Dell Chassis Management Controller Firmware Version 4.2 User’s Guide

Notes, Cautions, and Warnings

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

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

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

2012 - 10

Rev. A00

Contents

1

Overview

The Dell Chassis Management Controller (CMC) is a systems management hardware and software solution for managing multiple Dell blade chassis. It is a hot-pluggable module that sits at the back of Dell PowerEdge M1000e chassis. The CMC has its own microprocessor and memory and is powered by the modular chassis into which it is plugged.

The CMC enables an IT administrator to:

- View inventory
- Perform configuration and monitoring tasks
- Remotely power on or off blades
- Enable alerts for events on servers and components in the blade chassis

You can configure the M1000e chassis either with a single CMC, or with redundant CMCs. In redundant CMC configurations, if the primary CMC loses communication with the M1000e chassis or the management network, the standby CMC takes over chassis management.

The CMC provides multiple systems management functions for blade servers. Power and thermal management are the primary functions of the CMC.

- Enclosure-level real-time automatic power and thermal management.
  - CMC monitors system power requirements and supports the optional Dynamic Power Supply Engagement mode. This enables CMC to enable or set power supplies in standby, dynamically depending on load and redundancy requirements to improve power efficiency.
  - CMC reports real-time power consumption, which includes logging high and low points with a time stamp.
  - CMC supports setting an optional enclosure Maximum Power Limit, which either alerts or takes actions, such as throttling server modules and/or preventing the power up of new blades to keep the enclosure under the defined maximum power limit.
  - CMC monitors and automatically controls cooling of fans based on actual ambient and internal temperature measurements.
  - CMC provides comprehensive enclosure inventory and status/error reporting.
- CMC provides a mechanism for centralized configuration of the following:
  - The M1000e enclosure’s network and security settings
  - Power redundancy and power ceiling settings
  - I/O switches and iDRAC network settings
  - First boot device on the server blades
  - Checks I/O fabric consistency between the I/O modules and blades and disables components, if necessary, to protect the system hardware
  - User access security

You can configure CMC to send e-mail alerts or SNMP trap alerts for warnings or errors related to temperatures, hardware misconfigurations, power outages, and fan speeds.

New In This Release

This release of CMC supports the following features:

- Dell PowerEdge M IO Aggregator support.
- Support for Microsoft Internet Explorer v.10.
- Dell EqualLogic PS-M4110 Blade Array support.

Key Features

The CMC features are grouped into management and security features.

Management Features

The CMC provides the following management features:

- Redundant CMC Environment.
- Dynamic Domain Name System (DDNS) registration for IPv4 and IPv6.
- Remote system management and monitoring using SNMP, a Web interface, iKVM, Telnet or SSH connection.
- Monitoring — Provides access to system information and status of components.
- Access to system event logs — Provides access to the hardware log and CMC log.
- Firmware updates for various chassis components — Enables you to update the firmware for CMC, servers, iKVM, and I/O module infrastructure devices.
- Firmware update of server components such as BIOS, Network Controllers, Storage Controllers, and so on across multiple servers in the chassis using Lifecycle Controller.
- Dell OpenManage software integration — Enables you to launch the CMC Web interface from Dell OpenManage Server Administrator or IT Assistant.
- CMC alert — Alerts you about potential managed node issues through an e-mail message or SNMP trap.
- Remote power management — Provides remote power management functions, such as shutdown and reset on any chassis component, from a management console.
- Power usage reporting.
- Secure Sockets Layer (SSL) encryption — Provides secure remote system management through the Web interface.
- Launch point for the Integrated Dell Remote Access Controller (iDRAC) Web interface.
- Support for WS-Management.
- FlexAddress feature — Replaces the factory-assigned World Wide Name/Media Access Control (WWN/MAC) IDs with chassis-assigned WWN/MAC IDs for a particular slot, an optional upgrade.
- Graphical display of chassis component status and health.
- Support for single and multi-slot servers.
- LCD iDRAC configuration wizard supports iDRAC network configuration.
- iDRAC single sign-on.
- Network time protocol (NTP) support.
- Enhanced server summary, power reporting, and power control pages.
- Forced CMC failover, and virtual reseat of servers.
- Multi-chassis management, allows up to 8 other chassis to be visible from the lead chassis.

Security Features

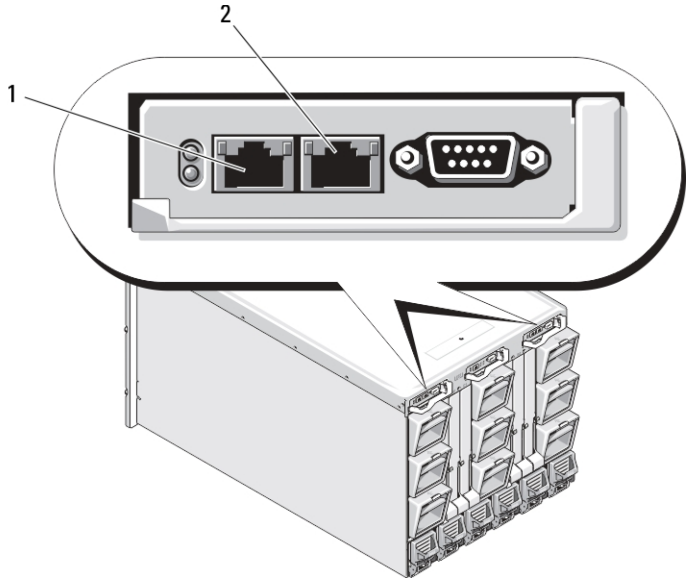
The CMC provides the following security features:

- Password-level security management — Prevents unauthorized access to a remote system.
- Centralized User authentication through:
  - Active Directory using Standard Schema or an Extended Schema(optional.)
  - Hardware-stored user IDs and passwords.
- Role-based authority — Enables an administrator to configure specific privileges for each user.
- User ID and password configuration through the Web interface.
- Web interface supports 128-bit SSL 3.0 encryption and 40-bit SSL 3.0 encryption (for countries where 128-bit is not acceptable).

