`	High aggregation metric value
`/admin1/system1/sp1/metricsvc1` `/avgamd1`	Average aggregation metric definition
`/admin1/system1/sp1/metricsvc1` `/avgamd1/avgamv*`	Average aggregation metric value

13

Deploying Your Operating System Using VMCLI

The Virtual Media Command Line Interface (VMCLI) utility is a command-line interface that provides virtual media features from the management station to the iDRAC6 in the remote system. Using VMCLI and scripted methods, you can deploy your operating system on multiple remote systems in your network.

This section provides information on integrating the VMCLI utility into your corporate network.

Before You Begin

Before using the VMCLI utility, ensure that your targeted remote systems and corporate network meet the requirements listed in the following sections.

Remote System Requirements

The iDRAC6 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 iDRAC6 Web user interface and then reboot the system.

The following sections provide specific information for creating image files for Linux and Microsoft® 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 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 VMCLI into your existing operating system deployment application. Use the sample **vm6deploy** script as a guide to using the utility.
- Use the existing **vm6deploy** script to deploy your operating system.

Deploying the Operating System

Use the VMCLI utility and the **vm6deploy** script included with the utility to deploy the operating system to your remote systems.

Before you begin, review the sample **vm6deploy** script included with the VMCLI 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 iDRAC6 IPv4 addresses of the remote systems that will be deployed in the **ip.txt** text file, one IPv4 address per line.

2 Insert a bootable operating system CD or DVD into the client media drive.

3 Run **vm6deploy** at the command line.

To run the **vm6deploy** script, enter the following command at the command prompt:

```
vm6deploy -r ip.txt -u <idrac-user> -p <idrac-passwd>
-c {<iso9660-img> | <path>} -f {<floppy-img>|<path>}
```

where:

- *<idrac-user>* is the iDRAC6 user name, for example **root**
- *<idrac-passwd>* is the password for the iDRAC6 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 , DVD, or Floppy
- `<floppy-img>` is the path to a valid floppy image

The **vm6deploy** script passes its command line options to the **VMCLI** utility. See "Command Line Options" for details about these options. The script processes the **-r** option slightly differently than the **vmcli -r** option. If the argument to the **-r** option is the name of an existing file, the script reads iDRAC6 IPv4 addresses from the specified file and runs the **VMCLI** 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 iDRAC6. In this case, the -**r** works as described for the **VMCLI** utility.

Using the VMCLI Utility

The VMCLI utility is a scriptable command line interface that provides virtual media features from the management station to the iDRAC6.

The VMCLI 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 iDRAC6 firmware boot once option is enabled
- Secure communications to the iDRAC6 using Secure Sockets Layer (SSL)

Before you run the utility, ensure that you have Virtual Media user privilege to the iDRAC6.

If your operating system supports administrator privileges or an operating system-specific privilege or group membership, administrator privileges are also required to run the VMCLI 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 VMCLI utility.

For Linux systems, you can access the VMCLI 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 VMCLI group, the administrator uses the **visudo** command. Users without administrator privileges can add the **sudo** command as a prefix to the VMCLI command line (or to the VMCLI script) to obtain access to the iDRAC6 in the remote system and run the utility.

Installing the VMCLI Utility

The VMCLI utility is located on the *Dell Systems Management Tools and Documentation* DVD, which is included with your Dell OpenManage System Management Software Kit. To install the utility, insert the *Dell Systems Management Tools and Documentation* DVD into your system's DVD drive and follow the on-screen instructions.

The *Dell Systems Management Tools and Documentation* DVD contains the latest systems management software products, including diagnostics, storage management, remote access service, and the IPMItool utility. This DVD also contains readme files, which provide the latest systems management software product information.

The *Dell Systems Management Tools and Documentation* DVD includes **vm6deploy**—a sample script that illustrates how to use the VMCLI and IPMItool utilities to deploy software to multiple remote systems.

NOTE: The vm6deploy script is dependent upon the other files that are present in its directory when it is installed. If you want to use the script from another directory, you must copy all of the files with it. If the IPMItool utility is not installed, the utility needs to be copied in addition to the other files.

Command Line Options

The VMCLI interface is identical on both Windows and Linux systems.

The VMCLI command format is as follows:

`VMCLI [parameter] [operating_system_shell_options]`

Command-line syntax is case sensitive. See "VMCLI Parameters" for more information.

If the remote system accepts the commands and the iDRAC6 authorizes the connection, the command continues to run until either of the following occurs:

- The VMCLI 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.

VMCLI Parameters

iDRAC6 IP Address

`-r <iDRAC-IP-address>[:<iDRAC-SSL-port>]`

This parameter provides the iDRAC6 IPv4 address and SSL port, which the utility needs to establish a Virtual Media connection with the target iDRAC6. If you enter an invalid IPv4 address or DDNS name, an error message is displayed and the command is terminated.

<iDRAC-IP-address> is a valid, unique IPv4 address or the iDRAC6 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 iDRAC6 default SSL port.

iDRAC6 User Name

`-u <iDRAC-user-name>`

This parameter provides the iDRAC6 user name that will run Virtual Media.

The *<iDRAC-user-name>* must have the following attributes:

- Valid user name
- iDRAC6 Virtual Media User permission

If iDRAC6 authentication fails, an error message is displayed and the command is terminated.

iDRAC6 User Password

`-p <iDRAC-user-password>`

This parameter provides the password for the specified iDRAC6 user.

If iDRAC6 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 filename (for Linux systems); and *<image-file>* is the filename and path of a valid image file.

✏️ **NOTE:** Mount points are not supported for the VMCLI utility.

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)
```

✏️ **NOTE:** Red Hat® Enterprise Linux® version 4 does not and will not provide support for multiple LUNs. However, the kernel supports this functionality, but you must enable Red Hat Enterprise Linux version 4 to recognize a SCSI device with multiple LUNs by following these steps:

1 Edit **/etc/modprobe.conf** and add the following line:
```
options scsi_mod max_luns=8
```
(You can specify 8 LUNs or any number greater than 1.)

2 Get the name for the kernel image by typing the following command at the command line:

```
uname -r
```

3 Go to the **/boot** directory and delete the kernel image file, whose name you determined in Step 2:

```
mkinitrd /boot/initrd-'uname -r'.img 'uname -r'
```

4 Reboot the server.

5 Run the following command to confirm that support for multiple LUNs has been added for the number of LUNs that you specified in Step 1:

```
cat /sys/modules/scsi_mod/max_luns
```

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:\` (Microsoft® 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 VMCLI 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 VMCLI utility parameters. If no other non-switch options are provided, the command terminates without error.

Encrypted Data

−e

When this parameter is included in the command line, VMCLI will use an SSL-encrypted channel to transfer data between the management station and the iDRAC6 in the remote system. If this parameter is not included in the command line, the data transfer is not encrypted.

NOTE: Using this option does not change the displayed Virtual Media encryption status to *enabled* in other iDRAC6 configuration interfaces like RACADM or the Web interface.

VMCLI Operating System Shell Options

The following operating system features can be used in the VMCLI 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 VMCLI utility.

  NOTE: The VMCLI utility does not read from standard input (**stdin**). As a result, **stdin** redirection is not required.

- Background execution — By default, the VMCLI 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 VMCLI command (otherwise, the script would block until the VMCLI program is terminated). When multiple VMCLI 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.

VMCLI Return Codes

English-only text messages are issued to standard error output whenever errors are encountered.

14

Configuring Intelligent Platform Management Interface (IPMI)

Configuring IPMI

This section provides information about configuring and using the iDRAC6 IPMI interface. The interface includes the following:

- IPMI over LAN
- IPMI over Serial
- Serial over LAN

The iDRAC6 is fully IPMI 2.0 compliant. You can configure the iDRAC6 IPMI using:

- iDRAC6 GUI from your browser
- An open source utility, such as *IPMItool*
- The Dell™ OpenManage™ IPMI shell, *ipmish*
- RACADM

For more information about using the IPMI Shell, ipmish, see the *Dell OpenManage Baseboard Management Controller Utilities User's Guide* at **support.dell.com\manuals.**

For more information about using RACADM, see "Using RACADM Remotely."

Configuring IPMI Using the Web-Based Interface

For detailed information, see "Configuring IPMI."

Configuring IPMI Using the RACADM CLI

1 Login to the remote system using any of the RACADM interfaces.
   See "Using RACADM Remotely."

2 Configure IPMI over LAN.

   Open a command prompt, type the following command, and press
   <Enter>:

   ```
   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.

      At the command prompt, type the following command and press
      <Enter>:

      ```
      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.

   NOTE: The iDRAC6 IPMI supports the RMCP+ protocol. See the IPMI 2.0
   specifications for more information.

      At the command prompt, type the following command and press
      <Enter>:

      ```
      racadm config -g cfgIpmiLan -o
      cfgIpmiEncryptionKey <key>
      ```

where *<key>* is a 20-character encryption key in a valid hexadecimal format.

3 Configure IPMI Serial over LAN (SOL).

At the command prompt, type the following command and press <Enter>:

```
racadm config -g cfgIpmiSol -o cfgIpmiSolEnable 1
```

a Update the IPMI SOL minimum privilege level.

✐ **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.

At the command prompt, type the following command and press <Enter>:

```
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), type the following command:

```
racadm config -g cfgIpmiSol -o
cfgIpmiSolMinPrivilege 2
```

b Update the IPMI SOL baud rate.

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

At the command prompt, type the following command and press <Enter>:

```
racadm config -g cfgIpmiSol -o
cfgIpmiSolBaudRate <baud_rate>
```

where *<baud_rate>* is 9600, 19200, 57600, or 115200 bps.

For example:

```
racadm config -g cfgIpmiSol -o
cfgIpmiSolBaudRate 57600
```

c Enable SOL for an individual user.

📝 **NOTE:** SOL can be enabled or disabled for each individual user.

At the command prompt, type the following command and press <Enter>:

```
racadm config -g cfgUserAdmin -o
cfgUserAdminSolEnable -i <id> 2
```

where *<id>* is the user's unique ID.

4 Configure IPMI Serial.

a Change the IPMI serial connection mode to the appropriate setting.

At the command prompt, type the following command and press <Enter>:

```
racadm config -g cfgSerial -o
cfgSerialConsoleEnable 0
```

b Set the IPMI Serial baud rate.

Open a command prompt, type the following command, and press <Enter>:

```
racadm config -g cfgIpmiSerial -o
cfgIpmiSerialBaudRate <baud_rate>
```

where *<baud_rate>* is 9600, 19200, 57600, or 115200 bps.

For example:

```
racadm config -g cfgIpmiSerial -o
cfgIpmiSerialBaudRate 57600
```

c Enable the IPMI serial hardware flow control.

At the command prompt, type the following command and press <Enter>:

```
racadm config -g cfgIpmiSerial -o
cfgIpmiSerialFlowControl 1
```

d Set the IPMI serial channel minimum privilege level.

At the command prompt, type the following command and press <Enter>:

```
racadm config -g cfgIpmiSerial -o
cfgIpmiSerialChanPrivLimit <level>
```

where *<level>* is one of the following:

- 2 (User)
- 3 (Operator)
- 4 (Administrator)

For example, to set the IPMI serial channel privileges to 2 (User), type the following command:

```
racadm config -g cfgIpmiSerial -o
cfgIpmiSerialChanPrivLimit 2
```

e Ensure that the serial MUX is set correctly in the BIOS Setup program.

- Restart your system.
- During POST, press <F2> to enter the BIOS Setup program.
- Click **Serial Communication**.
- In the **Serial Connection** menu, ensure that **External Serial Connector** is set to **Remote Access Device**.
- Save and exit the BIOS Setup program.
- Restart your system.

The IPMI configuration is complete.

If IPMI serial is in terminal mode, you can configure the following additional settings using **racadm config cfgIpmiSerial** commands:

- Delete control
- Echo control
- Line edit
- New line sequences
- Input new line sequences

For more information about these properties, see the IPMI 2.0 specification.

Using the IPMI Remote Access Serial Interface

In the IPMI serial interface, the following modes are available:

- **IPMI terminal mode** — Supports ASCII commands that are submitted from a serial terminal. The command set has a limited number of commands (including power control) and supports raw IPMI commands that are entered as hexadecimal ASCII characters.

- **IPMI basic mode** — Supports a binary interface for program access, such as the IPMI shell (IPMISH) that is included with the Baseboard Management Utility (BMU).

To configure the IPMI mode using RACADM:

1 Disable the RAC serial interface.

   At the command prompt, type:

   ```
   racadm config -g cfgSerial -o
   cfgSerialConsoleEnable 0
   ```

2 Enable the appropriate IPMI mode.

   For example, at the command prompt, type:

   ```
   racadm config -g cfgIpmiSerial -o
   cfgIpmiSerialConnectionMode <0 or 1>
   ```

See "iDRAC6 Property Database Group and Object Definitions" for more information.

Configuring Serial Over LAN Using the Web-Based Interface

For detailed information, see "Configuring IPMI."

Ø **NOTE:** You can use Serial Over LAN with the following Dell OpenManage tools: SOLProxy and IPMItool. For more information, see the *Dell OpenManage Baseboard Management Controller Utilities User's Guide* at **support.dell.com\manuals.**

15

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 15-1 shows the overall architecture of **Virtual Media**.

Figure 15-1.   Overall Architecture of Virtual Media
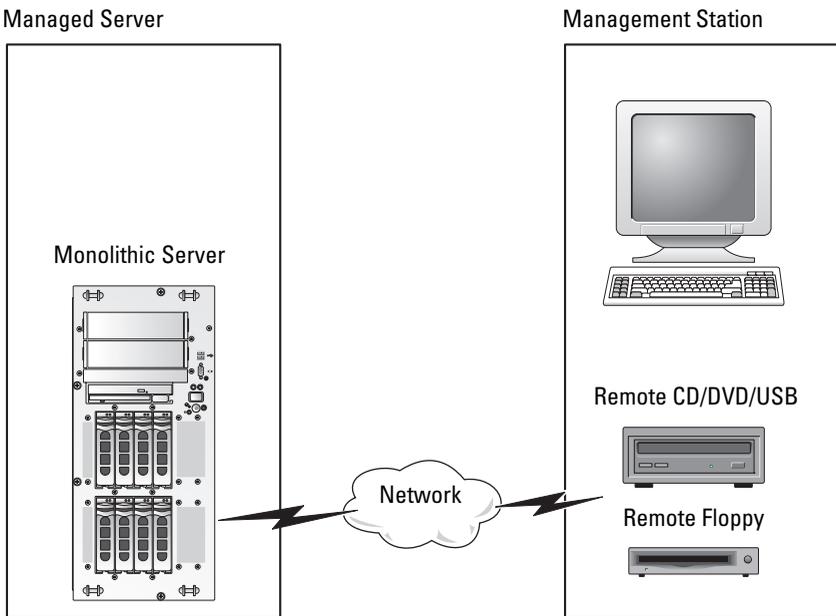
Using **Virtual Media**, administrators can remotely boot their managed servers, install applications, update drivers, or even install new operating systems remotely from the virtual CD/DVD and diskette drives.

> ✎ **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 attached or auto-attached, all virtual CD/floppy drive access requests from the managed server are directed to the management station across the network. Connecting **Virtual Media** is the equivalent of inserting media into physical devices on the managed system. When **Virtual Media** is in attached state, virtual devices on the managed system appear as two drives without the media being installed in the drives.

Table 15-1 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 15-1. 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 or Firefox with Java Runtime Environment (JRE).

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.

A Java Runtime Environment (JRE) 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 iDRAC6 Web interface.

2 Select **System**→**Console/Media**.

3 Click **Configuration**→**Virtual Media** to configure the Virtual Media settings.

   Table 15-2 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 15-3.

Table 15-2.   Virtual Media Configuration Properties

Attribute	Value
Remote Media Attached State	**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.
Max Sessions	Displays the maximum number of **Virtual Media** sessions allowed, which is always 1.
Active Sessions	Displays the current number of Virtual Media sessions.
Virtual Media Encryption Enabled	Select or deselect the checkbox to enable or disable encryption on **Virtual Media** connections. Selected enables encryption; deselected disables encryption.

Table 15-2.   Virtual Media Configuration Properties *(continued)*

Attribute	Value
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. Use this attribute to boot from the Virtual Media. On the next boot, the system will boot from the next device in the boot order. This option automatically disconnects the **Virtual Media** devices after the system has booted once.

Table 15-3.   Configuration Page Buttons

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

Running Virtual Media

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

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

📝 **NOTE:** Perform the following steps to enable Red Hat® Enterprise Linux® (version 4) to recognize a SCSI device with multiple Logical Units (LUNs):

1 Add the following line to /**ect**/**modprobe**:

```
options scsi_mod max_luns=256

cd /boot

mkinitrd -f initrd-2.6.9.78ELsmp.img 2.6.3.78ELsmp
```

2 Reboot the server.

3 Run the following commands to see the Virtual CD/DVD and/or the Virtual Floppy:

