Integrated Dell Remote
Access Controller 6 (iDRAC6)
Version 1.7

User's Guide

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

7   Using the iDRAC6 Directory Service . . . 141

1

iDRAC6 Overview

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 the 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).

What's New in This Release

- Improved Web GUI performance.
- Improved vFlash performance.
- Out of Band Hardware and Firmware Inventory support.
- Console launch without SSO.
- Work notes.

- Improved System Field Replaceable Unit(FRU) data (Product name, serial number, asset tag, and version in product information area of FRU).
- Identify in Command Line Interface (CLI).
- OEM SEL Event filtering.
- Plain English SEL events.
- Default web certificate update through Command Line Interface.
- Display Life Cycle Controller firmware version display on CLI and GUI.
- Support for platforms PowerEdge(TM) R415, and EqualLogic(TM) DX6000G.
- Support for operating system Redhat Enterprise Linux 6 x64.
- Virtual MAC support.

iDRAC6 Express Management Features

The iDRAC6 Express provides the following management features:

- Provides Dynamic Domain Name System (DDNS) registration.
- Provides remote system management and monitoring using a Web interface and the Server Management Command Line Protocol (SM-CLP) command line over a serial, Telnet, or SSH connection.
- Provides support for Microsoft Active Directory authentication — Centralizes iDRAC6 user IDs and passwords in Active Directory using an extended schema or a standard schema.
- Provides a generic solution to support Lightweight Directory Access Protocol (LDAP) based authentication — This feature does not require any schema extension on your directory services.
- Provides access to system information and status of components for monitoring.
- 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.
- Provides option to add work notes to the Lifecycle Controller Log through the GUI or the CLI.

- Enables you to launch the iDRAC6 Web interface from Dell OpenManage Server Administrator or Dell OpenManage IT Assistant.

- Alerts you to potential managed node issues through an e-mail message or SNMP trap.

- Provides remote power management functions, such as shutdown and reset, from a management console.

- Provides Intelligent Platform Management Interface (IPMI) support.

- Provides secure remote system management through the Web interface.

- Prevents unauthorized access to a remote system through password-level security management.

- Provides assignable permissions for different systems management tasks through role-based authority.

- 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.

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

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

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

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

iDRAC6 Enterprise and vFlash Media

iDRAC6 Enterprise with vFlash Media adds support for RACADM, Virtual Console, Virtual Media features, a dedicated NIC, and vFlash (with an optional Dell vFlash Media card). vFlash allows you to store emergency boot images and diagnostic tools on the vFlash Media. For more information about the 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	iDRAC6 Enterprise with vFlash
Interface and Standards Support				
IPMI 2.0	✓	✓	✓	✓
Web-based GUI	✗	✓	✓	✓
SNMP	✗	✓	✓	✓
WSMAN	✗	✓	✓	✓
SMASH-CLP (SSH-only)	✗	✓	✓	✓
RACADM Command Line (SSH and local)	✗	✓	✓	✓
RACADM Command Line (remote)	✗	✗	✓	✓
Connectivity				
Shared/Failover Network Modes	✓	✓	✓	✓
IPv4	✓	✓	✓	✓
VLAN Tagging	✓	✓	✓	✓
IPv6	✗	✓	✓	✓
Dynamic DNS	✗	✓	✓	✓
Dedicated NIC	✗	✗	✓	✓
Security and Authentication				
Role-based Authority	✓	✓	✓	✓
Local Users	✓	✓	✓	✓
SSL Encryption	✓	✓	✓	✓

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

Feature	BMC	iDRAC6 Express	iDRAC6 Enterprise	iDRAC6 Enterprise with vFlash
Active Directory	✘	✔	✔	✔
Generic LDAP Support	✘	✔	✔	✔
Two-factor Authentication[1]	✘	✔	✔	✔
Single sign-on	✘	✔	✔	✔
PK Authentication (for SSH)	✘	✘	✔	✔
Remote Management and Remediation				
Remote Firmware Update	✔[2]	✔	✔	✔
Server Power Control	✔[2]	✔	✔	✔
Serial-over-LAN (with proxy)	✔	✔	✔	✔
Serial-over-LAN (no proxy)	✔	✔	✔	✔
Power Capping	✔	✔	✔	✔
Last Crash Screen Capture	✘	✔	✔	✔
Boot Capture	✘	✔	✔	✔
Virtual Media[3]	✘	✘	✔	✔
Virtual Console[3]	✘	✘	✔	✔
Virtual Console Sharing[3]	✘	✘	✔	✔
Remote Virtual Console Launch	✘	✘	✔	✔
vFlash	✘	✘	✘	✔

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

Feature	BMC	iDRAC6 Express	iDRAC6 Enterprise	iDRAC6 Enterprise with vFlash
Monitoring				
Sensor Monitoring and Alerting	✔[2]	✔	✔	✔
Real-time Power Monitoring	✔	✔	✔	✔
Real-time Power Graphing	✖	✔	✔	✔
Historical Power Counters	✖	✔	✔	✔
Logging				
System Event Log (SEL)	✔	✔	✔	✔
RAC Log	✖	✔	✔	✔
Remote Syslog	✖	✖	✔	✔
Lifecycle Controller				
Unified Server Configurator	✔[4]	✔	✔	✔
Remote Services (through WS-MAN)	✖	✔	✔	✔
Part Replacement	✖	✖	✖	✔

[1]Two-factor authentication requires Internet Explorer.

[2]Feature is available only through IPMI and not through a Web GUI.

[3]Virtual Console and Virtual Media are available using both Java and Active-X plug-ins.

[4]The Unified Server Configurator available through BMC is limited to operating system installation and diagnostics only.

✔ = Supported; ✖ =Not Supported

The iDRAC6 provides the following security features:

- Single Sign-on, Two-Factor Authentication, and Public Key Authentication.

- User authentication through Active Directory (optional), LDAP authentication (optional) or hardware-stored user IDs and passwords.

- Role-based authorization, 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.

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**.

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**.

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**.

> **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. Internet Explorer 6.0 is not supported.

Supported Remote Access Connections

Table 1-2 lists the connection features.

Table 1-2. Supported Remote Access Connections

Connection	Features
iDRAC6 NIC	• 10 Mbps/100 Mbps Ethernet
	• DHCP support
	• SNMP traps and e-mail event notification
	• Support for SM-CLP (Telnet, SSH, and RACADM) 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
623	RMCP/RMCP+
5900*	Virtual Console keyboard/mouse, Virtual Media Service, Virtual Media Secure Service, and Virtual Console 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 available on the Dell Support website at **support.dell.com/manuals** provide additional information about the setup and operation of the iDRAC6 in your system. On the **Manuals** page, click **Software→ Systems Management**. Click on the appropriate product link on the right-side to access the documents.

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

- The *RACADM Command Line Reference Guide for iDRAC6 and CMC* provides information about the RACADM subcommands, supported interfaces, and iDRAC6 property database groups and object definitions.

- 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 Server Administrator Installation Guide* contains instructions to help you install Dell OpenManage Server Administrator.

- The *Dell OpenManage Management Station Software Installation Guide* contains instructions to help you install Dell OpenManage management station software that includes Baseboard Management Utility, DRAC Tools, and Active Directory Snap-In.

- 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 *Glossary* provides information about the terms used in this document.

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 **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 features like Virtual Console, Virtual Media, Smart Card authentication, and Single Sign-On (SSO).

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. **(Optional)** For 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. **(Optional)** Configure Smart Card authentication — Smart Card provides an added level of security to your enterprise.

4. Configure remote access points, such as Virtual Console 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

Ensure that you have 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" on page 36.

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, only if NIC 1 failure is corrected.

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 **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 on the iDRAC6 software components, see "Installing the Software on the Managed System" on page 37.

Installing iDRAC6 Software

To install iDRAC6 software:

1 Install the iDRAC6 software on the managed system. See "Installing the Software on the Managed System" on page 37.

2 Install the iDRAC6 software on the management station. See "Installing the Software on the Management Station" on page 37.

Configuring iDRAC6

To configure iDRAC6:

1 Use one of the following configuration tools:

   • Web-based interface (see "Configuring the iDRAC6 Using the Web Interface" on page 45)

   • RACADM CLI (see *RACADM Command Line Reference Guide for iDRAC6 and CMC* available at **support.dell.com/manuals**)

   • Telnet console (see "Using a Telnet Console" on page 87)

   ⬛ **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" on page 107.

3 Add and configure iDRAC6 users. See "Adding and Configuring iDRAC6 Users" on page 127.

4 Configure the Web browser to access the Web-based interface. See "Configuring a Supported Web Browser" on page 41.

5 Disable the Microsoft Windows Automatic Reboot Option. See "Disabling the Windows Automatic Reboot Option" on page 314.

6 Update the iDRAC6 Firmware. See "Updating the iDRAC6 Firmware" on page 39.

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" on page 334.

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

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" on page 40)

- RACADM CLI (see "Updating the iDRAC6 Firmware Using RACADM" on page 40)

- Dell Update Packages (see "Updating the iDRAC6 Firmware Using Dell Update Packages for Supported Windows and Linux Operating Systems" on page 41)

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" on page 75.

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
    including the TFTP server IP address.

    Path: *<TFTP server IP>* -d *< Firmware image path on TFTP server>*

    • Case1: If firmimg.d6 image is in tftp root folder, path:
      <TFTPServerIP>
    • Case2: If firmimg.d6 image is in subfolder of tftp root, path:
      <TFTPServerIP> -d /*<SubfolderPath>*

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.

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.

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 Virtual Console on a Red Hat Enterprise Linux (version 4) client with a Simplified Chinese Graphical User Interface (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" on page 85.

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" on page 229. For more information about RACADM commands see the *RACADM iDRAC6 and CMC Command Line Reference Guide* available on the Dell Support website at **support.dell.com/manuals**.

△ **CAUTION: When you refresh the browser by clicking "Refresh" or pressing F5, you may get logged out of the Web Graphical User Interface (GUI) session or be redirected to the "System Summary" page.**

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 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**.

⚠ **CAUTION: If you have opened multiple Web GUI sessions either through <Ctrl+T> or <Ctrl+N> to access the same iDRAC6 from the same management station, and then log out of any one session, all the Web GUI sessions will be terminated.**

Using Multiple Browser Tabs and Windows

Different versions of Web browsers exhibit different behaviors when opening new tabs and windows. Microsoft Internet Explorer version 7 and version 8 have the option to open tabs and windows.

A tab inherits characteristics of a recently opened tab.

Press <Ctrl-T> to open a new tab from the active session and log in again.

Press <Ctrl-N> to open a new browser window from the active session. You are logged in with already authenticated credentials.

Closing a tab expires all iDRAC6 Web interface tabs.

Also, if you log in with Power User privileges on one tab, and then log in as Administrator on another tab, then privileges of the first log in is acquired on both tabs.

Tab behavior for Mozilla Firefox 3 is same as Microsoft Internet Explorer version 7 and version 8 .

Table 4-1. User Privilege Behavior in Supported Browsers

Browser	Tab Behavior	Window Behavior
Microsoft Internet Explorer 6	Not applicable	New session
Microsoft IE7 and IE8	From latest session opened	New session

Configuring the iDRAC6 NIC

This section assumes that the iDRAC6 has already been configured and is accessible on the network. See "Configuring iDRAC6" on page 36 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 Virtual Console 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 **iDRAC Settings→ Network/Security→ Network.**

2 On the **Network** page, you can enter Network settings, Common iDRAC6 settings, IPv4 settings, IPv6 settings, IPMI settings, and VLAN settings. See Table 4-2, Table 4-3, Table 4-4, Table 4-5, Table 4-6, and Table 4-7 for descriptions of these settings.

3 After entering the required settings, click **Apply**.

   The new settings made to the Network page are saved.

🖉 **NOTE:** Changes to the NIC IP address settings close all user sessions and users must reconnect to the iDRAC6 Web interface using the updated IP address settings. For all other changes the NIC must be reset, which may cause a brief loss in connectivity.

Table 4-2. Network Settings

Setting	Description
NIC Selection	Configures the current mode out of the four possible modes: • Dedicated • Shared (LOM1) • Shared with Failover LOM2 • Shared with Failover All LOMs **NOTE:** The **Dedicated** option is only available for iDRAC Enterprise cards and the **Shared with Failover All LOMs** option may be available only for few systems. 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. If the NIC selection is set to **Shared with Failover** (LOM 2 or all LOMs), it is recommended not to connect the LOMs to different network broadcast domains. It is recommended not to team LOMs with add-in network controllers when iDRAC is configured for any shared mode. Any type of team between the LOMs is acceptable irrespective of the NIC selection mode (shared/shared with failover LOM2/shared with failover all LOMs.)
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 4-2. Network Settings *(continued)*

Setting	Description
Auto Negotiation	If set to **On**, displays the Network Speed and Mode by communicating with the nearest router or switch. If set to **Off**, allows you to set the Network Speed and Duplex Mode manually.
	If **NIC Selection** is *not* set to **Dedicated**, Auto Negotiation setting will always be enabled (**On**).
	NOTE: When the server is off, the embedded LOM ports support a maximum speed of 100Mbps. Therefore, configuring the LOMs and switch to support auto-negotiation ensures connectivity to iDRAC through system power transitions.
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**.
NIC MTU	Enables you to set the Maximum Transmission Unit (MTU) size on the NIC.

Table 4-3. Common 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.
Auto Config 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**.

Table 4-3. Common Settings *(continued)*

Setting	Description
DNS Domain Name	The default **DNS Domain Name** is blank. When the **Auto Config Domain Name** checkbox is selected, this option is disabled.

Table 4-4. IPv4 Settings

Setting	Description
Enable IPv4	If NIC is enabled, this selects IPv4 protocol support and sets the other fields in this section to be enabled.
DHCP Enable	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 DNS Server IP address.

Table 4-5. IPv6 Settings

Setting	Description
Enable IPv6	If the checkbox is selected, IPv6 is enabled. If the checkbox is not selected, IPv6 is disabled. The default is disabled.
Autoconfiguration Enable	Check this box to allow the iDRAC6 to obtain the IPv6 address for the iDRAC6 NIC from the Dynamic Host Configuration Protocol (DHCPv6) server. Enabling autoconfiguraion 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.
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 Link Local IPv6 address.
IP Address 2...15	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 4-5.   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 clear **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 clear **Use DHCP to obtain DNS Server Addresses**.

Table 4-6.   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 value is all zeros.

Table 4-7.   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.

Configuring IP Filtering and IP Blocking

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

1 Click **iDRAC Settings**→ **Network/Security** 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**.

3 After configuring the settings, click **Apply**.

Saves any new settings that you made to the Network Security page.

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. Log ins 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.**

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 4-9.

Table 4-9.   Platform Event Filters

Index	Platform Event
1	Fan Critical Assert
2	Battery Warning Assert
3	Battery Critical Assert
4	Voltage Critical Assert
5	Temperature Warning Assert
6	Temperature Critical Assert
7	Intrusion Critical Assert
8	Redundancy Degraded
9	Redundancy Lost
10	Processor Warning Assert
11	Processor Critical Assert
12	Processor Absent Critical Assert
13	Power Supply Warning Assert
14	Power Supply Critical Assert
15	Power Supply Absent Critical Assert
16	Event Log Critical Assert
17	Watchdog Critical Assert
18	System Power Warning Assert
19	System Power Critical Assert
20	Removable Flash Media Absent Informational Assert
21	Removable Flash Media Critical Assert

Table 4-9. Platform Event Filters *(continued)*

Index	Platform Event
22	Removable Flash Media Warning 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" on page 46.

2 Click **System**→ **Alerts**→ **Platform Events**.

3 Under **Platform Event Filters Configuration**, select the **Enabled** option to **Enable Platform Event Filter Alerts**.

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 **Platform Event Filters List** table, do the following for the filter(s) that you want to configure:

- Select one of the following actions:

  - Reboot System

  - Power Cycle System

  - Power Off System

  - No Action

- In the **Generate Alert** column, select the checkbox to enable alert generation or clear the checkbox to disable alert generation for the selected action.

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

5 Click **Apply**. The settings are saved.

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.

2 Ensure that you have performed the procedures in "Configuring Platform Event Filters (PEF)" on page 57.

3 Click **System→ Alerts→ Traps Settings**.

4 In the **IPv4 Destination List** or the **IPv6 Destination List**, do the following for the **Destination Number** to configure the IPv4 or IPv6 SNMP alert destination:

a Select or clear the **State** checkbox. A selected checkbox indicates that the IP address is enabled to receive the alerts. A clear checkbox indicates that the IP address is disabled for receiving alerts.

b In **Destination IPv4 Address** or **Destination IPv6 Address**, enter a valid platform event trap destination IP address.

c   In **Test Trap**, click **Send** to test the configured alert.

✍ NOTE: Your user account must have **Test Alerts** permission to send a test trap. See Table 6-6 for more information.

The changes you specified are displayed in either the IPv4 or IPv6 **Destination List**.

5   In the **Community String** field, enter the iDRAC SNMP community name.

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

6   Click **Apply**. The settings are saved.

✍ NOTE: If you disable a Platform Event Filter, the trap associated with that sensor going "bad" is also disabled. If the **Enable Platform Event Filter Alerts** option is enabled, Traps associated with "bad to good" transitions are always generated. For example, if you disable the **Generate Alert** option for the **Removable Flash MEdia Absent Informational Assert Filter** and remove the SD card, the associated trap is not displayed. The trap is generated if you insert the SD card again. But if you enable the **Enable Platform Event Filter Alerts** option, a trap is generated when you remove or insert the SD card.

Configuring E-Mail Alerts

✍ NOTE: If your mail server is Microsoft Exchange Server 2007, ensure that iDRAC domain name is configured for the mail server to receive the email alerts from iDRAC.

✍ 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 have performed the procedures in "Configuring Platform Event Filters (PEF)" on page 57.

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

4   In the **Destination Email Addresses** table, do the following to configure a destination address for the **Email Alert Number**:

a   Select or clear the **State** checkbox. A selected checkbox indicates that the email address is enabled to receive the alerts. A clear checkbox indicates that the email address is disabled for receiving alert messages.

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

> **c** In the **E-mail Description** field, type a short description.

5 In **Test Email**, click **Send** to test the configured e-mail alert settings.

6 In the **SMTP (e-mail) Server IP Address** field, enter a valid IP address or FQDN (fully qualified domain name) of the SMTP server to be used in the configuration.

> ✐ **NOTE:** To successfully send a test e-mail, the **SMTP (email) Server IP Address** must be configured on the **Email 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.

7 Click **Apply**. The settings are saved.

Configuring IPMI Using Web Interface

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

2 Configure IPMI over LAN.

> **a** In the **System** tree, click **iDRAC Settings**.

> **b** Click the **Network/Security** tab and click **Network**.

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

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

> **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**.

> ✐ **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 **iDRAC Settings**.

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

    c In the **Serial Over LAN** 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**.

    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 and then select either **User**, or **Operator**, or **Administrator**.

    g Click **Apply**.

4 Configure IPMI Serial.

    a In the **Network/Security** tab, click **Serial**.

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

      Under **IPMI Serial**, click the **Connection Mode Setting**s drop-down menu, and 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**.

    d Set the **Channel Privilege Level Limit** and **Flow Control**.

    e Click **Apply**.

    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" on page 127 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 **iDRAC Settings**→ **Network/Security**.

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 4-10 describes the above **SSL** page options.

Table 4-10. 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. 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

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 4-11 describes the CSR attributes.

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

4 Click **Go Back to SSL Main Menu** to return to the SSL page.

Table 4-11.   Generate Certificate Signing Request (CSR) Attributes

Field	Description
Common Name	The exact name being certified (usually the iDRAC's domain name, for example, **xyzcompany.com**). Alphanumeric characters, hyphens and periods are valid.
Organization Name	The name associated with this organization (for example, XYZ Corporation). Alphanumeric characters, hyphens and periods are valid.
Organization Unit	The name associated with an organizational unit, such as a department (for example, Information Technology). Alphanumeric characters, hyphens and periods are valid.
Locality	The city or other location of the entity being certified (for example, Round Rock). Alphanumeric characters, hyphens and periods are valid.
State Name	The state or province where the entity who is applying for a certification is located (for example, Texas). Alphanumeric characters, hyphens and periods 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.

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 **Go Back to SSL Main Menu** to return to the **SSL Main Menu** page.

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 4-12 describes the fields and associated descriptions listed in the **Certificate** table.

2   Click **Go Back to SSL Main Menu** to return to the **SSL Main Menu** page.

Table 4-12.   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

Configuring and Managing Active Directory

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

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

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

note: **NOTE:** For detailed information about Active Directory configuration and how to configure Active Directory with Extended Schema or Standard Schema, see "Using the iDRAC6 Directory Service" on page 141.

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

1 Click **iDRAC Settings→ Network/Security**.

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

Table 4-13 lists the **Active Directory Configuration and Management** page options.

3 Click **Configure Active Directory** to configure Active Directory. See "Using the iDRAC6 Directory Service" on page 143 for detailed configuration information.

4 Click **Test Settings** to test the Active Directory configuration using the settings you specified. See "Using the iDRAC6 Directory Service" on page 143 for details on using the Test Settings option.

Table 4-13.   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. Select the check box to enable sign–on.

Table 4-13.   Active Directory Configuration and Management Page Options *(continued)*

Attribute	Description
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) feature is not supported if the Active Directory is configured for Extended schema. The Single Sign-On (SSO) feature is supported for both Standard and Extended schema.
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.
Look Up Domain Controllers with DNS	Select the **Look Up Domain Controllers with DNS** option to obtain the Active Directory domain controllers from a DNS lookup. When this option is selected, Domain Controller Server Addresses 1-3 are ignored. Select User **Domain from Login** to perform the DNS lookup with the domain name of the login user. Otherwise, select **Specify a Domain** and enter the domain name to use on the DNS lookup. iDRAC6 attempts to connect to each of the addresses (first 4 addresses returned by the DNS look up) one by one until it makes a successful connection. If **Extended Schema** is selected, the domain controllers are where iDRAC6 device object and the Association objects are located. If **Standard Schema** is selected, the domain controllers are where the user accounts and the role groups are located.

Table 4-13.   Active Directory Configuration and Management Page Options *(continued)*

Attribute	Description
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. iDRAC6 attempts to connect to each of the configured addresses one-by-one until it makes a successful connection. If extended schema is selected, these are the addresses of the domain controllers where the iDRAC6 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	iDRAC6 uses Security Socket Layer (SSL) while connecting to Active Directory. By default, iDRAC6 uses the CA certificate loaded in iDRAC6 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 4-13.   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.

Table 4-13.   Active Directory Configuration and Management Page Options *(continued)*

Attribute	Description
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. iDRAC6 attempts to connect to each of the configured addresses one-by-one until it makes a successful connection. 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.
	Select the **Look Up Global Catalog Servers** with DNS option and enter the **Root Domain Name** to use on a DNS lookup to obtain the Active Directory Global Catalog Servers. When this option is selected, **Global Catalog Server Addresses 1-3** are ignored. iDRAC6 attempts to connect to each of the addresses (first 4 addresses returned by the DNS lookup) one by one until it makes a successful connection. A Global Catalog server is required only for Standard Schema in the case that the user accounts and the role groups are in different domains.