  NOTE: Telnet does not support SSL encryption.
- Configurable IP ports (if applicable).
- Login failure limits per IP address, with login blocking from the IP address when the limit is exceeded.
- Configurable session auto time out, and more than one simultaneous sessions.
- Limited IP address range for clients connecting to the CMC.
- Secure Shell (SSH), which uses an encrypted layer for higher security.
- Single Sign-on, Two-Factor Authentication, and Public Key Authentication.

Chassis Overview

The following figure shows the facing edge of a CMC (inset) and the locations of the CMC slots in the chassis.



1	GB Port
2	STK Port

CMC Port Information

The following TCP/IP ports are required to remotely access CMC through firewalls. These are the ports CMC listens to for connections.

Table 1. CMC Server Listening Ports

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

* Configurable port

The following table lists the ports that CMC uses as a client.

Table 2. CMC Client Port

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

* Configurable port

Supported Remote Access Connections

The following table lists the supported Remote Access Controllers.

Table 3. Supported Remote Access Connections

Connection	Features
CMC Network Interface ports	• GB port: Dedicated network interface for the CMC Web interface. Two 10/100/1000 Mbps ports; one for management and the other for chassis to chassis cable consolidation • STK: Uplink port for chassis to chassis management network cable consolidation • 10Mbps/100Mbps/1Gbps Ethernet through CMC GbE port • DHCP support • SNMP traps and e-mail event notification

Connection	Features
	• Network interface for the iDRAC and I/O Modules (IOMs) • Support for Telnet/SSH command console and RACADM CLI commands including system boot, reset, power-on, and shutdown commands
Serial port	• Support for serial console and RACADM CLI commands including system boot, reset, power-on, and shutdown commands • Support for binary interchange for applications specifically designed to communicate with a binary protocol to a particular type of IOM • Serial port can be connected internally to the serial console of a server, or I/O module, using the connect (or racadm connect) command
Other connections	• Access to the Dell CMC Console through the Avocent Integrated KVM Switch Module (iKVM)

Supported Platforms

The CMC supports modular systems designed for the M1000e platform. For information about compatibility with the CMC, see the documentation for your device.

For the latest supported platforms, see the *Dell Systems Software Support Matrix* located at **support.dell.com/manuals**.

Supported Web Browsers

For the latest information on supported Web browsers, see the *Dell Systems Software Support Matrix* located at **support.dell.com/manuals**.

Viewing Localized Versions of the CMC Web Interface

To view localized versions of the CMC Web interface:

1. Open the Windows **Control Panel**.
2. Double-click the **Regional Options** icon.
3. Select the required locale from the **Your locale (location)** drop-down menu.

Supported Management Console Applications

The CMC supports integration with Dell OpenManage IT Assistant. For more information, see the IT Assistant documentation set available on the Dell Support Web site at **support.dell.com/manuals**.

Other Documents You May Need

In addition to this guide, you can access the following guides available at **support.dell.com/manuals**. On the Manuals page, click **Software** → **Systems Management** . Click on the appropriate product link on the right-side to access the documents:

- The *CMC Online Help* provides information about using the Web interface.
- The *Chassis Management Controller (CMC) Secure Digital (SD) Card Technical Specification* provides minimum BIOS and firmware version, installation and usage information.

- The *Integrated Dell Remote Access Controller 7(iDRAC7) User's Guide* provides information about installation, configuration and maintenance of the iDRAC on managed systems.
- The *Dell OpenManage IT Assistant User's Guide* provides information about IT Assistant.
- Documentation specific to your third-party management console application.
- The *Dell OpenManage Server Administrator's User's Guide* provides information about installing and using Server Administrator.
- The *Dell Update Packages User's Guide* provides information about obtaining and using Dell Update Packages as part of your system update strategy.

The following system documents provide more information about the system in which CMC is installed:

- The safety instructions that came with your system provide important safety and regulatory information. For additional regulatory information, see the Regulatory Compliance home page at **www.dell.com/regulatory_compliance**. Warranty information may be included within this document or as a separate document.
- The *Rack Installation Guide* and *Rack Installation Instructions* included with your rack solution describe how to install your system into a rack.
- 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.
- Documentation for any components you purchased separately provides information to configure and install these options.
- 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.
- For more information on IOM network settings, refer to the *Dell PowerConnect M6220 Switch Important Information* document and the *Dell PowerConnect 6220 Series Port Aggregator White Paper*.

Updates are sometimes included with the system to describe changes to the system, software, and/or documentation.

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

2

Installing and Setting Up CMC

This section provides information about how to install your CMC hardware, establish access to CMC, configure your management environment to use CMC, and guides you through the next steps for configuring the CMC:

- Set up initial access to CMC.
- Access CMC through a network.
- Add and configure CMC users.
- Update CMC firmware.

For more information about installing and setting up redundant CMC environments, see Understanding Redundant CMC Environment.

Before You Begin

Before setting up your CMC environment, download the latest version of CMC firmware from the Dell Support website at **support.dell.com**.

Also, make sure that you have the *Dell Systems Management Tools and Documentation* DVD that was included with your system.

Installing CMC Hardware

CMC is pre-installed on your chassis and hence no installation is required. You can install a second CMC to run as a standby to the active CMC.

Related Links

Understanding Redundant CMC Environment

Checklist To Set up Chassis

The following steps enable you to setup the chassis accurately:

1. CMC and the management station where you use your browser must be on the same network, which is called the management network. Connect an Ethernet network cable from CMC port labelled **GB** to the management network.

   NOTE: Do not place a cable in CMC Ethernet port labelled **STK**. For more information to cable the STK port, see Understanding Redundant CMC Environment.

2. Install the IO modules in the chassis and cable them.
3. Insert the servers in the chassis.
4. Connect the chassis to the power source.
5. Push the power button at the lower left corner of the chassis or power on the chassis from the CMC Web interface after completing step 7.

   NOTE: Do not power on the servers.