```
cat /proc/scsi/scsi
```

📝 **NOTE:** Using Virtual Media, you can virtualize only one floppy/USB drive/image/key and one optical drive from your management station to be available as a (virtual) drive on the managed server.

Supported Virtual Media Configurations

You can enable Virtual Media for one floppy drive and one optical drive. Only one drive for each media type can be virtualized at a time.

Supported floppy drives include a floppy image or one available floppy drive. Supported optical drives include a maximum of one available optical drive or one ISO image file.

Connecting Virtual Media

Perform the following steps to run Virtual Media:

1 Open a supported Web browser on your management station.

2 Start the iDRAC6 Web interface. See "Accessing the Web Interface" for more information.

3 Select **System→Console/Media**.

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

✐ **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/USB flash drive at the same time to be virtualized.

✐ **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 system 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 **iDRAC KVM Agent** application launches in a separate window.

5 Click **Tools→Launch Virtual Media**.

The Media Redirection wizard is displayed.

✐ **NOTE:** Do not close this wizard unless you want to terminate the Virtual
Media session.

6 If media is connected, you must disconnect it before connecting a
different media source. Uncheck the box to the left of the media you want
to disconnect.

7 Check the box next to the media types you want to connect.

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

The media is connected and the **Status** window is updated.

Disconnecting Virtual Media

1 Click **Tools**→**Launch Virtual Media**.

2 Uncheck the box next to the media you want to disconnect.

The media is disconnected and the **Status** window is updated.

3 Click **Exit** to terminate the Media Redirection wizard.

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" 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.

It is important to follow these steps for multi-disk installation:

   1   Unmap the virtualized (redirected) CD/DVD from the Virtual Media console.

   2   Insert the next CD/DVD into the remote optical drive.

   3   Map (redirect) this CD/DVD from the Virtual Media console.

   Inserting a new CD/DVD into the remote optical drive without remapping may not work.

Boot Once Feature

The Boot Once feature helps you change the boot order temporarily for booting from a remote Virtual Media device. This feature is used in conjunction with Virtual Media, generally while installing operating systems.

Ø **NOTE:** You must have **Configure iDRAC6** privilege to use this feature.

Ø **NOTE:** Remote devices must be redirected using Virtual Media to use this feature.

Using the Boot Once Feature:

1 Power up the server and enter the BIOS Boot Manager.

2 Change the boot sequence to boot from the remote Virtual Media device.

3 Log in to the iDRAC6 through the Web interface and click **System**→ **Console/Media**→**Configuration**.

4 Check the **Enable Boot Once** option under Virtual Media.

5 Power cycle the server.

   The server boots from the remote Virtual Media device. The next time the server reboots, the remote Virtual Media connection is detached.

   NOTE: Virtual Media should be in the Attached state for the virtual drives to appear in the boot sequence. Ensure that the bootable media is present in the virtualized drive to enable Boot Once.

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 about Virtual Media

Table 15-4 lists frequently asked questions and answers.

Table 15-4.   Using Virtual Media: Frequently Asked Questions

Question	Answer
Sometimes, I notice my Virtual Media client connection drop. Why?	When a network timeout occurs, the iDRAC6 firmware drops the connection, disconnecting the link between the server and the Virtual Drive.
	If the Virtual Media configuration settings are changed in the iDRAC6 Web-based 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 iDRAC6?	See "Supported Operating Systems" for a list of supported operating systems.
Which Web browsers support the iDRAC6?	See "Supported Web Browsers" for a list of supported Web browsers.
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 iDRAC6 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 RACADM commands. To reconnect to the Virtual Drive, use the **Virtual Media** feature.

Table 15-4.   Using Virtual Media: Frequently Asked Questions *(continued)*

Question	Answer
An installation of the Windows operating system through vMedia seems to take too long. Why?	If you are installing the Windows operating system using the *Dell Systems Management Tools and Documentation* DVD and a slow network connection, the installation procedure may require an extended amount of time to access the iDRAC6 Web interface due to network latency. While the installation window does not indicate the installation progress, the installation procedure is in progress.
How do I configure my virtual device as a bootable device?	On the managed server, access the BIOS Setup and click the boot menu. Locate the virtual CD, Virtual Floppy, or Virtual Flash and change the device boot order as needed. Also, make the virtual device bootable by pressing the "spacebar" key in the boot sequence in the CMOS setup. 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 iDRAC6 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.

Table 15-4. Using Virtual Media: Frequently Asked Questions *(continued)*

Question	Answer
I cannot locate my Virtual Floppy/Virtual CD 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.

Table 15-4.   Using Virtual Media: Frequently Asked Questions *(continued)*

Question	Answer

I cannot locate my Virtual Floppy/Virtual CD 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?	*(Answer Continued)*
	
	To mount the Virtual CD drive, locate the device node that Linux assigns to the Virtual CD drive. Follow these steps to find and mount the Virtual CD drive:
	
	1 Open a Linux command prompt and run the following command:
	
	grep "Virtual CD" /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 timestamp 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 CD."
	
	5 Ensure that you are attached and connected to the Virtual CD Drive.
	
	6 At the Linux prompt, run the following command:
	
	mount */dev/sdx* /mnt/CD
	
	where:
	
	    `/dev/sdx` is the device name found in step 4
	
	    `/mnt/floppy` is the mount point.

When I performed a firmware update remotely using the iDRAC6 Web interface, my virtual drives at the server were removed. Why?	Firmware updates cause the iDRAC6 to reset, drop the remote connection, and unmount the virtual drives.

Table 15-4.   Using Virtual Media: Frequently Asked Questions *(continued)*

Question	Answer
Why are all my USB devices detached after I connect a USB device?	Virtual Media devices and Virtual Flash devices are connected as a composite USB device to the Host USB BUS, and they share a common USB port. Whenever any Virtual Media or Virtual Flash USB device is connected to or disconnected from the host USB BUS, all the Virtual Media and Virtual Flash devices will be disconnected momentarily from the host USB bus, and then they will be connected again. If a Virtual Media device is being used by the host operating system, you must avoid attaching or detaching one or more Virtual Media or Virtual Flash devices. It is recommended that you connect all the required USB devices first before using them.
What does the USB reset button do?	It resets the remote and local USB devices connected to the server.

16

Configuring the vFlash Media Card for Use With iDRAC6

The vFlash media card is a Secure Digital (SD) card that plugs into the optional iDRAC6 Enterprise card slot at the back of your system. It provides storage space and behaves like a common USB Flash Key device. For information on how to install and remove the vFlash media card from your system, see your *Hardware Owner's Manual* at **support.dell.com\manuals**.

Configuring the vFlash Media Card Using the iDRAC6 Web Interface

Enabling or Disabling the vFlash Media Card

> **NOTE:** The Virtual Flash Enable option is active only if a vFlash media card is present. If a card is not present, the following message displays:
>
> ```
> SD Card not inserted. Please insert an SD card of
> size greater than 256MB.
> ```

1 Ensure that the vFlash media card has been installed.

2 Open a supported Web browser window and log in to the iDRAC6 Web interface.

3 In the system tree, select **System**.

4 Click the **VFlash** tab.

The **VFlash** screen is displayed.

5 Select the **Virtual Flash Enable** option to enable the vFlash Media Card. Enabling the Virtual Flash will expose the Image file **ManagedStore.IMG** created on the SD card as a USB key of the selected size. Virtual Flash can be enabled only if a valid **ManagedStore.IMG** image is present on the SD card. To disable, clear the option.

> **NOTE:** The ManagedStore.IMG and ManagedStore.ID files seen on the *Virtual Flash* GUI page are not visible on the host server's operating system but on the SD card.

6 Click **Apply Changes**.

Formatting the vFlash Media Card

> **NOTE:** The Format option is active only if a vFlash media card is present. Also, the SD card can be formatted only if the Virtual Flash is disabled.

1 Log in to the iDRAC6 Web interface.

2 In the system tree, select **System**.

3 Click the **VFlash** tab.

The **VFlash** screen is displayed.

4 Clear the **Virtual Flash Enable** option.

5 Click **Format** to create the Virtual Flash image file, **ManagedStore.IMG**, on the SD card. The text file **ManagedStore.ID** is also created on the SD card and it provides information about the Virtual Flash image.

An alert box is displayed, warning that any existing image on the card will be erased during formatting and requesting confirmation. Click **OK** to continue.

The progress of the formatting, measured in percentages, will appear in the **Progress** column.

Uploading Disk Image

1 Ensure that the image file size is not larger than 256 MB.

    ✍ **NOTE:** Though your vFlash card may be larger than 256 MB, only 256 MB is accessible at this time.

    ✍ **NOTE:** Virtual Flash allows you to store emergency boot image and diagnostic tools directly on the vFlash Media.The image file can be a DOS bootable floppy image as a ***.img** file for Windows or a **diskboot.img** file from the Red Hat® Enterprise Linux® media for Linux. The **diskboot.img** can be used to create a rescue disk or create a disk to perform network installations. You can use virtual flash to house a persistent image for general or emergency use in future.

2 Log in to the iDRAC6 Web interface.

3 In the system tree, select **System**.

4 Click the **VFlash** tab.

    The **VFlash** screen is displayed.

5 Clear the **Virtual Flash Enable** option.

6 In the **Virtual Flash Drive** section, enter the path to the image file or click **Browse** to navigate to its location on your system.

    Click **Upload**.

    A status bar is displayed, indicating upload progress.

    ✍ **NOTE:** You can upload a bootable ISO image to the virtual flash partition, but it will no longer be bootable. Convert the ISO image to an IMG image to make the IMG image bootable.

Viewing the Virtual Flash Key Size

The **Virtual Flash Key Size** drop-down menu displays the current size setting.

Configuring the vFlash Media Card Using RACADM

Enabling or Disabling the vFlash Media Card

Open a local console to the server, log in, and enter:

```
racadm cfgRacVirtual cfgVirMediaKeyEnable [ 1 or 0 ]
```

where 1 is enabled and 0 is disabled.

NOTE: For more information about cfgRacVirtual, including output details, see "cfgRacVirtual."

NOTE: The RACADM command functions only if a vFlash media card is present. If a card is not present, the following message is displayed: *ERROR: Unable to perform the requested operation. Make sure that a non–write protected SD Card is inserted*.

Resetting the vFlash Media Card

Open a Telnet/SSH text console to the server, log in, and enter:

```
racadm vmkey reset
```

CAUTION: Resetting the vFlash media card with the RACADM command resets the size of the key to 256MB and deletes all existing data.

NOTE: For more information about vmkey, see "vmkey." The RACADM command functions only if a vFlash media card is present. If a card is not present, the following message is displayed: *ERROR: Unable to perform the requested operation. Make sure that a SD Card is inserted*.

17

Power Monitoring and Management

Dell™ PowerEdge™ systems incorporate many new and enhanced power management features. The entire platform, from hardware to firmware to systems management software, has been designed with a focus on power efficiency, power monitoring, and power management.

The base hardware design has been optimized from a power perspective:

- High efficiency power supplies and voltage regulators have been incorporated in to the design.
- Where applicable, the lowest power components were selected.
- The chassis design has optimized air flow through the system to minimize fan power.

PowerEdge systems provide many features to control and manage power:

- **Power Inventory and Budgeting:** At boot, a system inventory enables a system power budget of the current configuration to be calculated.
- **Power Capping:** Systems can be throttled to maintain a specified power cap.
- **Power Monitoring:** The iDRAC6 polls the power supplies to gather power measurements. The iDRAC6 collects a history of power measurements and calculates running averages, and peaks. Using the iDRAC6 Web-based interface, you can view the information, which is displayed on the **Power Monitoring** page.

Power Inventory, Power Budgeting, and Capping

From a usage perspective, you may have a limited amount of cooling at the rack level. With a user-defined power cap, you can allocate power as needed to meet your performance requirements.

The iDRAC6 monitors power consumption and dynamically throttles processors to meet your defined power cap level, which maximizes performance while meeting your power requirements.

Power Monitoring

The iDRAC6 monitors the power consumption in PowerEdge servers continuously. iDRAC6 calculates the following power values and provides the information through its Web-based interface or RACADM CLI:

- Cumulative power
- Average, minimum, and maximum power
- Power headroom values
- Power consumption (also shown in graphs in the Web-based interface)

Configuring and Managing Power

You can use the iDRAC6 Web-based interface and RACADM command line interface (CLI) to manage and configure power controls on the PowerEdge system. Specifically, you can:

- View the power status of the server
- Execute power control operations on the server (for example, power on, power off, system reset, power cycle)
- View power budget information for the server and the installed power supply units, such as, the minimum and maximum potential power consumption
- View and configure power budget threshold for the server

Viewing the Health Status of the Power Supply Units

The **Power Supplies** page displays the status and rating of the power supply units installed in the server.

Using the Web-Based Interface

To view the health status of the power supply units:

1 Log in to the iDRAC6 Web-based interface.

2 Select **Power Supplies** in the system tree. The **Power Supplies** page displays and provides the following information:

- **Power Supplies Redundancy Status**: The possible values are:

   – **Full**: Power supplies, PS1 and PS2, are of the same type and they are functioning properly.

   – **Lost**: Power supplies, PS1 and PS2, are of different types or one of them is malfunctioning. No redundancy exists.

   – **Disabled**: Only one of the two power supplies is available. No redundancy exists.

- **Individual Power Supply Elements**: The possible values are:

   – **Status** displays the following:

      - **OK** indicates that the power supply unit is present and communicating with the server.

      - **Warning** indicates that only warning alerts have been issued and corrective action must be taken by the administrator. If corrective actions are not taken, it could lead to critical or severe power failures that can affect the integrity of the server.

      - **Severe** indicates at least one failure alert has been issued. Failure status indicates a power failure on the server, and corrective action must be taken immediately.

   – **Location** displays the name of the power supply unit: PS-n, where n is the power supply number.

   – **Type** displays the type of power supply, such as AC or DC (AC-to-DC or DC-to-DC voltage conversion).

- **Input Wattage** displays the input wattage of the power supply, which is the maximum AC power load that the system could place on the datacenter.

- **Maximum Wattage** displays the maximum wattage of the power supply, which is the DC power available to the system. This value is used to confirm that sufficient power supply capacity is available for the system configuration.

- **Online Status** indicates the power state of the power supplies: present and OK, input lost, absent, or predictive failure.

- **FW Version** displays the firmware version of the power supply.

NOTE: The Maximum Wattage is different than Input Wattage because of the power supply efficiency. For example, if the efficiency of the power supply is 89% and Maximum Wattage is 717W, the Input Wattage is estimated at 797W.

Using RACADM

Open a Telnet/SSH text console to the iDRAC, log in, and type:

```
racadm getconfig -g cfgServerPower
```

Viewing Power Budget

The server provides power budget status overviews of the power subsystem on the **Power Budget Information** page.

Using the Web Interface

NOTE: To perform power management actions, you must have **Administrative** privilege.

1 Log in to the iDRAC6 Web-based interface.

2 Click the **Power Management** tab.

3 Select the **Power Budget** option.

4 The **Power Budget Information** page displays.

The first table displays the minimum and maximum limits of user-specified power capping thresholds for the current system configuration. These represent the range of AC power consumptions you may set as the system cap. Once selected, this cap would be the maximum AC power load that the system could place upon the datacenter.

Minimum Potential Power Consumption displays the lowest Power Budget Threshold value that you may specify.

Maximum Potential Power Consumption displays the highest Power Budget Threshold value that you may specify. This value is also the current system configuration's absolute maximum power consumption.

Using RACADM

Open a Telnet/SSH text console to the iDRAC, log in, and type:

```
racadm getconfig -g cfgServerPower
```

NOTE: For more information about cfgServerPower, including output details, see "cfgServerPower."

Power Budget Threshold

Power Budget Threshold, if enabled, allows a power capping limit to be set for the system. System performance will be dynamically adjusted to maintain power consumption near the specified threshold. Actual power consumption may be less for light workloads and may momentarily exceed the threshold until performance adjustments have completed.

If you check **Enabled** for the Power budget Threshold, the system will enforce the user-specified threshold. If you leave the Power budget Threshold value **unchecked**, the system will not be power capped. For example, for a given system configuration, the Maximum Potential Power Consumption is 700W and the Minimum Potential Power Consumption is 500W. You can specify and enable a Power Budget Threshold to reduce consumption from its current 650W down to 525W. From that point on the system's performance will be dynamically adjusted to maintain power consumption so as to not exceed the user-specified threshold of 525W.

Using the Web-Based Interface

1   Log in to the iDRAC6 Web-based interface.

2   Click the **Power Management** tab.

3   Select the **Power Budget** option. The **Power Budget Information** page displays.

4   Enter a value in Watts, BTU/hr, or percent in the **Power Budget Threshold** table. The value you specify in Watts or BTU/hr will be the power budget threshold limit value. If you specify a percentage value, it will be a percentage of the Maximum-to-Minimum Potential Power Consumption interval. For example, 100% Threshold means Maximum Potential Power Consumption while 0% means Minimum Potential Power Consumption.

   NOTE: The power budget threshold cannot be more than Maximum Potential Power Consumption or less than Minimum Potential Power Consumption.

5   Check **Enabled** to enable the threshold or leave unchecked. If you specify **Enabled**, the system will enforce the user-specified threshold. If you leave **unchecked**, the system will not be power capped.

6   Click **Apply Changes**.

Using RACADM

```
racadm config -g cfgServerPower -o
cfgServerPowerCapWatts <power cap value in Watts>

racadm config -g cfgServerPower -o
cfgServerPowerCapBTUhr <power cap value in BTU/hr>

racadm config -g cfgServerPower -o -
cfgServerPowerCapPercent <power cap value in % >
```

   NOTE: When setting the power budget threshold in BTU/hr, the conversion to Watts is rounded to the nearest integer. When reading the power budget threshold back, the Watts to BTU/hr conversion is again rounded in this manner. As a result, the value written could be nominally different than the value read; for example, a threshold set to 600 BTU/hr will be read back as 601 BTU/hr.

Viewing Power Monitoring

Using the Web Interface

To view the power monitoring data:

1 Log in to the iDRAC6 Web interface.

2 Select **Power Monitoring** in the system tree. The **Power Monitoring** page displays.

The information provided on the **Power Monitoring** page is described below:

Power Monitoring

- **Status**: **OK** indicates that the power supply units are present and communicating with the server, **Warning** indicates that a warning alert was issued, and **Severe** indicates a failure alert was issued.

- **Probe Name**: System Board System Level. This description indicates the probe is being monitored by its location in the system.

- **Reading**: The current power consumption in Watts/BTU/hr.

Amperage

- **Location**: Displays the name of the power supply unit: PS-n, where n is the power supply number

- **Reading**: The current power consumption in Amps

Power Tracking Statistics

NOTE: There is an outstanding defect in the listing of current time and peak time. The value listed under current time is actually the peak time, and the value under peak time is actually the current time.

- **Cumulative** displays the current cumulative energy consumption for the server measured from the input side of the power supplies. The value is displayed in KWh and it is a cumulative value, which is the total energy used by the system. You can reset this value with the **Reset Cumulative** button.

- **Max Peak Amps** specifies the peak current value within the interval specified by the Start and current times. You can reset this value with the **Reset Max Peaks** button.

- **Max Peak Watts** specifies the peak power value within the interval specified by the Start and current times. You can reset this value with the **Reset Max Peaks** button.

- **Start Time** displays the date and time recorded when the system energy consumption value was last cleared and the new measurement cycle began. For **Cumulative**, you can reset this value with the **Reset Cumulative** button, but it will persist through a system reset or failover operation. For **Max Peak Amps** and **Max Peak Watts**, you can reset this value with the **Reset Max Peaks** button, but it will also persist through a system reset or failover operation.

- **Finish Time** for **Cumulative** displays the current date and time when the system energy consumption was calculated for display. For **Max Peak Amps** and **Max Peak Watts**, the **Finish Time** fields display the time when these peaks occurred.

NOTE: Power Tracking Statistics are maintained across system resets and so reflect all activity in the interval between the stated Start and Finish times. The Reset Max Peaks button will reset the respective field back to zero. In the next table, Power Consumption data is not maintained across system resets and so will reset back to zero on those occasions. The power values displayed are cumulative averages over the respective time interval (previous minute, hour, day and week). Since the Start to Finish time intervals here may differ from those of the Power Tracking Statistics ones, peak power values (Max Peak Watts versus Max Power Consumption) may differ.

Power Consumption

- Displays the average, maximum, and minimum power consumption in the system for the last minute, last hour, last day, and last week.

- Average Power Consumption: Average over previous minute, previous hour, previous day and previous week.

- Max and Min Power Consumption: The maximum and minimum power consumptions observed within the given time interval.

- Max and Min Time: The time when the maximum and minimum power consumptions occurred.

Headroom

System Instantaneous Headroom displays the difference between the power available in the power supply units and the system's current power consumption.

System Peak Headroom displays the difference between the power available in the power supply units and the system's peak power consumption.

Show Graph

Clicking this button displays graphs showing the iDRAC6 Power and Current Consumption in Watts and Amperes, respectively, over the last hour. The user has the option to view these statistics up to a week before, using the drop down menu provided above the graphs.

NOTE: Each data point plotted on the graphs represents the average of readings over a 5 minute period. As a result, the graphs may not reflect brief fluctuations in power or current consumption.

Executing Power Control Operations on the Server

NOTE: To perform power management actions, you must have **Chassis Control Administrator** privilege.

The iDRAC6 enables you to remotely perform several power management actions, such as an orderly shutdown.

Using the Web Interface

1 Log in to the iDRAC6 Web interface.

2 Click the **Power Management** tab. The **Power Control** page displays.

3 Select one of the following **Power Control Operations** by clicking its radio button:

- – **Power On System** turns ON the server's power (the equivalent of pressing the power button when the server power is OFF). This option is disabled if the system is already powered ON.

- – **Power Off System** turns OFF the server's power. This option is disabled if the system is already powered OFF.

- – **NMI (Non-Masking Interrupt)** generates an NMI to halt system operation.

- – **Graceful Shutdown** shuts down the system.

- – **Reset System** (warm boot) resets the system without powering off. This option is disabled if the system is already powered off.

- – **Power Cycle System** (cold boot) powers off and then reboots the system. This option is disabled if the system is already powered OFF.

4 Click **Apply**. A dialog box is displayed requesting confirmation.

5 Click **OK** to perform the power management action you selected (for example, cause the system to reset).

Using RACADM

Open a Telnet/SSH text console to the server, log in, and type:

```
racadm serveraction <action>
```

where `<action>` is powerup, powerdown, powercycle, hardreset, or powerstatus.

18

Using the iDRAC6 Configuration Utility

Overview

The iDRAC6 Configuration Utility is a pre-boot configuration environment that allows you to view and set parameters for the iDRAC6 and for the managed server. Specifically, you can:

- View the firmware revision numbers for the iDRAC6 and Primary Backplane firmware
- Enable, or disable the iDRAC6 local area network
- Enable or disable IPMI Over LAN
- Configure LAN parameters
- Enable or disable Auto–Discovery
- Configure Virtual Media
- Configure Smart Card
- Change the administrative username and password
- Reset the iDRAC6 configuration to the factory defaults
- View System Event Log (SEL) messages or clear messages from the log
- Configure LCD
- Configure System Services

The tasks you can perform using iDRAC6 configuration utility can also be performed using other utilities provided by the iDRAC6 or Dell™ OpenManage™ software, including the Web-based interface, the SM-CLP command line interface, and the local RACADM command line interface.

Starting the iDRAC6 Configuration Utility

1   Turn on or restart the server by pressing the power button on the front of the server.

2   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 **iDRAC6 Configuration Utility** window is displayed. The first two lines provide information about the iDRAC6 firmware and primary backplane firmware revisions. The revision levels can be useful in determining whether a firmware upgrade is needed.

The iDRAC6 firmware is the portion of the information concerned with external interfaces, such as the Web-based 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 iDRAC6 Configuration Utility

Beneath the firmware revision messages, the remainder of the iDRAC6 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 is displayed 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 iDRAC6 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 iDRAC6 Configuration Utility menu items.

iDRAC6 LAN

Use <Left Arrow>, <Right Arrow>, and the spacebar to select between **On** and **Off**.

The iDRAC6 LAN is enabled in the default configuration. The LAN must be enabled to permit the use of iDRAC6 facilities, such as the Web-based interface, telnet/SSH, console redirection, and virtual media.

If you choose to disable the LAN the following warning is displayed:

```
iDRAC6 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 iDRAC6 HTTP, HTTPS, telnet, or SSH ports directly, out-of-band management network traffic, such as IPMI messages sent to the iDRAC6 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 iDRAC6 LAN.