Configuring and Managing Generic LDAP

iDRAC6 provides a generic solution to support Lightweight Directory Access Protocol (LDAP)-based authentication. This feature does not require any schema extension on your directory services. For information on configuring generic LDAP Directory Service, see "Generic LDAP Directory Service" on page 176.

Configuring iDRAC6 Services

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

1 Click **iDRAC Settings**→ **Network/Security**. Click the **Services** tab to display the **Services** configuration page.

2 Configure the following services, as required:

- Local Configuration — see Table 4-14.

- Web server — see Table 4-15 for Web server settings.

- SSH — see Table 4-16 for SSH settings.

- Telnet — see Table 4-17 for Telnet settings.

- Remote RACADM — see Table 4-18 for Remote RACADM settings.

- SNMP Agent — see Table 4-19 for SNMP settings.

- Automated System Recovery (ASR) Agent — see Table 4-20 for ASR Agent settings.

3 Click **Apply** to apply the **Service** page settings.

Table 4-14. 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 4-15. 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**.

Table 4-15.   Web Server Settings *(continued)*

Setting	Description
Max Sessions	The maximum number of simultaneous Web server 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 4-16.   SSH Settings

Setting	Description
Enabled	Enables or disable SSH. When checked, SSH is enabled.
Max Sessions	Maximum number of simultaneous SSH sessions allowed for this system. You cannot edit this field. **NOTE:** iDRAC6 supports up to 2 SSH sessions simultaneously.
Active Sessions	Number of current SSH sessions on the system, less than or equal to the setting for **Max Sessions**. You cannot edit this field.
Timeout	The secure shell idle timeout, in seconds. The Timeout range is 60 to 10800 seconds. Enter 0 seconds to disable the Timeout feature. The default is 1800.
Port Number	The port on which the iDRAC6 listens for an SSH connection. The default is 22.

Table 4-17.   Telnet Settings

Setting	Description
Enabled	Enables or disables Telnet. When checked, Telnet is enabled.
Max Sessions	Maximum number of simultaneous Telnet sessions allowed for this system. You cannot edit this field. **NOTE:** iDRAC6 supports up to 2 Telnet sessions simultaneously.
Active Sessions	Number of current Telnet sessions on the system, less than or equal to the setting for **Max Sessions**. You cannot edit this field.
Timeout	The Telnet idle timeout in seconds. Timeout range is 60 to 10800 seconds. Enter 0 seconds to disable the Timeout feature. The default is **1800**.
Port Number	The port on which the iDRAC6 listens for a Telnet connection. The default is **23**.

Table 4-18.   Remote RACADM Settings

Setting	Description
Enabled	Enables/disables remote RACADM. When checked, remote RACADM is enabled.
Active Sessions	The number of current remote RACADM sessions on the system. You cannot edit this field.

Table 4-19.   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. Define the SNMP community string to be used. The Community Name may be up to 31 characters (without spaces) in length. The default is **public**.

Table 4-20.   Automated System Recovery Agent Setting

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

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 **iDRAC Settings**, and then click the **Update** tab.

3   In the **Upload/Rollback (Step 1 of 3)** page, click **Browse** to select 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 system recovery image file uploaded successfully and passed all verification checks, the system recovery 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 clear the **Preserve Configuration** checkbox, iDRAC6 is reset to its default settings. In the default settings, LAN is enabled with a static IPv4 address. You may not be able to log in to the iDRAC6 Web interface. You must 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→ iDRAC Settings**, 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 clear the **Preserve Configuration** checkbox, iDRAC6 is reset to its default settings. In the default settings, LAN is enabled. You may not be able to log in to the iDRAC6 Web interface. You must 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.

Remote Syslog

iDRAC6 Enterprise offers Remote Syslog, a feature that allows you to remotely write the RAC log and the System Event Log (SEL) to an external syslog server. You can read the entire server farm logs from a central log.

The Remote Syslog protocol does not need any user authentication. For the logs to be entered in the Remote Syslog server, ensure that there is proper network connectivity between iDRAC6 and the Remote Syslog server and that the Remote Syslog server is running on the same network as iDRAC6. The Remote Syslog entries are User Datagram Protocol (UDP) packets sent to the Remote Syslog server's syslog port. If network failures occur, iDRAC6 does not send the same log again. The remote logging happens real-time as and when the logs are recorded in iDRAC6's RAC log and SEL log.

Remote Syslog can be enabled through the remote Web interface:

1 Open a supported Web browser window.

2 Log in to iDRAC6 Web interface.

3 In the system tree, select **System→ Setup** tab→ **Remote Syslog Settings**. The **Remote Syslog Settings** screen is displayed.

Table 4-21 lists the Remote Syslog settings.

Table 4-21.   Remote Syslog Settings

Attribute	Description
Remote Syslog Enabled	Select this option to enable the transmission and remote capture of the syslog on the specified server. Once syslog is enabled, new log entries are sent to the Syslog server(s).

Table 4-21. Remote Syslog Settings *(continued)*

Attribute	Description
Syslog Server 1–3	Enter the Remote Syslog server address to log iDRAC6 messages like SEL Log and RAC Log. Syslog server addresses allow alphanumeric, -, ., :, and _ symbols.
Port Number	Enter the port number of the Remote Syslog server. The port number should be between 1 to 65535. Default is 514.

NOTE: The severity levels defined by the Remote Syslog protocol differ from the standard IPMI System Event Log (SEL) severity levels. Hence all iDRAC6 Remote Syslog entries are reported in the syslog server with severity level as **Notice**.

The following example shows the configuration objects and the RACADM command usage to change remote syslog settings:

```
racadm config -g cfgRemoteHosts -o
cfgRhostsSyslogEnable [1/0] ; default is 0

racadm config -g cfgRemoteHosts -o
cfgRhostsSyslogServer1 <servername1> ; default is
blank

racadm config -g cfgRemoteHosts -o
cfgRhostsSyslogServer2 <servername2>; default is
blank

racadm config -g cfgRemoteHosts -o
cfgRhostsSyslogServer3 <servername3>; default is
blank

racadm config -g cfgRemoteHosts -o
cfgRhostsSyslogPort <portnumber>; default is 514
```

First Boot Device

This feature allows you to select the first boot device for your system and enable **Boot Once**. The system boots from the selected device on the next and subsequent reboots and remains as the first boot device in the BIOS boot order, until it is changed again either from the iDRAC6 GUI or from the BIOS Boot sequence.

The first boot device can be selected through the remote Web interface:

1 Open a supported Web browser window.

2 Log in to iDRAC6 Web interface.

3 In the system tree, select **System**→ **Setup**→ **First Boot Device**. The **First Boot Device** screen is displayed.

Table 4-22 lists the **First Boot Device** settings.

Table 4-22.   First Boot Device

Attribute	Description
First Boot Device	Select the first boot device from the drop-down list. The system will boot from the selected device on next and subsequent reboots.
Boot Once	Selected = Enabled; Deselected = Disabled. Check this option to boot from the selected device on the next boot. Thereafter, the system will boot from the first boot device in the BIOS boot order.

Remote File Share

iDRAC6 Remote File Share (RFS) feature allows you to specify an ISO or IMG image file located on a network share and make it available to the managed server's operating system as a virtual drive by mounting it as a CD/DVD or Floppy using a Network File System (NFS) or Common Internet File System (CIFS).

The format of the CIFS shared image path is:

`//<ipaddress or domain name>/<pathtoimage>`

The format of the NFS shared image path is:

`<ipaddress>:/<pathtoimage>`

> **NOTE:** If you are using NFS, ensure that you provide the exact `<pathtoimage>` including the image file extension as it is case sensitive.

> **NOTE:** `<ipaddress>` must be an IPv4 address. IPv6 address is currently not supported.

If a username contains a domain name, then the username must be entered in the form of *<user name>@<domain>*. For example, **user1@dell.com** is a valid username whereas **dell\user1** is not.

A filename with the IMG extension is redirected as a Virtual Floppy and a filename with the ISO extension is redirected as a Virtual CDROM. Remote file share supports only .IMG and .ISO image file formats.

The RFS feature utilizes the underlying Virtual Media implementation in iDRAC6. You must have Virtual Media privileges to perform an RFS mounting. If a virtual drive is already used by Virtual Media, then the drive is not available to mount as RFS and vice versa. For RFS to work, Virtual Media in iDRAC6 must be in the *Attach* or *Auto–Attach* modes.

Connection status for RFS is available in iDRAC6 log. Once connected, an RFS mounted virtual drive does not disconnect even if you log out from iDRAC6. The RFS connection is closed if iDRAC6 is reset or the network connection is dropped. GUI and command line options are also available in iDRAC6 to close the RFS connection.

NOTE: iDRAC6 vFlash feature and RFS are not related.

To enable remote file sharing through the iDRAC6 Web interface, do the following:

1 Open a supported Web browser window.

2 Log in to iDRAC6 Web interface.

3 Select the **System**→ **Remote File Share** tab.

The **Remote File Share** screen is displayed.

Table 4-23 lists the remote file share settings.

Table 4-23. Remote File Server Settings

Attribute	Description
User Name	Username to connect for NFS/CIFS file system.
Password	Password to connect for NFS/CIFS file system.
Image File Path	Path of the file to be shared through remote file share.
Status	**Connected**: The file is shared.
	Not Connected: The file is not shared.
	Connecting: Connection to the share is in-progress.

Click **Connect** to connect to RFS. After successfully establishing the connection, **Connect** is disabled.

> ✎ **NOTE:** Even if you have configured remote file sharing, the GUI does not display this information due to security reasons.

For remote file share, the remote RACADM command is:

`racadm remoteimage.`

`racadm remoteimage <options>`

Options are:

- `-c` ; connect image
- `-d` ; disconnect image
- `-u <username>`; username to access the network share
- `-p <password>`; password to access the network share

- `-l <image_location>`; image location on the network share; use double quotes around the location
- `-s` ; display current status

> ✎ **NOTE:** The maximum number of characters supported for **User Name** and **Password** is 40 and for **Image File Path** it is 511. All characters including alphanumeric and special characters are allowed for these three fields except the following characters:
>
> - ' (single quote)
> - " (double quote)
> - , (comma)
> - < (less than)
> - > (greater than)

Internal Dual SD Module

The Internal Dual SD Module (IDSDM) provides redundancy on the hypervisor SD card by using another SD card that mirrors the first SD card content. The second SD card can be set to IDSDM along with the other SD card by setting the **Redundancy** option to **Mirror mode** in the **Integrated**

Devices screen of the system BIOS setup. For more information about the BIOS options for IDSDM, see the *Hardware Owner's Manual* available on the Dell Support website at **support.dell.com/manuals**.

NOTE: In the BIOS setup, **Integrated Devices** screen, the **Internal USB Port** option must be set to **On**. If this is set to **Off**, the IDSDM is not visible to the system as a boot device.

One of the two SD cards can be the master. For example, if two SD cards are installed in the IDSDM while AC power is removed from the system, SD1 is considered the active or master card. SD2 is the backup card, and all file system IDSDM writes will go to both cards, but reads will occur only from SD1. At any time if SD1 fails or is removed, SD2 will automatically become the active (master) card. The vFlash SD card is disabled in Mirror Mode.

Table 4-24.   IDSDM Status

IDSDM - Mirror Mode	SD1 Card	SD2 Card	vFlash SD Card
Enabled	Active	Active	Inactive
Disabled	Active	Inactive	Active

Using iDRAC you can view the status, health, and availability of IDSDM.

The SD card redundancy status and failure events are logged to SEL, displayed on LCD, and PET alerts are generated if alerts are enabled.

Viewing Internal Dual SD Module Status Using GUI

1   Log in to the iDRAC Web GUI.

2   Click **Removable Flash Media**. The **Removable vFlash Media** page is displayed. This page displays the following two sections:

• **Internal Dual SD Module** — Displayed only if IDSDM is in redundant mode. The **Redundancy Status** is displayed as **Full**. If this section is not present, then the card is in the non-redundant mode state. The valid **Redundancy Status** indications are:

– **Full** — SD card 1 and 2 are functioning properly.

– **Lost** — Either one of the SD card or both the SD cards are not functioning properly.

- **Internal SD Module Status** — Displays the SD card state for SD1, SD2, and vFlash cards with the following information:
  - Status:
    - ![ok icon] — Indicates that the card is ok.
    - ![warning icon] — Indicates that the card is offline or write-protected.
    - ![alert icon] — Indicates that an alert is issued.
  - Location — Location of the SD cards.
  - Online Status — SD1, SD2, and vFlash cards can be in one of the states listed in Table 4-25.

Table 4-25. SD Card States

SD Card	State	Description
SD1 and SD2	Boot	The controller is powering up.
	Active	The card is ready to accept SD read/write requests.
	Standby	The card is the secondary card. It is receiving a copy of the all the SD writes.
	Failed	An error is reported during a SD card read or write.
	Absent	The SD card is not detected.
	Offline	At boot, the Card Indentification (CID) signature of the card is different from the Non-volatile (NV) storage value or the card is the destination of a copy operation that is in-progress.
	Write Protected	The card is write-protected by the physical latch on the SD card. IDSDM cannot use a write-protected card.
vFlash	Active	The card is ready to accept SD read/write requests.
	Absent	The SD card is not detected.

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" on page 33 for more information.

Configuring iDRAC6 for Viewing Serial Output Remotely Over SSH/Telnet

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

First, configure the BIOS to enable serial console:

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`

   ✎ **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" on page 110.

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

1 Expand the **System** tree and click **iDRAC Settings**.

2 Click the **Network/Security** 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 During Boot" on page 91.

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 **microsoft.com/downloads/** and search for *Windows Services for UNIX 3.5*.

Enabling Microsoft Telnet for Telnet Virtual Console

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

> **NOTE:** When you configure the client VT100 emulation window, set the window or application that is displaying the redirected Virtual 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.

> *image* **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 two SSH sessions are supported at any given time. The session timeout is controlled by the `cfgSsnMgtSshIdleTimeout` property as described in the *RACADM iDRAC6 and CMC Command Line Reference Guide* available on the Dell Support website at **support.dell.com/manuals**.

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 the *RACADM iDRAC6 and CMC Command Line Reference Guide* available on the Dell Support website at **support.dell.com/manuals**.

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 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 Virtual 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.
```

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

```
#           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
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 Virtual Console. To disable the graphical interface, comment out the line starting with `splashimage`.

2 To enable multiple GRUB options to start Virtual 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 Virtual 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
```

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

```
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

# 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"
```

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

```
# 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
```

NOTE: Use the Break Key Sequence (~B) to execute the Linux **Magic SysRq** key commands on serial console using IPMI Tool.

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.

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

   a Turn on or restart your system.

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

      `<F2> = System Setup`

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

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

      `external serial connector....remote access device`

   e Select **Save Changes**.

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

2 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" on page 101.

3 Ensure that your management terminal emulation software is configured for serial connection. See "Configuring the Management Station Terminal Emulation Software" on page 102.

4 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 **iDRAC Settings**.

2 Click the **Network/Security** 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 **iDRAC Settings**.

2 Click the **Network/Security** 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** drop-down menu to **Direct Connect Basic Mode**.

For Direct Connect Terminal mode:

Under the **IPMI Serial** section change the **Connection Mode Settings** drop-down 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" on page 105.

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

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

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 Tera Term) 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 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 Mode when in RAC Serial Interface Communication Mode, use the following key sequence:

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

When in terminal mode, to switch the connection to the system COM2 port use:

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

When connected to the system COM2 port, to go back to the terminal mode use:

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

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 Virtual Console.

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

Table 5-5.   Required Pinout for DB-9 Null Modem Cable *(continued)*

Signal Name	DB-9 Pin (server pin)	DB-9 Pin (workstation pin)
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" on page 104 to configure other versions of Minicom.

Configuring Minicom Version 2.0 for Serial Console Emulation

NOTE: To ensure that the text displays properly, it is recommended 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 Virtual Console 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
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

HyperTerminal is the Microsoft Windows serial port access utility. To set the size of your Virtual 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 Virtual Console. Hence, use edition 6.3 instead or any terminal emulation software that supports VT100/VT220 or ANSI emulation mode. An example of a full VT100/VT220 or ANSI terminal emulator that supports Virtual Console on your system is Hilgraeve's HyperTerminal Private.**

To configure HyperTerminal for serial console:

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 **iDRAC Settings**.

2 Click the **Network/Security** 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 to a**pply the IPMI and iDRAC6 serial changes.

6 Click the appropriate **Serial** page button to continue. See the *iDRAC6 Online Help* 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 Virtual Console. 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 Virtual Console. The maximum and default = 8192 characters.
Login Command	The iDRAC6 command line to be executed upon valid login.

Configuring Terminal Mode

1 Expand the **System** tree and click **iDRAC Settings**.

2 Click the **Network/Security** tab and then click **Serial**.

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

4 Configure the terminal mode settings.

See Table 5-10 for description of the terminal mode settings.

5 Click **Apply Changes**.

6 Click the appropriate **Terminal Mode Settings** page button to continue. See the *iDRAC6 Online Help* for description of the **Terminal Mode Settings** page buttons.

Table 5-10.   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>**.

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" on page 49.

• RACADM CLI — See cfgLanNetworking in the *RACADM iDRAC6 and CMC Command Line Reference Guide* available on the Dell Support website at **support.dell.com/manuals**.

• iDRAC6 Configuration Utility — See "Configuring Your System to Use an iDRAC6" on page 34.

✍ **NOTE:** If you are deploying the iDRAC6 in a Linux environment, see "Installing RACADM" on page 38.

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 5-11 describes each iDRAC6 interface.

Table 5-11.   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" on page 110.
	
	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`

Table 5-11.   iDRAC6 Interfaces *(continued)*

Interface	Description
Telnet Console	Provides access to the iDRAC6 and support for serial and RACADM commands including **powerdown**, **powerup**, **powercycle**, and **hardreset** commands.
	NOTE: Telnet is not a secure protocol and Telnet transmits all data, including passwords,in plain text. When transmitting sensitive information, use the SSH interface.
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 *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" on page 33.

RACADM provides a remote capability option (**-r**) that allows you to connect to the managed system and execute RACADM subcommands from a remote Virtual 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" on page 62.

```
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
```

On Linux systems, ensure that you perform the following intermediate steps for certificate validation to be successful using remote RACADM:

1 Convert certificate in DER format to PEM format (using openssl cmdline tool):

```
openssl x509 -inform pem -in
<yourdownloadedderformatcert.crt> -outform pem -
out <outcertfileinpemformat.pem> -text
```

2 Find the location of the default CA certificate bundle on the management station. For example, for RHEL5 64-bit, it is /etc/pki/tls/cert.pem.

3 Append the PEM formatted CA certificate to the management station CA certificate.

For example, use the cat command:

```
- cat testcacert.pem >> cert.pem
```

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 5-12 lists the options for the RACADM command.

Table 5-12.   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.

Table 5-12.   racadm Command Options *(continued)*

Option	Description
-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

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 5-13 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 the *RACADM iDRAC6 and CMC Command Line Reference Guide* available on the Dell Support website at **support.dell.com/manuals**.

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

```
racadm help
```

Table 5-13. 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.
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.
sshpkauth	Enables you to upload up to 4 different SSH public keys, delete existing keys, and view the keys already in iDRAC6.
getniccfg	Displays the current IP configuration for the controller.
getsvctag	Displays system 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.

Table 5-13. RACADM Subcommands *(continued)*

Command	Description
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	Uploads SSL key from the client to the iDRAC6.
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.
closessn	Closes a communication session on the device.
getsel	Displays SEL entries.
krbkeytabupload	Uploads a Kerberos keytab file.
localConRedirDisable	Disables Server Console. There is no video output from the server video port.
testemail	Tests the RAC's e-mail alerting feature.
usercertupload	Uploads a user certificate or a user CA certificate from the client to the iDRAC6.
usercertview	Displays the user certificate or user CA certificate that exists on the iDRAC6.
vflashsd	Initializes or gets the status of the vflash SD card.
vflashpartition	Creates, deletes, lists, or view the status of partitions on an initialized vFlash SD card.

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.

Remote RACADM fails to connect to iDRAC from SUSE Linux Enterprise Server (SLES) 11 SP1

Ensure that you have installed the official openssl and libopenssl versions. Run the following command to install the RPM packages:

```
rpm -ivh --force  < filename >
```

where, <filename> is the openssl or libopenssl rpm package file.

For example:

```
rpm -ivh --force openssl-0.9.8h-30.22.21.1.x86_64.rpm
```

```
rpm -ivh --force libopenssl0_9_8-0.9.8h-
30.22.21.1.x86_64.rpm
```

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 **.cfg** configuration file from the retrieved information. Filename is user specified, for example **racadm.cfg**. 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:** For information about the **getconfig** command, see getconfig command in the *RACADM iDRAC6 and CMC Command Line Reference Guide* available on the Dell Support website at **support.dell.com/manuals**.

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, the index of the group is used as the anchor. Any modifications to the objects within the indexed group is also associated with the index value.

  For example:

  ```
  [cfgUserAdmin]

  # cfgUserAdminIndex=11

  cfgUserAdminUserName=

  # cfgUserAdminPassword=******** (Write-Only)

  cfgUserAdminEnable=0

  cfgUserAdminPrivilege=0x00000000

  cfgUserAdminIpmiLanPrivilege=15

  cfgUserAdminIpmiSerialPrivilege=15

  cfgUserAdminSolEnable=0
  ```

- The indexes are read-only and cannot be modified. Objects of the indexed group are bound to the index under which they are listed and any valid configuration to the object value is applicable only to that particular index.

- A predefined set of indexes are available for each indexed group. For more information, see the *RACADM iDRAC6 and CMC Command Line Reference Guide* available on the Dell Support website at **support.dell.com/manuals**.

- 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 the *RACADM iDRAC6 and CMC Command Line Reference Guide* available on the Dell Support website at **support.dell.com/manuals**.

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 `racadm getconfig -f <filename>.cfg` command places a comment in front of index objects, allowing the user to see the included comments.

  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]

  cfgUserAdminIndex=11
  ```

  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" on page 34.

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 5-14 provides a description of each mode.

Table 5-14.   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 **iDRAC Settings**.

2 Click the **Network/Security** 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" on page 349 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" on page 349 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 **iDRAC Settings→ Network/Security→ Users**.

The **Users** page (see Table 6-1) displays the following information for iDRAC6 users: **User ID, State** (Enabled/Disabled)**, User Name, iDRAC**, **LAN**, **Serial Port**, and **Serial Over LAN** (Enabled/Disabled).

📝 **NOTE:** User 1 is reserved for the IPMI anonymous user and you cannot change this configuration.

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

On the **User Main Menu** page (see Table 6-2 and Table 6-7), you can configure a user, view or upload a user certificate, upload a trusted certification authority (CA) certificate, view a trusted CA certificate, upload a Secure Shell (SSH) public key file or view or delete a specified SSH key or all SSH keys.

If you select **Configure User** and click **Next**, the **User Configuration** page is displayed.

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

- The username, password, and access permissions for a new or existing iDRAC user. Table 6-3 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 **Go Back To Users Page** to return to the Users Page.