6. Using the LCD panel on the front of the system, provide CMC with a static IP address or configure it for DHCP.
7. Connect to the CMC IP address through the Web browser using the default username (root) and password (calvin).

8. Provide each iDRAC with an IP address in the CMC Web interface and enable the LAN and IPMI interface.

   NOTE: iDRAC LAN interface on some servers are disabled by default.

9. Provide each IO module with an IP address in the CMC Web interface.
10. Connect to each iDRAC through the Web browser and provide final configuration of iDRAC. Default user name is *root* and password is *calvin*.
11. Connect to each IO module through the Web browser and provide final configuration of the IO module.
12. Power on the servers and install the operating system.

Basic CMC Network Connection

For the highest degree of redundancy, connect each available CMC to your management network.

Each CMC has two RJ-45 Ethernet ports, labeled **GB** (the uplink port) and **STK** (the stacking or cable consolidation port). With basic cabling, you connect the GB port to the management network and leave the STK port unused.

CAUTION: Connecting the STK port to the management network can have unpredictable results. Cabling GB and STK to the same network (broadcast domain) can cause a broadcast storm.

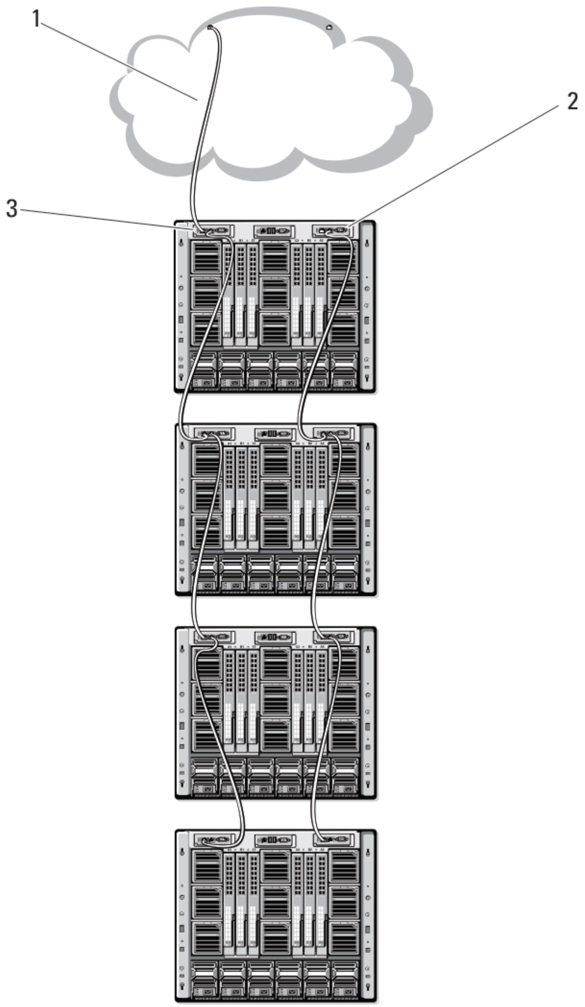
Daisy chain CMC Network Connection

If you have multiple chassis in a rack, you can reduce the number of connections to the management network by daisy-chaining up to four chassis together. If each of the four chassis contains a redundant CMC, by daisy-chaining you can reduce the number of management network connections required from eight to two. If each chassis has only one CMC, you can reduce the connections required from four to one.

When daisy-chaining chassis together, GB is the uplink port and STK is the stacking (cable consolidation) port. Connect the GB ports to the management network or to the STK port of CMC in a chassis that is closer to the network. You must connect the STK port only to a GB port further from the chain or network.

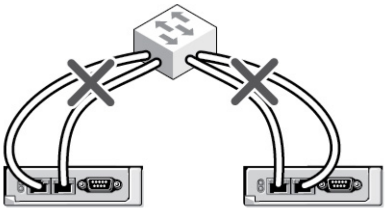
Create separate chains for CMCs in the active CMC slot and the second CMC slot.

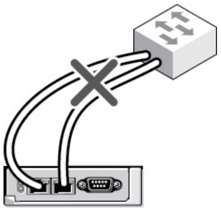
The following figure illustrates the arrangement of cables for four daisy-chained chassis, each with active and standby CMCs.

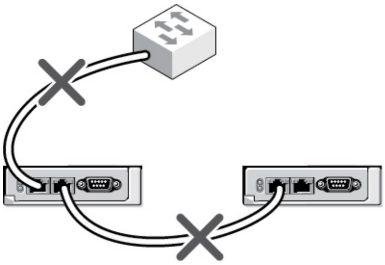


1	Management Network
2	Standby CMC
3	Active CMC

The following figures provide examples of incorrect cabling of CMC.







To daisy-chain up to four chassis:

1. Connect the GB port of the active CMC in the first chassis to the management network.
2. Connect the GB port of the active CMC in the second chassis to the STK port of the active CMC in the first chassis.
3. If you have a third chassis, connect the GB port of its active CMC to the STK port of the active CMC in the second chassis.
4. If you have a fourth chassis, connect the GB port of its active CMC to the STK port of the third chassis.
5. If you have redundant CMCs in the chassis, connect them using the same pattern.

   CAUTION: The STK port on any CMC must never be connected to the management network. It can only be connected to the GB port on another chassis. Connecting a STK port to the management network can disrupt the network and cause a loss of data. Cabling GB and STK to the same network (broadcast domain) can cause a broadcast storm.

   NOTE: Do not connect an active CMC to a standby CMC.

   NOTE: Resetting a CMC whose STK port is chained to another CMC can disrupt the network for CMCs that appear later in the chain. The child CMCs may log messages indicating that the network link has been lost and they may fail over to their redundant CMCs.

6. To get started with CMC, see Installing Remote Access Software on a Management Station.

Installing Remote Access Software on a Management Station

You can access CMC from a management station using remote access software, such as the Telnet, Secure Shell (SSH), or serial console utilities provided on your operating system or using the Web interface.