IPMI Over LAN

Press <Left Arrow>, <Right Arrow> and the spacebar to choose between **On** and **Off**. When **Off** is selected, the iDRAC6 will not accept IPMI messages arriving over the LAN interface.

If you choose **Off**, the following warning is displayed:

```
iDRAC IPMI Over LAN Out-of-Band interface will be
disabled if the LAN Channel is OFF.
```

Press any key to clear the message and continue. See "iDRAC6 LAN" 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 18-1. LAN Parameters

Item	Description
Common Settings	
NIC Selection	Press <Right Arrow>, <Left Arrow >, and spacebar to switch between the modes.
	The available modes are **Dedicated, Shared**, **Shared with Failover LOM2**, and **Shared with Failover All LOMs**.
	These modes will allow the iDRAC6 to use the corresponding interface for communication to the outside world.
MAC Address	This is the non-editable MAC address of the iDRAC6 network interface.
VLAN Enable	Select **On** to enable the Virtual LAN filtering for the iDRAC6.
VLAN Id	If **VLAN Enable** is set to **On**, enter any VLAN ID value between 1-4094.
VLAN	If **VLAN Enable** is set to **On**, select the priority of the VLAN between 0-7
Register iDRAC6 Name	Select **On** to register the iDRAC6 name in the DNS service. Select **Off** if you do not want users to locate the iDRAC6 name in DNS.
iDRAC6 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 iDRAC6 name. Press <Esc> to return to the previous menu. The iDRAC6 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 set to **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`.
Host Name String	Press <Enter> to edit. Enter the name of the host for Platform Event Trap (PET) alerts.

Table 18-1. LAN Parameters *(continued)*

Item	Description
LAN Alert Enabled	Select **On** to enable the PET LAN alert.
Alert Policy Entry 1	Select **Enable** or **Disable** to activate the first alert destination.
Alert Destination 1	if **LAN Alert Enabled** is set to **On**, enter the IP address where PET LAN alerts will be forwarded.
IPv4 Settings	Enable or disable support for the IPv4 connection.
IPv4	Select **Enabled** or **Disabled** IPv4 protocol support.
RMCP+ Encryption Key	Press <Enter> to edit the value and <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 (zeros).
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 want to assign to the iDRAC6.
	The default is **192.168.0.120**.
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 iDRAC6. The default is **255.255.255.0**.
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**.

Table 18-1.   LAN Parameters *(continued)*

Item	Description
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.
IPv6 Settings	Enable or disable support for the IPv6 connection.
IP Address Source	Select between **AutoConfig** and **Static**. When **AutoConfig** is selected, the **IPv6 Address 1**, **Prefix Length**, and **Default Gateway** fields are obtained from DHCP.
	When **Static** is selected, the **IPv6 Address 1**, **Prefix Length**, and **Default Gateway** items become editable.
IPv6 Address 1	If the **IP Address Source** is set to **AutoConfig**, this field displays the IP address obtained from DHCP.
	If the **IP Address Source** is set to **Static**, enter the IP address you want to assign to the iDRAC6.
Prefix Length	Configures the Prefix length of the IPv6 address. It can be a value between 1 an 128, inclusive.
Default Gateway	If the **IP Address Source** is set to **AutoConfig**, 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.
IPv6 Link-local Address	This is the non-editable **IPv6 Link-local Address** of the iDRAC6 network interface.
IPv6 Address 2	This is the non-editable **IPv6 Address 2** of the iDRAC6 network interface.
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.

Table 18-1. LAN Parameters *(continued)*

Item	Description
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 first DNS server.
Advanced LAN Configurations	
Auto-Negotiate	If **NIC Selection** is set to **Dedicated**, select between **Enabled** and **Disabled**. When **Enabled** is selected, **LAN Speed Setting** and **LAN Duplex Setting** are configured automatically.
LAN Speed Setting	If **Auto-Negotiate** is set to **Disabled**, select between 10 Mbps and 100 Mbps.
LAN Duplex Setting	If **Auto-Negotiate** is set to **Disabled**, select between **Half Duplex and Full Duplex.**

Virtual Media Configuration

Virtual Media

Press <Enter> to select **Detached, Attached**, or **Auto-Attached**. 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.

Virtual Flash

Press <Enter> to select **Disabled** or **Enabled**.

Disable/Enable will cause a **Detach** and an **Attach** of all Virtual Media devices from the USB bus.

Disable will cause the Virtual Flash to be removed and to become unavailable for use.

⚠ **NOTE:** This field will be read-only if an SD card of a size larger than 256 MB is not present on the iDRAC6 Express card slot.

Smart Card Logon

Press <Enter> to select **Enabled** or **Disabled**. This option configures the Smart Card Logon feature. The available options are **Enabled**, **Disabled**, and **Enabled with RACADM**.

⚠ **NOTE:** When you select Enabled, IPMI Over LAN will be switched off and blocked for editing.

System Services Configuration

System Services

Press <Enter> to select **Enabled** or **Disabled**. See the *Dell Lifecycle Controller User Guide*, available on the Dell Support Website at **support.dell.com\manuals** for more information.

⚠ **NOTE:** Modifying this option will restart the server when you Save and Exit to apply the new settings.

Cancel System Services

Press <Enter> to select **No** or **Yes**.

When you select **Yes**, all Unified Server Configurator sessions are closed and the server is restarted when you **Save** and **Exit** to apply the new settings.

LCD Configuration

Press <Enter> to display the **LCD Configuration** submenu. When you have finished configuring the LCD parameters, press <Esc> to return to the previous menu.

Table 18-2. LCD User Configuration

LCD Line 1	Press <Right Arrow>, <Left Arrow >, and spacebar to switch between the options.
	This feature sets the **Home** display on the LCD to one of the following options:
	Ambient Temp, **Asset Tag**, **Host Name**, **iDRAC6 IPv4 Address**, **iDRAC6 IPv6 Address**, **iDRAC6 MAC Address**, **Model Number**, **None**, **Service Tag**, **System Power**, **User-Defined String**.
LCD User-Defined String	If **LCD Line 1** is set to **User-Defined String**, view or enter the string to be displayed on the LCD.
	The string can be maximum of 62 characters long.
LCD System Power Units	If **LCD Line 1** is set to **System Power**, select **Watt** or **BTU/hr** to specify the Unit to be displayed on the LCD.
LCD Ambient Temp Units	If **LCD Line 1** is set to **Ambient Temp**, select **Celsius** or **Fahrenheit** to specify the Unit to be displayed on the LCD.
LCD Error Display	Select **Simple** or **SEL** (System Event Log).
	This feature allows error messages to be displayed on the LCD in one of two formats:
	The Simple format provides an English language description of the event.
	The SEL format displays a System Event Log text string
LCD Remote KVM Indication	Select **Enabled** to display the text *KVM* whenever a virtual KVM is active on the unit.
LCD Front Panel Access	Press <Right Arrow>, <Left Arrow >, and spacebar to switch between the options: **Disabled, View/Modify**, and **View Only**.
	This setting defines the user access level for the LCD.

LAN User Configuration

The LAN user is the iDRAC6 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 18-3.   LAN User Configuration

Item	Description
Auto–Discovery	The auto–discovery feature enables automated discovery of unprovisioned systems on the network; further, it *securely* establishes initial credentials so that these discovered systems can be managed. This feature enables iDRAC6 to locate the provisioning server. iDRAC6 and provisioning service server mutually authenticate each other. The remote provisioning server sends the user credentials to have iDRAC6 create a user account with these credentials. Once the user account is created, a remote console can establish WS-MAN communication with iDRAC6 using the credentials specified in the discovery process and then send the secure instructions to iDRAC6 to deploy an operating system remotely.
	For information on remote operating system deployment, see the *Dell Lifecycle Controller User Guide* available on the Dell Support website at **support.dell.com/manuals**.
	Do the following prerequisite actions in a *separate* **iDRAC6 Configuration Utility** session *before manually enabling auto-discovery*:
	• Enable NIC
	• Enable IPv4
	• DHCP enable
	• Get domain name from DHCP
	• Disable admin account (account #2)
	• Get DNS server address from DHCP
	• Get DNS domain name from DHCP
	Select **Enabled** to enable the auto discovery feature. By default, this option is **Disabled**. If you have ordered a Dell system with the auto discovery feature **Enabled**, then iDRAC6 on the Dell system is shipped with DHCP enabled with no default credentials for a remote login.

Table 18-3. LAN User Configuration

Item	Description
Auto–Discovery (*continued...*)	Before adding your Dell system to the network and using the auto–discovery feature, ensure that: • Dynamic Host Configuration Protocol (DHCP) server/Domain Name System (DNS) are configured. • Provisioning Web services is installed, configured, and registered.
Account Access	Select **Enabled** to enable the administrator account. Select **Disabled** to disable the administrator account.
IPMI LAN 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 iDRAC6 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 iDRAC6 from the default settings.

Press <Enter> to select the item. The following warning message is displayed:

```
Resetting to factory defaults will restore remote Non-
Volatile user settings. Continue?

< NO (Cancel)   >

< YES (Continue) >
```

Select **YES** and press <Enter> to reset the iDRAC6 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.

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 iDRAC6 Configuration Utility

When you have finished making changes to the iDRAC6 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 iDRAC6 Configuration Utility.

19

Monitoring and Alert Management

This section explains how to monitor the iDRAC6 and provides procedures to configure your system and the iDRAC6 to receive alerts.

Configuring the Managed System to Capture the Last Crash Screen

Before the iDRAC6 can capture the last crash screen, you must configure the managed system with the following prerequisites.

1 Install the managed system software. For more information about installing the managed system software, see the *Server Administrator User's Guide*.

2 Run a supported Microsoft® Windows® operating system with the Windows "automatically reboot" feature deselected in the **Windows Startup and Recovery Settings**.

3 Enable the Last Crash Screen (disabled by default).

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

   ```
   racadm config –g cfgRacTuning –o
   cfgRacTuneAsrEnable 1
   ```

4 Enable the Auto Recovery timer and set the **Auto Recovery** action to **Reset**, **Power Off**, or **Power Cycle**. To configure the **Auto Recovery** timer, you must use Server Administrator or IT Assistant.

   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 must be set to 60 seconds or greater. 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 system has crashed.

Disabling the Windows Automatic Reboot Option

To ensure that the iDRAC6 Web-based interface last crash screen feature works properly, disable the **Automatic Reboot** option on managed systems running the Microsoft Windows Server® 2008 and Windows Server 2003 operating systems.

Disabling the Automatic Reboot Option in Windows 2008 Server

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

2 Click **Advanced System Settings** under **Tasks** on the left.

3 Click the **Advanced** tab.

4 Under **Startup and Recovery**, click **Settings**.

5 Deselect the **Automatically Restart** check box.

6 Click **OK** twice.

Disabling the Automatic Reboot Option in Windows Server 2003

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.

Configuring Platform Events

Platform event configuration provides a mechanism for configuring the remote access device to perform selected actions on certain event messages. These actions include reboot, power cycle, power off, and triggering an alert (Platform Events Trap [PET] and/or e-mail).

The filterable Platform Events include the following:

- Fan Critical Assert Filter

- Battery Warning Assert Filter

- Battery Critical Assert Filter

- Discrete Voltage Critical Assert Filter

- Temperature Warning Assert Filter
- Temperature Critical Assert Filter
- Intrusion Critical Assert Filter
- Redundancy Degraded Filter
- Redundancy Lost Filter
- Processor Warning Assert Filter
- Processor Critical Assert Filter
- Processor Absent Filter
- Event Log Critical Assert Filter
- Watchdog Critical Assert Filter
- System Power Warning Assert Filter
- System Power Critical Assert Filter

When a platform event occurs (for example, a fan probe failure), a system event is generated and recorded in the System Event Log (SEL). If this event matches a platform event filter (PEF) in the Platform Event Filters list in the Web-based interface and you have configured this filter to generate an alert (PET or e-mail), then a PET or e-mail alert is sent to a set of 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)

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

Configuring PEF Using the Web-Based Interface

For detailed information, see "Configuring Platform Event Filters (PEF)."

Configuring PEF Using the RACADM CLI

1 Enable PEF.

   Open a command prompt, type the following command, and press <Enter>:

```
racadm config -g cfgIpmiPef -o cfgIpmiPefEnable -i
1 1
```

where 1 and 1 are the PEF index and the enable/disable selection, respectively.

The PEF index can be a value from 1 through 19. The enable/disable selection can be set to 1 (Enabled) or 0 (Disabled).

For example, to enable PEF with index 5, type the following command:

```
racadm config -g cfgIpmiPef -o cfgIpmiPefEnable -i
5 1
```

2 Configure your PEF actions.

At the command prompt, type the following command and press <Enter>:

```
racadm config -g cfgIpmiPef -o cfgIpmiPefAction -i
1 <action>
```

where the *<action>* values bits are as follows:

- 0 = No alert action
- 1 = power off server
- 2 = reboot server
- 3 = power cycle server

For example, to enable PEF to reboot the server, type the following command:

```
racadm config -g cfgIpmiPef -o cfgIpmiPefAction -i
1 2
```

where 1 is the PEF index and 2 is the PEF action to reboot.

Configuring PET

Configuring PET Using the Web User Interface

For detailed information, see "Configuring Platform Event Traps (PET)."

Configuring PET Using the RACADM CLI

1 Enable your global alerts.

Open a command prompt, type the following command, and press <Enter>:

```
racadm config -g cfgIpmiLan -o
cfgIpmiLanAlertEnable 1
```

2 Enable PET.

At the command prompt, type the following commands and press <Enter> after each command:

```
IPv4:racadm config -g cfgIpmiPet -o
cfgIpmiPetAlertEnable -i 1 1
```

```
IPv6:racadm config -g cfgIpmiPetIpv6 -o
cfgIpmiPetIpv6PetAlertEnable -i 1 1
```

where 1 and 1 are the PET destination index and the enable/disable selection, respectively.

The PET destination index can be a value from 1 through 4. The enable/disable selection can be set to 1 (Enabled) or 0 (Disabled).

For example, to enable PET with index 4, type the following command:

```
iPv4:racadm config -g cfgIpmiPet -o
cfgIpmiPetAlertEnable -i 4 1
```

```
iPv6:racadm config -g cfgIpmiPetIpv6 -o
cfgIpmiPetIpv6PetAlertEnable -i 4 1
```

3 Configure your PET policy.

At the command prompt, type the following command and press <Enter>:

```
iPv4:racadm config -g cfgIpmiPet -o
cfgIpmiPetAlertDestIPAddr -i 1 <IPv4_address>
```

```
iPv6:racadm config -g cfgIpmiPetIpv6 -o
cfgIpmiPetIPv6AlertDestIPAddr -i 1 <IPv6_address>
```

where 1 is the PET destination index and <IPv4_address> and <IPv6_address> are the destination IP addresses 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>
```

Configuring E-Mail Alerts

Configuring E-mail Alerts Using the Web User Interface

For detailed information, see "Configuring E-Mail Alerts."

Configuring E-Mail Alerts Using the RACADM CLI

1 Enable your global alerts.

Open a command prompt, type the following command, and press <Enter>:

```
racadm config -g cfgIpmiLan -o
cfgIpmiLanAlertEnable 1
```

2 Enable e-mail alerts.

At the command prompt, type the following commands and press <Enter> after each command:

```
racadm config -g cfgEmailAlert -o
cfgEmailAlertEnable -i 1 1
```

where 1 and 1 are the e-mail destination index and the enable/disable selection, respectively.

The e-mail destination index can be a value from 1 through 4. The enable/disable selection can be set to 1 (Enabled) or 0 (Disabled).

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.

At the command prompt, type the following command and press <Enter>:

```
racadm config -g cfgEmailAlert -o
cfgEmailAlertAddress -i 1 <e-mail_address>
```

where 1 is the e-mail destination index and <e-mail_address> is the destination e-mail address that receives the platform event alerts.

To configure a custom message, at the command prompt, type the following command and press <Enter>:

```
racadm config -g cfgEmailAlert -o
cfgEmailAlertCustomMsg -i 1 <custom_message>
```

where 1 is the e-mail destination index and <custom_message> is the message displayed in the e-mail alert.

Testing E-mail Alerting

The RAC e-mail alerting feature allows users to receive e-mail alerts when a critical event occurs on the managed system. The following example shows how to test the e-mail alerting feature to ensure that the RAC can properly send out e-mail alerts across the network.

```
racadm testemail -i 2
```

NOTE: Ensure that the SMTP and Email Alert settings are configured before testing the e-mail alerting feature. See "Configuring E-Mail Alerts" for more information.

Testing the RAC SNMP Trap Alert Feature

The RAC SNMP trap alerting feature allows SNMP trap listener configurations to receive traps for system events that occur on the managed system.

The following example shows how a user can test the SNMP trap alert feature of the RAC.

```
racadm testtrap -i 2
```

Before you test the RAC SNMP trap alerting feature, ensure that the SNMP and trap settings are configured correctly. See "**testtrap**" and "**sslkeyupload**" subcommand descriptions to configure these settings.

Frequently Asked Question about SNMP Authentication

Why is the following message displayed:

```
Remote Access: SNMP Authentication Failure
```

As part of discovery, IT Assistant attempts to verify the device's get and set community names. In IT Assistant, you have the get **community name = public** and the set **community name = private.** By default, the community name for the iDRAC6 agent is **public.** When IT Assistant sends out a set request, the iDRAC6 agent generates the SNMP authentication error because it will only accept requests from **community = public.**

NOTE: This is the SNMP agent community name used for discovery.

You can change the iDRAC6 community name using RACADM.

To see the iDRAC6 community name, use the following command:

```
racadm getconfig -g cfgOobSnmp
```

To set the iDRAC6 community name, use the following command:

```
racadm config -g cfgOobSnmp -o
cfgOobSnmpAgentCommunity <community name>
```

To access/configure the iDRAC6 SNMP agent community name using the Web-based interface, go to **Remote Access→Configuration→Services** and click **SNMP Agent**.

To prevent SNMP authentication errors from being generated, you must enter community names that will be accepted by the agent. Since the iDRAC6 only allows one community name, you must use the same **get** and **set** community name for IT Assistant discovery setup.

20

Recovering and Troubleshooting the Managed System

This section explains how to perform tasks related to recovering and troubleshooting a crashed remote system using the iDRAC6 Web-based interface.

- "First Steps to Troubleshoot a Remote System"
- "Managing Power on a Remote System"
- "IPv6 Information"
- "Viewing the Last System Crash Screen"

First Steps to Troubleshoot a Remote System

The following questions are commonly used to troubleshoot high-level problems in the managed system:

1   Is the system powered on or off?

2   If powered on, is the operating system functioning, crashed, or just frozen?

3   If powered off, did the power turn off unexpectedly?

For crashed systems, check the last crash screen (see "Viewing the Last System Crash Screen"), and use console redirection and remote power management (see "Managing Power on a Remote System") to restart the system and watch the reboot process.

Managing Power on a Remote System

The iDRAC6 enables you to remotely perform several power management actions on the managed system so you can recover after a system crash or other system event.

Selecting Power Control Actions from the iDRAC6 Web-Based Interface

To perform power management actions using the Web-based interface, see "Executing Power Control Operations on the Server."

Selecting Power Control Actions from the iDRAC6 CLI

Use the `racadm serveraction` command to perform power management operations on the host system.

`racadm serveraction <action>`

The options for the *<action>* string are:

- **powerdown** — Powers down the managed system.
- **powerup** — Powers up the managed system.
- **powercycle** — Issues a power-cycle operation on the managed system. 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 system.

Viewing System Information

The **System Summary** page displays information about the following system components:

- Main System Chassis
- Integrated Dell Remote Access Controller 6 - Enterprise

To access the system information, expand the **System** tree and click **Properties**.

Main System Chassis

Table 20-1 and Table 20-2 describes the main system chassis properties.

NOTE: To receive Host Name and OS Name information, you must have iDRAC6 services installed on the managed system.

Table 20-1. System Information Fields

Field	Description
Description	System description.
BIOS Version	System BIOS version.
Service Tag	System Service Tag number.
Host Name	Host system's name.
OS Name	Operating system running on the system.

Table 20-2. Auto Recovery Fields

Field	Description
Recovery Action	When a "system hang" is detected, the iDRAC6 can be configured to do 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 time the iDRAC6 will perform a Recovery Action.
Present Countdown	The current value, in seconds, of the countdown timer.

Integrated Dell Remote Access Controller 6 Enterprise

Table 20-3 describes the iDRAC6 Enterprise properties.

Table 20-3. iDRAC6 Enterprise Information Fields

Field	Description
Name	iDRAC6
Product Information	Integrated Dell Remote Access Controller 6 – Enterprise
Date/Time	Current time in the form: Day Month DD HH:MM:SS:YYYY
Firmware Version	iDRAC6 firmware version
Firmware Updated	Date the firmware was last flashed in the form: Day Month DD HH:MM:SS:YYYY

Table 20-3. iDRAC6 Enterprise Information Fields *(continued)*

Field	Description
Hardware Version	Remote Access Controller version
MAC Address	The Media Access Control (MAC) address that uniquely identifies each node in a network

IPv4 Information

Table 20-4 describes the IPv4 properties.

Table 20-4. IPv4 Information Fields

Field	Description
Enabled	**Yes** or **No**
IP Address	The 32-bit address that identifies the Network Interface Card (NIC) to a host. The value is in the dot separated format, such as 143.166.154.127.
Subnet Mask	The Subnet Mask identifies the parts of the IP Address that are the Extended Network Prefix and the Host Number. The value is in the dot separated format, such as 255.255.0.0.
Gateway	The address of a router or a switch. The value is in the dot separated format, such as 143.166.154.1.
DHCP Enabled	**Yes** or **No**. Indicates if the Dynamic Host Configuration Protocol (DHCP) is enabled.

IPv6 Information

Table 20-5 describes the IPv6 properties.

Table 20-5. IPv6 Information Fields

Field	Description
Enabled	Indicates whether Ipv6 stack is enabled.
IP Address 1	Specifies the iDRAC6 NIC IPv6 address.
Prefix Length	An integer specifying the prefix length of the IPv6 address. It can be a value between 1 and 128 inclusive.
IP Gateway	Specifies the iDRAC6 NIC gateway.

Table 20-5. IPv6 Information Fields *(continued)*

Field	Description
Link Local Address	Specifies the iDRAC6 NIC IPv6 address.
IP Address 2	Specifies the iDRAC6 NIC additional IPv6 address if one is available.
Auto Config	AutoConfig lets the Server Administrator obtain the IPv6 address for the iDRAC NIC from the Dynamic Host Configuration Protocol (DHCPv6) server. Also, deactivates and flushes out the Static IP Address, Prefix Length, and Static Gateway values.

Using the System Event Log (SEL)

The **SEL** page displays system-critical events that occur on the managed system.

To view the System Event Log:

1   In the **System** tree, click **System**.

2   Click the **Logs** tab and then click **System Event Log**.

   The **System Event Log** page displays the event severity and provides other information as shown in Table 20-6.

3   Click the appropriate **System Event Log** page button to continue (see Table 20-6).

Table 20-6. Status Indicator Icons

Icon/Category	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.
Date/Time	The date and time that the event occurred. If the date is blank, then the event occurred at System Boot. The format is mm/dd/yyyy hh:mm:ss, based on a 24-hour clock.

Table 20-6. Status Indicator Icons *(continued)*

Icon/Category	Description
Description	A brief description of the event

Table 20-7. SEL Page Buttons

Button	Action
Print	Prints the SEL in the sort order that it is displayed in the window.
Refresh	Reloads the SEL page.
Clear Log	Clears the SEL. **NOTE:** The Clear Log button is displayed 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.

Using the Command Line to View System Log

```
racadm getsel -i
```

The **getsel -i** command displays the number of entries in the SEL.

```
racadm getsel <options>
```

NOTE: If no arguments are specified, the entire log is displayed.

NOTE: See "getsel" for more information on the options you can use.

The **clrsel** command removes all existing records from the SEL.

```
racadm clrsel
```

Using the POST Boot Logs

> **NOTE:** All logs are cleared after the iDRAC6 is rebooted.

This feature of the iDRAC6 allows you to play back a stop motion video of the last three instances of the BIOS POST boot.

To view the POST boot capture logs:

   1   In the **System** tree, click **System**.

   2   Click the **Logs** tab and then click **BOOT Capture** tab.

   3   Select the log number of the POST boot capture log, and click **Play**.

      The video of the logs is opened on a new screen.

      > **NOTE:** You must close an open POST boot capture log video before you play another one. You cannot play two logs simultaneously.

   4   Click **Playback→Play** to start the POST boot capture log video.

   5   Click **STOP** to stop the video.

> **NOTE:** A message asking you to save a **data.jnlp** file instead of opening the viewer may be displayed. To fix this problem, do the following in Internet Explorer: Go to **Tools→Internet Options→Advanced** tab and deselect the option "*Do not save encrypted pages to disk*".

The iDRAC6 Express Card is bonded to the iDRAC6 when you enter the Unified Server Configurator (USC) application by pressing **F10** during boot. If bonding is successful, the following message is logged in the SEL and LCD—iDRAC6 Upgrade Successful. If bonding fails, the following message is logged in the SEL and LCD—iDRAC6 Upgrade Failed. Further, when an iDRAC6 Express Card containing an old or out–of–date iDRAC6 firmware which does not support the specific platform is inserted on the motherboard and the system is booted, a log is generated on the POST screen—iDRAC firmware is out-of-date. Please update to the latest firmware. Update the iDRAC6 Express Card with the latest iDRAC6 firmware for the specific platform. For more information, see the *Dell Lifecycle Controller User Guide*.

Viewing the Last System Crash Screen

> **NOTE:** The last crash screen feature requires the managed system with the **Auto Recovery** feature configured in Server Administrator. In addition, ensure that the **Automated System Recovery** feature is enabled using the iDRAC6. Navigate to the **Services** page under the **Configuration** tab in the **Remote Access** section to enable this feature.

The **Last Crash Screen** page displays the most recent crash screen. The last system crash information is saved in iDRAC6 memory and is remotely accessible.

To view the **Last Crash Screen** page:

1 In the **System** tree, click **System**.

2 Click the **Logs** tab and then click **Last Crash Screen**.

The **Last Crash Screen** page provides the following buttons (see Table 20-8) in the top-right corner of the screen:

Table 20-8.   Last Crash Screen Page Buttons

Button	Action
Print	Prints 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 set to a value less than 30 seconds. Use Server Administrator or IT Assistant to set the System Reset Timer to at least 30 seconds and ensure that the **Last Crash Screen** functions properly. See "Configuring the Managed System to Capture the Last Crash Screen" for additional information.

21

Recovering and Troubleshooting the iDRAC6

This section explains how to perform tasks related to recovering and troubleshooting a crashed iDRAC6.

You can use one of the following tools to troubleshoot your iDRAC6:

- RAC Log
- Diagnostic Console
- Trace Log
- racdump
- coredump

Using the RAC Log

The **RAC Log** is a persistent log maintained in the iDRAC6 firmware. The log contains a list of user actions (such as log in, log out, and security policy changes) and alerts issued by the iDRAC6. The oldest entries are overwritten when the log becomes full.

To access the RAC Log from the iDRAC6 user interface (UI):

1   In the **System** tree, click **Remote Access**.

2   Click the **Logs** tab and then click **RAC Log**.

The **RAC Log** provides the information listed in Table 21-1.

Table 21-1. RAC Log Page Information

Field	Description
Date/ Time	The date and time (for example, `Dec 19 16:55:47`).
	When the iDRAC6 initially starts and is unable to communicate with the managed system, the time will be displayed as `System Boot`.
Source	The interface that caused the event.
Description	A brief description of the event and the user name that logged into the iDRAC6.

Using the RAC Log Page Buttons

The **RAC Log** page provides the buttons listed in Table 21-2.

Table 21-2. RAC Log Buttons

Button	Action
Print	Prints the **RAC Log** page.
Clear Log	Clears the **RAC Log** entries.
	NOTE: The Clear Log button is displayed only if you have Clear Logs permission.
Save As	Opens a pop-up window that enables you to save the **RAC 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 **RAC Log** page.

Using the Command Line

Use the `getraclog` command to view the RAC log entries.

```
racadm getraclog –i
```

The **getraclog -i** command displays the number of entries in the iDRAC6 log.

```
racadm getraclog [options]
```

> **NOTE:** For more information, see "getraclog."

You can use the `clrraclog` command to clear all entries from the RAC log.

```
racadm clrraclog
```

Using the Diagnostic Console

The iDRAC6 provides a standard set of network diagnostic tools
(see Table 21-3) that are similar to the tools included with Microsoft®
Windows® or Linux-based systems. Using the iDRAC6 Web-based interface,
you can access the network debugging tools.

To access the **Diagnostic Console** page:

1 In the **System** tree, click **Remote Access**.

2 Click the **Diagnostics** tab.

Table 21-3 describes the options that are available on the **Diagnostic Console**
page. Type a command and click **Submit**. The debugging results appear in the
Diagnostic Console page.

To refresh the **Diagnostic Console** page, click **Refresh**. To execute another
command, click **Go Back to Diagnostics Page**.

Table 21-3.   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. If the optional interface number is provided in the text field to the right of the **netstat** option, then netstat prints additional information regarding the traffic across the interface, buffer usage, and other network interface information.
ping *<IP Address>*	Verifies that the destination IP address is reachable from the iDRAC6 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.
gettracelog	Displays the iDRAC6 trace log. See "gettracelog" for more information.

Using the Trace Log

The internal iDRAC6 Trace Log is used by administrators to debug iDRAC6 alerting and networking issues.

To access the Trace Log from the iDRAC6 Web-based interface:

1   In the **System** tree, click **Remote Access**.

2   Click the **Diagnostics** tab.

3   Type the **gettracelog** command, or the **racadm gettracelog** command in the **Command** field.

   NOTE: You can use this command from the command line interface also. See "gettracelog" for more information.

The Trace Log tracks the following information:

- DHCP — Traces packets sent to and received from a DHCP server.
- IP — Traces IP packets sent and received.

The trace log may also contain iDRAC6 firmware-specific error codes that are related to the internal iDRAC6 firmware, not the managed system's operating system.

NOTE: The iDRAC6 will not echo an ICMP (ping) with a packet size larger than 1500 bytes.

Using the racdump

The racadm racdump command provides a single command to get dump, status, and general iDRAC6 board information.

NOTE: This command is available only on Telnet and SSH interfaces. For more inform, see the "racdump" command.

Using the coredump

The racadm coredump command displays detailed information related to any recent critical issues that have occurred with the RAC. The coredump information can be used to diagnose these critical issues.

If available, the coredump information is persistent across RAC power cycles and will remain available until either of the following conditions occur:

- The coredump information is cleared using the coredumpdelete subcommand.
- Another critical condition occurs on the RAC. In this case, the coredump information will be relative to the last critical error that occurred.

The racadm coredumpdelete command can be used to clear any currently resident **coredump** data stored in the RAC.

See the "coredump" and "coredumpdelete" subcommands for more information.

22

Sensors

Hardware sensors or probes help you to monitor the systems on your network in a more efficient way by enabling you to take appropriate actions to prevent disasters, such as system instability or damage.

You can use the iDRAC6 to monitor hardware sensors for batteries, fan probes, chassis intrusion, power supplies, power consumed, temperature, and voltages.

Battery Probes

The Battery probes provide information about the system board CMOS and storage RAM on motherboard (ROMB) batteries.

Ø **NOTE:** The Storage ROMB battery settings are available only if the system has a ROMB.

Fan Probes

The fan probe sensor provides information on:

- fan redundancy — the ability of the secondary fan to replace the primary fan if the primary fan fails to dissipate heat at a pre-set speed.
- fan probe list — provides information on the fan speed for all fans in the system.

Chassis Intrusion Probes

The chassis intrusion probes provides status of the chassis, whether chassis is open or closed.

Power Supplies Probes

The power supplies probes provides information on:

• Status of the power supplies

• Power supply redundancy, that is, the ability of the redundant power supply to replace the primary power supply if the primary power supply fails.

NOTE: If there is only one power supply in the system, the Power Supply Redundancy will be set to **Disabled**.

Power Monitoring Probes

Power monitoring provides information about the *real time* consumption of power, in watts and amperes.

You can also view a graphical representation of the consumption of power for the last minute, last hour, last day, or last week from the current time set in the iDRAC6.

Temperature Probe

The temperature sensor provides information about the system board ambient temperature. The temperature probe indicates whether the status of the probe is within the pre-set warning and critical threshold value.

Voltage Probes

The following are typical voltage probes. Your system may have these and/or others present.

• CPU [n] VCORE

• System Board 0.9V PG

• System Board 1.5V ESB2 PG

• System Board 1.5V PG

• System Board 1.8V PG

- System Board 3.3V PG
- System Board 5V PG
- System Board Backplane PG
- System Board CPU VTT
- System Board Linear PG

The voltage probes indicate whether the status of the probes is within the pre-set warning and critical threshold values.

23

Configuring Security Features

The iDRAC6 provides the following security features:

- Advanced Security options for the iDRAC6 administrator:

  - The Console Redirection disable option allows the *local* system user to disable console redirection using the iDRAC6 Console Redirection feature.

  - The local configuration disable features allows the *remote* iDRAC6 administrator to selectively disable the ability to configure the iDRAC6 from:

    – BIOS POST option-ROM

    – operating system using the local RACADM and Dell™ OpenManage™ Server Administrator utilities

- RACADM CLI and Web-based interface operation, which supports 128-bit SSL encryption and 40-bit SSL encryption (for countries where 128-bit is not acceptable)

  Ø **NOTE:** Telnet does not support SSL encryption.

- Session time-out configuration (in seconds) through the Web-based interface or RACADM CLI

- Configurable IP ports (where applicable)

- 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 iDRAC6

Security Options for the iDRAC6 Administrator

Disabling the iDRAC6 Local Configuration

Administrators can disable local configuration through the iDRAC6 graphical user interface (GUI) by selecting **Remote Access→Configuration→Services**. When the **Disable the iDRAC Local Configuration using option ROM** check box is selected, the iDRAC6 Configuration Utility—accessed by pressing <Ctrl+E> during system boot—operates in read-only mode, preventing local users from configuring the device. When the administrator selects the **Disable the iDRAC Local Configuration using RACADM** check box, local users cannot configure the iDRAC6 through the RACADM utility, or the Dell OpenManage Server Administrator, although they can still read the configuration settings.

Administrators can enable one or both of these options at the same time. In addition to enabling them through the Web-based interface, administrators can do so using local RACADM commands.

Disabling Local Configuration During System Reboot

This feature disables the ability of the managed system's user to configure the iDRAC6 during system reboot.

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

NOTE: This option is supported only on the iDRAC6 Configuration Utility. To upgrade to this version, upgrade your BIOS using the BIOS update package from the Dell Support website at **support.dell.com**.

Disabling Local Configuration From Local RACADM

This feature disables the ability of the managed system's user to configure the iDRAC6 using the local RACADM or the Dell OpenManage Server Administrator utilities.

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

CAUTION: These features severely limit the ability of the local user to configure the iDRAC6 from the local system, including performing a reset to default of the configuration. Dell recommends that you use these features with discretion and should disable only one interface at a time to help avoid losing login privileges altogether.

NOTE: See the white paper on *Disabling Local Configuration and Remote Virtual KVM in the DRAC* on the Dell Support site at **support.dell.com** for more information.

Although administrators can set the local configuration options using local RACADM commands, for security reasons they can reset them only from an out-of-band iDRAC6 Web-based interface or command line interface. The `cfgRacTuneLocalConfigDisable` option applies once the system power-on self-test is complete and the system has booted into an operating system environment. The operating system could be one such as Microsoft® Windows Server® or Enterprise Linux operating systems that can run local RACADM commands, or a limited-use operating system such as Microsoft Windows® Preinstallation Environment or vmlinux used to run Dell OpenManage Deployment Toolkit local RACADM commands.

Several situations might call for administrators to disable local configuration. For example, in a data center with multiple administrators for servers and remote access devices, those responsible for maintaining server software stacks may not require administrative access to remote access devices. Similarly, technicians may have physical access to servers during routine systems maintenance—during which they can reboot the systems and access password-protected BIOS—but should not be able to configure remote access devices. In such situations, remote access device administrators may want to disable local configuration.

Administrators should keep in mind that because disabling local configuration severely limits local configuration privileges—including the ability to reset the iDRAC6 to its default configuration—they should only use these options when necessary, and typically should disable only one interface at a time to help avoid losing login privileges altogether. For example, if administrators have disabled all local iDRAC6 users and allow only Microsoft Active Directory® directory service users to log in to the iDRAC6, and the Active Directory authentication infrastructure subsequently fails, the administrators may be unable to log in. Similarly, if administrators have disabled all local configuration and place an iDRAC6 with a static IP address on a network that already includes a Dynamic Host Configuration Protocol (DHCP) server, and the DHCP server subsequently assigns the iDRAC6 IP address to another device on the network, the resulting conflict may disable the out-of-band connectivity of the DRAC, requiring administrators to reset the firmware to its default settings through a serial connection.

Disabling iDRAC6 Remote Virtual KVM

Administrators can selectively disable the iDRAC6 remote KVM, providing a flexible, secure mechanism for a local user to work on the system without someone else viewing the user's actions through console redirection. Using this feature requires installing the iDRAC managed node software on the server. Administrators can disable remote vKVM using the following command:

```
racadm LocalConRedirDisable 1
```

The command LocalConRedirDisable disables existing remote vKVM session windows when executed with the argument 1

To help prevent a remote user from overriding the local user's settings, this command is available only to local RACADM. Administrators can use this command in operating systems that support RACADM, including Microsoft Windows Server 2003 and SUSE Linux Enterprise Server 10. Because this command persists across system reboots, administrators must specifically reverse it to re-enable remote vKVM. They can do so by using the argument 0:

```
racadm LocalConRedirDisable 0
```

Several situations might call for disabling iDRAC6 remote vKVM. For example, administrators may not want a remote iDRAC6 user to view the BIOS settings that they configure on a system, in which case they can disable remote vKVM during the system POST by using the LocalConRedirDisable command. They may also want to increase security by automatically disabling remote vKVM every time an administrator logs in to the system, which they can do by executing the LocalConRedirDisable command from the user logon scripts.

NOTE: See the white paper on *Disabling Local Configuration and Remote Virtual KVM in the DRAC* on the Dell Support site at **support.dell.com** for more information.

For more information on logon scripts, see **technet2.microsoft.com/windowsserver/en/library/31340f46-b3e5-4371-bbb9-6a73e4c63b621033.mspx.**

Securing iDRAC6 Communications Using SSL and Digital Certificates

This subsection provides information about the following data security features that are incorporated in your iDRAC6:

- "Secure Sockets Layer (SSL)"
- "Certificate Signing Request (CSR)"
- "Accessing the SSL Main Menu"
- "Generating a Certificate Signing Request"

Secure Sockets Layer (SSL)

The iDRAC6 includes a Web server that is configured to use the industry-standard SSL security protocol to transfer encrypted data over the Internet. Built upon public-key and private-key encryption technology, SSL is a widely accepted technique for providing authenticated and encrypted communication between clients and servers to prevent eavesdropping across a network.

An SSL-enabled system:

- Authenticates itself to an SSL-enabled client
- Allows the client to authenticate itself to the server
- Allows both systems to establish an encrypted connection

This encryption process provides a high level of data protection. The iDRAC6 employs the 128-bit SSL encryption standard, the most secure form of encryption generally available for Internet browsers in North America.

The iDRAC6 Web server includes a Dell self-signed SSL digital certificate (Server ID). To ensure high security over the Internet, replace the Web server SSL certificate by submitting a request to the iDRAC6 to generate a new Certificate Signing Request (CSR).

Certificate Signing Request (CSR)

A CSR is a digital request to a Certificate Authority (CA) for a secure server certificate. Secure server certificates protect the identity of a remote system and ensure that information exchanged with the remote system cannot be

viewed or changed by others. To ensure security for your DRAC, it is strongly recommended that you generate a CSR, submit the CSR to a CA, and upload the certificate returned from the CA.

A CA 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.

After the CA approves the CSR and sends you a certificate, you must upload the certificate to the iDRAC6 firmware. The CSR information stored on the iDRAC6 firmware must match the information contained in the certificate.

Accessing the SSL Main Menu

1   Expand the **System** tree and click **Remote Access**.

2   Click the **Configuration** tab and then click **SSL**.

Use the **SSL Main Menu** (see Table 23-1) to generate a CSR, upload an existing server certificate, or view an existing server certificate. The CSR information is stored on the iDRAC6 firmware. Table 23-2 describes the buttons available on the **SSL** page.

Table 23-1.   SSL Main Menu

Field	Description
Generate Certificate Signing Request (CSR)	Click **Next** to open the page that enables you to generate a CSR to send to a CA to request a secure Web certificate.
Upload Server Certificate	Click **Next** to upload an existing certificate that your company has title to, and uses to control access to the iDRAC6.
	NOTE: Only X509, Base 64 encoded certificates are accepted by the iDRAC6. DER encoded certificates are not accepted. Upload a new certificate to replace the default certificate you received with your iDRAC6.
View Server Certificate	Click **Next** to view an existing server certificate.

Table 23-2.   SSL Main Menu Buttons

Button	Description
Print	Prints the **SSL Main Menu** page.
Refresh	Reloads the **SSL Main Menu** page.
Next	Navigates to the next page.

Generating a Certificate Signing Request

NOTE: Each CSR overwrites any previous CSR on the firmware. Before iDRAC can accept your signed CSR, the CSR in the firmware must match the certificate returned from the CA.

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

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

   Table 23-3 describes the **Generate Certificate Signing Request (CSR)** page options.

3 Click **Generate** to open or save the CSR.

4 Click the appropriate **Generate Certificate Signing Request (CSR)** page button to continue. Table 23-4 describes the buttons available on the **Generate Certificate Signing Request (CSR)** page.

Table 23-3.   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, spaces, and periods are 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, Enterprise Group). Only alphanumeric characters, hyphens, underscores, periods, and spaces are valid.

Table 23-3.   Generate Certificate Signing Request (CSR) Page Options *(continued)*

Field	Description
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 some 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. Use the drop-down menu to select the country.
Email	The e-mail address associated with the CSR. You can type your company's e-mail address, or any e-mail address you desire to have associated with the CSR. This field is optional.

Table 23-4.   Generate Certificate Signing Request (CSR) Page Buttons

Button	Description
Print	Print the **Generate Certificate Signing Request (CSR)** page.
Refresh	Reloads the **Generate Certificate Signing Request (CSR)** page.
Go Back to SSL Main Menu	Return to the **SSL Main Menu** page.
Generate	Generate a CSR.

Viewing a Server Certificate

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

Table 23-5 describes the fields and associated descriptions listed in the **Certificate** window.

2 Click the appropriate **View Server Certificate** page button to continue.

Table 23-5.   Certificate Information

Field	Description
Serial Number	Certificate serial number

Table 23-5. Certificate Information *(continued)*

Field	Description
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

Using the Secure Shell (SSH)

For information about using SSH, see " Using the Secure Shell (SSH)."

Configuring Services

> **NOTE:** To modify these settings, you must have **Configure iDRAC** permission. Additionally, the remote RACADM command-line utility can only be enabled if the user is logged in as **root**.

1 Expand the **System** tree and click **Remote Access**.

2 Click the **Configuration** tab and then click **Services**.

3 Configure the following services as required:

- Local Configuration (Table 23-6)
- Web server (Table 23-7)
- SSH (Table 23-8)
- Telnet (Table 23-9)
- Remote RACADM (Table 23-10)
- SNMP agent (Table 23-11)
- Automated System Recovery Agent (Table 23-12)

Use the **Automated Systems Recovery Agent** to enable the **Last Crash Screen** functionality of the iDRAC6.

> **NOTE:** **Server Administrator** must be installed with its **Auto Recovery** feature activated by setting the **Action** to either: **Reboot System**, **Power Off System**, or **Power Cycle System**, for the **Last Crash Screen** to function in the iDRAC6.

4 Click **Apply Changes**.

5 Click the appropriate **Services** page button to continue. See Table 23-13.

Table 23-6. Local Configuration Settings

Setting	Description
Disable the iDRAC local configuration using option ROM	Disables local configuration of the iDRAC using option ROM. The option ROM prompts you to enter the setup module by pressing <Ctrl+E> during system reboot.
Disable the iDRAC local configuration using RACADM	Disables local configuration of the iDRAC using local RACADM.

Table 23-7. Web Server Settings

Setting	Description
Enabled	Enables or disables the Web server. Checked=Enabled; Unchecked=Disabled.
Max Sessions	The maximum number of simultaneous sessions allowed for this system.
Active Sessions	The number of current sessions on the system, less than or equal to the **Max Sessions**.
Timeout	The time, in seconds, that a connection is allowed to remain idle. The session is cancelled when the time-out is reached. Changes to the timeout setting take affect immediately and terminate the current Web interface session. The web server will also be reset. Please wait for a few minutes before opening a new Web interface session. The time-out range is 60 to 10800 seconds. The default is 1800 seconds.
HTTP Port Number	The port used by the iDRAC that listens for a server connection. The default setting is 80.
HTTPS Port Number	The port used by the iDRAC that listens for a server connection. The default setting is 443.

Table 23-8. SSH Settings

Setting	Description
Enabled	Enables or disable SSH. When checked, the checkbox indicates that SSH is enabled.
Timeout	The secure shell idle timeout, in seconds. The 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 iDRAC6 listens for an SSH connection. The default is **22**.

Table 23-9. Telnet Settings

Setting	Description
Enabled	Enables or disables telnet. When checked, telnet is enabled.
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 **300**.
Port Number	The port on which the iDRAC6 listens for a telnet connection. The default is **23**.

Table 23-10. Remote RACADM Settings

Setting	Description
Enabled	Enables/disables Remote RACADM. When checked, Remote RACADM is enabled.
Active Sessions	The number of current sessions on the system.
Active Sessions	The number of current sessions on the system, less than or equal to the **Max Sessions**.

Table 23-11. SNMP Agent Settings

Setting	Description
Enabled	Enables or disables the SNMP agent. Checked=Enabled; Unchecked=Disabled.

Table 23-11. SNMP Agent Settings

Setting	Description
Community Name	The name of the community that contains the IP address for the SNMP Alert destination. The Community Name can be up to 31 non-blank characters in length. The default setting is **public**.

Table 23-12. Automated System Recovery Agent Setting

Setting	Description
Enabled	Enables the Automated System Recovery Agent.

Table 23-13. Services Page Buttons

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

Enabling Additional iDRAC6 Security Options

To prevent unauthorized access to your remote system, the iDRAC6 provides the following features:

- IP address filtering (IPRange) — Defines a specific range of IP addresses that can access the iDRAC6.
- IP address blocking — Limits the number of failed login attempts from a specific IP address

These features are disabled in the iDRAC6 default configuration. Use the following subcommand or the Web-based interface to enable these features:

```
racadm config -g cfgRacTuning -o <object_name> <value>
```

Additionally, use these features in conjunction with the appropriate session idle time-out values and a defined security plan for your network.

The following subsections provide additional information about these features.

IP Filtering (IpRange)

IP address filtering (or *IP Range Checking*) allows iDRAC6 access only from clients or management workstations whose IP addresses are within a user-specific range. All other logins 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 of both properties are identical, the incoming login request is allowed to access the iDRAC6. 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 "iDRAC6 Property Database Group and Object Definitions" for a complete list of **cfgRacTuning** properties.

Table 23-14.   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'd 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 establish an iDRAC6 session. Logins from IP addresses that are outside this range will fail. The default values in each property allow an address range from 192.168.1.0 to 192.168.1.255 to establish an iDRAC6 session.
cfgRacTuneIpRangeMask	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.

Enabling IP Filtering

Below is an example command for IP filtering setup.

See "Using RACADM Remotely" for more information about RACADM and RACADM commands.

NOTE: The following RACADM commands block all IP addresses except 192.168.0.57)

To restrict the login to a single IP address (for example, 192.168.0.57), use the full mask, as shown below.

```
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
```

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
```

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 of all 0's in the lower-order bits.

- Use the range base address you prefer as the value for **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.

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 iDRAC6 for a preselected time span.

The IP blocking parameter uses **cfgRacTuning** group features that include:

- The number of allowable login failures

- The timeframe in seconds when these failures must occur

- The amount of time in seconds when the "guilty" IP address is prevented from establishing a session after the total allowable number of failures is exceeded

As login failures accumulate from a specific IP address, they are "aged" 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 "iDRAC6 Property Database Group and Object Definitions" for a complete list of **cfgRacTuning** properties.

Table 23-15 lists the user-defined parameters.

Table 23-15.   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 timespan (**cfgRacTuneIpBlkPenaltyTime**).
cfgRacTuneIpBlkFailCount	Sets the number of login failures from an IP address before the login attempts are rejected.
cfgRacTuneIpBlkFailWindow	The timeframe in seconds when the failure attempts are counted. When the failures exceed this limit, they are dropped from the counter.
cfgRacTuneIpBlkPenaltyTime	Defines the timespan in seconds when all 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 its 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
cfgRacTuneIpBlkFailWindows 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
cfgRacTuneIpBlkFailWindows 60
```

```
racadm config -g cfgRacTuning -o
cfgRacTuneIpBlkPenaltyTime 3600
```

Configuring the Network Security Settings Using the iDRAC6 GUI

NOTE: You must have **Configure iDRAC6** permission to perform the following steps.

1   In the **System** tree, click **Remote Access**.

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

3   In the **Network Configuration** page, click **Advanced Settings**.

4   In the **Network Security** page, configure the attribute values and then click **Apply Changes**.

   Table 23-16 describes the **Network Security** page settings.

5   Click the appropriate **Network Security** page button to continue. See Table 23-17 for description of the **Network Security** page buttons.

Table 23-16. Network Security Page Settings

Settings	Description
IP Range Enabled	Enables the IP Range checking feature, which defines a specific range of IP addresses that can access the iDRAC6.
IP Range Address	Determines the acceptable IP address bit pattern, depending on the 1's in the subnet mask. This value is bitwise AND'd with the IP Range Subnet Mask 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 establish an iDRAC6 session. Logins from IP addresses that are outside this range will fail. The default values in each property allow an address range from 192.168.1.0 to 192.168.1.255 to establish an iDRAC6 session.
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. For example: **255.255.255.0**
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.
IP Blocking Fail Count	Sets the number of login failures attempted from an IP address before the login attempts are rejected from that address.
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.
IP Blocking Penalty Time	The time span in seconds within which login attempts from an IP address with excessive failures are rejected.

Table 23-17. Network Security Page Buttons

Button	Description
Print	Prints the **Network Security** page
Refresh	Reloads the **Network Security** page
Apply Changes	Saves the changes made to the **Network Security** page.
Go Back to Network Configuration Page	Returns to the **Network Configuration** page.

A

RACADM Subcommand Overview

This section provides descriptions of the subcommands that are available in the RACADM command line interface.

⚠️ **CAUTION: Racadm sets the value of objects without performing any functional validation on them. For example, RACADM allows you to set the Certificate Validation object to 1 with the Active Directory object set to 0, even though Certificate Validation will happen only if Active Directory® is enabled. Similarly, the cfgADSSOEnable object can be set to 0 or 1 even if the cfgADEnable object is 0, but it will take effect only if Active Directory is enabled.**

help

📝 **NOTE:** To use this command, you must have **Login to iDRAC** permission.

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
- Remote RACADM
- telnet/ssh/serial RACADM

arp

✎ **NOTE:** To use this command, you must have **Execute Diagnostic Commands** permission.

Table A-2 describes the **arp** command.

Table A-2.   arp Command

Command	Definition
arp	Displays the contents of the ARP table. ARP table entries cannot be added or deleted.

Synopsis

```
racadm arp
```

Supported Interfaces

- Remote RACADM
- telnet/ssh/serial RACADM

clearasrscreen

✎ **NOTE:** To use this command, you must have **Clear Logs** permission.

Table A-3 describes the **clearasrscreen** subcommand.

Table A-3.   clearasrscreen

Subcommand	Definition
clearasrscreen	Clears the last crash screen that is in memory.

Synopsis

`racadm clearasrscreen`

Supported Interfaces

- Local RACADM
- Remote RACADM
- telnet/ssh/serial RACADM

config

NOTE: To use the **getconfig** command, you must have **Log In iDRAC** permission.

Table A-4 describes the **config** and **getconfig** subcommands.

Table A-4. config/getconfig

Subcommand	Definition
config	Configures the iDRAC6.
getconfig	Gets the iDRAC6 configuration data.

Synopsis

`racadm config [-c|-p] -f <filename>`

`racadm config -g <groupName> -o <objectName> [-i <index>] <Value>`

Supported Interfaces

- Local RACADM
- Remote RACADM
- telnet/ssh/serial RACADM

Description

The **config** subcommand allows the user to set iDRAC6 configuration parameters individually or to batch them as part of a configuration file. If the data is different, that iDRAC6 object is written with the new value.

Input

Table A-5 describes the **config** subcommand options.

📖 **NOTE:** The **-f** and **-p** options are not supported for the serial/telnet/ssh console.

Table A-5.   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 iDRAC6. The file must contain data in the format specified in "Parsing Rules."
-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 a decimal integer from 1 through 16. 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 the user to parse the **.cfg** file to locate 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 iDRAC6. 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 10.35.10.100`

  Sets the **cfgNicIpAddress** configuration parameter (object) to the value 10.35.10.110. This IP address object is contained in the group **cfgLanNetworking**.

- `racadm config -f myrac.cfg`

  Configures or reconfigures the iDRAC6. The **myrac.cfg** file may be created from 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 password information. To include this information in the file, it must be input manually. If you want to remove password information from the **myrac.cfg** file during configuration, use the **-p** option.

getconfig

getconfig Subcommand Description

The **getconfig** subcommand allows the user to retrieve iDRAC6 configuration parameters on an individual basis, or all the iDRAC6 configuration groups may be retrieved and saved into a file.

Input

Table A-6 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-6.   getconfig Subcommand Options

Option	Description
-f	The -f *<filename>* option directs getconfig to write the entire iDRAC6 configuration to a configuration file. This file can 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.
-i	The **-i** *<index>*, or **index** option, is valid only for indexed groups and can be used to specify a unique group. The *<index>* is a decimal integer from 1 through 16. If **-i** *<index>* is not specified, a value of 1 is assumed for groups, which are tables that have multiple entries. The index is specified by the index value, not a "named" value.
-o	The -o *<objectname>* or object option specifies the object name that is used in the query. This option is optional and 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** 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 iDRAC6 to **myrac.cfg**.

- `racadm getconfig -h`

  Displays a list of the available configuration groups on the iDRAC6.

- `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 verbose 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
- Remote RACADM
- telnet/ssh/serial RACADM

coredump

📖 **NOTE:** To use this command, you must have **Execute Debug Commands** permission.

Table A-7 describes the **coredump** subcommand.

Table A-7. coredump

Subcommand	Definition
coredump	Displays the last iDRAC6 core dump.

Synopsis

```
racadm coredump
```

Description

The **coredump** subcommand displays detailed information related to any recent critical issues that have occurred with the RAC. The coredump information can be used to diagnose these critical issues.

If available, the coredump information is persistent across iDRAC6 power cycles and will remain available until either of the following conditions occur:

- The coredump information is cleared with the **coredumpdelete** subcommand.
- Another critical condition occurs on the RAC. In this case, the coredump information will be relative to the last critical error that occurred.

See the **coredumpdelete** subcommand for more information about clearing the **coredump**.

Supported Interfaces

- Remote RACADM
- telnet/ssh/serial RACADM

coredumpdelete

📝 **NOTE:** To use this command, you must have **Clear Logs** or **Execute Debug Commands** permission.

Table A-8 describes the **coredumpdelete** subcommand.

Table A-8. coredumpdelete

Subcommand	Definition
coredumpdelete	Deletes the core dump stored in the iDRAC6.

Synopsis

```
racadm coredumpdelete
```

Description

The **coredumpdelete** subcommand can be used to clear any currently resident **coredump** data stored in the RAC.

📝 **NOTE:** If a **coredumpdelete** command is issued and a coredump is not currently stored in the RAC, the command will display a success message. This behavior is expected.

See the **coredump** subcommand for more information on viewing a coredump.

Supported Interfaces

- Local RACADM
- Remote RACADM
- telnet/ssh/serial RACADM

fwupdate

📝 **NOTE:** To use this command, you must have **Configure iDRAC6** permission.

📝 **NOTE:** Before you begin your firmware update, see "Advanced iDRAC6 Configuration" for additional information.

Table A-9 describes the **fwupdate** subcommand.

Table A-9. fwupdate

Subcommand	Definition
fwupdate	Updates the firmware on the iDRAC6

Synopsis

```
racadm fwupdate -s

racadm fwupdate -g -u -a <TFTP_Server_IP_Address> [-d
<path>]

racadm fwupdate -p -u -d <path>

racadm fwupdate -r
```

Description

The **fwupdate** subcommand allows users to update the firmware on the iDRAC6. The user can:

- Check the firmware update process status
- Update the iDRAC6 firmware from a TFTP server by providing an IP address and optional path
- Update the iDRAC6 firmware from the local file system using local RACADM
- Rollback to the standby firmware

Supported Interfaces

- Local RACADM
- Remote RACADM
- telnet/ssh/serial RACADM

Input

Table A-10 describes the **fwupdate** subcommand options.

> **NOTE:** The **-p** option is only supported in local RACADM and is not supported with the remote or the serial/telnet/ssh console. The **-p** option is also not supported on Linux Operating Systems.

Table A-10. fwupdate Subcommand Options

Option	Description
-u	The **update** option performs a checksum of the firmware update file and starts the actual update process. This option may be used along with the **-g** or **-p** options. At the end of the update, the iDRAC6 performs a soft reset.
-s	The **status** option returns the current status of where you are in the update process. This option is always used by itself.
-g	The **get** option instructs the firmware to get the firmware update file from the TFTP server. The user must also specify the **-a** and **-d** options. In the absence of the **-a** option, the defaults are read from properties contained in the group **cfgRemoteHosts**, using properties **cfgRhostsFwUpdateIpAddr** and **cfgRhostsFwUpdatePath**.
-a	The **IP Address** option specifies the TFTP server IP address.
-d	The **-d,** or **directory**, option specifies the directory on the TFTP server or on the iDRAC6's host server where the firmware update file resides.
-p	The **-p**, or **put**, option is used to update the firmware file from the managed system to the iDRAC6. The **-u** option must be used with the **-p** option.
-r	The **rollback** option is used to rollback to the standby firmware.

Output

Displays a message indicating which operation is being performed.

Examples

- `racadm fwupdate -g -u - a 143.166.154.143 -d <path>`

  In this example, the **-g** option tells the firmware to download the firmware update file from a location (specified by the **-d** option) on the TFTP server at a specific IP address (specified by the **-a** option). After the image file is downloaded from the TFTP server, the update process begins. When completed, the iDRAC6 is reset.

- `racadm fwupdate -s`

  This option reads the current status of the firmware update.

- `racadm fwupdate -p -u -d <path>`

  In this example, the firmware image for the update is provided by the host's file system.

NOTE: The **-p** option is not supported in the Remote RACADM interface for the fwupdate subcommand. Remote RACADM firmware update through the local path is not supported on Linux Operating Systems.

getssninfo

NOTE: To use this command, you must have **Login to iDRAC** permission.

Table A-11 describes the **getssninfo** subcommand.

Table A-11. 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 iDRAC6. The summary information provides the following information:

- Username
- IP address (if applicable)
- Session type (for example, serial or telnet)
- Consoles in use (for example, Virtual Media or Virtual KVM)

Supported Interfaces

- Local RACADM
- Remote RACADM
- telnet/ssh/serial RACADM

Input

Table A-12 describes the **getssninfo** subcommand options.

Table A-12.   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 "*" 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-13 provides an example of output from the **racadm getssninfo** command.

Table A-13.   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

📝 **NOTE:** To use this command, you must have **Login to iDRAC** permission.

Table A-14 describes the **racadm getsysinfo** subcommand.

Table A-14.   getsysinfo

Command	Definition
getsysinfo	Displays iDRAC6 information, system information, and watchdog status information.

Synopsis

```
racadm getsysinfo [-d] [-s] [-w] [-A] [-c] [-4] [-6]
[-r]
```

Description

The **getsysinfo** subcommand displays information related to the RAC, managed system, and watchdog configuration.

Supported Interfaces

- Local RACADM
- Remote RACADM
- telnet/ssh/serial RACADM

Input

Table A-15 describes the **getsysinfo** subcommand options.

Table A-15.   getsysinfo Subcommand Options

Option	Description
-4	Displays IPv4 settings
-6	Displays IPv6 settings
-c	Displays common settings
-d	Displays iDRAC6 information
-s	Displays system information
-w	Displays watchdog information
-A	Eliminates the printing of headers/labels

If the **-w** option is not specified, then the other options are used as defaults.

Output

The **getsysinfo** subcommand displays information related to the RAC, managed system, and watchdog configuration.

Sample Output

```
RAC Information:
RAC Date/Time           = 10/01/2008 09:39:53
Firmware Version        = 0.32
Firmware Build          = 55729
Last Firmware Update    = 09/25/2008 18:08:31
Hardware Version        = 0.01
MAC Address             = 00:1e:c9:b2:c7:1f


Common settings:
Register DNS RAC Name   = 0
DNS RAC Name            = iDRAC6
Current DNS Domain      =
Domain Name from DHCP   = 0


IPv4 settings:
Enabled                 = 1
Current IP Address      = 192.168.0.120
Current IP Gateway      = 192.168.0.1
Current IP Netmask      = 255.255.255.0
DHCP Enabled            = 0
Current DNS Server 1    = 0.0.0.0
Current DNS Server 2    = 0.0.0.0
DNS Servers from DHCP   = 0


IPv6 settings:
Enabled                 = 0
Current IP Address 1    = 2002:0000:0000::0001
Current IP Gateway      = ::
Prefix Length           = 64
Autoconfig              = 1
DNS Server from DHCPv6  = 0
Current DNS Server 1    = ::
Current DNS Server 2    = ::
```

```
System Information:
System Model           = PowerEdge R610
System BIOS Version    = 0.2.4
BMC Firmware Version   = 0.32
Service Tag            = AC056
Host Name              =
OS Name                =
Power Status           = ON


Watchdog Information:
Recovery Action        = None
Present countdown value = 15 seconds
Initial countdown value = 15 seconds
```

Examples

- racadm getsysinfo -A -s

  "System Information:" "PowerEdge 2900" "A08" "1.0"
  "EF23VQ-0023" "Hostname"

  "Microsoft Windows 2000 version 5.0, Build Number
  2195, Service Pack 2" "ON"

- racadm getsysinfo -w -s

```
System Information:
System Model           = PowerEdge 2900
System BIOS Version    = 0.2.3
BMC Firmware Version   = 0.17
Service Tag            = 48192
Host Name              = racdev103
OS Name                = Microsoft Windows Server
2003
Power Status           = OFF


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™ systems software is installed on the managed system. If OpenManage is not installed on the managed system, these fields may be blank or inaccurate.

getractime

✎ **NOTE:** To use this command, you must have **Login to iDRAC** permission.