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:** If the user name is changed, the new name will not appear in the user interface until the next user login.
iDRAC	Displays the group (privilege level) to which the user is assigned (Administrator, Operator, Read Only, or None).
LAN	Displays the IPMI LAN privilege level to which the user is assigned (Administrator, Operator, Read Only, or None).
Serial Port	Displays the IPMI Serial Port privilege level to which the user is assigned (Administrator, Operator, Read Only, or None).
Serial Over LAN	Allows or disallows the user to use IPMI Serial Over LAN.

Table 6-2. Smart Card Configuration Options

Option	Description
Upload User Certificate	Enables the user to upload the user certificate to iDRAC6 and import it to the user profile.
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 cleared, user access is disabled.
User Name	A User Name with up to 16 characters. The following characters are supported: • 0-9 • A-Z • a-z • Special characters: + %) ' > : $ [| ! & = * , - {] § # (? < ; _ } I
Change Password	Enables the **New Password** and **Confirm New Password** fields. When cleared, the user's Password cannot be changed.

Table 6-3. General User Settings *(continued)*

New Password	Enter a **Password** with up to 20 characters. The characters will not be displayed and are masked. The following characters are supported:

- 0-9
- A-Z
- a-z
- Special characters:

+	&	?	>	-	}	|	.
!	(	'	,	_	[	"	@
#	)	*	;	$	]	/	§
%	=	<	:	{	I	\	

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.

Table 6-5. iDRAC User Privileges *(continued)*

Property	Description
Configure iDRAC	Enables the user to configure the iDRAC.
Configure Users	Enables the user to allow specific users to access the system. **CAUTION: This privilege is normally reserved for users who are members of the Administrator role on iDRAC. However, users in the 'Operator' role can be assigned this privilege. A user with this privilege can modify any user's configuration. This includes creation or deletion of any user, SSH Key management for users, and so on. For these reasons, assign this privilege carefully.**
Clear Logs	Enables the user to clear the iDRAC logs.
Execute Server Control Commands	Enables the user to execute Server Control commands.
Access Virtual Console	Enables the user to run Virtual Console.
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 Virtual Console, 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 Virtual Console, Access Virtual Media, Test Alerts, Execute Diagnostic Commands**
Read Only	Login to iDRAC
None	No assigned permissions

Public Key Authentication over SSH

iDRAC6 supports the Public Key Authentication (PKA) over SSH. This authentication method improves SSH scripting automation by removing the need to embed or prompt for a user ID/password.

Before You Begin

You can configure up to 4 public keys *per user* that can be used over an SSH interface. Before adding or deleting public keys, ensure that you use the view command to see what keys are already set up, so a key is not accidentally overwritten or deleted. When the PKA over SSH is set up and used correctly, you do not have to enter the username or password when logging into the iDRAC6. This can be very useful for setting up automated scripts to perform various functions.

When getting ready to set up this functionality, be aware of the following:

- You can manage this feature with RACADM and also from the GUI.

- When adding new public keys, ensure that the existing keys are not already at the index where the new key is added. iDRAC6 does not perform checks to ensure previous keys are deleted before a new one is added. As soon as a new key is added, it is automatically in effect as long as the SSH interface is enabled.

Generating Public Keys for Windows

Before adding an account, a public key is required from the system that will access the iDRAC6 over SSH. There are two common ways to generate the public/private key pair: using *PuTTY Key Generator* application for clients running Windows or *ssh-keygen* CLI for clients running Linux. The *ssh-keygen* CLI utility comes by default on all standard installations.

This section describes simple instructions to generate a public/private key pair for both applications. For additional or advanced usage of these tools, see the application Help.

To use the *PuTTY Key Generator* for Windows clients to create the basic key:

1. Start the application and select either SSH-2 RSA or SSH-2 DSA for the type of key to generate. (SSH-1 is not supported).

2. The supported key generation algorithms are RSA and DSA only. Enter the number of bits for the key. The number should be between 768 and 4096 bits for RSA and 1024 bits for DSA.

3. Click **Generate** and move the mouse in the window as directed. After the key is created, you can modify the key comment field. You can also enter a passphrase to make the key secure. Ensure that you save the private key.

4. You can save the public key to a file using the "Save public key" option to upload it later. All uploaded keys should be in RFC 4716 or openssh format. If not, you must convert the same into that format.

Generating Public Keys for Linux

The *ssh-keygen* application for Linux clients is a command line tool with no graphical user interface.

Open a terminal window and at the shell prompt, enter:

```
ssh-keygen –t rsa –b 1024 –C testing
```

NOTE: The options are case-sensitive.

where,

-t option could be either *dsa* or *rsa*.

–b option specifies the bit encryption size between 768 and 4096.

–C option allows modifying the public key comment and is optional.

Follow the instructions. After the command executes, upload the public file.

⚠ **CAUTION: Keys generated from the Linux management station using ssh-keygen are in non-4716 format. Convert the keys into the 4716 format using** `ssh-keygen -e -f /root/.ssh/id_rsa.pub > std_rsa.pub`. **Do not change the permissions of the key file. The above conversion should be done using default permissions.**

NOTE: iDRAC6 does not support ssh-agent forward of keys.

Logging in Using Public Key Authentication

After the public keys are uploaded, you can log into the iDRAC6 over SSH without entering a password. You also have the option of sending a single RACADM command as a command line argument to the SSH application. The command line options behave similar to remote RACADM since the session ends after the command is completed.

For example:

Logging in:

```
ssh username@<domain>
```

or

```
ssh username@<IP_address>
```

where IP_address is the IP address of the iDRAC6.

Sending racadm commands:

```
ssh username@<domain> racadm getversion
ssh username@<domain> racadm getsel
```

Uploading, Viewing, and Deleting SSH Keys Using the iDRAC6 Web-Based Interface

1   Click **iDRac Settings**→ **Network/Security**→ **Users**. The **Users** page is displayed.

2   In the **User ID** column, click a user ID number. The **User Main Menu** page is displayed.

3   Use the **SSH Key Configurations** options to upload, view, or remove SSH Key(s).

⚠ **CAUTION: The capability to upload, view, and/ or delete SSH keys is based on the 'Configure Users' user privilege. This privilege allows user(s) to configure another user's SSH key. You should grant this privilege carefully. For more information on user privileges, see "Adding and Configuring iDRAC6 Users" on page 127.**

Table 6-7.   SSH Key Configurations

Option	Description
Upload SSH Key(s)	Allows the local user to upload a Secure Shell (SSH) public key file. If a key is uploaded, the content of the key file is displayed in a non-editable text box on the **User Configuration** page.
View/Remove SSH Key(s)	Allows the local user to view or delete a specified SSH key or all SSH keys.

The **Upload SSH Key(s)** page enables you to upload a Secure Shell (SSH) public key file. If a key is uploaded, the contents of the key file is displayed in a non-editable text box on the **View/Remove SSH Key(s)** page

Table 6-8.   Upload SSH Key(s)

Option	Description
File/Text	Select the **File** option and type the path where the key is located. You can also select the **Text** option and paste the contents of the key file in the box. You can upload new key(s) or overwrite existing key(s). To upload a key file, click **Browse**, select the file, and then click the **Apply** button.
Browse	Click this button to locate the full path and file name of the key.

The **View/Remove SSH Key(s)** page enables you to view or remove the user's SSH public keys.

Table 6-9.   View/Remove SSH Key(s)

Option	Description
Remove	The uploaded key is displayed in the box. Select the Remove option and click **Apply** to delete the existing key.

Uploading, Viewing, and Deleting SSH Keys Using RACADM

Upload

The upload mode allows you to upload a keyfile or to copy the key text on the command line. You cannot upload and copy a key at the same time.

Local RACADM and Remote RACADM:

```
racadm sshpkauth -i <2 to 16> -k <1 to 4> -f
<filename>
racadm sshpkauth -i <2 to 16> -k <1 to 4> -t
<key-text>
```

Telnet/SSH/Serial RACADM:

```
racadm sshpkauth -i <2 to 16> -k <1 to 4> -t
<key-text>
```

Example:

Upload a valid key to the iDRAC6 User 2 in the first key space using a file:

```
$ racadm sshpkauth -i 2 -k 1 -f pkkey.key
```

PK SSH Authentication Key file successfully uploaded to the RAC.

⚠ **CAUTION: The "key text" option is supported on local and remote RACADM. The "file" option is not supported on Telnet/ssh/serial RACADM.**

View

The view mode allows the user to view a key specified by the user or all keys.

```
racadm sshpkauth -i <2 to 16> -v -k <1 to 4>
racadm sshpkauth -i <2 to 16> -v -k all
```

Delete

The delete mode allows the user to delete a key specified by the user or all keys.

```
racadm sshpkauth -i <2 to 16> -d -k <1 to 4>
racadm sshpkauth -i <2 to 16> -d -k all
```

For information on the subcommand options, see sshpkauth subcommand in the *iDRAC6 and CMC Command Line Reference Guide* available on the Dell Support website at **support.dell.com/manuals**.

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 the *iDRAC6 and CMC Command Line Reference Guide* available on the Dell Support website at **support.dell.com/manuals** 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
- LAN
- Serial Port
- Serial Over LAN

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 iDRAC6 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" on page 137. Next, type the following command lines with the new user name and password.

NOTE: For a list of valid bit mask values for specific user privileges, see the *iDRAC6 and CMC Command Line Reference Guide* available on the Dell Support website at **support.dell.com/manuals**. 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 Directory Service

A directory service maintains a common database for storing information about users, computers, printers, etc. on a network. If your company uses either the Microsoft Active Directory or the LDAP 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 directory service.

Using iDRAC6 With Microsoft Active Directory

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

You can configure user authentication through Microsoft Active Directory to log in to the iDRAC6. You can also provide role-based authority, which enables an administrator to configure specific privileges for each user. For more information, see the subsequent sections.

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 Virtual Console	Enables the user to run Virtual Console
Access Virtual Media	Enables the user to run and use Virtual Media

Table 7-1. iDRAC6 User Privileges *(continued)*

Privilege	Description
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

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 lists all the user domains in the pull-down menu for you 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 log in as an Active Directory user if you use the login syntax described earlier in this section.

You can also log into the iDRAC6 using Smart Card or Single Sign-On. For more information, see "Configuring iDRAC6 for Single Sign-On or Smart Card Login" on page 185.

NOTE: The Windows 2008 Active Directory server supports only a *<username>*@*<domain_name>* string with a maximum length of 256 characters.

Prerequisites for Enabling Microsoft Active Directory Authentication for 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 do not 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" on page 143 for more specific information.

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:

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

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

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

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

4 Click **Next** and click **Finish**.

Exporting the Domain Controller Root CA Certificate to the iDRAC6

📝 **NOTE:** If your system is running Windows 2000 or 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 Microsoft Active Directory With Extended Schema Using the iDRAC6 Web-Based Interface" on page 160 or "Configuring Microsoft Active Directory With Standard Schema Using RACADM" on page 171.

To upload the certificate using the Web-based interface, see "Configuring Microsoft Active Directory With Extended Schema Using the iDRAC6 Web-Based Interface" on page 160 or "Configuring Microsoft Active Directory With Standard Schema Using the iDRAC6 Web-Based Interface" on page 168.

Importing the iDRAC6 Firmware SSL Certificate

![NOTE icon] **NOTE:** If the Active Directory Server is set to authenticate the client during an SSL session initialization phase, you need to upload the iDRAC6 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 icon] **NOTE:** If your system is running Windows 2000, the following steps may vary.

![NOTE icon] **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 iDRAC6 SSL certificate is the identical certificate used for the iDRAC6 Web server. All iDRAC controllers are shipped with a default self-signed certificate.

To download the iDRAC6 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 iDRAC6 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**.

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 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 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.

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 the attributes and classes that are added into the directory service.

Dell extension: dell

Dell base OID: 1.2.840.113556.1.8000.1280

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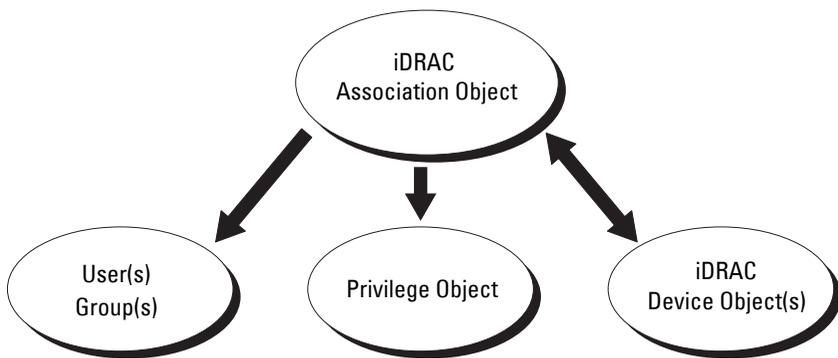
You can create as many or as few association objects as required. However, you must create at least one Association Object, and you must have one iDRAC Device Object for each iDRAC on the network that you want to integrate with Active Directory for Authentication and Authorization with the iDRAC.

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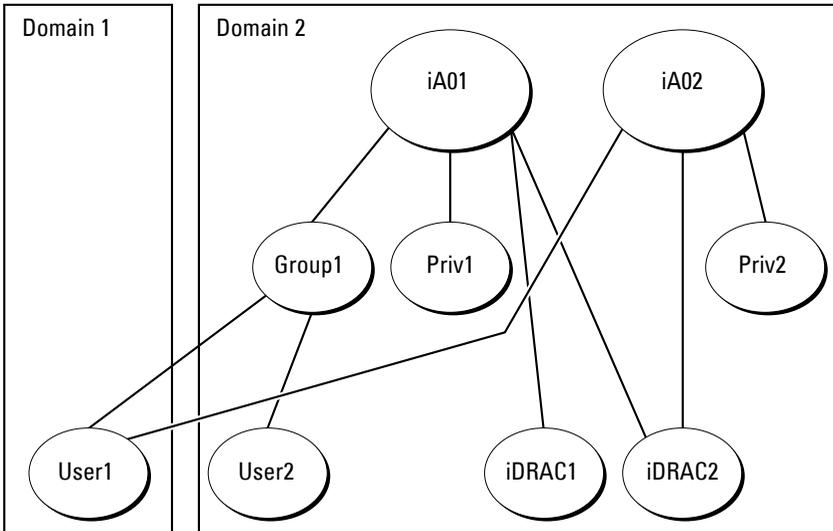
The figure shows two Association Objects—iA01 and iA02. User1 is associated to iDRAC2 through both association objects. Therefore, User1 has accumulated privileges that are the result of combining the privileges set for objects Priv1 and Priv2 on iDRAC2.

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 iDRAC6

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

1   Extend the Active Directory schema (see "Extending the Active Directory Schema" on page 151.)

2   Extend the Active Directory Users and Computers Snap-in (see "Installing Dell Extension to Microsoft Active Directory Users and Computers Snap-In" on page 157.)

3   Add iDRAC6 users and their privileges to Active Directory (see "Adding iDRAC Users and Privileges to Microsoft Active Directory" on page 158.)

4   Configure the iDRAC6 Active Directory properties using either the iDRAC6 Web-based interface or the RACADM (see "Configuring Microsoft Active Directory With Extended Schema Using the iDRAC6 Web-Based Interface" on page 160 or "Configuring Microsoft Active Directory With Extended Schema Using RACADM" on page 163.)

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 available on the *Dell Systems Management Tools and Documentation* DVD. For information on installing these, see "Installing Dell Extension to Microsoft Active Directory Users and Computers Snap-In" on page 157. 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**.

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" on page 152.

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.
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)	
delIsLogClearAdmin	1.2.840.113556.1.8000.1280.1.1.2.6	TRUE
TRUE if the user has Log Clearing rights on the device.	Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
dellIsServerResetUser	1.2.840.113556.1.8000.1280.1.1.2.7	TRUE
TRUE if the user has Server Reset rights on the device.	Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
dellIsConsoleRedirectUser	1.2.840.113556.1.8000.1280.1.1.2.8	TRUE
TRUE if the user has Virtual Console 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
dellIsVirtualMediaUser TRUE if the user has Virtual Media rights on the device.	1.2.840.113556.1.8000.1280.1.1.2.9 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsTestAlertUser TRUE if the user has Test Alert User rights on the device.	1.2.840.113556.1.8000.1280.1.1.2.10 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsDebugCommandAdmin TRUE if the user has Debug Command Admin rights on the device.	1.2.840.113556.1.8000.1280.1.1.2.11 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellSchemaVersion The Current Schema Version is used to update the schema.	1.2.840.113556.1.8000.1280.1.1.2.12 Case Ignore String (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellRacType This attribute is the Current RAC Type for the delliDRACDevice object and the backward link to the dellAssociationObjectMembers forward link.	1.2.840.113556.1.8000.1280.1.1.2.13 Case Ignore String (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellAssociationMembers List of dellAssociationObjectMembers that belong to this Product. This attribute is the backward link to the dellProductMembers linked attribute. Link ID: 12071	1.2.840.113556.1.8000.1280.1.1.2.14 Distinguished Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE

Installing Dell Extension to Microsoft 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 Microsoft Active Directory Users and Computers Snap-In" on page 157 for more information.

Opening the Microsoft 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 Microsoft 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 Microsoft Active Directory With Extended Schema Using the iDRAC6 Web-Based Interface" on page 160.

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 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 Microsoft 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 Go to **iDRAC Settings**→ **Network/Security** tab→ **Directory Service** tab→ **Microsoft Active Directory**.

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

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

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

6 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.

7 Click **Upload**.

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

8 (Optional: For AD authentication) 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 iDRAC6.

9 Click **Next**. The **Active Directory Configuration and Management Step 2 of 4** page is displayed.

10 Select **Enable Active Directory**.

⚠ **CAUTION: In this release, the Smart Card based Two Factor Authentication (TFA) feature is not supported if the Active directory is configured for Extended schema. The Single Sign-On (SSO) feature is supported for both Standard and Extended schema.**

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

12 Type the user domain name in the prompt and click **OK**.

✎ **NOTE:** 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.

13 In the **Timeout** field, type time (in seconds) iDRAC must wait for Active Directory responses. The default is 120 seconds.

14 Select one of the following options:

   a **Look Up Domain Controllers with DNS** to obtain the Active Directory domain controllers from a DNS lookup. Domain Controller Server Addresses 1-3 are ignored. Select **User Domain from Login** to perform the DNS lookup with the domain name of the login user. Else, select **Specify a Domain** and enter the domain name to use on the DNS lookup. iDRAC6 attempts to connect to each of the addresses (first 4 addresses returned by the DNS look up) one by one until it makes a successful connection. For **Extended Schema**, the domain controllers are where the iDRAC6 device object and the Association objects are located.

   b **Specify Domain Controller Addresses** option to allow iDRAC6 to use the Active Directory domain controller server addresses that are specified. DNS lookup is not performed. Specify the IP address or the Fully Qualified Domain Name (FQDN) of the domain controllers. When the **Specify Domain Controller Addresses** option is selected, at least one of the three addresses must be configured. iDRAC6 attempts to connect to each of the configured addresses one by one until it makes a successful connection. For **Extended Schema**, these are the

addresses of the domain controllers where the iDRAC6 device object and the Association objects are located.

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

15 Click **Next**. The **Active Directory Configuration and Management Step 3 of 4** page is displayed.

16 Under **Schema Selection**, select **Extended Schema.**

17 Click **Next**. The **Active Directory Configuration and Management Step 4 of 4** page is displayed.

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

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

The iDRAC6 Web server automatically returns you to the **Active Directory Configuration and Management** page.

20 Click **Test Settings** to check the Active Directory Extended Schema settings.

21 Type your Active Directory user name and password.

The test results and the test log are displayed. For additional information, see "Testing Your Configurations" on page 175.

> **NOTE:** You must have a DNS server configured properly on iDRAC to support Active Directory login. Click **iDRAC Settings→ Network/Security→ 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 Microsoft Active Directory With Extended Schema Using RACADM

Use the following commands to configure the iDRAC6 Microsoft 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
cfgADDomainController1 <fully qualified domain name
or IP Address of the domain controller>

racadm config -g cfgActiveDirectory -o
cfgADDomainController2 <fully qualified domain name
or IP Address of the domain controller>

racadm config -g cfgActiveDirectory -o
cfgADDomainController3 <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 it makes a successful connection. 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) feature is not supported if the Active directory is configured for Extended schema. The Single Sign-On (SSO) feature is supported for both Standard and Extended schema.**

If you want to use DNS lookup to obtain the Active Directory Domain Controller server address, type the following command:

```
racadm config -g cfgActiveDirectory -o
cfgADDcSRVLookupEnable=1
```

- To perform the DNS lookup with the domain name of the login user:

  ```
  racadm config -g cfgActiveDirectory -o
  cfgADDcSRVLookupbyUserdomain=1
  ```

- To specify the domain name to use on the DNS lookup:

  ```
  racadm config -g cfgActiveDirectory -o
  cfgADDcSRVLookupDomainName <domain name to use
  on the DNS lookup>
  ```

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" on page 145 for additional information.

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

2 If you want to specify the time in seconds to wait for Active Directory (AD) queries to complete before timing out, type the following command:

```
racadm config -g cfgActiveDirectory -o
cfgADAuthTimeout <time in seconds>
```

3 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
```

4 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>
```

5 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 "Generic LDAP Directory Service" on page 176 for details about user domains.

6 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 iDRAC6.

Figure 7-3. Configuration of iDRAC with Microsoft Active Directory and Standard Schema

Configuration on Active Directory Side

Configuration on iDRAC Side
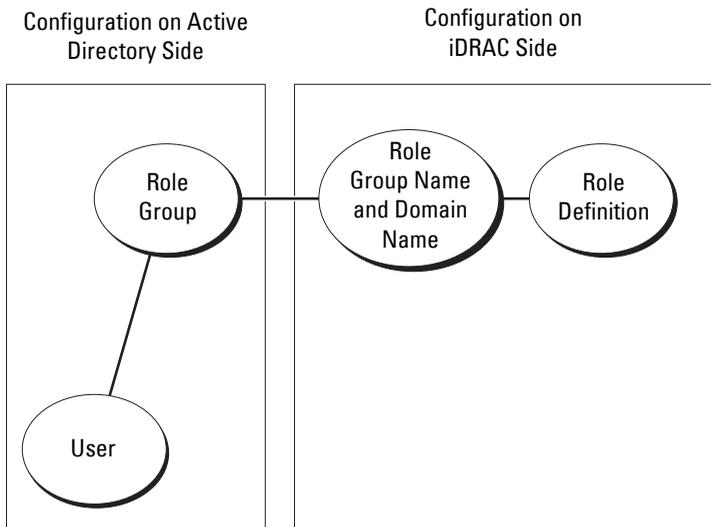
On the Active Directory side, a standard group object is used as a role group. A user who has iDRAC6 access will be a member of the role group. To give this user access to a specific iDRAC6, the role group name and its domain name need to be configured on the specific iDRAC6. Unlike the extended schema 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.

NOTE: The Default Role Group Privilege Level for all five role groups is **None**. You have to choose one of the default role group privileges from the drop-down box.