To use remote RACADM from your management station, install remote RACADM using the *Dell Systems Management Tools and Documentation* DVD that is available with your system. This DVD includes the following Dell OpenManage components:

- DVD root — Contains the Dell Systems Build and Update Utility.
- SYSMGMT — Contains the systems management software products including Dell OpenManage Server Administrator.
- Docs — Contains documentation for systems, systems management software products, peripherals, and RAID controllers.
- SERVICE — Contains the tools required to configure your system, and delivers the latest diagnostics and Dell-optimized drivers for your system.

For information about installing Dell OpenManage software components, see the *Dell OpenManage Installation and Security User's Guide* available on the DVD or at **support.dell.com/manuals**. You can also download the latest version of the Dell DRAC Tools from **support.dell.com**.

Installing RACADM on a Linux Management Station

1. Log in as root to the system running a supported Red Hat Enterprise Linux or SUSE Linux Enterprise Server operating system where you want to install the managed system components.
2. Insert the *Dell Systems Management Tools and Documentation DVD* into the DVD drive.
3. To mount the DVD to a required location, use the mount command or a similar command.

   NOTE: On the Red Hat Enterprise Linux 5 operating system, DVDs are auto-mounted with the `-noexec mount` option. This option does not allow you to run any executable from the DVD. You need to mount the DVD-ROM manually and then run the executables.
4. Navigate to the **SYSMGMT/ManagementStation/linux/rac** directory. To install the RAC software, type the following command:

   ```
   rpm -ivh *.rpm
   ```
5. For help on the RACADM command, type `racadm help` after you run the previous commands. For more information about RACADM, see *RACADM Command Line Reference Guide for iDRAC7 and CMC*.

   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>`

Uninstalling RACADM From a Linux Management Station

1. Log on as root to the system where you want to uninstall the management station features.
2. Use the following rpm query command to determine which version of the DRAC Tools is installed:

   ```
   rpm -qa | grep mgmtst-racadm
   ```
3. Verify the package version to be uninstalled and uninstall the feature by using the rpm `-e `rpm -qa | grep mgmtst-racadm` command.

Configuring Web Browser

You can configure and manage CMC, servers, and modules installed in the chassis through a Web browser. See the *Supported Browsers* section in the *Dell Systems Software Support Matrix* at **support.dell.com/manuals**.

The CMC and the management station where you use your browser must be on the same network, which is called the *management network*. Depending on your security requirements, the management network can be an isolated, highly secure network.

NOTE: Make sure that the security measures on the management network, such as firewalls and proxy servers, do not prevent your Web browser from accessing CMC.

Some browser features can interfere with connectivity or performance, especially if the management network does not have a route to the Internet. If your management station is running a Windows operating system, some Internet Explorer settings can interfere with connectivity even though you use a command line interface to access the management network.

Related Links

Proxy Server
Microsoft Phishing Filter
Certificate Revocation List (CRL) Fetching
Downloading Files From CMC With Internet Explorer
Allow Animations in Internet Explorer

Proxy Server

To browse through a proxy server that does not have access to the management network, you can add the management network addresses to the browser’s exception list. This instructs the browser to bypass the proxy server while accessing the management network.

Internet Explorer

To edit the exception list in Internet Explorer:

1. Start Internet Explorer.
2. Click **Tools** → **Internet Options** → **Connections** .
3. In the **Local Area Network (LAN) settings** section, click **LAN Settings**.
4. In the **Proxy server** section, click **Advanced**.
5. In the **Exceptions** section, add the addresses for CMCs and iDRACs on the management network to the semicolon-separated list. You can use DNS names and wildcards in your entries.

Mozilla FireFox

To edit the exception list in Mozilla Firefox version 3.0:

1. Start Mozilla Firefox.
2. Click **Tools** → **Options** (for Windows) or click **Edit** → **Preferences** (for Linux).
3. Click **Advanced** and then click the **Network** tab.
4. Click **Settings**.
5. Select the **Manual Proxy Configuration**.
6. In the **No Proxy for** field, type the addresses for CMCs and iDRACs on the management network to the comma-separated list. You can use DNS names and wildcards in your entries.

Microsoft Phishing Filter

If the Microsoft Phishing Filter is enabled in Internet Explorer 7 on your management system, and your CMC does not have Internet access, accessing CMC may be delayed by a few seconds. This delay can happen if you are using the browser or another interface such as remote RACADM. Follow these steps to disable the phishing filter:

1. Start Internet Explorer.
2. Click **Tools** → **Phishing Filter**, and then click **Phishing Filter** Settings.
3. Select the Disable Phishing Filter check box and click **OK**.

Certificate Revocation List (CRL) Fetching

If your CMC has no route to the Internet, disable the certificate revocation list (CRL) fetching feature in Internet Explorer. This feature tests whether a server such as the CMC Web server uses a certificate that is on a list of revoked certificates retrieved from the Internet. If the Internet is inaccessible, this feature can cause delays of several seconds when you access the CMC using the browser or with a command line interface such as remote RACADM.

To disable CRL fetching:

1. Start Internet Explorer.
2. Click **Tools** → **Internet Options**, and then click **Advanced**.

3. Scroll to the Security section, clear the **Check for publisher's certificate revocation** checkbox, and click **OK**.

Downloading Files From CMC With Internet Explorer

When you use Internet Explorer to download files from CMC you may experience problems when the **Do not save encrypted pages to disk** option is not enabled.

To enable the **Do not save encrypted pages** to disk option:

1. Start Internet Explorer.
2. Click **Tools** → **Internet Options** , then click **Advanced**.
3. Scroll to the Security section and select **Do not save encrypted pages to disk**.

Allow Animations in Internet Explorer

When transferring files to and from the Web interface, a file transfer icon spins to show transfer activity. For Internet Explorer, this requires that the browser be configured to play animations, which is the default setting.

To configure Internet Explorer to play animations:

1. Start Internet Explorer.
2. Click **Tools** → **Internet Options**, then click **Advanced**.
3. Scroll to the Multimedia section and check **Play animations in web pages**.