Table A-16 describes the **getractime** subcommand.

Table A-16. 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.mmmmmmms*, 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
20051208201542.000000
```

Supported Interfaces

- Local RACADM
- Remote RACADM
- telnet/ssh/serial RACADM

ifconfig

📝 **NOTE:** To use this command, you must have **Execute Diagnostic Commands** or **Configure iDRAC** permission.

Table A-17 describes the **ifconfig** subcommand.

Table A-17.   ifconfig

Subcommand	Definition
ifconfig	Displays the contents of the network interface table.

Synopsis

```
racadm ifconfig
```

netstat

📝 **NOTE:** To use this command, you must have **Execute Diagnostic Commands** permission.

Table A-18 describes the **netstat** subcommand.

Table A-18.   netstat

Subcommand	Definition
netstat	Displays the routing table and the current connections.

Synopsis

```
racadm netstat
```

Supported Interfaces

- Remote RACADM
- telnet/ssh/serial RACADM

ping

✍ **NOTE:** To use this command, you must have **Execute Diagnostic Commands** or **Configure iDRAC** permission.

Table A-19 describes the **ping** subcommand.

Table A-19. ping

Subcommand	Definition
ping	Verifies that the destination IP address is reachable from the iDRAC6 with the current routing-table contents. A destination IP address is required. An ICMP echo packet is sent to the destination IP address based on the current routing-table contents.

Synopsis

```
racadm ping <ipaddress>
```

Supported Interfaces

- Remote RACADM
- telnet/ssh/serial RACADM

setniccfg

✍ **NOTE:** To use the **setniccfg** command, you must have **Configure iDRAC** permission.

Table A-20 describes the **setniccfg** subcommand.

Table A-20. setniccfg

Subcommand	Definition
setniccfg	Sets the IP configuration for the controller.

✍ **NOTE:** The terms NIC and Ethernet management port may be used interchangeably.

Synopsis

```
racadm setniccfg -d

racadm setniccfg -d6

racadm setniccfg -s <IPv4Address> <netmask> <IPv4
gateway>

racadm setniccfg -s6 <IPv6 Address> <IPv6 Prefix
Length> <IPv6 Gateway>

racadm setniccfg -o
```

Description

The **setniccfg** subcommand sets the controller IP address.

- The **-d** option enables DHCP for the Ethernet management port (default is DHCP disabled).

- The **-d6** option enables AutoConfig for the Ethernet management port. It is enabled by default.

- The **-s** option enables static IP settings. The IPv4 address, netmask, and gateway can be specified. Otherwise, the existing static settings are used. `<IPv4Address>`, `<netmask>`, and `<gateway>` must be typed as dot-separated strings.

- The **-s6** option enables static IPv6 settings. The IPv6 address, Prefix Length, and the IPv6 Gateway can be specified.

- The **-o** option disables the Ethernet management port completely.

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
- Remote RACADM
- telnet/ssh/serial RACADM

getniccfg

📝 **NOTE:** To use the getniccfg command, you must have **Login to iDRAC** permission.

Table A-21 describes the **setniccfg** and **getniccfg** subcommands.

Table A-21.   setniccfg/getniccfg

Subcommand	Definition
getniccfg	Displays the current IP configuration for the controller.

Synopsis

```
racadm getniccfg
```

Description

The **getniccfg** subcommand displays the current Ethernet management port 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
- Remote RACADM
- telnet/ssh/serial RACADM

getsvctag

📝 **NOTE:** To use this command, you must have **Login to iDRAC** permission.

Table A-22 describes the **getsvctag** subcommand.

Table A-22. 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
- Remote RACADM
- telnet/ssh/serial RACADM

racdump

📝 **NOTE:** To use this command, you must have **Debug** permission.

Table A-23 describes the **racdump** subcommand.

Table A-23.   racdump

Subcommand	Definition
racdump	Displays status and general iDRAC6 information.

Synopsis

```
racadm racdump
```

Description

The **racdump** subcommand provides a single command to get dump, status, and general iDRAC6 board information.

The following information is displayed when the **racdump** subcommand is processed:

- General system/RAC information
- Coredump
- Session information
- Process information
- Firmware build information

Supported Interfaces

- Remote RACADM
- telnet/ssh/serial RACADM

racreset

📝 **NOTE:** To use this command, you must have **Configure iDRAC** permission.

Table A-24 describes the **racreset** subcommand.

Table A-24.   racreset

Subcommand	Definition
racreset	Resets the iDRAC6.

📝 **NOTE:** When you issue a racreset subcommand, the iDRAC6 may require up to one minute to return to a usable state.

Synopsis

```
racadm racreset [hard | soft]
```

Description

The **racreset** subcommand issues a reset to the iDRAC6. The reset event is written into the iDRAC6 log.

A hard reset performs a deep reset operation on the RAC. A hard reset should only be performed as a last-case resort to recover the RAC.

📝 **NOTE:** You must reboot your system after performing a hard reset of the iDRAC6 as described in Table A-25.

Table A-25 describes the **racreset** subcommand options.

Table A-25.   racreset Subcommand Options

Option	Description
hard	A *hard* reset performs a deep reset operation on the remote access controller. A hard reset should only be used as a last case resort of resetting the iDRAC6 controller for recovery purposes.
soft	A *soft* reset performs a graceful reboot operation on the RAC.

Examples

- `racadm racreset`

  Start the iDRAC6 soft reset sequence.

- `racadm racreset hard`

  Start the iDRAC6 hard reset sequence.

Supported Interfaces

- Local RACADM
- Remote RACADM
- telnet/ssh/serial RACADM

racresetcfg

✍ **NOTE:** To use this command, you must have **Configure iDRAC** permission.

Table A-26 describes the **racresetcfg** subcommand.

Table A-26.   racresetcfg

Subcommand	Definition
racresetcfg	Resets the entire iDRAC6 configuration to factory default values.

Synopsis

`racadm racresetcfg`

Supported Interfaces

- Local RACADM
- Remote RACADM
- telnet/ssh/serial RACADM

Description

The **racresetcfg** command removes all database property entries that have been configured by the user. The database has default properties for all entries that are used to restore the controller back to its original default settings. After resetting the database properties, the iDRAC6 resets automatically.

NOTE: This command deletes your current iDRAC6 configuration and resets the iDRAC6 and serial configuration to the original default settings. After reset, the default name and password is **root** and **calvin**, respectively, and the IP address is 192.168.0.120. If you issue **racresetcfg** from a network client (for example, a supported Web browser, telnet/ssh, or remote RACADM), you must use the default IP address.

NOTE: Certain iDRAC6 firmware processes need to be stopped and restarted for reset to defaults to complete. iDRAC6 will become unresponsive for about 30 seconds while this operation completes.

serveraction

NOTE: To use this command, you must have **Execute Server Control Commands** permission.

Table A-27 describes the **serveraction** subcommand.

Table A-27.   serveraction

Subcommand	Definition
serveraction	Executes a managed system 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-28 describes the **serveraction** power control options.

Table A-28.   serveraction Subcommand Options

String	Definition
\<action>	Specifies the action. The options for the *\<action>* string are:
	• **powerdown** — Powers down the managed system.
	• **powerup** — Powers up the managed system.
	• **powercycle** — Issues a power-cycle operation on the managed system. 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 system.

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
- Remote RACADM
- telnet/ssh/serial RACADM

getraclog

📝 **NOTE:** To use this command, you must have **Login to iDRAC** permission.

Table A-29 describes the **racadm getraclog** command.

Table A-29.   getraclog

Command	Definition
getraclog -i	Displays the number of entries in the iDRAC6 log.
getraclog	Displays the iDRAC6 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 iDRAC6 log.

The following options allow the **getraclog** command to read entries:

- **-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).
- **-o** — Displays the output in a single line.
- **-s** — Specifies the starting record used for the display

NOTE: If no options are provided, the entire log is displayed.

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 system boots. After the system boots, the system's timestamp is used.

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
- Remote RACADM
- telnet/ssh/serial RACADM

clrraclog

📝 **NOTE:** To use this command, you must have **Clear Logs** permission.

Synopsis

```
racadm clrraclog
```

Description

The **clrraclog** subcommand removes all existing records from the iDRAC6 log. A new single record is created to record the date and time when the log was cleared.

getsel

📝 **NOTE:** To use this command, you must have **Login to iDRAC** permission.

Table A-30 describes the **getsel** command.

Table A-30.   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.

-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).

✍ NOTE: If no arguments are specified, the entire log is displayed.

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
- Remote RACADM
- telnet/ssh/serial RACADM

clrsel

*✍ NOTE: To use this command, you must have **Clear Logs** permission.*

Synopsis

`racadm clrsel`

Description

The **clrsel** command removes all existing records from the system event log (SEL).

Supported Interfaces

- Local RACADM
- Remote RACADM
- telnet/ssh/serial RACADM

gettracelog

📝 **NOTE:** To use this command, you must have **Login to iDRAC** permission.

Table A-31 describes the **gettracelog** subcommand.

Table A-31. gettracelog

Command	Definition
gettracelog -i	Displays the number of entries in the iDRAC6 trace log.
gettracelog	Displays the iDRAC6 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:

-i — Displays the number of entries in the iDRAC6 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 — does 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 system boots. After the system boots, the system's timestamp is used.

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
- Remote RACADM
- telnet/ssh/serial RACADM

sslcsrgen

📖 **NOTE:** To use this command, you must have **Configure iDRAC** permission.

Table A-32 describes the **sslcsrgen** subcommand.

Table A-32.   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

NOTE: The **-f** option is not supported for the serial/telnet/ssh console.

Table A-33 describes the **sslcsrgen** subcommand options.

Table A-33.   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.

Restrictions

The **sslcsrgen** subcommand can only be executed from a local or remote RACADM client and cannot be used in the serial, telnet, or SSH interface.

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
- Remote RACADM
- telnet/ssh/serial RACADM (The **-f** option is not supported for the serial/telnet/ssh console)

sslcertupload

NOTE: To use this command, you must have **Configure iDRAC** permission.

Table A-34 describes the **sslcertupload** subcommand.

Table A-34.   sslcertupload

Subcommand	Description
sslcertupload	Uploads a custom SSL server or CA certificate from the client to the RAC.

Synopsis

```
racadm sslcertupload -t <type> [-f <filename>]
```

Options

Table A-35 describes the **sslcertupload** subcommand options.

Table A-35.   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

Table A-35.   sslcertupload Subcommand Options

Option	Description
-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.

Restrictions

The **sslcertupload** subcommand can only be executed from a local or remote RACADM client. The **sslcsrgen** subcommand cannot be used in the serial, telnet, or SSH interface.

Example

```
racadm sslcertupload -t 1 -f c:\cert\cert.txt
```

Supported Interfaces

- Local RACADM
- Remote RACADM

sslcertdownload

NOTE: To use this command, you must have **Configure iDRAC** permission.

Table A-36 describes the **sslcertdownload** subcommand.

Table A-36.   sslcertdownload

Subcommand	Description
sslcertupload	Downloads an SSL certificate from the iDRAC6 to the client's file system.

Synopsis

```
racadm sslcertdownload -t <type> [-f <filename>]
```

Options

Table A-37 describes the **sslcertdownload** subcommand options.

Table A-37.   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.

Restrictions

The **sslcertdownload** subcommand can only be executed from a local or remote RACADM client. The **sslcsrgen** subcommand cannot be used in the serial, telnet, or SSH interface.

Example

```
racadm sslcertdownload -t 1 -f c:\cert\cert.txt
```

Supported Interfaces

- Local RACADM
- Remote RACADM

sslcertview

📝 **NOTE:** To use this command, you must have **Configure iDRAC** permission.

Table A-38 describes the **sslcertview** subcommand.

Table A-38.   sslcertview

Subcommand	Description
sslcertview	Displays the SSL server or CA certificate that exists on the RAC.

Synopsis

```
racadm sslcertview -t <type> [-A]
```

Options

Table A-39 describes the **sslcertview** subcommand options.

Table A-39.   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)          : iDRAC6 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)          : iDRAC6 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
iDRAC6 default certificate
US
Texas
Round Rock
Dell Inc.
Remote Access Group
iDRAC6 default certificate
Jul 8 16:21:56 2005 GMT
Jul 7 16:21:56 2010 GMT
```

Supported Interfaces

- Local RACADM
- Remote RACADM
- telnet/ssh/serial RACADM

sslkeyupload

📝 **NOTE:** To use this command, you must have **Configure iDRAC** permission.

Table A-40 describes the **sslkeyupload** subcommand.

Table A-40. sslkeyupload

Subcommand	Description
sslkeyupload	Uploads SSL key from the client to the iDRAC6.

Synopsis

```
racadm sslkeyupload -t <type> -f <filename>
```

Options

Table A-41 describes the **sslkeyupload** subcommand options.

Table A-41. sslkeyupload Subcommand Options

Option	Description
-t	Specifies the key to upload.
	1 = SSL key used to generate the server certificate
-f	Specifies the file name of the SSL key to be uploaded.

The **sslkeyupload** command returns 0 when successful and returns a nonzero number when unsuccessful.

Restrictions

The **sslkeyupload** subcommand can only be executed from a local or remote RACADM client. It cannot be used in the serial, telnet, or SSH interface.

Example

```
racadm sslkeyupload -t 1 -f c:\sslkey.txt
```

Supported Interfaces

- Local RACADM
- Remote RACADM

testemail

Table A-42 describes the **testemail** subcommand.

Table A-42.   testemail configuration

Subcommand	Description
testemail	Tests the RAC's e-mail alerting feature.

Synopsis

```
racadm testemail -i <index>
```

Description

Sends a test e-mail from the iDRAC6 to a specified destination.

Prior to executing the test e-mail command, ensure that the specified index in the RACADM **cfgEmailAlert** group is enabled and configured properly. Table A-43 provides a list and associated commands for the **cfgEmailAlert** group.

Table A-43.   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 that the SMTP IP address is configured properly	racadm config -g cfgRemoteHosts -o cfgRhostsSmtpServerIpAddr 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-44 describes the **testemail** subcommand options.

Table A-44.   testemail Subcommands

Option	Description
-i	Specifies the index of the e-mail alert to test.

Output

None.

Supported Interfaces

- Local RACADM
- Remote RACADM
- telnet/ssh/serial RACADM

testtrap

NOTE: To use this command, you must have **Test Alerts** permission.

Table A-45 describes the **testtrap** subcommand.

Table A-45.   testtrap

Subcommand	Description
testtrap	Tests the RAC's SNMP trap alerting feature.

Synopsis

```
racadm testtrap -i <index>
```

Description

The **testtrap** subcommand tests the RAC's SNMP trap alerting feature by sending a test trap from the iDRAC6 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-46 provides a list and associated commands for the **cfgIpmiPet** group.

Table A-46.   cfgEmailAlert 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-47 describes the **testtrap** subcommand options.

Table A-47.   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
- Remote RACADM
- telnet/ssh/serial RACADM

vmdisconnect

> **NOTE:** To use this command, you must have **Access Virtual Media** permission.

Table A-48 describes the **vmdisconnect** subcommand.

Table A-48.   vmdisconnect

Subcommand	Description
vmdisconnect	Closes all open iDRAC6 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-based interface will reflect the correct connection status. This is available only through the use of local or remote RACADM.

The **vmdisconnect** subcommand enables a iDRAC6 user to disconnect all active virtual media sessions. The active virtual media sessions can be displayed in the iDRAC6 Web-based interface or by using the RACADM **getsysinfo** subcommand.

Supported Interfaces

- Local RACADM
- Remote RACADM
- telnet/ssh/serial RACADM

vmkey

> **NOTE:** To use this command, you must have **Access Virtual Media** permission.

Table A-49 describes the **vmkey** subcommand.

Table A-49.   vmkey

Subcommand	Description
vmkey	Performs virtual media key-related operations.

Synopsis

```
racadm vmkey <action>
```

If *<action>* is configured as reset, the Virtual Flash memory is reset to the default size of 256 MB.

Description

When a custom virtual media key image is uploaded to the RAC, the key size becomes the image size. The vmkey subcommand can be used to reset the key back to its original default size, which is 256MB on the iDRAC6.

Supported Interfaces

- Local RACADM
- Remote RACADM
- telnet/ssh/serial RACADM

usercertupload

> **NOTE:** To use this command, you must have **Configure iDRAC** permission.

Table A-50 describes the **usercertupload** subcommand.

Table A-50.   usercertupload

Subcommand	Description
usercertupload	Uploads a user certificate or a user CA certificate from the client to the iDRAC6.

Synopsis

```
racadm usercertupload -t <type> [-f <filename>] -i
<index>
```

Options

Table A-51 describes the **usercertupload** subcommand options.

Table A-51.   usercertupload Subcommand Options

Option	Description
-t	Specifies the type of certificate to upload, either the CA certificate or server certificate.
	1 = user certificate
	2 = user 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.
-i	Index number of the user. Valid values 1-16.

The **usercertupload** command returns 0 when successful and returns a nonzero number when unsuccessful.

Restrictions

The **usercertupload** subcommand can only be executed from a local or a remote RACADM client.

Example

```
racadm usercertupload -t 1 -f c:\cert\cert.txt -i 6
```

Supported Interfaces

- Local RACADM
- Remote RACADM

usercertview

📝 **NOTE:** To use this command, you must have **Configure iDRAC** permission.

Table A-52 describes the **usercertview** subcommand.

Table A-52.   usercertview

Subcommand	Description
usercertview	Displays the user certificate or user CA certificate that exists on the iDRAC6.

Synopsis

```
racadm sslcertview -t <type> [-A] -i <index>
```

Options

Table A-53 describes the **sslcertview** subcommand options.