Table 7-9. Default Role Group Privileges

Privilege Level	Permissions Granted	Bit Mask
Administrator	Login to iDRAC, Configure iDRAC, Configure Users, Clear Logs, Execute Server Control Commands, Access Virtual Console, Access Virtual Media, Test Alerts, Execute Diagnostic Commands	0x000001ff
Operator	Login to iDRAC, Configure iDRAC, Execute Server Control Commands, Access Virtual Console, Access Virtual Media, Test Alerts, Execute Diagnostic Commands	0x000000f9
Read Only	**Login to iDRAC**	0x00000001
None	No assigned permissions	0x00000000

NOTE: The Bit Mask values are used only when setting Standard Schema using RACADM.

Single Domain Versus Multiple Domain Scenarios

If all the login users and role groups, and 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 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 the role groups and the nested groups, if any, must be a Universal Group type.

Configuring Standard Schema Microsoft Active Directory to Access iDRAC6

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. Add the Active Directory user as a member of the Active Directory group to access the iDRAC6.

3 Configure the name of the group and the domain name on iDRAC6 using either the Web-based interface or RACADM. For more information, see "Configuring Microsoft Active Directory With Standard Schema Using the iDRAC6 Web-Based Interface" on page 168 or "Configuring Microsoft Active Directory With Standard Schema Using RACADM" on page 171.

Configuring Microsoft 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 Go to **iDRAC Settings**→ **Network/Security** tab→ **Directory Service** tab→ **Microsoft Active Directory**.

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

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

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

6 Under **Upload Active Directory CA Certificate**, browse to find the certificate file.

7 Click **Upload**.

The certificate information for the valid Active Directory CA certificate is displayed.

8 (**Optional: For AD authentication**) 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.

9 Click **Next**. The **Active Directory Configuration and Management Step 2 of 4** page is displayed.

10 Select **Enable Active Directory**.

11 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.

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

13 Type the user domain name in the prompt and click **OK**.

14 In the **Timeout** fields, type the time (in seconds) iDRAC must wait for Active Directory responses. The default is 120 seconds.

15 Select one of the following options:

a **Look Up Domain Controllers with DNS** option to obtain the Active Directory domain controllers from a DNS lookup. Domain Controller Server Addresses 1-3 are ignored. Select **User Domain from Login** to perform the DNS lookup with the domain name of the login user. Else, select **Specify a Domain** and enter the domain name to use on the DNS lookup. iDRAC6 attempts to connect to each of the addresses (first 4 addresses returned by the DNS look up) one by one until it makes a successful connection. For **Standard Schema**, the domain controllers are where the user accounts and the role groups are located.

b Select the **Specify Domain Controller Addresses** option to allow iDRAC6 to use the Active Directory domain controller server addresses that are specified. DNS lookup is not performed. Specify the IP address or the Fully Qualified Domain Name (FQDN) of the domain controllers. When the **Specify Domain Controller Addresses** option is selected, at least one of the three addresses must be configured. iDRAC6 attempts to connect to each of the configured addresses one by one until it makes a successful connection. For **Standard Schema**, these are the addresses of the domain controllers where the user accounts and the role groups are located.

> **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**. The **Active Directory Configuration and Management Step 3 of 4** page is displayed.

17 Under **Schema Selection**, select **Standard Schema.**

18 Click **Next**. The **Active Directory Configuration and Management Step 4a of 4** page is displayed.

19 Select one of the following options:

- Select the **Look Up Global Catalog Servers with DNS** option and enter the **Root Domain Name** to use on a DNS lookup to obtain the Active Directory Global Catalog Servers. Global Catalog Server Addresses 1-3 are ignored. iDRAC6 attempts to connect to each of the addresses (first 4 addresses returned by the DNS lookup) one by one until it makes a successful connection. A Global Catalog server is required only for Standard Schema in the case that the user accounts and the role groups are in different domains.

- Select the **Specify Global Catalog Server Addresses** option and enter the IP address or the Fully Qualified Domain Name (FQDN) of the Global Catalog server(s). DNS lookup is not performed. At least one of the three addresses must be configured. iDRAC6 attempts to connect to each of the configured addresses one by one until it makes a successful connection. Global Catalog server is required only for Standard Schema in the case that the user accounts and the role groups are in different domains.

> **NOTE:** The FQDN or IP address that you specify in the **Global Catalog Server Address** 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.

20 Under **Role Groups**, click a **Role Group**.

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

21 Specify the **Role Group Name**.

The **Role Group Name** identifies the role group in Active Directory associated with the iDRAC.

22 Specify the **Role Group Domain**, which is the domain of the Role Group.

23 Specify the **Role Group Privileges** by selecting the **Role Group Privilege Level**. For example, if you select **Administrator**, all the privileges are selected for that level of permission.

24 Click **Apply** to save the 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.

25 Configure additional Role Groups, if required.

26 Click **Finish** to return to the **Active Directory Configuration and Management** page.

27 Click **Test Settings** to check the Active Directory Standard Schema settings.

28 Type your iDRAC6 user name and password.

The test results and the test log are displayed. For additional information, see "Testing Your Configurations" on page 175.

> **NOTE:** You must have a DNS server configured properly on iDRAC to support Active Directory login. Click **iDRAC Settings→ Network/Security→ 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 Microsoft 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 the *RACADM iDRAC6 and CMC Command Line Reference Guide* available on the Dell Support website at **support.dell.com/manuals**.

```
racadm config -g cfgActiveDirectory -o
cfgADDomainController1 <fully qualified domain name
or IP address of the domain controller>
```

```
racadm config -g cfgActiveDirectory -o
cfgADDomainController2 <fully qualified domain name
or IP address of the domain controller>
```

```
racadm config -g cfgActiveDirectory -o
cfgADDomainController3 <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* only 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 it makes a successful connection. With Standard Schema, these are the addresses of the domain controllers where the user accounts and the role groups are located.

If you want to use DNS lookup to obtain the Active Directory Domain Controller server address, type the following command:

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

- To perform the DNS lookup with the domain name of the login user:

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

- To specify the domain name to use on the DNS lookup:

  ```
  racadm config -g cfgActiveDirectory -o
  cfgADDcSRVLookupDomainName <domain name to use
  on the DNS lookup>
  ```

To specify the Global Catalog server address, type the following command:

```
racadm config -g cfgActiveDirectory -o cfgADGlobal
Catalog1 <fully qualified domain name or IP
address of the domain controller>

racadm config -g cfgActiveDirectory -o cfgADGlobal
Catalog2 <fully qualified domain name or IP
address of the domain controller>

racadm config -g cfgActiveDirectory -o cfgADGlobal
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 use DNS lookup to obtain the Active Directory Global Catalog server address, type the following command:

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

racadm config -g cfgActiveDirectory -o
cfgADGcRootDomain <Domain Name>
```

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" on page 145 for additional information.

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

2   If you want to specify the time in seconds to wait for Active Directory (AD) queries to complete before timing out, type the following command:

```
racadm config -g cfgActiveDirectory -o
cfgADAuthTimeout <time in seconds>
```

3   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
```

4   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>
```

5 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 "Generic LDAP Directory Service" on page 176 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" on page 181.

If you need to make changes to your settings, click the **Active Directory** tab and change the configuration step-by-step.

Generic LDAP Directory Service

iDRAC6 provides a generic solution to support Lightweight Directory Access Protocol (LDAP) based authentication. This feature does not require any schema extension on your directory services.

To make the iDRAC6 LDAP implementation generic, the commonality between different directory services is utilized to group users and then map the user-group relationship. The directory service specific action is the schema. For example, they may have different attribute names for the group, user, and the link between the user and the group. These actions can be configured in iDRAC6.

Login Syntax (Directory User versus Local User)

Unlike Active Directory, special characters ("@", "\", and "/") are not used to differentiate an LDAP user from a local user. The login user should only enter the user name, excluding the domain name. iDRAC6 takes the user name as is and does not break it down to the user name and user domain. When generic LDAP is enabled, iDRAC6 first tries to login the user as a directory user. If it fails, local user lookup is enabled.

> **NOTE:** There is no behavior change on the Active Directory login syntax. When generic LDAP is enabled, the GUI login page displays only "This iDRAC" in the drop-down menu.

> **NOTE:** "<" and ">" characters are not allowed in the user name for openLDAP and OpenDS based directory services.

Configuring Generic LDAP Directory Service Using the iDRAC6 Web-Based Interface

1. Open a supported Web browser window.
2. Log in to the iDRAC6 Web-based interface.
3. Go to **iDRAC Settings**→ **Network/Security** tab→ **Directory Service** tab→ **Generic LDAP Directory Service**.

   The **Generic LDAP Configuration and Management** page displays the current iDRAC6 generic LDAP settings. Scroll to the bottom of the **Generic LDAP Configuration and Management** page, and click **Configure Generic LDAP**.

The **Generic LDAP Configuration and Management Step 1 of 3** page is displayed. Use this page to configure the digital certificate used during initiation of SSL connections when communicating with a generic LDAP server. These communications use LDAP over SSL (LDAPS). If you enable certificate validation, upload the certificate of the Certificate Authority (CA) that issued the certificate used by the LDAP server during initiation of SSL connections. The CA's certificate is used to validate the authenticity of the certificate provided by the LDAP server during SSL initiation.

NOTE: In this release, non-SSL port based LDAP bind is not supported. Only LDAP over SSL is supported.

4 Under **Certificate Settings**, select **Enable Certificate Validation** to enable certificate validation. If enabled, iDRAC6 uses the CA certificate to validate the LDAP server certificate during Secure Socket Layer (SSL) handshake; if disabled, iDRAC6 skips the certificate validation step of the SSL handshake. You can disable certificate validation during testing or if your system administrator chooses to trust the domain controllers in the security boundary without validating their SSL certificates.

CAUTION: Ensure that CN = open LDAP FQDN is set (for example, CN= openldap.lab) in the subject field of the LDAP server certificate during certificate generation. The LDAP server address field in iDRAC6 should be set to match the same FQDN address for certificate validation to work.

5 Under **Upload Directory Service 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.

6 Click **Upload**.

The certificate of the root CA that signs all the domain controllers' Security Socket Layer (SSL) server certificates is uploaded.

7 Click **Next**. The **Generic LDAP Configuration and Management Step 2 of 3** page is displayed. Use this page to configure location information about generic LDAP servers and user accounts.

NOTE: In this release, the Smart Card based Two Factor Authentication (TFA) and the Single Sign-On (SSO) features are not supported for generic LDAP Directory Service.

8 Enter the following information:

- Select **Enable Generic LDAP**.

  ![note icon] **NOTE:** In this release, nested group is not supported. The firmware searches for the direct member of the group to match the user DN. Also, only single domain is supported. Cross domain is not supported.

- Select the **Use Distinguished Name to Search Group Membership** option to use the Distinguished Name (DN) as group members. iDRAC6 compares the User DN retrieved from the directory to compare with the members of the group. If cleared, user name provided by the login user is used to compare with the members of the group.

- In the **LDAP Server Address** field, enter the fully qualified domain name (FQDN) or the IP address of the LDAP server. To specify multiple redundant LDAP servers that serve the same domain, provide the list of all servers separated by commas. iDRAC6 tries to connect to each server in turn, until it makes a successful connection.

- Enter the port used for LDAP over SSL in the **LDAP Server Port** field. The default is 636.

- In the **Bind DN** field, enter the DN of a user used to bind to the server when searching for the login user's DN. If not specified, an anonymous bind is used.

- Enter the **Bind Password** to use in conjunction with the **Bind DN**. This is required if anonymous bind is not allowed.

- In the **Base DN to Search** field, enter the DN of the branch of the directory where all searches should start.

- In the **Attribute of User Login** field, enter the user attribute to search for. Default is UID. It is recommended that this be unique within the chosen Base DN, else a search filter must be configured to ensure the uniqueness of the login user. If the user DN cannot be uniquely identified by the search combination of attribute and search filter, the login will fail.

- In the **Attribute of Group Membership** field, specify which LDAP attribute should be used to check for group membership. This should be an attribute of the group class. If not specified, iDRAC6 uses the *member* and *uniquemember* attributes.

- In the **Search Filter** field, enter a valid LDAP search filter. Use the filter if the user attribute cannot uniquely identify the login user within the chosen Base DN. If not specified, the value defaults to *objectClass=**, which searches for all objects in the tree. This additional search filter configured by the user applies only to userDN search and not the group membership search.

9 Click **Next**. The **Generic LDAP Configuration and Management Step 3a of 3** page is displayed. Use this page to configure the privilege groups used to authorize users. When generic LDAP is enabled, role group(s) are used to specify authorization policy for iDRAC6 users.

    🖉 **NOTE:** In this release, unlike AD, you do not need to use special characters ("@", "\", and "/") to differentiate an LDAP user from a local user. You should only enter your user name to log in, and should not include the domain name.

10 Under **Role Groups**, click a **Role Group**.

The **Generic LDAP Configuration and Management Step 3b of 3** page is displayed. Use this page to configure each Role Group used to control authorization policy for users.

11 In the **Group DN** field, enter the group distinguished name that identifies the role group in the generic LDAP Directory Service associated with iDRAC6.

12 In the **Role Group Privileges** section, specify the privileges associated with the group by selecting the **Role Group Privilege Level**. For example, if you select **Administrator,** all of the privileges are selected for that level of permission.

13 Click **Apply** to save role group settings.

The iDRAC6 Web server automatically returns you to the **Generic LDAP Configuration and Management Step 3a of 3** page where your Role Group settings are displayed.

14 Configure additional role groups if required.

15 Click **Finish** to return to the **Generic LDAP Configuration and Management** summary page.

16 Click **Test Settings** to check the generic LDAP settings.

17 Enter the user name and password of a directory user that is chosen to test the LDAP settings. The format depends on what *Attribute of User Login* is used and the user name entered must match the value of the chosen attribute.

The test results and the test log are displayed. You have completed the generic LDAP Directory Service configuration.

Configuring Generic LDAP Directory Service Using RACADM

```
racadm config -g cfgldap -o cfgLdapEnable 1

racadm config -g cfgldap -o cfgLdapServer <FQDN or
IP-Address>

racadm config -g cfgldap -o cfgLdapPort <Port Number>

racadm config -g cfgldap -o cfgLdapBaseDN dc=
common,dc=com

racadm config -g cfgldap -o
cfgLdapCertValidationenable 0

racadm config -g cfgldaprolegroup -i 1 -o
cfgLdapRoleGroupDN 'cn=everyone,ou=groups,dc=
common,dc=com'

racadm config -g cfgldaprolegroup -i 1 -o
cfgLdapRoleGroupPrivilege 0x0001
```

View the settings using the following commands

```
racadm getconfig -g cfgldap

racadm getconfig -g cfgldaprolegroup -i 1
```

Use RACADM to confirm whether login is possible

```
racadm -r <iDRAC6-IP> -u user.1 -p password getractime
```

Additional settings to test BindDN option

```
racadm config -g cfgldap -o cfgLdapBindDN "cn=
idrac_admin,ou=iDRAC_admins,ou=People,dc=common,dc=
com"
```

```
racadm config -g cfgldap -o cfgLdapBindPassword
password
```

NOTE: Configure iDRAC6 to use a Domain Name Server, which resolves the LDAP server hostname that iDRAC6 is configured to use in the LDAP server address. The hostname must match the "CN" or "Subject" in the LDAP server's certificate.

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 **iDRAC Settings**→ **Network/Security tab**→ **Directory Service**→ **Microsoft 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. 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 results show 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 cannot 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" on page 175.

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** option 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 iDRAC6 for Single Sign-On or Smart Card Login

This section provides information to configure iDRAC6 for Smart Card login for local users and Active Directory users, and Single Sign-On (SSO) login for Active Directory users.

iDRAC6 supports Kerberos based Active Directory authentication to support Active Directory Smart Card and SSO logins.

About 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 SSO 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 SSO and Active Directory Smart Card logins. For Active Directory SSO 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.

Prerequisites for Active Directory SSO and Smart Card Authentication

The pre-requisites for both Active Directory SSO and Smart Card authentication are:

- Configure the iDRAC6 for Active Directory login. For more information, see "Using the iDRAC6 Directory Service" on page 141.

- Register the iDRAC6 as a computer in the Active Directory root domain. To do this:

  a Click **iDRAC Settings**→ **Network/Security** 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 involves 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 **Use DES encryption types for this account** property enabled.

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. You can also use the following RACADM time zone offset command to synchronize the time:

```
racadm config -g cfgRacTuning -o

cfgRacTuneTimeZoneOffset <offset value>
```

- To enable single sign-on for Extended schema, ensure that the **Trust this user for delegation to any service (Kerberos only)** option is selected on the **Delegation** tab for the keytab user. This tab is available only after creating the keytab file using **ktpass** utility.

Browser Settings to Enable Active Directory SSO

To configure the browser settings for Internet Explorer:

1 Open Internet Explorer Web browser

2 Select **Tools**→ **Internet Options**→ **Security**→ **Local Intranet**.

3 Click **Sites**.

4 Select the following options only:

- Include all local (intranet) sites not listed on other zones.
- Include all sites that bypass the proxy server.

5 Click **Advanced**.

6 Add all relative domain names that will be used for Weblogic Server instances that is part of the SSO configuration (for example, myhost.example.com)

7 Click **Close** and click **OK**.

8 Click **OK**.

To configure the browser settings for Firefox:

1 Open Firefox Web browser.

2 In the address bar, enter `about:config`.

3 In **Filter**, enter `network.negotiate`.

4 Add the iDRAC name to network.negotiate-auth.trusted-uris (using comma separated list).

5 Add the iDRAC name to network.negotiate-auth.delegation-uris (using comma separated list).

Using Microsoft Active Directory SSO

The SSO feature 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 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.

You can enable iDRAC6 to use Kerberos—a network authentication protocol—to enable SSO. For more information, see "About Kerberos Authentication" on page 185. Ensure that you have performed the steps listed in the "Prerequisites for Active Directory SSO and Smart Card Authentication" on page 186 section before configuring iDRAC6 for SSO logon.

Configuring iDRAC6 to Use SSO

Perform the following steps to configure iDRAC6 for SSO using iDRAC Web interface:

1   Log in to iDRAC Web interface.

2   Go to **iDRAC Settings**→ **Network/Security** tab→ **Directory Service** tab→ **Microsoft Active Directory**.

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

4   Upload the keytab obtained from the Active Directory root domain, to the iDRAC6. To do this, under **Upload Kerberos Keytab**, type the path of the keytab file or click **Browse** to locate the file. Click **Upload**. The Kerberos keytab will be uploaded into iDRAC6. The keytab is the same file you created while performing the tasks listed in the "Prerequisites for Active Directory SSO and Smart Card Authentication" on page 186.

5   Click **Next**. The **Active Directory Configuration and Management Step 2 of 4** page is displayed.

6   Select **Enable Single Sign-On** to enable SSO login.

7 Click **Next** until the last page is displayed. If Active Directory is configured to use standard schema, then **Active Directory Configuration and Management Step 4a of 4** page is displayed. If Active Directory is configured to use extended schema, then **Active Directory Configuration and Management Step 4 of 4** page is displayed.

8 Click **Finish** to apply the settings.

Using RACADM:

You can upload the keytab file to iDRAC6 using the following CLI racadm command:

```
racadm krbkeytabupload -f <filename>
```

where <filename> is the name of the keytab file. The racadm command is supported by both local and remote racadm.

To enable single sign–on using the CLI, run the racadm command:

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

Logging Into iDRAC6 Using SSO

1 Log in to your system using a valid Active Directory account.

2 To access the iDRAC6 Web page, type:

```
https://<FQDN address>
```

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