Setting Up Initial Access to CMC

To manage CMC remotely, connect CMC to your management network and then configure CMC network settings.

NOTE: To manage the M1000e solution, it must be connected to your management network.

For information to configure CMC network settings, see Configuring Initial CMC Network. This initial configuration assigns the TCP/IP networking parameters that enable access to CMC.

CMC and iDRAC on each server and the network management ports for all switch I/O Modules are connected to a common internal network in the M1000e chassis. This allows the management network to be isolated from the server data network. It is important to separate this traffic for uninterrupted access to chassis management.

CMC is connected to the management network. All external access to CMC and iDRACs is accomplished through CMC. Access to the managed servers, conversely, is accomplished through network connections to I/O modules (IOMs). This allows the application network to be isolated from the management network.

It is recommended to isolate chassis management from the data network. Dell cannot support or guarantee uptime of a chassis that is improperly integrated into your environment. Due to the potential of traffic on the data network, the management interfaces on the internal management network can be saturated by traffic intended for servers. This results in CMC and iDRAC communication delays. These delays may cause unpredictable chassis behavior, such as CMC displaying iDRAC as offline even when it is up and running, which in turn causes other unwanted behavior. If physically isolating the management network is impractical, the other option is to separate CMC and iDRAC traffic to a separate VLAN. CMC and individual iDRAC network interfaces can be configured to use a VLAN.

If you have one chassis, connect CMC and the standby CMC to the management network. If you have a redundant CMC, use another network cable and connect the **GB** CMC port to a second port of the management network.

If you have more than one chassis you can choose between the basic connection, where each CMC is connected to the management network, or a daisy-chained chassis connection, where the chassis are connected in series and only one CMC is connected to the management network. The basic connection type uses more ports on the management network and provides greater redundancy. The daisy-chain connection type uses fewer ports on the management network but introduces dependencies between CMCs, reducing the redundancy of the system.

NOTE: Failure to cable CMC properly in a redundant configuration can cause loss of management and create broadcast storms.

Related Links

Basic CMC Network Connection
Daisy chain CMC Network Connection
Configuring Initial CMC Network

Configuring Initial CMC Network

NOTE: Changing your CMC Network settings may disconnect your current network connection.

You can perform the initial network configuration of CMC before or after CMC has an IP address. If you configure CMC's initial network settings before you have an IP address, you can use either of the following interfaces:

- The LCD panel on the front of the chassis
- Dell CMC serial console

If you configure initial network settings after the CMC has an IP address, you can use any of the following interfaces:

- Command line interfaces (CLIs) such as a serial console, Telnet, SSH, or the Dell CMC Console through iKVM
- Remote RACADM
- CMC Web interface

The CMC supports both IPv4 and IPv6 addressing modes. The configuration settings for IPv4 and IPv6 are independent of one another.

Configuring CMC Network Using LCD Panel Interface

NOTE: The option to configure CMC using the LCD panel is available only until CMC is deployed or the default password is changed. If the password is not changed, the LCD can continue to be used to reconfigure the CMC causing a possible security risk.

The LCD panel is located on the bottom left corner on the front of the chassis.

To set up a network using the LCD panel interface:

1. Press the chassis power button to turn it on.

   The LCD screen displays a series of initialization screens as it powers up. When it is ready, the **Language Setup** screen is displayed.

2. Select the language using the arrow buttons, press the center button to select the **Accept/Yes**, and press the center button again.

   The **Enclosure** screen displays the following question: **Configure Enclosure**?

   – Press the center button to continue to CMC **Network Settings** screen. See step 4.
   – To exit the **Configure Enclosure** menu, select the NO icon and press the center button. See step 9.

3. Press the center button to continue to CMC **Network Settings** screen.

4. Select the network speed (10Mbps, 100Mbps, Auto (1 Gbps)) using the down arrow button.

   The Network Speed setting must match your network configuration for effective network throughput. Setting the Network Speed lower than the speed of your network configuration increases bandwidth consumption and slows network communication. **Determine whether your network supports the above network speeds and set it**

accordingly. If the network configuration does not match any of these values, it is recommended to use Auto Negotiation (the **Auto** option) or refer to your network equipment manufacturer.

Press the center button to continue to the next **CMC Network Settings** screen.

5. Select the duplex mode (half or full) that matches the network environment.

   NOTE: The network speed and duplex mode settings are not available if Auto Negotiation is set to On or 1000MB (1Gbps) is selected.

   If auto negotiation is turned on for one device but not the other, then the device using auto negotiation can determine the network speed of the other device, but not the duplex mode; in this case, duplex mode defaults to the half duplex setting during auto negotiation. Such a duplex mismatch results in a slow network connection.

   Press the center button to continue to the next **CMC Network Settings** screen.

6. Select the Internet Protocol (IPv4, IPv6, or both) that you want to use for CMC and press the center button to continue to the next **CMC Network Settings** screen.
7. Select the mode in which CMC must obtain the NIC IP addresses:

   Dynamic Host Configuration Protocol (DHCP)
   CMC retrieves IP configuration (IP address, mask, and gateway) automatically from a DHCP server on your network. CMC is assigned a unique IP address allotted over your network. If you have selected the DHCP option, press the center button. The **Configure iDRAC7** screen appears; go to step 9.

   Static
   You manually enter the IP address, gateway, and subnet mask in the screens immediately following.

   If you have selected the Static option, press the center button to continue to the next **CMC Network Settings** screen, then:

   – Set the **Static IP Address** by using the right or left arrow keys to move between positions, and the up and down arrow keys to select a number for each position. When you have finished setting the **Static IP Address**, press the center button to continue.
   – Set the subnet mask, and then press the center button.
   – Set the gateway, and then press the center button. The **Network Summary** screen displays.

     The **Network Summary** screen lists the **Static IP Address**, **Subnet Mask**, and **Gateway** settings you entered. Check the settings for accuracy. To correct a setting, navigate to the left arrow button then press the center key to return to the screen for that setting. After making a correction, press the center button.
   – When you have confirmed the accuracy of the settings you entered, press the center button. The **Register DNS?** screen appears.