Table A-53.   sslcertview Subcommand Options

Option	Description
-t	Specifies the type of certificate to view, either the user certificate or the user CA certificate. 1 = user certificate 2 = user CA certificate
-A	Prevents printing headers/labels.
-i	Index number of the user. Valid values are 1-16.

Supported Interfaces

- Local RACADM
- Remote RACADM
- telnet/ssh/serial RACADM

localConRedirDisable

📖 **NOTE:** Only a local RACADM user can execute this command.

Table A-54 describes the **localConRedirDisable** subcommand.

Table A-54.   localConRedirDisable

Subcommand	Description
localConRedirDisable	Disables console redirection to the management station.

Synopsis

`racadm localConRedirDisable <option>`

If `<option>` is set to 1, console redirection is disabled.

If `<option>` is set to 0, console redirection is enabled.

Supported Interfaces

- Local RACADM

krbkeytabupload

📖 **NOTE:** To use this command, you must have **Configure iDRAC** permission.

Table A-55 describes the **krbkeytabupload** subcommand.

Table A-55.   kerbkeytabupload

Subcommand	Description
krbkeytabupload	Uploads a Kerberos keytab file.

Synopsis

`racadm krbkeytabupload [-f <filename>]`

<filename> is the name of the file including the path.

Options

Table A-56 describes the **krbkeytabupload** subcommand options.

Table A-56.   kerbkeytabupload Subcommand Options

Option	Description
-f	Specifies the file name of the keytab to be uploaded. If the file is not specified, the keytab file in the current directory is selected.

The **krbkeytabupload** command returns 0 when successful and returns a non–zero number when unsuccessful.

Restrictions

The **krbkeytabupload** subcommand can only be executed from a local or remote RACADM client.

Example

```
racadm krbkeytabupload -f c:\keytab\krbkeytab.tab
```

Supported Interfaces

- Local RACADM
- Remote RACADM

B

iDRAC6 Property Database Group and Object Definitions

The iDRAC6 property database contains the configuration information for the iDRAC6. 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 iDRAC6. The following sections describe each object and indicate whether the object is readable, writable, or both.

⚠ **CAUTION: Racadm sets the value of objects without performing any functional validation on them. For example, RACADM allows you to set the Certificate Validation object to 1 with the Active Directory object set to 0, even though Certificate Validation can happen only if Active Directory® is enabled. Similarly, the cfgADSSOEnable object can be set to 0 or 1 even if the cfgADEnable object is 0, but it will take effect only if Active Directory is enabled.**

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 iDRAC6 being queried.

One instance of the group is allowed. The following subsections describe the objects in this group.

idRacProductInfo (Read Only)

Legal Values

A 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

A 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 iDRAC type

idRacVersionInfo (Read Only)

Legal Values

A string of up to 63 ASCII characters

Default

<current version number>

Description

String containing the current product firmware version

idRacBuildInfo (Read Only)

Legal Values

A string of up to 16 ASCII characters

Default

The current iDRAC6 firmware build version

Description

String containing the current product build version

idRacName (Read Only)

Legal Values

A string of up to 15 ASCII characters

Default

iDRAC

Description

A user-assigned name to identify this controller

idRacType (Read Only)

Legal Values

Product ID

Default

10

Description

Identifies the remote access controller type as the iDRAC6

cfgLanNetworking

This group contains parameters to configure the iDRAC6 NIC.

One instance of the group is allowed. Some objects in this group may require the iDRAC6 NIC to be reset, which may cause a brief loss in connectivity. Objects that change the iDRAC6 NIC IP address settings will close all active user sessions and require users to reconnect using the updated IP address settings.

cfgNicIPv4Enable (Read/Write)

Legal Values

1 (TRUE)

0 (FALSE)

Default

1

Description

Enables or disables the iDRAC6 IPv4 stack

cfgNicSelection (Read/Write)

Legal Values

0 = Shared

1 = Shared with Failover LOM2

2 = Dedicated

3= Shared with Failover All LOMs (iDRAC6 Enterprise only)

Default

0 (iDRAC6 Express)

2 (iDRAC6 Enterprise)

Description

Specifies the current mode of operation for the RAC network interface controller (NIC). Table B-1 describes the supported modes.

Table B-1.   cfgNicSelection Supported Modes

Mode	Description
Shared	Used if the host server integrated NIC is shared with the RAC on the host server. This mode enables configurations to use the same IP address on the host server and the RAC for common accessibility on the network.
Shared with Failover: LOM 2	Enables teaming capabilities between host server LOM2 integrated network interface controllers.
Dedicated	Specifies that the RAC NIC is used as the dedicated NIC for remote accessibility.
Shared with Failover All LOMs	Enables teaming capabilities between all LOMs on the host server integrated network interface controllers.
	The remote access device network interface is fully functional when the host operating system is configured for NIC teaming. The remote access device receives data through NIC 1 and NIC 2, but transmits data only through NIC 1. Failover occurs from NIC 2 to NIC 3 and then to NIC 4. If NIC 4 fails, the remote access device fails over all data transmission back to NIC 1, but only if the original NIC 1 failure has been corrected.

cfgNicVLanEnable (Read/Write)

Legal Values

1 (TRUE)

0 (FALSE)

Default

0

Description

Enables or disables the VLAN capabilities of the RAC/BMC.

cfgNicVLanId (Read/Write)

Legal Values

1-4094

Default

1

Description

Specifies the VLAN ID for the network VLAN configuration. This property is only valid if **cfgNicVLanEnable** is set to **1** (enabled).

cfgNicVLanPriority (Read/Write)

Legal Values

0 – 7

Default

0

Description

Specifies the VLAN Priority for the network VLAN configuration.
This property is only valid if cfgNicVLanEnable is set to 1 (enabled).

cfgDNSDomainNameFromDHCP (Read/Write)

Legal Values

1 (TRUE)
0 (FALSE)

Default

0

Description

Specifies that the iDRAC6 DNS domain name should be assigned from the network DHCP server

cfgDNSDomainName (Read/Write)

Legal Values

A 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

<blank>

Description

This is the DNS domain name.

cfgDNSRacName (Read/Write)

Legal Values

A 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

idrac-<service tag>

Description

Displays the iDRAC6 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 iDRAC6 name on the DNS server

cfgDNSServersFromDHCP (Read/Write)

Legal Values

1 (TRUE)

0 (FALSE)

Default

0

Description

Specifies if the DNS server IPv4 addresses should be assigned from the DHCP server on the network

cfgDNSServer1 (Read/Write)

Legal Values

String representing a valid IPv4 address. For example: 192.168.0.20.

Default

0.0.0.0

Description

Specifies the IPv4 address for DNS server 1

cfgDNSServer2 (Read/Write)

Legal Values

String representing a valid IPv4 address. For example: 192.168.0.20.

Default

0.0.0.0

Description

Retrieves the IPv4 address for DNS server 2

cfgNicEnable (Read/Write)

Legal Values

1 (TRUE)

0 (FALSE)

Default

1

Description

Enables or disables the iDRAC6 network interface controller. If the NIC is disabled, the remote network interfaces to the iDRAC6 will no longer be accessible.

cfgNicIpAddress (Read/Write)

NOTE: This parameter is only configurable if the **cfgNicUseDhcp** parameter is set to 0 (FALSE).

Legal Values

String representing a valid IPv4 address. For example: 192.168.0.20.

Default

192.168.0.120

Description

Specifies the IPv4 address assigned to the iDRAC6

cfgNicNetmask (Read/Write)

NOTE: This parameter is only configurable if the **cfgNicUseDhcp** parameter is set to 0 (FALSE).

Legal Values

String representing a valid subnet mask. For example: 255.255.255.0.

Default

255.255.255.0

Description

The subnet mask used for the iDRAC6 IP address

cfgNicGateway (Read/Write)

NOTE: This parameter is only configurable if the **cfgNicUseDhcp** parameter is set to 0 (FALSE).

Legal Values

String representing a valid gateway IPv4 address. For example: 192.168.0.1.

Default

192.168.0.1

Description

The iDRAC6 gateway IPv4 address

cfgNicUseDhcp (Read/Write)

Legal Values

1 (TRUE)
0 (FALSE)

Default

0

Description

Specifies whether DHCP is used to assign the iDRAC6 IPv4 address. If this property is set to 1 (TRUE), then the iDRAC6 IPv4 address, subnet mask, and gateway are assigned from the DHCP server on the network. If this property is set to 0 (FALSE), the user can configure the **cfgNicIpAddress**, **cfgNicNetmask**, and **cfgNicGateway** properties.

cfgNicMacAddress (Read Only)

Legal Values

String representing the iDRAC6 NIC MAC address

Default

The current MAC address of the iDRAC6 NIC. For example, 00:12:67:52:51:A3.

Description

The iDRAC6 NIC MAC address

cfgRemoteHosts

This group provides properties that allow configuration of the SMTP server for e-mail alerts.

cfgRhostsFwUpdateTftpEnable (Read/Write)

Legal Values

1 (TRUE)

0 (FALSE)

Default

1

Description

Enables or disables the iDRAC6 firmware update from a network TFTP server

cfgRhostsFwUpdateIpAddr (Read/Write)

Legal Values

A string representing a valid IPv4 address. For example, `192.168.0.61`

Default

0.0.0.0

Description

Specifies the network TFTP server IPv4 address that is used for TFTP iDRAC6 firmware update operations

cfgRhostsFwUpdatePath (Read/Write)

Legal Values

A string with a maximum length of 255 ASCII characters

Default

<blank>

Description

Specifies TFTP path where the iDRAC6 firmware image file exists on the TFTP server. The TFTP path is relative to the TFTP root path on the TFTP server.

NOTE: The server may still require you to specify the drive (for example, **C:**).

cfgRhostsSmtpServerIpAddr (Read/Write)

Legal Values

A string representing a valid SMTP server IPv4 address. For example: 192.168.0.55

Default

0.0.0.0

Description

The IPv4 address of the network SMTP server or TFTP server. The SMTP server transmits e-mail alerts from the iDRAC6 if the alerts are configured and enabled. The TFTP server transfers files to and from the iDRAC6.

cfgUserAdmin

This group provides configuration information about the users who are allowed to access the iDRAC6 through the available remote interfaces.

Up to 16 instances of the user group are allowed. Each instance represents the configuration for an individual user.

cfgUserAdminIndex (Read Only)

Legal Values

1 – 16

Default

<instance>

Description

This number represents the user instance.

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, and 0x0

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-2 describes the user privilege bit values that can be combined to create bit masks.

Table B-2.   Bit Masks for User Privileges

User Privilege	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

Examples

Table B-3 provides sample privilege bit masks for users with one or more privileges.

Table B-3. 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 iDRAC, access virtual media, and access console redirection.	0x00000001 + 0x00000040 + 0x00000080 = 0x000000C1

cfgUserAdminUserName (Read/Write)

 NOTE: This property value must be unique among user names.

Legal Values

A string of up to 16 ASCII characters

Default

root (User 2)

<blank> (All others)

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. The string cannot 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 (Read/Write)

Legal Values

1 (TRUE)

0 (FALSE)

Default

1 (User 2)

0 (All others)

Description

Enables or disables an individual user

cfgUserAdminSolEnable (Read/Write)

Legal Values

1 (TRUE)

0 (FALSE)

Default

0

Description

Enables or disables Serial Over LAN (SOL) user access for the user

cfgUserAdminIpmiSerialPrivilege (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

cfgEmailAlert

This group contains parameters to configure the iDRAC6 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

Description

The unique index of an alert instance

cfgEmailAlertEnable (Read/Write)

Legal Values

1 (TRUE)

0 (FALSE)

Default

0

Description

Enables or disables the alert instance

cfgEmailAlertAddress (Read/Write)

Legal Values

E-mail address format, with a maximum length of 64 ASCII characters

Default

<blank>

Description

Specifies the destination email address for email alerts, for example, user1@company.com

cfgEmailAlertCustomMsg (Read/Write)

Legal Values

A string of up to 32 characters

Default

Description

Specifies a custom message that forms the subject of the alert

cfgSessionManagement

This group contains parameters to configure the number of sessions that can connect to the iDRAC6.

One instance of the group is allowed. The following subsections describe the objects in this group.

cfgSsnMgtRacadmTimeout (Read/Write)

Legal Values

10 –1920

Default

60

Description

Defines the idle timeout in seconds for the Remote RACADM interface. If a remote RACADM session remains inactive for more than the specified sessions, the session will be closed.

cfgSsnMgtConsRedirMaxSessions (Read/Write)

Legal Values

1 – 4

Default

4

Description

Specifies the maximum number of console redirection sessions allowed on the iDRAC6

cfgSsnMgtWebserverTimeout (Read/Write)

Legal Values

60 – 10800

Default

1800

Description

Defines the web server timeout. 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.

cfgSsnMgtSshIdleTimeout (Read/Write)

Legal Values

0 (No timeout)

60 – 1920

Default

300

Description

Defines the secure shell idle timeout. 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:

```
Connection timed out
```

After the message is displayed, the system returns you to the shell that generated the Secure Shell session.

cfgSsnMgtTelnetTimeout (Read/Write)

Legal Values

0 (No timeout)

60 – 1920

Default

300

Description

Defines the telnet idle timeout. 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:

```
Connection timed out
```

After the message is displayed, the system returns you to the shell that generated the telnet session.

cfgSerial

This group contains configuration parameters for the iDRAC6 services.

One instance of the group is allowed. The following subsections describe the objects in this group.

cfgSerialBaudRate (Read/Write)

Legal Values

9600, 28800, 57600, 115200

Default

57600

Description

Sets the baud rate on the iDRAC6 serial port.

cfgSerialConsoleEnable (Read/Write)

Legal Values

1 (TRUE)

0 (FALSE)

Default

0

Description

Enables or disables the RAC serial console interface.

cfgSerialConsoleQuitKey (Read/Write)

Legal Values

A string of up to 4 characters

Default

^\ (<Ctrl><\>)

✍ **NOTE:** The "^" is the <Ctrl> key.

Description

This key or key combination terminates text console redirection when using the **console com2** command. The **cfgSerialConsoleQuitKey** value can be represented by one of the following:

- Decimal value — For example: "95"
- Hexidecimal value — For example: "0x12"
- Octal value — For example: "007"
- ASCII value — For example: "^a"

  ASCII values may be represented using the following Escape Key codes:

  (a) ^ followed by any alphabetic (a-z, A-Z)

  (b) ^ followed by the listed special characters: [ ] \ ^ _

cfgSerialConsoleIdleTimeout (Read/Write)

Legal Values

0 = No timeout
60 – 1920

Default

300

Description

The maximum number of seconds to wait before an idle serial session is disconnected.

cfgSerialConsoleNoAuth (Read/Write)

Legal Values

0 (enables serial login authentication)
1 (disables serial login authentication)

Default

0

Description

Enables or disables the RAC serial console login authentication.

cfgSerialConsoleCommand (Read/Write)

Legal Values

A string of up to 128 characters

Default

<blank>

Description

Specifies a serial command that is executed after a user logs into the serial console interface.

cfgSerialHistorySize (Read/Write)

Legal Values

0 – 8192

Default

8192

Description

Specifies the maximum size of the serial history buffer.

cfgSerialCom2RedirEnable (Read/Write)

Default

1

Legal Values

1 (TRUE)
0 (FALSE)

Description

Enables or disables the console for COM 2 port redirection.

cfgSerialSshEnable (Read/Write)

Legal Values

1 (TRUE)

0 (FALSE)

Default

1

Description

Enables or disables the secure shell (SSH) interface on the iDRAC6

cfgSerialTelnetEnable (Read/Write)

Legal Values

1 (TRUE)

0 (FALSE)

Default

0

Description

Enables or disables the telnet console interface on the iDRAC6

cfgOobSnmp

This group contains parameters to configure the SNMP agent and trap capabilities of the iDRAC6.

One instance of the group is allowed. The following subsections describe the objects in this group.

cfgOobSnmpAgentCommunity (Read/Write)

Legal Values

A string of up to 31 characters

Default

public

Description

Specifies the SNMP Community Name used for SNMP traps

cfgOobSnmpAgentEnable (Read/Write)

Legal Values

1 (TRUE)

0 (FALSE)

Default

0

Description

Enables or disables the SNMP agent in the iDRAC6

cfgRacTuning

This group is used to configure various iDRAC6 configuration properties, such as valid ports and security port restrictions.

cfgRacTuneConRedirPort (Read/Write)

Legal Values

1 – 65535

Default

5900

Description

Specifies the port to be used for keyboard, mouse, video, and virtual media traffic to the RAC.

cfgRacTuneRemoteRacadmEnable (Read/Write)

Legal Values

1 (TRUE)

0 (FALSE)

Default

1

Description

Enables or disables the Remote RACADM interface in the iDRAC

cfgRacTuneCtrlEConfigDisable

Legal Values

1 (TRUE)

0 (FALSE)

Default

0

Description

Enables or disables the ability to disable the ability of the local user to configure the iDRAC from the BIOS POST option-ROM

cfgRacTuneHttpPort (Read/Write)

Legal Values

1 – 65535

Default

80

Description

Specifies the port number to use for HTTP network communication with the iDRAC6

cfgRacTuneHttpsPort (Read/Write)

Legal Values

1 – 65535

Default

443

Description

Specifies the port number to use for HTTPS network communication with the iDRAC6

cfgRacTuneIpRangeEnable (Read/Write)

Legal Values

1 (TRUE)
0 (FALSE)

Default

0

Description

Enables or disables the IPv4 Address Range validation feature of the iDRAC6

cfgRacTuneIpRangeAddr (Read/Write)

Legal Values

An IPv4 address formatted string, for example, 192.168.0.44

Default

192.168.1.1

Description

Specifies the acceptable IPv4 address bit pattern in positions determined by the "1"s in the range mask property (**cfgRacTuneIpRangeMask**)

cfgRacTuneIpRangeMask (Read/Write)

Legal Values

An IPv4 address formatted string, for example, `255.255.255.0`

Default

255.255.255.0

Description

Standard IP mask values with left-justified bits. For example, 255.255.255.0.

cfgRacTuneIpBlkEnable (Read/Write)

Legal Values

1 (TRUE)
0 (FALSE)

Default

0

Description

Enables or disables the IPv4 address blocking feature of the iDRAC6

cfgRacTuneIpBlkFailCount (Read/Write)

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 (Read/Write)

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 (Read/Write)

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 iDRAC6 SSH interface

cfgRacTuneTelnetPort (Read/Write)

Legal Values

1 – 65535

Default

23

Description

Specifies the port number used for the iDRAC6 telnet interface

cfgRacTuneConRedirEnable (Read/Write)

Legal Values

1 (TRUE)
0 (FALSE)

Default

1

Description

Enables console redirection

cfgRacTuneConRedirEncryptEnable (Read/Write)

Legal Values

1 (TRUE)

0 (FALSE)

Default

1

Description

Encrypts the video in a console redirection session

cfgRacTuneAsrEnable (Read/Write)

Ø **NOTE:** This object requires an iDRAC6 reset before it becomes active.

Legal Values

1 (TRUE)

0 (FALSE)

Default

0

Description

Enables or disables the iDRAC6 last crash screen capture feature.

cfgRacTuneDaylightOffset (Read/Write)

Legal Values

0 – 60

Default

0

Description

Specifies the daylight savings offset (in minutes) to use for the RAC Time.

cfgRacTuneTimezoneOffset (Read/Write)

Legal Values

–720 – 780

Default

0

Description

Specifies the timezone offset (in minutes) from GMT/UTC to use for the RAC Time. Some common timezone offsets for timezones in the United States are shown below:

–480 (PST — Pacific Standard Time)

–420 (MST — Mountain Standard Time)

–360 (CST — Central Standard Time)

–300 (EST — Eastern Standard Time).

cfgRacTuneLocalServerVideo (Read/Write)

Legal Values

1 (TRUE)

0 (FALSE)

Default

1

Description

Enables (switches on) or disables (switches off) the local server video.

cfgRacTuneLocalConfigDisable (Read/Write)

Legal Values

0 (TRUE)

1 (FALSE)

Default

0

Description

Disables write access to iDRAC6 configuration data by setting to 1

cfgRacTuneWebserverEnable (Read/Write)

Legal Values

1 (TRUE)

0 (FALSE)

Default

1

Description

Enables or disables the iDRAC6 web server. If this property is disabled, the iDRAC6 will not be accessible using client web browsers. This property has no effect on the telnet/SSH or RACADM interfaces.