```
https://<FQDN address>:<port number>
```

where *FQDN address* is the iDRAC FQDN (idracdnsname.domain name) and *port number* is the HTTPS port number.

  NOTE: If you use IP address instead of FQDN, SSO will fail.

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.

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 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 Local iDRAC6 Users for Smart Card Logon

You can configure the local iDRAC6 users to log into the iDRAC6 using the Smart Card. Click **iDRAC Settings**→ **Network/Security**→ **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.

NOTE: Ensure that CA certificate validation is enabled before configuring the Smart Card.

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

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 Directory Service" on page 141 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.

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 Directory Service" on page 141 for more information on how to set up Active Directory users.

You can configure the Active Directory from **iDRAC Settings**→ **Network/Security**→ **Directory Service**→ **Microsoft Active Directory**.

NOTE: Ensure that CA certificate validation is enabled before configuring the Smart Card.

Configuring Smart Card Using iDRAC6

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

1   In the iDRAC6 Web interface, go to **iDRAC Settings**→ **Network/Security**→ **Smart Card** tab.

2   Configure the Smart Card logon settings.

Table 8-1 provides information about the **Smart Card** page settings.

3 Click **Apply**.

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 because these services support only single-factor authentication.
	• **Enabled with Remote Racadm** — Enables Smart Card logon along with remote RACADM. All other CLI out-of-band interfaces are disabled.
	If you select **Enabled** or **Enabled with Remote Racadm**, you are prompted for a Smart Card logon during any subsequent logon attempts using the Web-based interface.
	It is recommended 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, it is recommended to use the **Enabled** setting for Smart Card logon. Ensure that the iDRAC6 local user configuration and/or Active Directory configuration is complete before enabling Smart Card Logon.
	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.

Table 8-1. **Smart Card Settings** *(continued)*

Setting	Description
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. The user's iDRAC certificate, which is downloaded from the Certificate Revocation List (CRL) distribution server is checked for revocation in the CRL.
	The CRL distribution servers are listed in the Smart Card certificates of the users.
	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 **iDRAC Settings**→ **Network/Security**→ **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 **Network/Security**→ **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**.

You are logged into the iDRAC6 with your credentials as set in Active Directory.

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 cfgSmartCard -o cfgSmartCardLogonEnable 0`

- For 64–bit Windows platforms, the iDRAC6 authentication Active–X plug–in is not installed if a 64–bit version of Microsoft Visual C++ 2005 Redistributable Package is deployed. To install and run the Active–X plug–in properly, deploy the 32–bit version of Microsoft Visual C++ 2005 SP1 Redistributable Package (x86). This package is required to launch the Virtual Console session on a Internet Explorer browser.

- If you receive the following error message "`Not able to load the Smart Card Plug-in. Please check your IE settings or you may have insufficient privileges to use the Smart Card Plug-in`", then install the Microsoft Visual C++ 2005 SP1 Redistributable Package (x86). This file is available on the Microsoft Website at **microsoft.com**. Two distributed versions of the C++ Redistributable Package have been tested and they allow the Dell Smart Card plug–in to load. See Table 8-2 for details.

Table 8-2.   Distributed Versions of the C++ Redistributable Package

Redistributable Package File Name	Version	Release Date	Size	Description
vcredist_x86.exe	6.0.2900.2180	March 21, 2006	2.56 MB	MS Redistributable 2005
vcredist_x86.exe	9.0.21022.8	November 7, 2007	1.73 MB	MS Redistributable 2008

- Ensure that iDRAC6 time and the domain controller time at the domain controller server are set within 5 minutes of each other for Kerberos authentication to work. See the **RAC Time** on the **System→ iDRAC Settings→ Properties→ iDRAC Information** page, and the domain controller time by right clicking on the time in the bottom right hand corner of the screen. The timezone offset is displayed in the pop up display. For US Central Standard Time (CST), this is –6). Use the following RACADM timezone offset command to synchronize the iDRAC6 time (through Remote or Telnet/SSH RACADM): `racadm config –g cfgRacTuning –o cfgRacTuneTimeZoneOffset <offset value in minutes>`. For example, if the system time is GMT -6 (US CST) and time is 2PM, set the iDRAC6 time to GMT time

of 18:00 which would require you to enter 360 in the above command for the offset. You can also use *cfgRacTuneDaylightoffset* to allow for daylight savings variation. This saves you from having to change the time on those two occasions every year when the daylight savings adjustments are made, or allow for it in the above offset using 300 in the above example.

Frequently Asked Questions About SSO

SSO login fails on Windows Server 2008 R2 x64. What should I do for SSO to work with Windows Server 2008 R2 x64?

1 Execute
   http://technet.microsoft.com/en-us/library/dd560670(WS.10).aspx for the domain controller and domain policy. Configure your computers to use the DES-CBC-MD5 cipher suite. These settings might affect compatibility with client computers or services and applications in your environment. The **Configure encryption types allowed for Kerberos** policy setting is located at **Computer Configuration\Security Settings\Local Policies\Security Options**.

2 The domain clients must have the updated GPO. At the command line, type `gpupdate /force` and delete the old key tab with `klist purge` cmd.

3 Once the GPO has been updated, create the new keytab.

4 Upload the keytab to the iDRAC6.

You can now log in to iDRAC using SSO.

SSO login fails with AD users on Windows 7 and Windows Server 2008 R2. What should I do to resolve this?

You must enable the encryption types for Windows 7 and Windows Server 2008 R2. To enable the encryption types:

1 Log in as administrator or as a user with adminstrative privilege.

2 Go to **Start** and run **gpedit.msc**. The **Local Group Policy Editor** window is displayed.

3 Navigate to **Local Computer Settings**→ **Windows Settings**→ **Security Settings**→ **Local Policies**→ **Security Options**.

4 Right-click **Network Security: Configure encryption types allowed for kerberos** and select **Properties**.

5 Enable all the options.

6 Click **OK**. You can now log in to iDRAC using SSO.

Perform the following additional settings for Extended Schema:

1 In the **Local Group Policy Editor** window, navigate to **Local Computer Settings**→ **Windows Settings**→ **Security Settings**→ **Local Policies**→ **Security Options**.

2 Right-click **Network Security: Restrict NTLM: Outgoing NTLM traffic to remote server** and select **Properties**.

3 Select **Allow all**.

4 Click **OK** and then close the **Local Group Policy Editor** window.

5 Go to **Start** and run **cmd**. The **command prompt** window is displayed.

6 Run the command `gpupdate /force`. The group policies are updated. Close the **command prompt** window.

7 Go to **Start** and run **regedit**. The **Registry Editor** window is displayed.

8 Navigate to **HKEY_LOCAL_MACHINE**→ **System**→ **CurrentControlSet**→ **Control**→ **LSA**.

9 In the right-pane, right-click and select **New**→ **DWORD (32-bit) Value**.

10 Name the new key as **SuppressExtendedProtection**.

11 Right-click **SuppressExtendedProtection** and click **Modify.**

12 In the **Value data** field, type **1** and click **OK**.

13 Close the **Registry Editor** window. You can now log in to iDRAC using SSO.

If you have enabled SSO for iDRAC and you are using Internet Explorer to log in to iDRAC, SSO fails and you are prompted to enter your user name and password. How do I resolve this?

Ensure that the iDRAC IP address is listed in the **Tools**→ **Internet Options**→ **Security**→ **Trusted sites**. If it is not listed, SSO fails and you are prompted to enter your user name and password. Click **Cancel** and proceed.

9

Using GUI Virtual Console

This section provides information about using the iDRAC6 Virtual Console feature.

Overview

The iDRAC6 Virtual Console feature enables you to access the local console remotely in either graphic or text mode. Using Virtual Console, 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 Virtual Console

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

NOTE: If a Virtual Console session is already open from the management station to a particular iDRAC6, any attempt to open a new session from the same management station to that iDRAC6 will fail.

NOTE: Multiple Virtual Console sessions can be opened from a single management station to multiple iDRAC6 controllers simultaneously.

The **Virtual Console** 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 Virtual Console session:

- A maximum of four simultaneous Virtual Console sessions are supported. All sessions view the same managed server console simultaneously.

- From 1.5 release version onwards, multiple sessions to multiple remote servers is possible from the same client, based on the order in which they are opened. If a Virtual Console session using Java plug-in is open, you can open another Virtual Console session using ActiveX plug-in. However, if a ActiveX based Virtual Console session is open, then another Virtual Console session using Java plug-in cannot be opened. You must close the first Virtual Console session to open a second Virtual Console session.

- A Virtual Console 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 Virtual Console session to the iDRAC6 is a full access session. If a second user requests a Virtual Console session, the first user is notified and is given the option (approve, reject, or allow as read-only) to send a sharing request to the second user. The second user is notified that another user has control. When the first user has not responded for each subsequent user's sharing request within a timeout of 30 seconds, Virtual Console access is granted based on the value set for the `cfgRacTuneVirtualConsoleAuthorizeMultipleSessions` object. This object is irrespective of the plug-in type (ActiveX or Java) set to be used in the second/third/fourth session. For more information about this object, see the *RACADM Command Line Reference Guide for iDRAC6 and CMC* available on the Dell Support website at **support.dell.com/manuals**.

  NOTE: This rule is applicable only with the remote or firmware (SSH or Telnet) RACADM and not with local RACADM.

Configuring Your Management Station

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

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

   - "Supported Web Browsers" on page 25
   - "Configuring a Supported Web Browser" on page 41

2. If you are using Firefox or want to use the Java Viewer with Internet Explorer, install a Java Runtime Environment (JRE). If you use the Internet Explorer browser, an ActiveX control is provided for the console viewer. You can also use the Java console viewer with Firefox if you install a JRE and configure the console viewer in iDRAC6 Web interface before you launch the viewer.

3. If you are using Internet Explorer (IE), 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 clear this option:

     ```
     Do not save encrypted pages to disk
     ```

4. If you are using Internet Explorer to launch a Virtual Console session with Active-X plug-in, ensure that you have added the iDRAC6 IP or hostname to the **Trusted Sites** list. You should also reset the custom settings to **Medium-low** or change the settings to allow installation of signed Active-X plug-ins. For more information, see "Internet Explorer Browser Configurations for ActiveX based Virtual Console and Virtual Media Applications" on page 205.

   NOTE: 64-bit ActiveX plug-in is not supported to launch a Virtual Console session using Internet Explorer.

5 It is recommended 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. Press <Ctrl><Alt><F1> at the iDRAC6 Virtual Console to 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**.

Clear Your Browser's Cache

If you have issues when operating the Virtual Console, (out of range errors, synchronization issues, and so on) clear the browser's cache to remove or delete any old versions of the viewer that may be stored on the system and try again.

NOTE: You must have administrator privilege to clear the browser's cache.

To clear older versions of Active-X viewer for IE7, do the following:

1 Close the Video Viewer and Internet Explorer browser.

2 Open the Internet Explorer browser again and go to **Internet Explorer**→ **Tools**→ **Manage Add-ons** and click **Enable or Disable Add-ons**. The **Manage Add-ons** window is displayed.

3 Select **Add-ons that have been used by Internet Explorer** from the **Show** drop-down menu.

4 Delete the *Video Viewer* add-on.

To clear older versions of Active-X viewer for IE8, do the following:

1 Close the Video Viewer and Internet Explorer browser.

2 Open the Internet Explorer browser again and go to **Internet Explorer**→ **Tools**→ **Manage Add-ons** and click **Enable or Disable Add-ons**. The **Manage Add-ons** window is displayed.

3 Select **All Add-ons** from the **Show** drop-down menu.

4 Select the *Video Viewer* add-on and click the **More Information** link.

5 Select **Remove** from the **More Information** window.

6 Close the **More Information** and the **Manage Add-ons** windows.

To clear older versions of Java viewer in Windows or Linux, do the following:

1 At the command prompt, run `javaws-viewer` or
`javaws-uninstall`

2 The **Java Cache viewer** is displayed.

3 Delete the items titled *iDRAC6 Virtual Console Client.*

Internet Explorer Browser Configurations for ActiveX based Virtual Console and Virtual Media Applications

This section provides information about the Internet Explorer browser settings required to launch and run ActiveX based Virtual Console and Virtual Media applications.

NOTE: Clear the browser's cache and then perform the browser configuration settings. For more information, see "Clear Your Browser's Cache" on page 204.

Common Settings for Microsoft Windows Operating Systems

1 In Internet Explorer, go to **Tools**→ **Internet Options**→ **Security** tab.

2 Select the Zone you want to use to run the application.

3 Click **Custom**. If you are using Internet Explorer 8, click **Custom level**. The **Security Settings** window is displayed.

4 Under **ActiveX controls and plug-ins**:

- Select the **Prompt** option for **Download signed ActiveX controls**

- Select the **Enable** or **Prompt** option for **Run ActiveX controls and plug-ins**

- Select the **Enable** or **Prompt** option for **Script ActiveX controls marked safe for scripting**

- Click **OK** and again click **OK**.

Additional Settings for Windows Vista or Newer Microsoft Operating Systems

The Internet Explorer browsers in Windows Vista or newer operating systems have an additional security feature called 'Protected Mode'.

You can launch and run ActiveX applications in Internet Explorer browsers with 'Protected Mode' in one of the following ways:

- Go to **Program Files→ Internet Explorer**. Right-click **iexplore.exe** and click **Run as administrator**.
- Add the iDRAC IP address to the Trusted Sites. To do this:

1 In Internet Explorer, go to **Tools→ Internet Options→ Security→ Trusted Sites**.

2 Ensure that the **Enable Protected Mode** option is not selected for Trusted Sites zone. Alternatively, you can add the iDRAC address to sites in the Intranet zone. By default, protected mode is turned off for sites in Intranet Zone and Trusted Sites zone.

3 Click **Sites**.

4 In the **Add this website to the zone** field, add the address of your iDRAC and click **Add**.

5 Click **Close** and then click **OK**.

6 Close and restart the browser for the settings to take effect.

Supported Screen Resolutions and Refresh Rates

Table 9-1 lists the supported screen resolutions and corresponding refresh rates for a Virtual Console session that is running on the managed server.

Table 9-1.   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 Virtual Console in the iDRAC6 Web Interface

To configure Virtual Console in the iDRAC6 Web interface, perform the following steps:

1 Click **System**→ **Console/Media**→ **Configuration** to configure iDRAC6 Virtual Console settings.

2 Configure the Virtual Console properties. Table 9-2 describes the settings for Virtual Console.

3 When completed, click **Apply** to save the new settings.

Table 9-2.   Virtual Console Configuration Properties

Property	Description
Enabled	Click to enable or disable Virtual Console. If this option is checked, it indicates that Virtual Console is enabled. The default option is **enabled**.
	NOTE: Checking or clearing the **Enabled** option once after the Virtual Console is launched may disconnect all your existing Virtual Console sessions.
Max Sessions	Select the maximum number of Virtual Console sessions that are allowed, 1 to 4. 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 Virtual Console 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 Console is launched may disconnect all your existing Virtual Console sessions.

Table 9-2.   Virtual Console Configuration Properties *(continued)*

Property	Description
Video Encryption Enabled	**Checked** indicates that video encryption is enabled. All traffic going to the video port is encrypted.
	Unchecked indicates that video encryption is disabled. Traffic going to the video port is not encrypted.
	The default is **Encrypted**. Disabling encryption can improve performance on slower networks.
	NOTE: Enabling or disabling the **Video Encryption Enabled** option once after the Virtual Console is launched may disconnect all your existing Virtual Console sessions.
Local Server Video Enabled	Checked indicates that output to the iDRAC6 Virtual Console monitor is disabled during Virtual Console. This ensures that the tasks you perform using **Virtual Console** will not be visible on the managed server's local monitor.
Plug-in Type	The type of plug-in to be configured.
	• **Native** (ActiveX for Windows and Java plug-in for Linux) — ActiveX viewer will only work on Internet Explorer.
	• **Java** — A Java viewer will be launched.

NOTE: For information about using Virtual Media with Virtual Console, see "Configuring and Using Virtual Media" on page 253.

Opening a Virtual Console Session

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

NOTE: Virtual Console launch from a Windows Vista management station may lead to Virtual Console restart messages. To avoid this, set the appropriate timeout values in the following locations: **Control Panel**→ **Power Options**→ **Power Saver**→ **Advanced Settings**→ **Hard Disk**→ **Turnoff Hard Disk After <time_out>** and in the **Control Panel**→ **Power Options**→ **High–Performance**→ **Advanced Settings**→ **Hard Disk**→ **Turnoff Hard Disk After <time_out>**.

To open a Virtual Console session in the Web interface, perform the following steps:

1 Click **System→ Console/Media→ Virtual Console and Virtual Media**.

2 Use the information in Table 9-3 to ensure that a Virtual Console session is available.

If you want to reconfigure any of the property values displayed, see "Configuring Virtual Console in the iDRAC6 Web Interface" on page 207.

Table 9-3.   Virtual Console

Property	Description
Virtual Console Enabled	Yes/No (checked\unchecked)
Video Encryption Enabled	Yes/No (checked\unchecked)
Max Sessions	Displays the maximum number of supported Virtual Console sessions.
Active Sessions	Displays the current number of active Virtual Console sessions.
Local Server Video Enabled	Yes = Enabled; No = Disabled.
Remote Presence Port	The network port number used for connecting to the Virtual Console 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.
Plug-in Type	Displays the type of plug-in you selected in the **Configuration** page. **NOTE:** For 64–bit Windows platforms, the iDRAC6 authentication Active–X plug–in will not get installed properly if a 64–bit version of Microsoft Visual C++ 2005 Redistributable Package is deployed. To install and run the Active–X plug–in properly, deploy the 32–bit version of Microsoft Visual C++ 2005 SP1 Redistributable Package (x86). This package is required to launch the Virtual Console session on an Internet Explorer browser.

NOTE: For information about using Virtual Media with Virtual Console, see "Configuring and Using Virtual Media" on page 253.

3 If a Virtual Console session is available, click **Launch Virtual Console** on the **Virtual Console and Virtual Media** page.

> **NOTE:** Multiple message boxes may appear after you launch the application. To prevent unauthorized access to the application, 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 iDRAC6 Virtual Console 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 iDRAC6 Virtual Console menu.

Virtual Console Preview

Before launching the Virtual Console, you can preview the state of the Virtual Console on the **System→ Properties→ System Summary** page. The **Virtual Console Preview** section displays an image showing the state of the Virtual Console. The image is automatically refreshed every 30 seconds.

> **NOTE:** The Virtual Console image is available only if you have enabled Virtual Console and if iDRAC6 Enterprise card is present.

Table 9-4 provides information about the available options.

Table 9-4.   Virtual Console Preview Options

Option	Descritpion
Launch	Click this link to launch the Virtual Console.
	If only Virtual Media is enabled, then clicking this link directly launches the Virtual Media.
	This link is not displayed if you do not have Virtual Console privileges or if both Virtual Console and Virtual Media are disabled.

Table 9-4. Virtual Console Preview Options *(continued)*

Option	Descritpion
Settings	Click this link to view or edit the Virtual Console configuration settings on the **Console/Media Configuration** page.
	NOTE: You must have configure iDRAC privileges to edit the Virtual Console configuration settings.
Refresh	Click this link to refresh the displayed Virtual Console image.

Using iDRAC6 Virtual Console (Video Viewer)

The iDRAC6 Virtual Console (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 iDRAC6 Virtual Console starts in a separate window.

NOTE: You must have administrator privileges to launch a iDRAC6 Virtual Console (Video Viewer).

NOTE: If the remote server is powered off, the message, **No Signal**, will be displayed.

NOTE: The Virtual Console title bar displays the DNS name or the IP address of the iDRAC you are connected to from the management station. If iDRAC does not have a DNS name, then the IP address is displayed. The format is:
`<DNS name / IPv6 address / IPv4 address>, <Model>, User: <username>, <fps>`

The iDRAC6 Virtual Console 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 **Virtual Console and Virtual Media** GUI page.

When you start a Virtual Console session and the iDRAC6 Virtual Console is displayed, you may need to synchronize the mouse pointers.

Table 9-5 describes the menu options that are available for use in the viewer.

Table 9-5.   Viewer Menu Bar Selections

Menu Item	Item	Description
"Pin" icon	NA	Click on the "pin" icon to lock the iDRAC6 Virtual Console menu bar. This prevents the tool bar from auto-hiding. **NOTE:** This is applicable only for the Active-X Viewer and not for Java plug-in.
Virtual Media	Launch Virtual Media	The **Virtual Media Session** is displayed which lists the devices available for mapping in the main window. To virtualize an ISO or IMG image, click **Add** and select the image file. The selected image file is displayed along with the list of devices available for mapping in the main window. To virtualize a device or am image, check the option in the **Mapped** column of the table. The device or the image will be mapped to the server at this point. To unmap, clear the checkbox. Click **Details** to display a panel that lists the Virtual devices and images. It also displays the read/write activity for each device or image.
File	Capture to File	Captures the current remote system screen to a **.bmp** file on Windows or a **.png** file on Linux. A dialog box is displayed that allows you to save the file to a specified location. **NOTE:** **.bmp** file format on Windows or **.png** file format on Linux are applicable only for the Native plug-in. Java plug-in supports only the **.jpg** and **.jpeg** file formats.
	Exit	When you have finished using the Console and have logged out (using the remote system's log out procedure), select **Exit** from the **File** menu to close the **iDRAC6 Virtual Console** window.

Table 9-5.   Viewer Menu Bar Selections *(continued)*

Menu Item	Item	Description
View	**Refresh**	Refreshes the view of the Video Virtual Console. The Virtual Console requests a reference video frame from the server.
	Full Screen/Windowed	View the Video Virtual Console in full screen mode. To exit from full screen mode, click **Windowed**.
	Fit	Resizes the Video Virtual Console window to the minimum size that is need to display the server's video. This menu item is not available in full screen mode.

Table 9-5.   Viewer Menu Bar Selections *(continued)*

Menu Item	Item	Description
Macros	• Alt+Ctrl+Del • Alt+Tab • Alt+Esc • Ctrl+Esc • Alt+Space • Alt+Enter • Alt+Hyphen • Alt+F4 • PrtScrn • Alt+PrtScrn • F1 • Pause • Tab • Ctrl+Enter • SysRq • Alt+LShift+RShift +Esc • Ctrl+Alt+Backspace • Alt+F? (Where F? represents the keys F1-F12) • Ctrl+Alt+F? (Where F? represents the keys F1-F12)	When you select a macro, or enter the hotkey specified for the macro, the action is executed on the remote system.

Table 9-5.   Viewer Menu Bar Selections *(continued)*

Menu Item	Item	Description
Tools	**Session Options**	The Sessions Options window provides additional session viewer control adjustments. This window has the **General** and **Mouse** tabs.
		You can control the **Keyboard pass through mode** from the General tab. Select **Pass all keystrokes to target** to pass your management station's keystrokes to the remote system.
		The mouse tab contains two sections: **Single Cursor** and **Mouse Acceleration**. The **Single Cursor** feature is provided in order to offset mouse alignment issues on some remote operating systems. Once the viewer enters **Single Cursor** mode, the mouse pointer is trapped within the viewer window. Press the termination key to exit out of this mode. Use this control to select the key that will exit out of single cursor mode.
		Mouse Acceleration optimizes the mouse performance depending upon your operating system.
	Single Cursor	Enables single cursor mode in the Viewer. In this mode, the client cursor is hidden from view so that only the server's cursor is visible. The client cursor is also trapped within the Viewer's frame. The user will not be able to use the cursor outside of the Viewer window until they press the **Termination Key** specified in the **Session Options - Mouse** tab.
	Stats	This menu option launches a dialog which displays performance statistics for the Viewer. The values displayed are:
		• Frame Rate
		• Bandwidth
		• Compression
		• Packet Rate

Table 9-5.   Viewer Menu Bar Selections *(continued)*

Menu Item	Item	Description
Power	**Power ON System**	Powers on the system.
	Power OFF System	Powers off the system.
	Graceful Shutdown	Shuts down the system. **NOTE:** Ensure that the shutdown option is configured for the operating system before you perform a graceful shutdown using this option. If you use this option without configuring it on the operating system, it reboots the managed system instead of performing a shutdown operation.
	Reset System (warm boot)	Reboots the system without powering it off.
	Power Cycle System (cold boot)	Powers off, and then reboots the system.
Help	**Contents and Index**	Provides instructions on how to view the online help.
	About iDRAC6 Virtual Console	Displays the **iDRAC6 Virtual Console** version.

Disabling or Enabling Local Server Video

You can configure the iDRAC6 to disallow iDRAC6 Virtual Console 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 **Virtual Console Configuration** page.

NOTE: By disabling (turning off) the local video on the server, the monitor, keyboard, and mouse connected to the iDRAC6 Virtual Console 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.

2 Click **System→ Console/Media→ Configuration**.

3 To disable (turn off) local video on the server, clear 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**.

Launching Virtual Console and Virtual Media Remotely

You can launch Virtual Console/Virtual Media by entering a single URL on a supported browser instead of launching it from the iDRAC6 Web GUI. Depending on your system configuration, you will either go through the manual authentication process (login page) or will be directed to the Virtual Console/Virtual Media viewer automatically.

If SSO is already configured on the system, you cannot use the URL format for launching Virtual Console/Virtual Media.

You can launch the Virtual Console with a user account created locally in iDRAC6, LDAP and Active Directory.

> **NOTE:** Internet Explorer supports Local, Active Directory (AD), Smart Card (SC) and Single Sign-On (SSO) logins. Firefox supports only Local, AD, and SSO logins on Windows-based operating system. It does not support SC login.

Launching Console Using URL Format

If you enter the `link<IP>/console` in a browser, then log in using the normal manual login procedure depending on the login configuration. If the login is successful, the Virtual Console/Virtual Media view is launched. Else, you are redirected to the iDRAC6 GUI home page.

The iDRAC Web GUI session is displayed in the background on the vKVM page.

You can launch only one session of the Virtual Console at a time.

If you have Read Only privileges then use the URL format to launch only the the Virtual Console page and not the Virtual Media page.

If Virtual Console is disabled in iDRAC6, the user or administrator can still launch the Virtual Media, if their privileges are sufficient. For more information on sufficient priveleges, see "Launching Virtual Console and Virtual Media Remotely" on page 217.

General Error Scenarios

Table 9-6 lists general error scenarios, the reasons for those errors, and the iDRAC6 behavior.

Table 9-6. Error Scenarios

Error Scenarios	Reason	Behavior
Login failed	You have entered either an invalid user name or an incorrect password.	Same behavior when *https://<IP>* is specified and login fails.
iDRAC6 Enterprise Card not present	The iDRAC6 Enterprise Card is not present. So the Virtual Console/Virtual Media feature is not available.	The iDRAC6 Virtual Console viewer is not launched. Redirects to the iDRAC6 GUI home page.
Insufficient Privileges	You do not have Virtual Console and Virtual Media privileges.	The iDRAC6 Virtual Console viewer is not launched and you are redirected to the Console/Media configuration GUI page.
Virtual Console disabled	Virtual Console is disabled on your system.	The iDRAC6 Virtual Console viewer is not launched and you are redirected to the Console/Media configuration GUI page.
Unknown URL parameters detected	The URL you have entered contains undefined parameters.	Page not Found (404) message is displayed.

Frequently Asked Questions on Virtual Console

Table 9-7 lists frequently asked questions and answers.

Table 9-7.   Using Virtual Console: Frequently Asked Questions

Question	Answer
Virtual Console fails to log out when the out–of–band Web GUI is logged out.	The Virtual Console and Virtual Media sessions stays active even if the Web session is logged off. Close the Virtual Media and Virtual Console viewer applications to log out of the corresponding session.
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.

Table 9-7. Using Virtual Console: Frequently Asked Questions *(continued)*

Question	Answer
How can I get the current status of the local server video?	The status is displayed on the **Virtual Console Configuration** page of the iDRAC6 Web interface.
	The RACADM CLI command `racadm getconfig –g cfgRacTuning` displays the status in the object **cfgRacTuneLocalServerVideo**.
I cannot see the bottom of the system screen from the Virtual Console window.	Ensure that the management station's monitor resolution is set to 1280x1024. Try using the scroll bars on the iDRAC6 Virtual Console 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 (either in Dell Unified Server Configurator (USC), Dell Lifecycle Controller or in Dell Unified Server Configurator Lifecycle Controller Enabled (USC-LCE)?	Virtual Console 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 Virtual Console session.
	Ensure that the **Single Cursor** option under **Tools** in the iDRAC6 Virtual Console menu is selected on the iDRAC6 Virtual Console client. The default is two cursor mode.

Table 9-7.   Using Virtual Console: Frequently Asked Questions *(continued)*

Question	Answer
Why can't I use a keyboard or mouse while installing a Microsoft operating system remotely by using iDRAC6 Virtual Console?	When you remotely install a supported Microsoft operating system on a system with Virtual Console 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 Virtual Console off in the BIOS.
	This message is generated by Microsoft to alert the user that Virtual Console is enabled. To ensure that this message does not appear, always turn off Virtual Console 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.
Why do multiple Session Viewer windows appear when I establish a Virtual Console session from the local host?	You are configuring a Virtual Console session from the local system. This is not supported.
If I am running a Virtual Console 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 Virtual Console session?	It is recommended to have a 5 MB/sec connection for good performance. A 1 MB/sec connection is required for minimal performance.

Table 9-7.   Using Virtual Console: Frequently Asked Questions *(continued)*

Question	Answer
What are the minimum system requirements for my management station to run Virtual Console?	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 iDRAC6 Virtual Console Video Viewer?	You may see this message because the iDRAC6 Virtual Console 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 iDRAC6 Virtual Console Video Viewer?	You may see this message because a parameter necessary to capture video is beyond the range for which the iDRAC6 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.

10

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 10-1.   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.
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 FRU information.

Table 10-1.   Standard DMTF (continued)

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.

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.

Table 10-1. Standard DMTF *(continued)*

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 10-1.   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.

6 Dell Job Control
Defines CIM and Dell extension classes for managing configuration jobs.

7 Dell LC Management Profile
Defines CIM and Dell extension classes for the configuration attributes of the Dell
Lifecycle Controller such as Auto-discovery. This profile also enables management of
Part Replacement, Motherboard Replacement, Export and Import of System Profile,
boot from network share and encryption certificate management.

8 Dell Persistent Storage
Defines CIM and Dell extension classes for managing the partitions on the vFlash
SD card of Dell platforms.

9 Dell Simple NIC
Defines CIM and Dell extension classes to represent the configuration of NIC
network controllers.

10 Dell BIOS and Boot Management Profile
Defines CIM and Dell extension classes to represent Dell BIOS attributes and to
configure the host's boot sequence.

Table 10-1. Standard DMTF *(continued)*

11 Dell RAID Profile
Defines CIM and Dell extension classes to represent the configuration of the host's RAID storage.

12 Dell Power Supply Profile
Defines CIM and Dell extension classes to represent the host's power supply inventory information.

13 Dell iDRAC Card Profile
Defines CIM and Dell extension classes to represent the iDRAC6 inventory information. This profile also provides representation and methods to configure iDRAC attributes and user accounts.

14 Dell Fan Profile
Defines CIM and Dell extension classes to represent the host's fan inventory information.

15 Dell Memory Profile
Defines CIM and Dell extension classes to represent the host's DIMM inventory information.

16 Dell CPU Profile
Defines CIM and Dell extension classes to represent the host's CPU inventory information.

17 Dell System Info Profile
Defines CIM and Dell extension classes to represent the host platform's inventory information.

18 Dell PCI Device Profile
Defines CIM and Dell extension classes to represent the host's PCI device inventory information.

19 Dell Video Profile
Defines CIM and Dell extension classes to represent the host's video card inventory information.

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.

For more information on Dell Lifecycle Controller Remote Services, see the following documents:

- User's Guide
- Release Notes
- Error Messages and Troubleshooting List

To access these documents:

1 Go to **support.dell.com/manuals**.

2 Click **Software**→ **Systems Management**→ **Dell Unified Server Configurator and Lifecycle Controller** .

3 Click the relevant version to view the all the documents for a particular release.

For Web Services Interface guides (Windows and Linux), profile documents, code samples, white papers, and other useful information, navigate to **OpenManage Systems Management**→ **Lifecycle Controller** on **delltechcenter.com**.

For more information, see the following:

- DMTF Web site at **dmtf.org/standards/profiles/**
- WS–MAN release notes or readme file.

11

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 **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 10-1.

The following sections provide an overview of the SM-CLP feature that is hosted from 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.

See the following 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 11-1.

Table 11-1.   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 11-2 provides a list of targets provided through the SM-CLP to support the operations described in Table 11-1 above.

Table 11-2.   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

Table 11-2. SM-CLP Targets *(continued)*

Target	Definitions
`admin1/system1/consoles1`	Managed system consoles SMASH collection
`admin1/system1/usbredirectsap1`	Virtual Media USB redirection SAP
`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/capabilitie s1`	Service processor capabilities SMASH collection
`admin1/system1/sp1/capabilitie s1/clpcap1`	CLP service capabilities
`admin1/system1/sp1/capabilitie s1/pwrmgtcap1`	Power state management service capabilities on the system
`admin1/system1/sp1/capabilitie s1/ipcap1`	IP interface capabilities
`admin1/system1/sp1/capabilitie s1/dhcpcap1`	DHCP client capabilities
`admin1/system1/sp1/capabilitie s1/NetPortCfgcap1`	Network port configuration capabilities
`admin1/system1/sp1/capabilitie s1/usbredirectcap1`	Virtual Media capabilities USB redirection SAP
`admin1/system1/sp1/capabilitie s1/vmsapcap1`	Virtual Media SAP capabilities
`admin1/system1/sp1/capabilitie s1/swinstallsvccap1`	Software installation service capabilities
`admin1/system1/sp1/capabilitie s1/acctmgtcap*`	Account management service capabilities
`admin1/system1/sp1/capabilitie s1/adcap1`	Active Directory capabilities
`admin1/system1/sp1/capabilitie s1/rolemgtcap*`	Local Role Based Management capabilities

Table 11-2. SM-CLP Targets (continued)

Target	Definitions
`admin1/system1/sp1/capabilitie s/PwrutilmgtCap1`	Power utilization management capabilities
`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

Table 11-2.   SM-CLP Targets *(continued)*

Target	Definitions
`admin1/system1/sp1/jobq1/job*`	CLP service protocol job
`admin1/system1/sp1/pwrmgtsvc1`	Power state management service
`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

Table 11-2. SM-CLP Targets _(continued)_

Target	Definitions
`admin1/sysetm1/sp1/ account1-16/identity4`	CLP identity account
`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

Table 11-2. SM-CLP Targets *(continued)*

Target	Definitions
`admin1/system1/sp1/` `pwrutilmgtsvc1/pwrcurr1`	Power utilization management service current power allocation setting data
`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

12

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 or IPv6 addresses of the remote systems that will be deployed in the **ip.txt** text file, one IPv4 or IPv6 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-user-
password> -c {<iso9660-img> | <path>} -f {<floppy-
device> or <floppy-image>}
```