     NOTE: If the Dynamic Host Configuration Protocol (DHCP) mode is selected for CMC IP configuration, then DNS registration is also enabled by default.

8. If you selected **DHCP** in the previous step, go to step 10.

   To register your DNS server's IP address, press the center button to proceed. If you have no DNS, press the right arrow key. The **Register DNS?** screen appears; go to step 10.

   Set the **DNS IP Address** using the right or left arrow keys to move between positions, and the up and down arrow keys to select a number for each position. When you have finished setting the DNS IP address, press the center button to continue.

9. Indicate whether you want to configure iDRAC:

   – **No**: Skip to step 13.
   – **Yes**: Press the center button to proceed.

   You can also configure iDRAC from the CMC GUI.

10. Select the Internet Protocol (IPv4, IPv6, or both) that you want to use for the servers.

    Dynamic Host Configuration Protocol (DHCP)
    iDRAC retrieves IP configuration (IP address, mask, and gateway) automatically from a DHCP server on your network. The iDRAC is assigned a unique IP address allotted over your network.Press the center button.

    Static
    You manually enter the IP address, gateway, and subnet mask in the screens immediately following.

    If you have selected the Static option, press the center button to continue to the next **iDRAC Network Settings** screen, then:

    - Set the **Static IP Address** by using the right or left arrow keys to move between positions, and the up and down arrow keys to select a number for each position. This address is the static IP of the iDRAC located in the first slot. The static IP address of each subsequent iDRAC is calculated as a slot number increment of this IP address. When you have finished setting the **Static IP Address**, press the center button to continue.
    - Set the subnet mask, and then press the center button.
    - Set the gateway, and then press the center button.

    - Select whether to **Enable** or **Disable** the IPMI LAN channel. Press the center button to continue.
    - On the **iDRAC Configuration** screen, to apply all iDRAC network settings to the installed servers, highlight the **Accept/Yes** icon and press the center button. To not apply the iDRAC network settings to the installed servers, highlight the **No** icon and press the center button and continue to step c.
    - On the next **iDRAC Configuration** screen, to apply all iDRAC network settings to newly installed servers, highlight the Accept/Yes icon and press the center button; when a new server is inserted into the chassis, the LCD prompts the user on whether to automatically deploy the server using the previously configured network settings/policies. To not apply the iDRAC network settings to newly installed servers, highlight the **No** icon and press the center button; when a new server is inserted into the chassis, the iDRAC network settings do not get configured.
11. On the **Enclosure** screen, to apply all enclosure settings highlight the **Accept/Yes** icon and press the center button. To not apply the enclosure settings, highlight the **No** icon and press the center button.
12. On the **IP Summary** screen, review the IP addresses you provided to make sure the addresses are accurate. To correct a setting, navigate to the left arrow button and then press the center key to return to the screen for that setting. After making a correction, press the center button. If necessary, navigate to the right arrow button and then press the center key to return to the **IP Summary** screen.

    When you have confirmed that the settings you entered are accurate, press the center button. The Configuration Wizard closes and returns you to the **Main Menu** screen.

    NOTE: If you selected **Yes/Accept**, a **Wait** screen is displayed before the **IP Summary** screen is displayed.

    CMC and iDRACs are now available on the network. You can access the CMC on the assigned IP address using the Web interface or CLIs such as a serial console, Telnet, and SSH.

    NOTE: After you have completed network setup through the LCD Configuration Wizard, the Wizard is no longer available.

Interfaces and Protocols to Access CMC

After you have configured CMC network settings, you can remotely access CMC using various interfaces. The following table lists the interfaces that you can use to remotely access CMC.

NOTE: Since telnet is not as secure as the other interfaces, it is disabled by default. Enable Telnet using Web, ssh, or remote RACADM.

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

Table 4. CMC Interfaces

Interface	Description
Web interface	Provides remote access to CMC using a graphical user interface. The Web interface is built into the CMC firmware and is accessed through the NIC interface from a supported Web browser on the management station. For a list of supported Web browsers, see the Supported Browsers section in the *Dell System Software Support Matrix* at **support.dell.com/manuals**.
Remote RACADM command line interface	Use this command line utility to manage CMC and its components. You can use remote or firmware RACADM: • Remote RACADM is a client utility that runs on a management station. It uses the out-of-band network interface to run RACADM commands on the managed system and uses the HTTPs channel. The `-r` option runs the RACADM command over a network. • Firmware RACADM is accessible by logging in to CMC using SSH or telnet. You can run the firmware RACADM commands without specifying the CMC IP, user name, or password. After you enter the RACADM prompt, you can directly run the commands without the racadm prefix.
Chassis LCD Panel	Use the LCD on the front panel to: • View alerts, CMC IP or MAC address, user programmable strings. • Set DHCP • Configure CMC static IP settings. To reset CMC without rebooting the server, press and hold the System Identification ⓘ button for 16 seconds.
Telnet	Provides command line access to CMC through the network. The RACADM command line interface and the connect command, which is used to connect to the serial console of a server or IO module, are available from the CMC command line. **NOTE:** Telnet is not a secure protocol and is disabled by default. Telnet transmits all data, including passwords in plain text. When transmitting sensitive information, use the SSH interface.
SSH	Use SSH to run RACADM commands. It provides the same capabilities as the Telnet console using an encrypted transport layer for higher security. The SSH service is enabled by default on CMC and can be disabled.
WS-MAN	The LC-Remote Services is based on the WS-Management protocol to do one-to-many systems management tasks. You must use WS-MAN client such as WinRM client (Windows) or the OpenWSMAN client (Linux) to use the LC-Remote Services functionality. You can also use Power Shell and Python to script to the WS-MAN interface. Web Services for Management (WS-Management) is a Simple Object Access Protocol (SOAP)–based protocol used for systems management. CMC uses WS–Management to convey Distributed Management Task Force (DMTF) Common Information Model (CIM)–based management information. The CIM information

Interface	Description
	defines the semantics and information types that can be modified in a managed system. The CMC WS-MAN implementation uses SSL on port 443 for transport security, and supports basic authentication. The data available through WS-Management is provided by CMC instrumentation interface mapped to the DMTF profiles and extension profiles. For more information, see the following: • MOFs and Profiles — **delltechcenter.com/page/DCIM.Library** • DTMF Web site — **dmtf.org/standards/profiles/** • WS-MAN release notes or Read Me file. • **www.wbemsolutions.com/ws_management.html** • DMTF WS-Management Specifications: **www.dmtf.org/standards/wbem/wsman** 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 client connection using Microsoft WinRM, the minimum required version is 2.0. For more information, refer to the Microsoft article, <**support.microsoft.com/kb/968929**>.