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 Only)

Legal Values

A string of up to 255 characters

Default

<blank>

Description

The host name of the managed server

ifcRacMnOsOsName (Read Only)

Legal Values

A string of up to 255 characters

Default

<blank>

Description

The operating system name of the managed server

cfgRacSecurity

This group is used to configure settings related to the iDRAC6 SSL certificate signing request (CSR) feature. The properties in this group must be configured before generating a CSR from the iDRAC6.

See the RACADM **sslcsrgen** subcommand details for more information on generating certificate signing requests.

cfgRacSecCsrCommonName (Read/Write)

Legal Values

A string of up to 254 characters

Default

<blank>

Description

Specifies the CSR Common Name (CN) that must be an IP or the iDRAC name as given in the certificate

cfgRacSecCsrOrganizationName (Read/Write)

Legal Values

A string of up to 254 characters

Default

<blank>

Description

Specifies the CSR Organization Name (O)

cfgRacSecCsrOrganizationUnit (Read/Write)

Legal Values

A string of up to 254 characters

Default

<blank>

Description

Specifies the CSR Organization Unit (OU)

cfgRacSecCsrLocalityName (Read/Write)

Legal Values

A string of up to 254 characters

Default

<blank>

Description

Specifies the CSR Locality (L)

cfgRacSecCsrStateName (Read/Write)

Legal Values

A string of up to 254 characters

Default

<blank>

Description

Specifies the CSR State Name (S)

cfgRacSecCsrCountryCode (Read/Write)

Legal Values

A string of up to 2 characters

Default

<blank>

Description

Specifies the CSR Country Code (CC)

cfgRacSecCsrEmailAddr (Read/Write)

Legal Values

A string of up to 254 characters

Default

Description

Specifies the CSR Email Address

cfgRacSecCsrKeySize (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 iDRAC6 virtual media feature. One instance of the group is allowed. The following subsections describe the objects in this group.

cfgVirMediaAttached (Read/Write)

Legal Values

0 = Detach

1 = Attach

2 = Auto-Attach

Default

0

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 iDRAC6 Web interface or the CLI. Setting this object to 0 will cause the devices to detach from the USB bus.

cfgVirtualBootOnce (Read/Write)

Legal Values

1 (TRUE)

0 (FALSE)

Default

0

Description

Enables or disables the Virtual Boot Once feature of the iDRAC6

cfgVirMediaFloppyEmulation (Read/Write)

NOTE: Virtual Media has to be reattached (using cfgVirMediaAttached) for this change to take effect.

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:.

cfgVirMediaKeyEnable (Read/Write)

Legal Values

1 (TRUE)

0 (FALSE)

Default

0

Description

Enables or disables the virtual media key feature of the RAC

cfgActiveDirectory

This group contains parameters to configure the iDRAC6 Active Directory feature.

cfgADRacDomain (Read/Write)

Legal Values

Any printable text string of up to 254 characters, with no white space

Default

<blank>

Description

Active Directory Domain in which the iDRAC6 resides

cfgADRacName (Read/Write)

Legal Values

Any printable text string of up to 254 characters, with no white space

Default

<blank>

Description

Name of iDRAC6 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 iDRAC6. If this property is disabled, only local iDRAC6 authentication is used for user logins.

cfgADSSOEnable (Read/Write)

Legal Values

1 (TRUE)

0 (FALSE)

Default

0

Description

Enables or disables Active Directory single sign-on authentication on iDRAC6.

cfgADSmartCardLogonEnable (Read/Write)

Legal Values

1 (TRUE)

0 (FALSE)

Default

0

Description

Enables or disables the Smart Card logon on iDRAC6.

cfgADCRLEnable (Read/Write)

Legal Values

1 (TRUE)

0 (FALSE)

Default

0

Description

Enables or disables the Certificate Revocation List (CRL) check for Active Directory-based Smart Card users.

cfgADDomainController1 (Read/Write)

Legal Values

A string of up to 254 ASCII characters representing a valid IP address or a fully qualified domain name (FQDN)

Default

<blank>

Description

The iDRAC6 uses the value you specify to search the LDAP server for user names.

cfgADDomainController2 (Read/Write)

Legal Values

A string of up to 254 ASCII characters representing a valid IP address or a fully qualified domain name (FQDN)

Default

<blank>

Description

The iDRAC6 uses the value you specify to search the LDAP server for user names.

cfgADDomainController3 (Read/Write)

Legal Values

A string of up to 254 ASCII characters representing a valid IP address or a fully qualified domain name (FQDN)

Default

<blank>

Description

The iDRAC6 uses the value you specify to search the LDAP server for user names.

cfgADAuthTimeout (Read/Write)

Legal Values

15 – 300 seconds

Default

120

Description

Specifies the number of seconds to wait for Active Directory authentication requests to complete before timing out

cfgADType (Read/Write)

Legal Values

1 (Extended schema)

2 (Standard schema)

Default

1

Description

Determines the schema type to use with Active Directory

cfgADGlobalCatalog1 (Read/Write)

Legal Values

A string of up to 254 ASCII characters representing a valid IP address or a fully qualified domain name (FQDN)

Default

Description

iDRAC6 uses the value you specify to search the Global Catalog server for user names.

cfgADGlobalCatalog2 (Read/Write)

Legal Values

A string of up to 254 ASCII characters representing a valid IP address or a fully qualified domain name (FQDN)

Default

<blank>

Description

iDRAC6 uses the value you specify to search the Global Catalog server for user names.

cfgADGlobalCatalog3 (Read/Write)

Legal Values

A string of up to 254 ASCII characters representing a valid IP address or a fully qualified domain name (FQDN)

Default

<blank>

Description

iDRAC6 uses the value you specify to search the Global Catalog server for user names.

cfgADCertValidationEnable (Read/Write)

Legal Values

1 (TRUE)

0 (FALSE)

Default

1

Description

Enables or disables Active Directory certificate validation as a part of the Active Directory configuration process.

cfgStandardSchema

This group contains parameters to configure the Active Directory standard schema settings.

cfgSSADRoleGroupIndex (Read Only)

Legal Values

An integer between 1 and 5

Default

<instance>

Description

Index of the Role Group as recorded in the Active Directory

cfgSSADRoleGroupName (Read/Write)

Legal Values

Any printable text string of up 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 of up to 254 characters, with no white space

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-4 to set role-based authority privileges for a Role Group.

Table B-4.   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

Table B-4.   Bit Masks for Role Group Privileges *(continued)*

Role Group Privilege	Bit Mask
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

1 (TRUE)

0 (FALSE)

Default

1

Description

Enables or disables SOL

cfgIpmiSolBaudRate (Read/Write)

Legal Values

9600, 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 iDRAC6 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

1 (TRUE)

0 (FALSE)

Default

0

Description

Enables or disables the IPMI over LAN interface

cfgIpmiLanPrivilegeLimit (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

1 (TRUE)

0 (FALSE)

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 40 characters with no spaces. Only an even amount of digits is allowed.

Default

00000000000000000000

Description

The IPMI encryption key.

cfgIpmiPetCommunityName (Read/Write)

Legal Values

A string of up to 18 characters

Default

public

Description

The SNMP community name for traps

cfgIpmiPetIpv6

This group is used to configure IPv6 platform event traps on the managed server.

cfgIpmiPetIPv6Index (Read Only)

Legal Values

1 – 4

Default

<index value>

Description

Unique identifier for the index corresponding to the trap

cfgIpmiPetIPv6AlertDestIpAddr

Legal Values

IPv6 address

Default

<blank>

Description

Configures the IPv6 alert destination IP address for the trap

cfgIpmiPetIPv6AlertEnable (Read/Write)

Legal Values

1 (TRUE)
0 (FALSE)

Default

0

Description

Enables or disables the IPv6 alert destination for the trap

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

A string of up to 255 characters

Default

The name of the index filter

Description

Specifies the name of the platform event filter

cfgIpmiPefIndex (Read/Write)

Legal Values

1 – 19

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

1 (TRUE)

0 (FALSE)

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 Only)

Legal Values

1 – 4

Default

The index value of a specific platform event trap

Description

Unique identifier for the index corresponding to the trap

cfgIpmiPetAlertDestIpAddr (Read/Write)

Legal Values

A string representing a valid IPv4 address. For example, 192.168.0.67.

Default

0.0.0.0

Description

Specifies the destination IPv4 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

1 (TRUE)

0 (FALSE)

Default

0

Description

Enables or disables a specific trap

cfgUserDomain

This group is used to configure the Active Directory user domain names. A maximum of 40 domain names can be configured at any given time.

cfgUserDomainIndex (Read Only)

Legal Values

1 – 40

Default

The index value

Description

Represents a specific domain

cfgUserDomainName (Read Only)

Legal Values

A string of up to 255 ASCII characters

Default

<blank>

Description

Specifies the Active Directory user domain name

cfgServerPower

This group provides several power management features.

cfgServerPowerStatus (Read Only)

Legal Values

1 (ON)

0 (OFF)

Default

<current server power state>

Description

Represents the server power state, either ON or OFF

cfgServerPowerAllocation (Read Only)

✍ **NOTE:** In case of more than one power supply, this property represents the minimum capacity power supply.

Legal Values

A string of up to 32 characters

Default

<blank>

Description

Represents the available allocated power supply for server usage

cfgServerActualPowerConsumption (Read Only)

Legal Values

A string of up to 32 characters

Default

Description

Represents the power consumed by the server at the current time

cfgServerMinPowerCapacity (Read Only)

Legal Values

A string of up to 32 characters

Default

<blank>

Description

Represents the minimum server power capacity

cfgServerMaxPowerCapacity (Read Only)

Legal Values

A string of up to 32 characters

Default

<blank>

Description

Represents the maximum server power capacity

cfgServerPeakPowerConsumption (Read Only)

Legal Values

A string of up to 32 characters

Default

Description

Represents the maximum power consumed by the server until the current time

cfgServerPeakPowerConsumptionTimestamp (Read Only)

Legal Values

A string of up to 32 characters

Default

Maximum power consumption timestamp

Description

Time when the maximum power consumption was recorded

cfgServerPowerConsumptionClear (Write Only)

Legal Values

1 (TRUE)
0 (FALSE)

Default

****

Description

Resets the cfgServerPeakPowerConsumption (Read/Write) property to 0 and the cfgServerPeakPowerConsumptionTimestamp property to the current iDRAC time.

cfgServerPowerCapWatts (Read/Write)

Legal Values

A string of up to 32 characters

Default

Server power threshold in Watts

Description

Represents the server power threshold in Watts

cfgServerPowerCapBtuhr (Read/Write)

Legal Values

A string of up to 32 characters

Default

Server power threshold in BTU/hr

Description

Represents the Server power threshold in BTU/hr

cfgServerPowerCapPercent (Read/Write)

Legal Values

A string of up to 32 characters

Default

Server power threshold in percentage

Description

Represents the server power threshold in percentage

cfgIPv6LanNetworking

This group is used to configure the IPv6 over LAN networking capabilities.

cfgIPv6Enable

Legal Values

1 (TRUE)

0 (FALSE)

Default

0

Description

Enables or disables the iDRAC6 IPv6 stack

cfgIPv6Address1 (Read/Write)

Legal Values

A string representing a valid IPv6 entry

Default

::

Description

An iDRAC6 IPv6 address

cfgIPv6Gateway (Read/Write)

Legal Values

A string representing a valid IPv6 entry

Default

::

Description

The iDRAC6 gateway IPv6 address

cfgIPv6PrefixLength (Read/Write)

Legal Values

1-128

Default

64

Description

The prefix length for iDRAC6 IPv6 address 1

cfgIPv6AutoConfig (Read/Write)

Legal Values

1 (TRUE)
0 (FALSE)

Default

1

Description

Enables or disables the IPv6 Auto Config option

cfgIPv6LinkLocalAddress (Read Only)

Legal Values

A string representing a valid IPv6 entry

Default

::

Description

The iDRAC6 IPv6 link local address

cfgIPv6Address2 (Read Only)

Legal Values

A string representing a valid IPv6 entry

Default

::

Description

An iDRAC6 IPv6 address

cfgIPv6DNSServersFromDHCP6 (Read/Write)

Legal Values

1 (TRUE)

0 (FALSE)

Default

0

Description

Specifies whether cfgIPv6DNSServer1 and cfgIPv6DNSServer2 are static or DHCP IPv6 addresses

cfgIPv6DNSServer1 (Read/Write)

Legal Values

A string representing a valid IPv6 entry

Default

::

Description

An IPv6 DNS server address

cfgIPv6DNSServer2 (Read/Write)

Legal Values

A string representing a valid IPv6 entry

Default

::

Description

An IPv6 DNS server address

cfgIPv6URL

This group specifies properties used to configure the iDRAC6 IPv6 URL.

cfgIPv6URLstring (Read Only)

Legal Values

A string of up to 80 characters

Default

<blank>

Description

The iDRAC6 IPv6 URL

cfgIpmiSerial

This group specifies properties used to configure the IPMI serial interface of the BMC.

cfgIpmiSerialConnectionMode (Read/Write)

Legal Values

0 (Terminal)

1 (Basic)

Default

1

Description

When the iDRAC6 **cfgSerialConsoleEnable** property is set to 0 (disabled), the iDRAC6 serial port becomes the IPMI serial port. This property determines the IPMI defined mode of the serial port.

In Basic mode, the port uses binary data with the intent of communicating with an application program on the serial client. In Terminal mode, the port assumes that a dumb ASCII terminal is connected and allows very simple commands to be entered.

cfgIpmiSerialBaudRate (Read/Write)

Legal Values

9600, 19200, 57600, 115200

Default

57600

Description

Specifies the baud rate for a serial connection over IPMI

cfgIpmiSerialChanPrivLimit (Read/Write)

Legal Values

2 (User)

3 (Operator)

4 (Administrator)

Default

4

Description

Specifies the maximum privilege level allowed on the IPMI serial channel

cfgIpmiSerialFlowControl (Read/Write)

Legal Values

0 (None)

1 (CTS/RTS)

2 (XON/XOFF)

Default

1

Description

Specifies the flow control setting for the IPMI serial port

cfgIpmiSerialHandshakeControl (Read/Write)

Legal Values

0 (FALSE)

1 (TRUE)

Default

1

Description

Enables or disables the IPMI terminal mode handshake control

cfgIpmiSerialLineEdit (Read/Write)

Legal Values

0 (FALSE)

1 (TRUE)

Default

1

Description

Enables or disables line editing on the IPMI serial interface

cfgIpmiSerialEchoControl (Read/Write)

Legal Values

0 (FALSE)

1 (TRUE)

Default

1

Description

Enables or disables echo control on the IPMI serial interface

cfgIpmiSerialDeleteControl (Read/Write)

Legal Values

0 (FALSE)

1 (TRUE)

Default

0

Description

Enables or disables delete control on the IPMI serial interface

cfgIpmiSerialNewLineSequence (Read/Write)

Legal Values

0 (None)

1 (CR-LF)

2 (NULL)

3 (<CR>)

4 (<LF-CR>)

5 (<LF>)

Default

1

Description

Specifies the newline sequence specification for the IPMI serial interface

cfgIpmiSerialInputNewLineSequence (Read/Write)

Legal Values

0 (<ENTER>)

1 (NULL)

Default

1

Description

Specifies the input newline sequence specification for the IPMI serial interface

cfgSmartCard

This group specifies properties used to support access to iDRAC6 using a smart card.

cfgSmartCardLogonEnable (Read/Write)

Legal Values

0 (Disabled)

1 (Enabled)

2 (Enabled with Remote RACADM)

Default

0

Description

Enables, disables, or enables with Remote RACADM support for access to iDRAC6 using a smart card

cfgSmartCardCRLEnable (Read/Write)

Legal Values

1 (TRUE)

0 (FALSE)

Default

0

Description

Enables or disables the Certificate Revocation List (CRL)

cfgNetTuning

This group enables users to configure the advanced network interface parameters for the RAC NIC. When configured, the updated settings may take up to a minute to become active.

⚠️ **CAUTION: Use extra precaution when modifying properties in this group. Inappropriate modification of the properties in this group can result in your RAC NIC become inoperable.**

cfgNetTuningNicAutoneg (Read/Write)

Legal Values

1 (TRUE)

0 (FALSE)

Default

1

Description

Enables autonegotiation of physical link speed and duplex. If enabled, autonegotiation takes priority over values set in the **cfgNetTuningNic100MB** and **cfgNetTuningNicFullDuplex** objects.

cfgNetTuningNic100MB (Read/Write)

Legal Values

0 (10 MBit)

1 (100 MBit)

Default

1

Description

Specifies the speed to use for the RAC NIC. This property is not used if the **cfgNetTuningNicAutoNeg** is set to **1** (enabled).

cfgNetTuningNicFullDuplex (Read/Write)

Legal Values

0 (Half Duplex)

1 (Full Duplex)

Default

1

Description

Specifies the duplex setting for the RAC NIC. This property is not used if the **cfgNetTuningNicAutoNeg** is set to **1** (enabled).

cfgNetTuningNicMtu (Read/Write)

Legal Values

576 – 1500

Default

1500

Description

The size in bytes of the maximum transmission unit used by the iDRAC6 NIC.

C

Supported RACADM Interfaces

The following table provides an overview of RACADM subcommands and their corresponding interface support.

Table C-1.   RACADM Subcommand Interface Support

Subcommand	Telnet/SSH/Serial	Local RACADM	Remote RACADM
arp	✔	✖	✔
clearasrscreen	✔	✔	✔
clrraclog	✔	✔	✔
clrsel	✔	✔	✔
coredump	✔	✖	✔
coredumpdelete	✔	✔	✔
fwupdate	✔	✔	✔
getconfig	✔	✔	✔
getniccfg	✔	✔	✔
getraclog	✔	✔	✔
getractime	✔	✔	✔
getsel	✔	✔	✔
getssninfo	✔	✔	✔
getsvctag	✔	✔	✔
getsysinfo	✔	✔	✔
gettracelog	✔	✔	✔
help	✔	✔	✔

Table C-1. RACADM Subcommand Interface Support *(continued)*

Subcommand	Telnet/SSH/Serial	Local RACADM	Remote RACADM
ifconfig	✓	✗	✓
netstat	✓	✗	✓
ping	✓	✗	✓
racdump	✓	✗	✓
racreset	✓	✓	✓
racresetcfg	✓	✓	✓
serveraction	✓	✓	✓
setniccfg	✓	✓	✓
sslcertdownload	✗	✓	✓
sslcertupload	✗	✓	✓
sslcertview	✓	✓	✓
sslcsrgen	✗	✓	✓
sslkeyupload	✗	✓	✓
testemail	✓	✓	✓
testtrap	✓	✓	✓
vmdisconnect	✓	✓	✓
vmkey	✓	✓	✓
usercertupload	✗	✓	✓
usercertview	✓	✓	✓
localConRedirDisable	✗	✓	✗

✓ = Supported; ✗ = Not supported

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.

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.

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.

DSU

Abbreviation for disk storage unit.

extended schema

A solution used with Active Directory to determine user access to iDRAC6; 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 iDRAC6.

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).

iDRAC6

Acronym for integrated Dell Remote Access Controller, the integrated System-on-Chip monitor/control system for the Dell 11G 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.

LUN

Acronym for logical unit.

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 iDRAC6 is embedded.

managed system

A system that is monitored by a management station is called a managed system.

management station

The management station is the system from which an administrator remotely manages a Dell system that has an iDRAC6.

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.

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 iDRAC6.

RAM disk
A memory-resident program which emulates a hard drive. The iDRAC6 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.

rollback
To revert back to a previous software or firmware version.

RPM
Abbreviation for RPM 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.

SM-CLP
Abbreviation for Server Management-Command Line Protocol. SM-CLP is a subcomponent of the DMTF SMASH initiative to streamline server management across multiple platforms. The SM-CLP specification, in conjunction with the Managed Element Addressing Specification and numerous profiles to SM-CLP mapping specifications, describes the standardized verbs and targets for various management task executions.

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 iDRAC6 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 iDRAC6; 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.

Unified Server Configurator

The Dell Unified Server Configurator is an embedded configuration utility that enables systems and storage management tasks from an embedded environment throughout the server's lifecycle.

UPS

Abbreviation for uninterruptible power supply.

USB

Abbreviation for Universal Serial Bus.

USC

Abbreviation for Unified Server Configurator.

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.

WS-MAN

Abbreviation for Web Services for Management (WS-MAN) protocol. WS-MAN is a transport mechanism for information exchange. WS-MAN provides a universal language for devices to share data so they can be managed more easily.

Index

S