where:

- *<idrac-user>* is the iDRAC6 user name, for example **root**
- *<idrac-user-password>* 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
- -f {*<floppy-device>*} is the path to the device containing the operating system installation CD, DVD, or Floppy
- *<floppy-image>* 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 or IPv6 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.

⚠ **CAUTION: It is recommended to use the interactive flag '-i' option, when starting up the VMCLI command line utility. This ensures tighter security by keeping the username and password private because on many Windows and Linux operating systems, the username and password are visible when processes are examined by other users.**

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 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" on page 242 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 or IPv6 address and SSL port, which the utility needs to establish a Virtual Media connection with the target iDRAC6. If you enter an invalid IPv4 or IPv6 address or DDNS name, an error message is displayed and the command is terminated.

<iDRAC-IP-address> is a valid, unique IPv4 or IPv6 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>`

This parameter provides the iDRAC6 user name that will run Virtual Media.

The *<iDRAC-user>* 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 {<floppy-device> or <floppy-image>}` and/or

`-c {<CD-DVD-device> or <CD-DVD-image>}`

where `<floppy-device>` or `<CD-DVD-device>` is a valid drive letter (for Windows systems) or a valid device filename (for Linux systems), and `<floppy-image> or <CD-DVD-image>` 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 provide support for multiple LUNs. However, the kernel supports this functionality. 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 is displayed 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 displayed 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 is displayed 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.

13

Configuring Intelligent Platform Management Interface

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" on page 110.

Configuring IPMI Using Web-Based Interface

For detailed information, see "Configuring IPMI Using Web Interface" on page 60.

Configuring IPMI Using the RACADM CLI

1 Login to the remote system using any of the RACADM interfaces. See "Using RACADM Remotely" on page 110.

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>
   ```

For more information, see iDRAC6 Property Database Group and Object Definitions in the RACADM *Command Line Reference Guide for iDRAC6 and CMC* available on the Dell Support website at **support.dell.com/manuals**.

Configuring Serial Over LAN Using the Web-Based Interface

For detailed information, see "Configuring IPMI Using Web Interface" on page 60.

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**.

14

Configuring and Using Virtual Media

Overview

The **Virtual Media** feature, accessed through the Virtual Console viewer, provides the managed server access to media connected to a remote system on the network. Figure 14-1 shows the overall architecture of **Virtual Media**.

Figure 14-1.   Overall Architecture of Virtual Media

Managed Server

Monolithic Server

Management Station

Remote CD/DVD/USB

Network

Remote Floppy
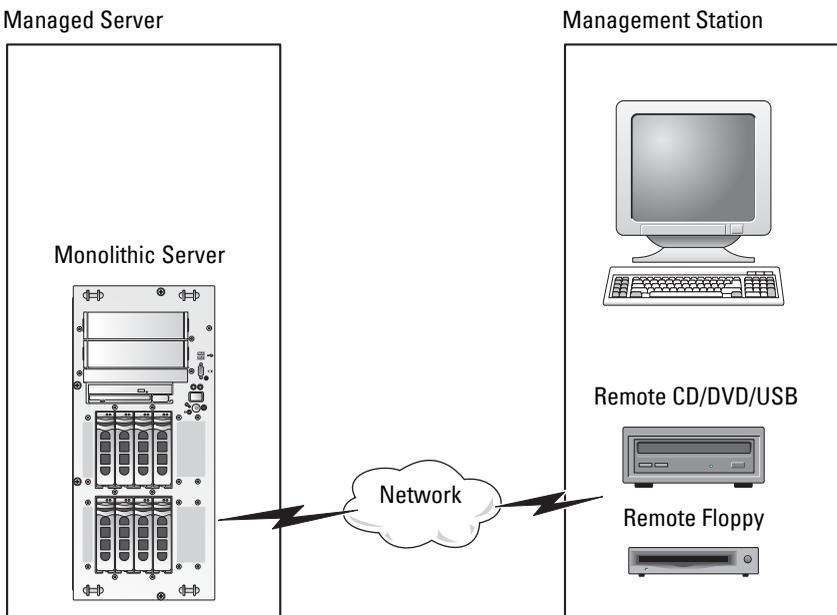
Using **Virtual Media**, administrators can remotely boot their managed servers, install applications, update drivers, or even install new operating systems remotely from the virtual CD/DVD and diskette drives.

> **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 14-1 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 14-1. 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 32-bit Java Runtime Environment (JRE) is required to run the Virtual Console plugin. You can download a JRE from **java.sun.com**.

⚠ **CAUTION: To successfully launch Virtual Media, ensure that you have installed a 32-bit or 64-bit JRE version on a 64-bit operating system or a 32-bit JRE version on a 32-bit operating system. iDRAC6 does *not* support 64-bit ActiveX versions. Also ensure that for Linux, the "compat-libstdc++-33-3.2.3-61" related package must be installed for launching Virtual Media. On Windows, the package may be included in the .NET framework package.**

Configuring Virtual Media

1 Log in to the iDRAC6 Web interface.

2 Select **System**→ **Console/Media** tab→ **Configuration**→ **Virtual Media** to configure the Virtual Media settings.

Table 14-2 describes the **Virtual Media** configuration values.

3 When you have finished configuring the settings, click **Apply**.

Table 14-2. Virtual Media Configuration Properties

Attribute	Value
Status	**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.

Table 14-2. Virtual Media Configuration Properties *(continued)*

Attribute	Value
Virtual Media Encryption Enabled	Select or deselect the checkbox to enable or disable encryption on **Virtual Media** connections. Selected enables encryption; deselected disables encryption.
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 cleared, it appears as a USB Key drive. **NOTE:** On certain Windows Vista and Red Hat environments, you may not be able to virtualize a USB with **Floppy Emulation** enabled.
Connection Status	**Connected** - A Virtual Media session is currently in progress. **Not connected** - A Virtual Media session is not in progress.
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, select the boot device from the the BIOS boot menu. This option automatically disconnects the **Virtual Media** devices after the system has booted once.

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" on page 46 for more information.

3 Select **System→ Console/Media→ Virtual Console and Virtual Media.**

4 The **Virtual Console and Virtual Media** page is displayed. If you want to change the values of any of the displayed attributes, see "Configuring Virtual Media" on page 255.

> **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.

5 Click **Launch Virtual Console**.

> **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 **iDRAC6 Virtual Console** application launches in a separate window.

6 Click **Virtual Media→ Launch Virtual Media**.

The **Virtual Media Session** wizard is displayed.

> **NOTE:** Do not close this wizard unless you want to terminate the Virtual Media session.

7 If media is connected, you must disconnect it before connecting a different media source. Clear the box to the left of the media you want to disconnect.

8 Select 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 Clear 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 **Virtual Media Session** wizard.

NOTE: Whenever a Virtual Media session is initiated or a vFlash is connected, an extra drive named "LCDRIVE" is displayed on the host operating system and the BIOS. The extra drive disappears when the vFlash or the Virtual Media session is disconnected.

Booting From Virtual Media

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

To change the BIOS setting, perform the following steps:

1 Boot the managed server.

2 Press <F2> to enter the BIOS setup window.

3 Scroll to the boot sequence and press <Enter>.

In the pop-up window, the virtual optical drives and virtual floppy drives are listed with the standard boot devices.

4 Ensure that the virtual drive is enabled and listed as the first device with bootable media. If required, follow the on-screen instructions to modify the boot order.

5 Save the changes and exit.

The managed server reboots.

The managed server attempts to boot from a bootable device based on the boot order. If the virtual device is connected and a bootable media is present, the system boots to the virtual device. Otherwise, the system overlooks the device—similar to a physical device without bootable media.

Installing Operating Systems Using Virtual Media

This section describes a manual, interactive method to install the operating system on your management station that may take several hours to complete. A scripted operating system installation procedure using **Virtual Media** may take less than 15 minutes to complete. See "Deploying the Operating System" on page 239 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" on page 259 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.

NOTE: You must have **Configure iDRAC6** privilege to use this feature.

NOTE: Remote devices must be redirected using Virtual Media to use this feature.

To use the Boot Once Feature, do the following:

1 Log in to the iDRAC6 through the Web interface and click **System→ Console/Media→ Configuration**.

2 Select the **Enable Boot Once** option under **Virtual Media**.

3 Power up the server and enter the BIOS Boot Manager.

4 Change the boot sequence to boot from the remote Virtual Media device.

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 14-3 lists frequently asked questions and answers.

Table 14-3.   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" on page 25 for a list of supported operating systems.
Which Web browsers support the iDRAC6?	See "Supported Web Browsers" on page 25 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 14-3. Using Virtual Media: Frequently Asked Questions *(continued)*

Question	Answer
An installation of the Windows operating system through Virtual Media 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 vFlash 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 14-3. 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 14-3. 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 14-3.   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 vFlash 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 vFlash USB device is connected to or disconnected from the host USB BUS, all the Virtual Media and vFlash 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 vFlash 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.
How do I get the maximum performance from Virtual Media?	To get the maximum performance from Virtual Media, launch the Virtual Media with the Virtual Console disabled or do one of the following: • Reduce the video resolution and color depth of the Virtual Console screen to minimum possible. • Disable encryption for both Virtual Media and Virtual Console. **NOTE:** In this case, the data transfer between managed server and iDRAC for Virtual Media and Virtual Console will not be secured. • If you are using any Windows server operating systems, stop the Windows service named Windows Event Collector. To do this, go to **Start > Administrative Tools > Services**. Right-click on **Windows Event Collector** and click **Stop**.

15

Configuring vFlash SD Card and Managing vFlash Partitions

The vFlash SD 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. It is the storage location for user-defined partition(s) that can be configured to be exposed to the system as a USB device and also used to create a bootable USB device. Depending on the emulation mode selected, the partitions will be exposed to the system as a floppy drive, and hard drive, or a CD/DVD drive. You can set any of these as a bootable device.

For information on how to install and remove the card from your system, see your system's *Hardware Owner's Manual* at **support.dell.com/manuals**.

The vFlash SD cards and standard SD cards are supported. A *vFlash SD card* refers to the card that supports the new enhanced vFlash features. A *standard SD card* refers to a normal off-the-shelf SD card that supports only limited vFlash features.

With vFlash SD card, you can create up to 16 partitions. You can provide a label name for the partition when you create it and can perform a range of operations to manage and use the partitions. A vFlash SD card can be of any size up to 8GB. Each partition size can be up to 4GB.

A standard SD card can be of any size but supports only one partition. The size of the partition is limited to 256MB. The label name for the partition is VFLASH by default.

> **NOTE:** Ensure that you only insert a vFlash SD card or standard SD card in the iDRAC6 Enterprise card slot. If you insert a card in any other format (example, Multi-Media Card (MMC)), the following error message is displayed when you initialize the card: *An error has occurred while initializing SD card.*

If you are an administrator, you can perform all operations on the vFlash partitions. If not, you must have Access Virtual Media privilege to create, delete, format, attach, detach, or copy the contents for the partition.

Configuring vFlash or Standard SD Card Using iDRAC6 Web Interface

After you install the vFlash or standard SD card, you can view its properties, enable or disable vFlash, and initialize the card. The vFlash functionality must be enabled to perform partition management. When the card is disabled, you can only view its properties. The initialize operation removes existing partitions and resets the card.

> **NOTE:** You must have Configure iDRAC permission to enable or disable vFlash, or to initialize the card.

If the card is not available in the system's iDRAC6 Enterprise card slot, the following error message is displayed.

```
SD card not detected. Please insert an SD card of size
256MB or greater.
```

To view and configure the vFlash or standard SD card:

1 Open a supported Web browser window and log in to the iDRAC6 Web interface.

2 In the system tree, select **System**.

3 Click the **vFlash** tab. The **SD Card Properties** page is displayed.

Table 15-1 lists the properties displayed for the SD card.

Table 15-1.   SD Card Properties

Attribute	Description
Name	Displays the name of the card inserted into the server's iDRAC6 Enterprise card slot. If the card supports the new enhanced vFlash features, it displays *vFlash SD Card*. If it supports limited vFlash features, it displays *SD Card*.
Size	Displays the size of the card in gigabytes (GB).
Available Space	Displays the unused space on the vFlash SD card in MB. This space is available to create more partitions on the vFlash SD card.
	If the inserted vFlash SD card is uninitialized, then the available space displays that the card is uninitialized.
	For the standard SD card, the available space is not displayed.
Write-protected	Displays whether the card is write-protected or not.
Health	Displays the overall health of the vFlash SD card. This can be:
	• OK
	• Warning
	• Critical
	If it is warning, re-initialize the card.
	If it is critical, reinstall and reinitialize the card.
	For the standard SD card, the health is not displayed.
vFlash Enabled	Select the checkbox to perform vFlash partition management on the card. Clear the checkbox to disable vFlash partition management.

4 Click **Apply** to enable or disable the vFlash partition management on the card.

If any vFlash partition is attached, you cannot disable vFlash and an error message is displayed.

NOTE: If vFlash is disabled, only the **SD Card Properties** subtab is displayed.

5 Click **Initialize**. All existing partitions are removed and the card is reset. A confirmation message is displayed.

6 Click **OK**. After initialize operation is complete, a successful message is displayed.

> ✍ **NOTE:** Initialize is enabled only if you select the **vFlash Enabled** option.

If any vFlash partition is attached, the initialize operation fails and an error message is displayed.

If you click any option on the vFlash pages when an application such as WSMAN provider, iDRAC6 Configuration Utility, or RACADM is using vFlash, or if you navigate to some other page in the GUI, iDRAC6 may display the following message

```
vFlash is currently in use by another process. Try
again after some time.
```

Configuring vFlash or Standard SD Card Using RACADM

You can view and configure the vFlash or standard SD card using RACADM commands from local, remote, or Telnet/SSH console.

> ✍ **NOTE:** You must have Configure iDRAC permission to enable or disable vFlash, and initialize the card.

Displaying the vFlash or Standard SD Card Properties

Open a telnet/SSH/Serial console to the server, log in, and enter the following command:

```
racadm getconfig -g cfgvFlashSD
```

The following read-only properties are displayed:

- `cfgvFlashSDSize`
- `cfgvFlashSDLicense`
- `cfgvFlashSDAvailableSize`
- `cfgvFlashSDHealth`

Enabling or Disabling the vFlash or Standard SD Card

Open a telnet/SSH/Serial console to the server, log in, and enter the following commands:

- To enable vFlash or standard SD card:

  ```
  racadm config -g cfgvFlashsd -o cfgvflashSDEnable
  1
  ```

- To disable vFlash or standard SD card:

  ```
  racadm config -g cfgvFlashsd -o cfgvflashSDEnable
  0
  ```

✐ **NOTE:** The RACADM command functions only if a vFlash or standard SD card is present. If a card is not present, the following message is displayed: *ERROR: SD Card not present*.

Initializing the vFlash or Standard SD Card

Open a telnet/SSH/Serial console to the server, log in, and enter the following command to initialize the card:

```
racadm  vflashsd  initialize
```

All existing partitions are deleted and the card is reset.

Getting the Last Status on the vFlash or Standard SD Card

Open a telnet/SSH/Serial console to the server, log in, and enter the following command to get the status of the last initialize command sent to the vFlash or standard SD card:

```
racadm vFlashsd status
```

✐ **NOTE:** This command only shows the status of commands sent to the SD card. To get the status of commands sent to individual partitions on the SD card use the command:
```
racadm vflashpartition status
```

Resetting the vFlash or Standard SD Card

Open a telnet/SSH/Serial console to the server, log in, and enter:

`racadm vflashsd initialize`

For more information about `vflashsd`, see the *RACADM Command Line Reference Guide for iDRAC6 and CMC* available on the Dell Support website at **support.dell.com/manuals**.

> **NOTE:** The `racadm vmkey reset` command is deprecated from 1.5 release onwards. The functionality of this command is now covered by `vflashsd initialize`. While execution of the `vmkey reset` command will be successful, it is recommended to use the `vflashsd initialize` command. For more information, see "Initializing the vFlash or Standard SD Card" on page 271.

Managing vFlash Partitions Using iDRAC6 Web Interface

You can perform the following:

- Create an empty partition
- Create a partition using an image file
- Format a partition
- View available partitions
- Modify a partition
- Attach/Detach a partition
- Delete existing partitions
- Download the contents of a partition
- Boot to a partition

Creating an Empty Partition

An empty partition is similar to an empty USB key. You can create empty partitions on a vFlash or standard SD card. You can choose to create partition of type *Floppy* or *Hard Disk*. The partition type CD is not supported for creating empty partitions.

> **NOTE:** You must have Access Virtual Media privilege to create empty partitions.

Before creating an empty partition, ensure the following:

- The card is initialized.
- The card is not write-protected.
- An initialize operation is not already being performed on the card.

To create an empty vFlash partition:

1 On the iDRAC6 Web interface, select **System**→ **vFlash** tab→ **Create Empty Partition** subtab. The **Create Empty Partition** page is displayed.

2 Enter the information mentioned in Table 15-2.

3 Click **Apply**. A new partition is created. A page indicating the progress percentage is displayed.

   An error message is displayed if:

   - The card is write-protected.
   - The label name matches the label of an existing partition.
   - A non-integer value is entered for the partition size, the value exceeds the available space on the card, or the partition size is greater than 4GB.
   - An initialize operation is already being performed on the card.

   ✎ **NOTE:** The new partition is unformatted (RAW).

Table 15-2.   Create Empty Partition Page Options

Field	Description
Index	Select a partition index. Only unused indices are displayed in the drop-down list. The lowest available index is selected by default. You can change it to any other index value from the drop-down list. **NOTE:** For the standard SD card, only index 1 is available.
Label	Enter a unique label for the new partition. The label name can contain up to six alphanumeric characters. Do not include any space in the label name. The characters are displayed in upper case. **NOTE:** For the standard SD card, the label name is VFLASH by default and you cannot modify this name.

Table 15-2. Create Empty Partition Page Options *(continued)*

Field	Description
Emulation Type	Select the emulation type for the partition from the drop-down list. The available options are **Floppy** and **Hard Disk**.
Size	Enter the partition size in megabytes (MB). The maximum partition size is 4GB, or less than or equal to the available space on the vFlash SD card. **NOTE:** For the standard SD card, the partition size is 256MB and cannot be changed.

Creating a Partition Using an Image File

You can create a new partition on the vFlash or standard SD card using an image file (available in the **.img** or **.iso** format.) You can create a partition of type Floppy, Hard Disk, or CD.

NOTE: You must have Access Virtual Media privileges to create partitions.

If a **.iso** image file (for CD) is used, a read-only partition is created. If a **.img** image file (for floppy and hard disk) is used, a read-write partition is created.

The size of the newly created partition is equal to the image file size. The image file size must be:

- Less than or equal to the available space on the card.
- Less than or equal to 4GB. The maximum partition size is 4GB.

Using the Web interface, the size of image that can be uploaded to the vFlash SD card is limited to a maximum of 2GB on both 32-bit and 64-bit browsers (Internet Explorer and FireFox).

Using the RACADM and WSMAN interface, the image size that can be uploaded to a vFlash SD card is a maximum of 4 GB.

For the standard SD card, the image size should be less than or equal to 256MB.

Before creating a partition from an image file, ensure the following:

- The card is initialized.
- The card is not write-protected.
- An initialize operation is not already being performed on the card.

> ![NOTE icon] **NOTE:** When creating partition from an image file, ensure that the image type and the emulation type match. iDRAC emulates the image as the image type specified. There may be issues when the uploaded image and the emulation type do not match. For example, if the partition is created using an ISO image and the emulation type is specified as Hard Disk, then the BIOS will not be able to boot from this image.

To create a vFlash partition using an image file:

1 On the iDRAC6 Web interface, select **System**→ **vFlash** tab→ **Create From Image** subtab. The **Create Partition from Image File** page is displayed.

2 Enter the information mentioned in Table 15-3.

3 Click **Apply**. A new partition is created.

   An error message is displayed if:

   - The card is write-protected.
   - The label name matches the label of an existing partition.
   - The size of the image file is greater than 4GB or exceeds the available space on the card.
   - The image file does not exist or the image file extension is neither **.img** nor **.iso**.
   - An initialize operation is already being performed on the card.

Table 15-3.   Create Partition from Image File Page Options

Field	Description
Index	Select a partition index. Only unused indices are displayed in the drop-down list. The lowest available index is selected by default. You can change it to any other index value from the drop-down list.
	NOTE: For the standard SD card, only index 1 is available.
Label	Enter a unique label for the new partition. This can contain up to six alphanumeric characters. Do not include spaces in the label name. The characters are displayed in upper case.
	NOTE: For the standard SD card, the label name is VFLASH and cannot be modified.
Emulation Type	Select the emulation type for the partition from the drop-down list. The available options are **Floppy**, **Hard Disk**, and **CD**.
Image Location	Click **Browse** and specify the image file location. Only **.img** or **.iso** file types are supported.

Formatting a Partition

You can format an existing partition on the vFlash SD card based on the type of file system. The supported file system types are EXT2, EXT3, FAT16, and FAT32. The standard SD card with limited vFlash features supports only the FAT32 format.

You can only format Hard Disk or Floppy partitions. Formatting partition of type CD is not supported. You cannot format read-only partitions.

NOTE: You must have Access Virtual Media privileges to format partitions.

Before formatting the partition, ensure the following:

- The card is enabled.
- The partition is not attached.
- The card is not write-protected.
- An initialize operation is not already being performed on the card.

To format vFlash partition:

1 On the iDRAC6 Web interface, select **System→ vFlash** tab→ **Format** subtab. The **Format Partition** page is displayed.

2 Enter the information mentioned in Table 15-4.

3 Click **Apply**. A warning message indicating that all the data on the partition will be erased is displayed. Click **OK**. The selected partition is formatted to the specified file system type.

An error message is displayed if:

• The card is write-protected.

• An initialize operation is already being performed on the card.

Table 15-4.   Format Partition Page Options

Field	Description
Label	Select the partition label that you want to format. The first available partition is selected by default.
	All existing partitions of type Floppy or Hard Disk are available in the drop-down list. Partitions that are attached or that are read-only are not available in the drop-down list.
Format Type	Select the file system type you want to format the partition to. The available options are EXT2, EXT3, FAT16, and FAT32.

Viewing Available Partitions

Ensure that the vFlash or standard SD card is enabled to view the list of available partitions.

To view the available partitions on the card:

1 On the iDRAC6 Web interface, select **System→ vFlash→ Manage** subtab. The **Manage Partitions** page lists the available partitions.

2 For each partition, you can view the information mentioned in Table 15-5.

Table 15-5. Viewing Available Partitions

Field	Description
Index	Partitions are indexed from 1 to 16. The partition index is unique for a particular partition. It is specified when the partition is created.
Label	Identifies the partition. It is specified when the partition is created.
Size	Size of the partition in megabytes (MB).
Read-Only	Read-write access state of the partition. • Checked = Read-only partition. • Unchecked=Read-write partition **NOTE:** For the standard SD card, the partition is read-write, and this column is not displayed.
Attached	Indicates whether the partition is visible to the operating system as a USB device. To attach or detach partitions, see the section "Attaching and Detaching Partition" on page 279.
Type	Displays whether the partition type is Floppy, Hard Disk or CD.
Status	Status of an ongoing or the last operation performed on the partition with the progress percentage. The status values are: • Idle - No operation is performed. • Formatting - Partition is being formatted. • Creating - Partition is being created.

Modifying a Partition

Ensure that the card is enabled to modify the partition.

You can change a read-only partition to read-write or vice-versa. To do this:

1 On the iDRAC6 Web interface, select **System**→ **vFlash** tab→ **Manage** subtab. The **Manage Partitions** page is displayed.

2 In the **Read-Only** column, select the checkbox for the partition(s) that you want to change to read-only or clear the checkbox for the partition(s) that you want to change to read-write.

> **NOTE:** If the partition is of type CD, the state is read-only and the checkbox is selected by default. You cannot change the state to read-write.
> If the partition is attached, the checkbox is grayed-out.
> For the standard SD card, the partition is read-write and the **Read-Only** column is not displayed.

3 Click **Apply**. The partitions are changed to read-only or read-write based on the selections.

Attaching and Detaching Partition

You can attach one or more partitions as a virtual USB mass storage device such that they are visible to the operating system and BIOS as mass storage devices. When multiple partitions are attached simultaneously, they are presented in ascending order to the host operating system based on the index. The corresponding drive letter assignment is controlled by the operating system.

If you detach a partition, it is no longer seen as a virtual USB mass storage device in the host operating system and it is removed from the BIOS boot order menu.

If you are attaching or detaching a partition, the USB bus of the system is reset. This may affect any applications (like the operating system) that are using vFlash and will disconnect the iDRAC Virtual Media sessions.

> **NOTE:** You must have Access Virtual Media privileges to attach or detach a partition.

Before attaching or detaching a partition, ensure the following:

• The card is enabled.

• An initialize operation is not already being performed on the card.

To attach or detach partitions:

1 On the iDRAC6 Web interface, select **System**→ **vFlash** tab→ **Manage** subtab. The **Manage Partitions** page is displayed.

2 In the **Attached** column, select the checkbox for the partition(s) that you want to attach or clear the checkbox for the partition(s) that you want to detach.

> **NOTE:** The detached partitions are not displayed in the boot sequence.

3 Click **Apply**. The partitions are attached or detached based on the selections.

Operating System Behavior for Attached Partitions

When partitions are attached and the host operating system is Windows, the drive letters that is assigned to the attached partitions are controlled by the operating system.

If a partition is read-only, it will read-only as seen in the host operating system.

If the host operating system does not support the file system of an attached partition, you cannot read or modify the contents of the partition from the host operating system. For example, partition type EXT2 cannot be read from Windows operating system.

When you change the label name of an attached partition from the host operating system, it does not impact the label name stored by iDRAC for that partition.

Deleting Existing Partitions

NOTE: You can delete existing partitions for the vFlash or standard SD card.

Before deleting existing partition(s), ensure the following:

- The card is enabled.
- The card is not write-protected.
- The partition is not attached.
- An initialize operation is not already being performed on the card.

To delete existing partition(s):

1 On the iDRAC6 Web interface, select **System**→ **vFlash** tab→ **Manage** subtab. The **Manage Partitions** page is displayed.

2 In the **Delete** column, click the delete icon for the partition(s) that you want to delete and click **Apply**. The partition(s) are deleted.

Downloading Partition Contents

You can download the contents of a vFlash partition to a local or remote location as an image file in the **.img** or **.iso** format. Local location is on your management system where iDRAC6 Web interface is operated from. Remote location is a network location mapped onto the management station.

> **NOTE:** You must have Access Virtual Media privileges to download partitions.

Before downloading the contents to a local or remote location, ensure the following:

- The card is enabled.
- An initialize operation is not already being performed on the card.
- For a read-write partition, it must not be attached.

To download the contents of the vFlash partition to a location on your system:

1 On the iDRAC6 Web interface, select **System**→ **vFlash** tab→ **Download** subtab. The **Download Partition** page is displayed.

2 From the **Label** drop-down menu, select a partition that you want to download. All existing partitions are displayed in the list except partitions that are attached. The first partition is selected by default.

3 Click **Download**.

4 Specify the location to save the file.

If only the folder location is specified, then the partition label is used as the file name, along with the extension **.iso** for CD type partitions and **.img** for floppy and hard-disk type partitions.

5 Click **Save**. The contents of the selected partition are downloaded to the specified location.

Booting to a Partition

You can set an attached vFlash partition as the boot device for the next boot operation. The vFlash partition must contain a bootable image (in the **.img** or **.iso** format) to set it as a boot device. Ensure that the card is enabled to set a partition as a boot device and to perform the boot operation.

> **NOTE:** You must have Access Virtual Media privileges to set a partition as the boot device.

You can perform the boot operation for the vFlash or standard SD card. For the steps, see the section "First Boot Device" on page 79.

> **NOTE:** If the system BIOS does not support vFlash as the first boot device, then the attached vFlash partition(s) may not be listed in the **First Boot Device** drop-down menu. Therefore, ensure that you update the BIOS to the latest version that supports setting the vFlash partition as the first boot device. If the BIOS is the latest version, then rebooting the server will cause the BIOS to inform iDRAC that it supports vFlash as the first boot device and iDRAC lists the vFlash partition in the **First Boot Device** drop-down menu.

Managing vFlash Partitions Using RACADM

You can use the `vFlashPartition` subcommand to create, delete, list, or view the status of partitions on an already initialized vFlash or standard SD card. The format is:

```
racadm vflashpartition <create | delete | status |
list> <options>
```

> **NOTE:** You must have Access Virtual Media privileges to perform vFlash partition management.

Valid Options:

-i <index>	Index of the partition for which this command applies. <index> must be an integer from 1 to 16.
	NOTE: For the standard SD card, index value is limited to 1 because only one partition of size 256MB is supported.

Options only valid with the create action:

-o <label>	Label that is shown when the partition is mounted on the operating system.
	<label> must be a string up to six alphanumeric characters and must not contain spaces.
-e <type>	Emulation type for the partition. <type> must be floppy, cddvd, or HDD.
-t <type>	Create a partition of type <type>. <type> must be:

- empty - Create an empty partition.
  - -s <size> - Partition size in MB.
  - -f <type>- Format type for the partition based on the type of file system. Valid options are RAW, FAT16, FAT32, EXT2, or EXT3.
- image - Create a partition using an image relative to the iDRAC. The following options are valid with the image type:
  - -l <path> - Specifies the remote path relative to the iDRAC. The path can be on a mounted drive:
    SMB path: //<ip or domain>/<share_name>/<path_to_image>
    NFS path: <ipaddress>:/<path_to_image>
  - -u <user> - Username for accessing the remote image.
  - -p <password> - Password for accessing the remote image.

Options only valid with the status action:

-a	Displays the status of operations on all existing partitions.

Creating a Partition

- To create a 20MB empty partition:

  ```
  racadm vflashpartition create -i 1 -o drive1 -t
  empty -e HDD -f fat16 -s 20
  ```

- To create a partition using an image file on a remote system:

  ```
  racadm vflashpartition create -i 1 -o drive1 -e
  HDD -t image -l //myserver/sharedfolder/foo.iso -u
  root -p mypassword
  ```

  📝 **NOTE:** This command is case sensitive for the image file name extension. If the file name extension is in upper case, for example FOO.ISO instead of FOO.iso, then the command returns a syntax error.

  📝 **NOTE:** Creating a partition using an image file is not supported in local RACADM.

Deleting a Partition

- To delete a partition:

  ```
  racadm vflashpartition delete -i 1
  ```

- To delete all partitions, re-initialize the vFlash SD card. For information, see "Initializing the vFlash or Standard SD Card" on page 271.

Getting the Status of a Partition

- To get the status of operation on partition 1:

  ```
  racadm vflashpartition status -i 1
  ```

- To get the status of all existing partitions:

  ```
  racadm vflashpartition status -a
  ```

Viewing Partition Information

To list all existing partitions and its properties:

```
racadm vflashpartition list
```

Booting to a Partition

- To list the available devices in the boot list:

```
racadm  getconfig –g cfgServerInfo –o
cfgServerFirstBootDevice
```

If it is a vFlash SD card, the label names of the attached partitions appears in the boot list. If it is a standard SD card and if the partition is attached, then VFLASH appears in the boot list.

- To set a vFlash partition as a boot device:

```
racadm  config –g cfgServerInfo –o
cfgServerFirstBootDevice "<vFlash partition name>"
```

where, <vFlash partition name> is the label name for vFlash SD card and VFLASH for the standard SD card.

> **NOTE:** When you run this command, the vFlash partition label is automatically set to boot once, that is, **cfgserverBootOnce** is set to 1. Boot once boots the device to the partition only once and does not keep it persistently first in the boot order.

Attaching or Detaching a Partition

- To attach a partition:

```
racadm config –g cfgvflashpartition  –i 1 –o
cfgvflashPartitionAttachState 1
```

- To detach a partition:

```
racadm config –g cfgvflashpartition  –i 1 –o
cfgvflashPartitionAttachState 0
```

Modifying a Partition

- To change a read-only partition to read-write:

```
racadm config -g cfgvflashpartition  -i 1 -o
cfgvflashPartitionAccessType 1
```

- To change a read-write partition to read-only:

```
racadm config -g cfgvflashpartition  -i 1 -o
cfgvflashPartitionAccessType 0
```

For more information about the RACADM subcommands and the iDRAC6 property database group and object definitions, see the *RACADM Command Line Reference Guide for iDRAC6 and CMC* available on the Dell Support website at **support.dell.com/manuals**.

Frequently Asked Questions

When is the vFlash or standard SD card locked?

The virtual flash media is locked by iDRAC when the operation it is performing needs exclusive access to the media. For example, during an initialize operation.

16

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**: The power supplies installed in the system are of the same type and they are functioning properly.

   – **Lost**: In systems with two power supply units, the power supplies installed in the system are of different types or one of them is malfunctioning or removed. In systems with four power supply units, the power supplies installed in the system are of different types, or two or three units are malfunctioning or removed.

   – **Disabled**: Only one of the power supplies is available. No redundancy exists.

   – **Degraded** (only in systems with four power supply units): Four power supply units are installed in the system but one of them is malfunctioning or removed.

   • **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.

– **Max 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 **Max Wattage** is different than **Input Wattage** because of the power supply efficiency. For example, if the efficiency of the power supply is 89% and **Max 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** 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.

System Minimum Power Consumption displays the default lowest power cap value.

System Maximum Power Consumption displays the default highest Power Cap value. This 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 in the *RACADM Command Line Reference Guide for iDRAC6 and CMC* available on the Dell Support website at **support.dell.com/manuals**.

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** 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** 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 Select **Enabled** to enable the threshold. The system enforces the user-specified threshold. If you clear the checkbox, 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 % >

racadm config –g cfgServerPower -o
cfgServerPowerCapEnable <1 to enable, 0 to disable>
```

 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 following section describes the information provided on the **Power Monitoring** page:

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.

- **Warning Threshold**: Displays the acceptable power consumption (in Watts and BTU/hr) recommended for system operation. Power consumption that exceeds this value results in warning events.
- **Failure Threshold**: Displays the highest acceptable power consumption (in Watts and BTU/hr) required for system operation. Power consumption that exceeds this value results in critical/failure events.

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

- **Energy Consumption** 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** button.
- **System Peak Power** specifies the maximum 1-minute average of power for the system since Measurement Start Time. You can reset this value with the **Reset** button.
- **System Peak Amperage** specifies the peak current value within the interval specified by the Start and Peak times. You can reset this value with the **Reset** button.
- **Measurement Start Time** displays the date and time recorded when the statistic was last cleared and the new measurement cycle began. For **Energy Consumption**, you can reset this value with the **Reset** button, but it will persist through a system reset or failover operation. For **System Peak Power** and **System Peak Amperage**, you can reset this value with the **Reset** button, but it will also persist through a system reset or failover operation.

- **Measurement Finish Time** displays the current date and time when the system energy consumption was calculated for display. **Peak Time** displays the time when the 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 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 Power 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

Click **Show Graph** to display 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.

Using RACADM

Open a Telnet/SSH text console to the iDRAC, log in, and type:

`racadm getconfig –g cfgServerPower`

For more information about **cfgServerPower**, including output details, see **cfgServerPower** in the *RACADM Command Line Reference Guide for iDRAC6 and CMC* available on the Dell Support website at **support.dell.com/manuals**.

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** 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.

   📝 **NOTE:** Ensure that the shutdown option is configured for the operating system before you perform a graceful shutdown using this option. If you use this option without configuring it on the operating system, it reboots the managed system instead of performing a shutdown operation.

- **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.

17

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 and configure the Provisioning Server
- 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 and remote 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, Virtual Console, 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:

```
iDRAC6 Out-of-Band IPMI interface will be disabled if
IPMI Over LAN is OFF.
```

Press any key to clear the message and continue. See "iDRAC6 LAN" on page 301 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 17-1. 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 Priority	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.

Table 17-1. LAN Parameters (continued)

Item	Description
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.
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**.

Table 17-1.   LAN Parameters *(continued)*

Item	Description
Default Gateway	If the **IP Address Source** is set to **DHCP**, this field displays the IP address of the default gateway obtained from DHCP.
	If the **IP Address Source** is set to **Static**, enter the IP address of the default gateway. The default is **192.168.0.1**.
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.

Table 17-1. 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 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 **Virtual Console** sessions.

If you select **Detached,** users cannot access Virtual Media devices during **Virtual Console** 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.

vFlash

Press <Enter> to select **Enabled** or **Disabled**.

- **Enabled** - vFlash is available for partition management.
- **Disabled** - vFlash is not available for partition management.

⚠ **CAUTION: vFlash cannot be disabled if one or more partitions are in-use or is attached.**

Initialize vFlash

Choose this option to initialize the vFlash card. Initialize operation erases existing data on the SD card and all existing partitions are removed. You cannot perform initialize operation if one or more partitions are in use or attached. This option is accessible only if a card of size greater than 256 MB is present in the iDRAC Enterprise card slot and if vFlash is enabled.

Press <Enter> to initialize the vFlash SD card.

The initialize operation mail fail due to the following reasons:

- SD card is currently not present.
- vFlash is currently in use by another process.
- vFlash is not enabled.
- SD card is write-protected.
- One or more partitions are currently in-use.
- One or more partitions are currently attached.

vFlash Properties

Press <Enter> to view the following vFlash SD card properties:

- **Name** - Displays the name of the vFlash SD card inserted into the server's vFlash SD card slot. If it is a Dell SD card, it displays vFlash SD Card. If it is a non-Dell SD card, it displays SD Card.
- **Size** - Displays the vFlash SD card size in gigabytes (GB).
- **Available Space** - Displays the unused space on the vFlash SD card in megabytes (MB). This space is available to create more partitions on the vFlash SD card. For SD cards, the available space is displayed as 256MB.

- **Write Protected** - Displays whether the vFlash SD card is write-protected or not.
- **Health** - Displays the overall health of the vFlash SD card. This can be:
  - OK
  - Warning
  - Critical

Press <Esc> to exit.

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** or **Enabled with RACADM, 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.

NOTE: If you choose to restore to factory defaults, the settings for System Services does not change.

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.