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

Launching CMC Using Other Systems Management Tools

You can also launch CMC from the Dell Server Administrator or Dell OpenManage IT Assistant.

To access CMC interface using Dell Server Administrator, launch Server Administrator on your management station. 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 the *Dell Server Administrator User's Guide*.

Downloading and Updating CMC Firmware

To download the CMC firmware, see Downloading CMC Firmware.

To update the CMC firmware, see Updating CMC Firmware.

Setting Chassis Physical Location and Chassis Name

You can set the chassis location in a data center and the chassis name to identify the chassis on the network (the default name is **Dell Rack System**.) For example, an SNMP query on the chassis name returns the name you configure.

Setting Chassis Physical Location and Chassis Name Using Web Interface

To set the chassis location and chassis name using the CMC Web interface:

1. In the system tree, go to **Chassis Overview**, and then click **Setup** → **General** .

   The **General Chassis Settings** page is displayed.
2. Type the location properties and the chassis name. For more information, see the *CMC Online Help*.

NOTE: The Chassis Location field is optional. It is recommended to use the **Data Center**, **Aisle**, **Rack**, and **Rack Slot** fields to indicate the physical location of the chassis.

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

Setting Chassis Physical Location and Chassis Name Using RACADM

To set the chassis name or location, date and time using the command line interface, see the **setsysinfo** and **setchassisname** commands. For more information, see *RACADM Command Line Reference Guide for iDRAC7 and CMC*.

Setting Date and Time on CMC

You can set the date and time manually, or you can synchronize the date and time with a Network Time Protocol (NTP) server.

Setting Date and Time on CMC Using CMC Web Interface

To set the date and time on CMC using the CMC Web interface:

1. In the system tree, go to Chassis Overview, and then click **Setup** → **Date/Time** .
   The **Date/Time** page is displayed.
2. To synchronize the date and time with a Network Time Protocol (NTP) server, select **Enable NTP** and specify up to three NTP servers.
3. To set the date and time manually, clear **Enable NTP** and edit the **Date** and **Time** fields, select the **Time Zone** from the drop-down menu, and then click **Apply**.

Setting Date and Time on CMC Using RACADM

To set the date and time using the command line interface, see the config command and `cfgRemoteHosts` database property group sections in the *RACADM Command Line Reference Guide for iDRAC7 and CMC*.

Configuring LEDs to Identify Components on the Chassis

You can set component LEDs for all or individual components (chassis, servers, and IOMs) to blink as a means of identifying the component on the chassis.

NOTE: To modify these settings, you must have **Chassis Configuration Administrator** privilege.

Configuring LED Blinking Using CMC Web Interface

To enable blinking for one, multiple, or all component LEDs using the CMC Web interface:

1. Go to any of the following pages:
   - **Chassis Overview** → **Troubleshooting** → **Identify** .
   - **Chassis Overview** → **Chassis Controller** → **Troubleshooting** → **Identify**.
   - **Chassis Overview** → **Server Overview** → **Troubleshooting** → **Identify**.

     NOTE: Only servers can be selected on this page.
   - **Chassis Overview** → **I/O Module Overview** → **Troubleshooting** → **Identify**.

The **Identify** page is displayed.

2. To enable blinking for a component LED, select required component and click **Blink**.
3. To disable blinking for a component LED, clear the required component and click **UnBlink**.

Configuring LED Blinking Using RACADM

Open a serial/Telnet/SSH text console to CMC, log in, and type:

```
racadm setled -m <module> [-l <ledState>]
```

where `<module>` specifies the module whose LED you want to configure. Configuration options:

- `server-nx` where *n* = 1-8 and *x* = a, b, c, or d
- `switch-n` where *n*=1–6
- `cmc-active`

and `<ledState>` specifies whether the LED should blink. Configuration options:

- 0 — not blinking (default)
- 1 — blinking

Configuring CMC Properties

You can configure CMC properties such as power budgeting, network settings, users, and SNMP and e-mail alerts using the Web interface or RACADM.

Understanding Redundant CMC Environment

You can install a standby CMC that takes over if your active CMC fails. The redundant CMC may be pre-installed or can be installed later. It is important that CMC network is properly cabled to ensure full redundancy or best performance.

Failovers can occur when you:

- Run the RACADM **cmcchangeover** command. (See the **cmcchangeover** command section in the *RACADM Command Line Reference Guide for iDRAC7 and CMC)*.
- Run the RACADM racreset command on the active CMC. (See the **racreset** command section in the *RACADM Command Line Reference Guide for iDRAC6 and CMC)*.
- Reset the active CMC from Web interface. (See the **Reset CMC** option for **Power Control Operations** that is described in Executing Power Control Operations.)
- Remove the network cable from the active CMC.
- Remove the active CMC from the chassis.
- Initiate a CMC firmware flash on the active CMC.
- Have an active CMC that is no longer functional.

  NOTE: In the event of a CMC failover, all iDRAC connections and all active CMC sessions are lost. Users with lost sessions must reconnect to the new active CMC.

Related Links

About Standby CMC
CMC Failsafe Mode
Active CMC Election Process
Obtaining Health Status of Redundant CMC

About Standby CMC

The standby CMC is identical to and is maintained as a mirror of the active CMC. The active and standby CMCs must both be installed with the same firmware revision. If the firmware revisions differ, the system reports as redundancy degraded.