Collect System Inventory on Restart

Select **Enabled** to allow the collection of inventory during boot. 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 restarts the server after you have saved your settings and exited from the iDRAC6 Configuration Utility.

NOTE: If you choose to restore to factory defaults, the settings for Collect System Inventory on Restart does not change.

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 17-2.   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	View or enter the string to be displayed on the LCD. The string can be maximum of 62 characters long.
LCD System Power Units	Select **Watt** or **BTU/hr** to specify the Unit to be displayed on the LCD.
LCD Ambient Temp Units	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 Virtual Console Indication	Select **Enabled** to display the text *Virtual Console* whenever a Virtual Console is active on the unit.
LCD Front Panel Access	Press <Right Arrow>, <Left Arrow >, and spacebar to switch between the options: **Disabled, View And 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.

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.

Any of the following error messages is displayed if this operation fails:

- Reset command was not successful. Please try later- iDRAC is busy.
- Failed to restore settings to default values - Timeout.
- Not able to send Reset command. Please try later- iDRAC is busy.

Table 17-3.   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 17-3.   LAN User Configuration *(continued)*

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.
Provisioning Server	This field is used to configure the provisioning server. The provisioning server address can be a combination of IPv4 addresses or hostname and should not exceed 255 characters. Each address should be separated by a comma.
	If the auto-discovery feature is enabled, and after the auto-discovery process completes successfully, user credentials are retrieved from the configured provisioning server to allow future remote provisioning.
	For more information, see the *Dell Lifecycle Controller User Guide* available on the Dell Support website at **support.dell.com/manuals**.
Account Access	Select **Enabled** to enable the administrator account. Select **Disabled** to disable the administrator account or when Auto-Discovery is enabled.
Account Privilege	Select between **Admin**, **User**, **Operator**, and **No Access**.
Account User Name	Press <Enter> to edit the user name and press <Esc> when you have finished. The default user name is **root**.
Enter Password	Type the new password for the administrator account. The characters are not echoed on the display as you type them.
Confirm Password	Retype the new password for the administrator account. If the characters you enter do not match the characters you entered in the **Enter Password** field, a message is displayed and you must re-enter the password.

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. If this operation fails, one of the following message is displayed:
  - iDRAC6 Communication Failure — Displayed if iDRAC is not accessible.
  - Some of the settings cannot be applied — Displayed when few settings cannot be applied.
- 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.

18

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:

1 Fan Critical Assert Filter

2 Battery Warning Assert Filter

3 Battery Critical Assert Filter

4 Voltage Critical Assert Filter

5 Temperature Warning Assert Filter

6 Temperature Critical Assert Filter

7 Intrusion Critical Assert Filter

8 Redundancy Degraded Filter

9 Redundancy Lost Filter

10 Processor Warning Assert Filter

11 Processor Critical Assert Filter

12 Processor Absent Critical Assert Filter

13 Power Supply Warning Assert Filter

14 Power Supply Critical Assert Filter

15 Power Supply Absent Critical Assert Filter

16 Event Log Critical Assert Filter

17 Watchdog Critical Assert Filter

18 System Power Warning Assert Filter

19 System Power Critical Assert Filter

20 Removable Flash Media Absent Informational Assert Filter

21 Removable Flash Media Critical Assert Filter

22 Removable Flash Media Warning 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 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)" on page 57.

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 22. 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)" on page 58.

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" on page 59.

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" on page 318 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. To configure these settings, see testtrap and testemail subcommand descriptions in the *RACADM Command Line Reference Guide for iDRAC6 and CMC* available on the Dell Support website at **support.dell.com/manuals**.

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.

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 **iDRAC Settings**→ **Network/Security**→ **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.

19

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" on page 323.
- "Managing Power on a Remote System" on page 324.
- "Using the POST Boot Logs" on page 334.
- "Viewing the Last System Crash Screen" on page 335.

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" on page 335), and use Virtual Console and remote power management (see "Managing Power on a Remote System" on page 324) 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" on page 296.

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 allows you to view your system's health and other basic iDRAC6 information at a glance and provides you with links to access the system health and information pages. Also, you can quickly launch common tasks from this page and view recent events logged in the System Event Log (SEL).

To access the **System Summary** page, click **System**→ **Properties**→ **System Summary** tab. For more information, see the *iDRAC6 Online Help*.

The **System Details** page displays information about the following system components:

- Main System Chassis
- Remote Access Controller

To access the **System Details** page, expand the **System** tree and click the **Properties**→ **System Details** tab.

Main System Chassis

📝 **NOTE:** To receive **Host Name** and **OS Name** information, you must have iDRAC6 services installed on the managed system.

Table 19-1.   System Information

Field	Description
Description	System description.
BIOS Version	System BIOS version.
Service Tag	System Service Tag number.
Express Service Code	Service code of the system.
Host Name	Host system's name.
OS Name	Operating system running on the system.
OS Version	Version of operating system running on the system.
System Revision	System revision number.
Lifecycle Controller Firmware	Version of the Lifecycle Controller Firmware.

Table 19-2.   Auto Recovery

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.

Table 19-2. Auto Recovery *(continued)*

Field	Description
Present Countdown	The current value, in seconds, of the countdown timer.

Table 19-3. Embedded NIC MAC Addresses

Field	Description
Virtual MAC	Displays Virtual Media Access Control (MAC) addresses.
	Virtual MAC data is obtained from hardware inventory, hence the hardware Inventory needs to be collected once before viewing the vMAC data.
	Click **System Inventory**. The Inventory data is updated and displayed on the **System Inventory** page. Click **System Details** again. The Virtual MACs for each of the Embedded LAN Ports is now displayed on the **System Details** page.
	NOTE: The vMAC feature will be used by Dell Advanced Infrastructure Manager (AIM) in the future releases. If Dell AIM does not manage the server currently, then the Ethernet MAC address and the Virtual MAC address are identical.
NIC 1	Displays the Ethernet, Internet Small Computer System Interface (iSCSI), and the Virtual MAC address(es) of the embedded Network Interface Controller (NIC) 1.
	Ethernet NICs support the wired Ethernet standard and plug into the system bus of the server.
	iSCSI NIC is a network interface controller with the iSCSI stack running on the host computer.
	MAC addresses uniquely identify each node in a network at the Media Access Control layer.
NIC 2	Displays the Ethernet, iSCSI and the Virtual MAC address(es) of the embedded Network Interface Controller NIC 2 that uniquely identifies it in the network.
NIC 3	Displays the Ethernet, iSCSI and the Virtual MAC address(es) of the embedded Network Interface Controller NIC 3 that uniquely identifies it in the network.

Table 19-3. Embedded NIC MAC Addresses *(continued)*

Field	Description
Virtual MAC	Displays Virtual Media Access Control (MAC) addresses.
	Virtual MAC data is obtained from hardware inventory, hence the hardware Inventory needs to be collected once before viewing the vMAC data.
	Click **System Inventory**. The Inventory data is updated and displayed on the **System Inventory** page. Click **System Details** again. The Virtual MACs for each of the Embedded LAN Ports is now displayed on the **System Details** page.
	NOTE: The vMAC feature will be used by Dell Advanced Infrastructure Manager (AIM) in the future releases. If Dell AIM does not manage the server currently, then the Ethernet MAC address and the Virtual MAC address are identical.
NIC 4	Displays the Ethernet, iSCSI and the Virtual MAC address(es) of the embedded Network Interface Controller NIC 4 that uniquely identifies it in the network.

Remote Access Controller

Table 19-4. RAC Information

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
	Example: Fri Jan 28 16:27:29 2011
Firmware Version	iDRAC6 firmware version
Firmware Updated	Date the firmware was last flashed in the form:
	Day Month DD HH:MM:SS YYYY
	Example: Sat Jan 29 2011 13:31:50
Hardware Version	Remote Access Controller version

Table 19-4. RAC Information *(continued)*

Field	Description
MAC Address	The Media Access Control (MAC) address that uniquely identifies each node in a network

Table 19-5. IPv4 Information

Field	Description
IPv4 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.
Use DHCP to obtain DNS server addresses	**Yes** or **No**. Indicates if you want to use DHCP to obtain DNS server addresses.
Preferred DNS Server	Indicates the static IPv4 address of the preferred DNS server.
Alternate DNS Server	Indicates the static IPv4 address of the alternate DNS server.

Table 19-6. IPv6 Information Fields

Field	Description
IPv6 Enabled	Indicates whether IPv6 stack is enabled.
IP Address 1	Specifies the IPv6 address/prefix length for the iDRAC6 NIC. The *prefix length* is combined with the IP Address 1. This is an integer specifying the prefix length of the IPv6 address. It can be a value between 1 and 128.
IP Gateway	Specifies the gateway for the iDRAC6 NIC.
Link Local Address	Specifies the iDRAC6 NIC Link Local IPv6 address.

Table 19-6.   IPv6 Information Fields *(continued)*

Field	Description
IP Address 2...15	Specifies the additional IPv6 addresses for the iDRAC6 NIC, if available.
AutoConfig Enabled	**Yes** or **No.** AutoConfig lets the Server Administrator obtain the IPv6 address for the iDRAC NIC from the Dynamic Host Configuration Protocol (DHCPv6) server.
Use DHCPv6 to obtain DNS server Addresses	**Yes** or **No**. Indicates if you want to use DHCPv6 to obtain DNS server addresses.
Preferred DNS Server	Indicates the static IPv6 address of the preferred DNS server.
Alternate DNS Server	Indicates the static IPv6 address of the alternate DNS server.

System Inventory

The **System Inventory** page displays information about the hardware and firmware components installed on the system.

To access the **System Inventory** page, expand the **System** tree and click **Properties**→ **System Inventory**.

Hardware Inventory

This section displays information about the Hardware components currently present on system. If the Hardware Inventory data is not available when you click the **System Inventory** tab, the following message is displayed:

```
Hardware Inventory is unavailable.
```

Refresh the page to see the details.

Firmware Inventory:

This section displays firmware versions of the Dell components installed. If Firmware inventory data is not available when you click the **System Inventory** tab, the following message is displayed:

```
Hardware Inventory is unavailable.
```

Refresh the page to see the details.

After new hardware addition or removal to the system, the **System Inventory** page may not update the changes automatically. This is because inventory data collected during manufacturing process may not be updated with new changes.

To solve this, during BIOS POST select the **Cntl+E** option and enable **Collect system Inventory** on reboot. Save and exit from the **Cntl+E** option.

The system reboots to collect new system inventory. After inventory collection is completed, the **System Inventory** page displays correct hardware and software inventory data.

For more information, see the *iDRAC6 Online Help*.

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 19-7.

3   Click the appropriate **System Event Log** page button to continue. For more information see the iDRAC6 Online Help.

4   Click **Clear Log** to clear the SEL.

    ✎ **NOTE:** The Clear Log button is displayed only if you have Clear Logs permission.

5   Click **Save As** to save the SEL to a directory of your choice.

Table 19-7.   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 <day> <mon> dd yyyy hh:mm:ss, based on a 24-hour clock.
Description	A brief description of the event.

Enabling/Disabling OEM Event Logs

The OEM event logs are displayed on the **System Event Log** page automatically. The **Advanced Settings** button on the **Systems→ Logs** tab allows you to enable/disable the OEM event messages from the managed system from appearing on the **System Event Log** page.

To disable the OEM Event Logs from appearing on the **System Event Log** Page, select the **OEM SEL Event Filter Enabled** option.

NOTE: The the **OEM SEL Event Filter Enabled** option is not selected by default.

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: For more information on the options you can use, see getsel subcommand in the *RACADM Command Line Reference Guide for iDRAC6 and CMC* available on the Dell Support website at **support.dell.com/manuals**.

The **clrsel** command removes all existing records from the SEL.

`racadm clrsel`

Using the Work Notes

Work notes are notes or comments that a user can add. Any iDRAC user can add a work note. Work notes cannot be deleted. You can view as many as 1000 work notes at a time. For quick reference, the latest ten work notes are displayed on the iDRAC Home page.

NOTE: If number of work notes added are more than 800, the GUI page may take few extra seconds to load the page. This is due to relatively huge amount of data that gets transacted between GUI and iDRAC6.The newly added work notes may not be displayed after the page is loaded. To resolve this, click **Refresh**.

The **Work Notes** page enables you to enter work notes into the Lifecycle Log. The time stamp for the note is recorded automatically.

To access the **Work Notes** page, expand the **System** tree and click **Systems→ Logs→ Work Notes**.

The **Work Notes** page displays enables you to enter work notes and provides other information as shown in Table 19-8.

To enter the work notes:

1   In the **Work Notes** page, under the **Add Work Notes** section, enter the work note in the field displayed.

   📝 **NOTE:** A maximum of 50 alphanumeric characters is supported for the work note.

2   Click **Save**.

   The new work note is displayed in the work notes table below the **Add Work Notes** section.

T
Table 19-8.   Work Notes

Field	Description
Date/Time	Displays the time stamp recorded for each work note entry. The format is yyyy-mm-ddThh:mm:ssZ, based on a 24-hour clock, where, yyyy : Year mm : Month dd : Day T : Time hh : Hour mm : Minute ss : Seconds Z : The Time zone designator. **NOTE:** If the time is in UTC, add a **Z** directly after the time without a space. **Z** is the zone designator for the zero UTC offset. **09:30** UTC is therefore represented as **09:30Z** or **0930Z**. **14:45:15** UTC would be **14:45:15Z** or **144515Z**.
Notes	Displays the work note entry contents.

Using the POST Boot Logs

NOTE: All logs are cleared after you reboot the iDRAC6.

The **Boot Capture** page provides access to recordings of up to the last three available boot cycles. They are arranged in the order of latest to oldest. If the server has experienced no boot cycles then **No Recording Available** is displayed. Click **Play** after selecting an available boot cycle to display it in a new window.

NOTE: Viewing Boot Capture is supported only on Java and not Active-X.

To view the Boot Capture logs:

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

2   Click the **Logs** tab and then click the **Boot Capture** tab.

3   Select a boot cycle and click **Play**.

    The video of the logs is opened on a new screen.

    NOTE: You must close an open Boot Capture log video before you play another one. You cannot play two logs simultaneously.

4   Click **Playback**→ **Play** to start the Boot Capture log video.

5   Click **Playback**→ **Media Controls** 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*.

NOTE: If iDRAC is reset, the boot capture video is not available since it is stored in RAM and is deleted when iDRAC resets.

The iDRAC6 Express Card is bonded to 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 **Network/Security** tab in the **iDRAC Settings** section to enable this feature.

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 displays the most recent crash screen. The last system crash information is saved in iDRAC6 memory and is remotely accessible.

 For more information on the buttons displayed on the **Last Crash Screen** page see the *iDRAC6 Online Help*.

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" on page 313 for additional information.

20

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
- Diagnostics Console
- Identify Server
- 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 **iDRAC Settings**.

2 Click the **Logs** tab and then click **iDRAC Log**.

The **iDRAC Log** page displays the information listed in Table 20-1.

Table 20-1. iDRAC 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.

📝 **NOTE:** For information on using the **iDRAC Log Page** buttons see the *iDRAC6 Online Help*.

Using the Command Line

Use the `getraclog` command to view the iDRAC6 log entries.

`racadm getraclog [options]`

`racadm getraclog –i`

The **getraclog -i** command displays the number of entries in the iDRAC6 log.

📝 **NOTE:** For more information, see getraclog in the *RACADM Command Line Reference Guide for iDRAC6 and CMC* available on the Dell Support website at **support.dell.com/manuals**.

You can use the `clrraclog` command to clear all entries from the iDRAC log.

`racadm clrraclog`

Using the Diagnostics Console

The iDRAC6 provides a standard set of network diagnostic tools (see Table 20-2) 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.

Click **Reset iDRAC6** to reset the iDRAC. A normal boot operation is performed on the iDRAC.

To access the **Diagnostics Console** page:

1 In the **System** tree, click **iDRAC Settings**→ **Troubleshooting** tab→ **Diagnostics Console**.

2 Type a command and click **Submit**. Table 20-2 describes the commands that can be used. The debugging results appear in the **Diagnostics Console** page.

3 To refresh the **Diagnostics Console** page, click **Refresh**. To execute another command, click **Go Back to the Diagnostics Page**.

Table 20-2.   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. For more information, see gettracelog in the *RACADM Command Line Reference Guide for iDRAC6 and CMC* available on the Dell Support website at **support.dell.com/manuals**.

Using Identify Server

The **Identify** page allows you to enable the system identification feature.

To identify the server:

1 Click **System**→ **iDRAC Settings**→ **Troubleshooting**→ **Identify.**

2 On the **Identify** screen, select the **Identify Server** checkbox to enable blinking of the LCD and the rear identify server LED.

3 The **Identify Server Timeout** field displays the number of seconds the LCD blinks. Enter the amount of time (in seconds) that you want the LCD to blink. Timeout range is 1 to 255 seconds. If the timeout is set to 0 seconds, the LCD blinks continuously.

4 Click **Apply.**

If you entered **0** seconds, follow these steps to disable it:

1 Click **System**→ **iDRAC Settings**→ **Troubleshooting**→ **Identify**.

2 On the **Identify** screen, deselect the **Identify Server** option click **Apply.**

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 **iDRAC Settings**.

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. For more information, see gettracelog in the *RACADM Command Line Reference Guide for iDRAC6 and CMC* available on the Dell Support website at **support.dell.com/manuals**.

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,SSH and remote racadm interfaces. For more information, see the racdump command in the *RACADM Command Line Reference Guide for iDRAC6 and CMC* available on the Dell Support website at **support.dell.com/manuals**.

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. For more information, see the `coredump` and `coredumpdelete` subcommands in the *RACADM Command Line Reference Guide for iDRAC6 and CMC* available on the Dell Support website at **support.dell.com/manuals**.

21

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.

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**.

Removable Flash Media Probes

The Removable Flash Media sensor provides information about the vFlash SD card status (active or absent). For more information about the vFlash SD card, see "Configuring vFlash SD Card and Managing vFlash Partitions" on page 267.

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.

22

Configuring Security Features

The iDRAC6 provides the following security features:

- Advanced Security options for the iDRAC6 administrator:
  - The Virtual Console disable option allows the *local* system user to disable Virtual Console using the iDRAC6 Virtual Console 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)

  📝 **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 **iDRAC Settings→ Network/Security→ 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 using Web-based interface.

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, you must upgrade BIOS. Upgrade 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. It is recommended that you use these features with discretion. 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 Virtual Console

Administrators can selectively disable the iDRAC6 remote Virtual Console, providing a flexible, secure mechanism for a local user to work on the system without someone else viewing the user's actions through Virtual Console. Using this feature requires installing the iDRAC managed node software on the server. Administrators can disable Virtual Console using the following command:

```
racadm LocalConRedirDisable 1
```

The command LocalConRedirDisable disables existing Virtual Console 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 Virtual Console. They can do so by using the argument 0:

```
racadm LocalConRedirDisable 0
```

Several situations might call for disabling iDRAC6 Virtual Console. 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 Virtual Console during the system POST by using the `LocalConRedirDisable` command. They may also want to increase security by automatically disabling Virtual Console every time an administrator logs in to the system, which they can do by executing the `LocalConRedirDisable` command from the user logon scripts.

![NOTE icon] **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)" on page 349
- "Certificate Signing Request (CSR)" on page 350
- "Accessing the SSL Main Menu" on page 351
- "Generating a Certificate Signing Request" on page 351

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:

1 Replace the default Web server SSL certificate with a valid certificate from a Certificate Authority(CA).

2 Generate a Certificate Signing Request(CSR) by submitting a request to the iDRAC6.

3 Provide the CSR to the Certificate Authority(CA) to get a valid certificate.

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 **iDRAC Settings**.

2 Click the **Network/Security** tab and then click **SSL**.

Use the **SSL Main Menu** (see Table 22-1) to generate a CSR, upload an existing server certificate, or view an existing server certificate. The CSR information is stored on the iDRAC6 firmware. For information on the buttons available on the **SSL** page, see the *iDRAC6 Online Help*.

Table 22-1.   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.

Generating a Certificate Signing Request

NOTE: Each CSR overwrites any previous CSR on the firmware. Before iDRAC can accept a signed certificate, 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 22-2 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. For more information on the buttons available on the **Generate Certificate Signing Request (CSR)** page see the *iDRAC6 Online Help*.

Table 22-2.   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, **xyzcompany.com**). Alphanumeric characters, hyphens and periods are valid.
Organization Name	The name associated with this organization (for example, XYZ Corporation). Alphanumeric characters, hyphens and periods are valid.
Organization Unit	The name associated with an organizational unit, such as a department (for example, Enterprise Group). Alphanumeric characters, hyphens and periods are valid.
Locality	The city or other location of the entity being certified (for example, Round Rock). Alphanumeric characters, hyphens and periods are valid.
State Name	The state or province where the entity who is applying for a certification is located (for example, Texas). Alphanumeric characters, hyphens and periods are valid.
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.

Viewing a Server Certificate

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

Table 22-3 describes the fields and associated descriptions listed in the **Certificate** window.

2 Click the appropriate **View Server Certificate** page button to continue.

Table 22-3. 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

Using the Secure Shell (SSH)

For information about using SSH, see "Using the Secure Shell (SSH)" on page 89.

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 **iDRAC Settings**.

2 Click the **Network/Security** tab and then click **Services**.

3 Configure the following services as required:

- Local Configuration (Table 22-4)
- Web server (Table 22-5)
- SSH (Table 22-6)
- Telnet (Table 22-7)
- Remote RACADM (Table 22-8)

- SNMP agent (Table 22-9)
- Automated System Recovery Agent (Table 22-10)

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** to apply the Services page settings.

Table 22-4. 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 22-5. 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.

Table 22-5. Web Server Settings (continued)

Setting	Description
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 22-6. SSH Settings

Setting	Description
Enabled	Enables or disable SSH. When selected, 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 22-7. 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 22-8. 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 22-9. SNMP Agent Settings

Setting	Description
Enabled	Enables or disables the SNMP agent. Checked=Enabled; Unchecked=Disabled.
Community Name	Define the SNMP community string to be used. The Community Name can be up to 31 non-blank characters in length. The default setting is **public**.

Table 22-10. Automated System Recovery Agent Setting

Setting	Description
Enabled	Enables the Automated System Recovery Agent.

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 the *RACADM Command Line Reference Guide for iDRAC6 and CMC* available on the Dell Support website at **support.dell.com/manuals** for a complete list of **cfgRacTuning** properties.

Table 22-11. 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.

Table 22-11.   IP Address Filtering (IpRange) Properties *(continued)*

Property	Description
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

See the following example command for IP filtering setup.

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 in the following sectio:

```
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 in the following section:

```
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 the *RACADM Command Line Reference Guide for iDRAC6 and CMC* available on the Dell Support website at **support.dell.com/manuals** for a complete list of **cfgRacTuning** properties.

Table 22-12 lists the user-defined parameters.

Table 22-12.   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 **iDRAC Settings**.

2 Click the **Network/Security** 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 22-13 describes the **Network Security** page settings.

5 Click the appropriate **Network Security** page button to continue. For more information on the **Network Security** page buttons, see the *iDRAC6 Online Help*.

Table 22-13.   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.

Table 22-13. Network Security Page Settings *(continued)*

Settings	Description
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.

Index