The standby CMC assumes the same settings and properties of the active CMC. You must maintain the same firmware version on both CMCs, but you do not need to duplicate configuration settings on the standby CMC.

NOTE: For information about installing a standby CMC, see the *Hardware Owner's Manual*. For instructions on installing CMC firmware on your standby CMC, follow the instructions in Updating Firmware.

CMC Failsafe Mode

In the failsafe mode, similar to the failover protection offered by the redundant CMC, the M1000e enclosure enables the fail-safe mode to protect the blades and I/O modules from failures. The fail-safe mode is enabled when no CMC is in control of the chassis. During the CMC failover period or during a single CMC management loss:

- You cannot turn on newly installed blades.
- You cannot access existing blades remotely.
- Chassis cooling fans run at 100% for thermal protection of the components.
- Blade performance reduces to limit power consumption until management of the CMC is restored.

The following are some of the conditions that can result in CMC management loss:

- CMC removal — Chassis management resumes after replacing CMC, or after failover to standby CMC.
- CMC network cable removal or network connection loss — Chassis management resumes after the chassis fails over to the standby CMC. Network failover is only enabled in redundant CMC mode.
- CMC reset — Chassis management resumes after CMC reboots or chassis fails over to the standby CMC.
- CMC failover command issued — Chassis management resumes after the chassis fails over to the standby CMC.
- CMC firmware update — Chassis management resumes after CMC reboots or chassis fails over to the standby CMC. It is recommended that you update the standby CMC first so that there is only one failover event.
- CMC error detection and correction — Chassis management resumes after CMC resets or chassis fails over to the standby CMC.

  NOTE: You can configure the enclosure either with a single CMC or with redundant CMCs. In redundant CMC configurations, if the primary CMC loses communication with the enclosure or the management network, the standby CMC takes over chassis management.

Active CMC Election Process

There is no difference between the two CMC slots; that is, slot does not dictate precedence. Instead, CMC that is installed or booted first assumes the role of the active CMC. If AC power is applied with two CMCs installed, CMC installed in CMC chassis slot 1 (the left) normally assumes the active role. The active CMC is indicated by the blue LED.

If two CMCs are inserted into a chassis that is already powered on, automatic active/standby negotiation can take up to two minutes. Normal chassis operation resumes when the negotiation is complete.

Obtaining Health Status of Redundant CMC

You can view the health status of the standby CMC in the Web interface. For more information about accessing CMC health status in the Web interface, see Viewing Chassis Information and Monitoring Chassis and Component Health.

3

Logging In to CMC

You can log in to CMC as a CMC local user, as a Microsoft Active Directory user, or as an LDAP user. The default user name and password is root and calvin, respectively. You can also log in using Single Sign-On or Smart Card.

Related Links

Accessing CMC Web Interface
Logging Into CMC as Local User, Active Directory User, or LDAP User
Logging Into CMC Using Smart Card
Logging Into CMC Using Single Sign-on
Logging In to CMC Using Serial, Telnet, or SSH Console
Accessing CMC Using RACADM
Logging in to CMC Using Public Key Authentication

Accessing CMC Web Interface

Before you log in to CMC using the Web interface, make sure that you have configured a supported Web browser (Internet Explorer or Firefox) and the user account is created with the required privileges.

NOTE: If you are using Microsoft Internet Explorer, connecting through a proxy, and if you see the error "The XML page cannot be displayed," you need to disable the proxy to continue.

To access the CMC Web interface:

1. Open a supported Web browser window.

   For the latest information on supported Web browsers, see the *Dell Systems Software Support Matrix* located at **support.dell.com/manuals**.

2. In the **Address** field, type the following URL, and press <Enter>:

   – To access CMC using IPv4 address: `https://<CMC IP address>`

     If the default HTTPS port number (port 443) was changed, type: `https://<CMC IP address>:<port number>`

   – To access CMC using IPv6 address: `https://[<CMC IP address>]`

     If the default HTTPS port number (port 443) was changed, type: `https://[<CMC IP address>]:<port number>`

     NOTE: While using IPv6, you must enclose the *<CMC IP address>* in square brackets ([ ]).

     where *<CMC IP address>* is the IP address for CMC and *<port number>* is the HTTPS port number.

     The **CMC Login** page appears.

Related Links

Configuring Web Browser
Logging Into CMC as Local User, Active Directory User, or LDAP User
Logging Into CMC Using Smart Card
Logging Into CMC Using Single Sign-on

Logging Into CMC as Local User, Active Directory User, or LDAP User

To log in to CMC, you must have a CMC account with **Log In to CMC** privilege. The default CMC user name is root, and the password is calvin. The root account is the default administrative account that ships with CMC.

NOTE: For added security, it is strongly recommended that you change the default password of the root account during initial setup.

CMC does not support extended ASCII characters, such as ß, å, é, ü, or other characters used primarily in non-English languages.

You cannot log in to the Web interface with different user names in multiple browser windows on a single workstation.

To log in as local user, Active Directory user, or LDAP user.

1. In the **Username** field, type your user name:

   – CMC user name: <user name>

   – Active Directory user name: <domain>\<user name>, <domain>/<user name> or <user>@<domain>.

   – LDAP user name: <user name>

   NOTE: This field is case sensitive. For Active Directory user.

2. In the **Password** field, type the user password.

   NOTE: This field is case-sensitive.

3. Optionally, select a session timeout. This is the amount of time you can stay logged in with no activity before you are automatically logged out. The default value is the Web Service Idle Timeout.
4. Click **OK**.

   You are logged into CMC with the required user privileges.

Related Links

Configuring User Accounts and Privileges
Accessing CMC Web Interface

Logging Into CMC Using Smart Card

You can log in to CMC using a smart card. Smart cards provide Two Factor Authentication (TFA) that provide two-layers of security:

- Physical smart card device.
- Secret code such as a password or PIN.

Users must verify their credentials using the smart card and the PIN.

NOTE: You cannot use the IP address to log in to CMC using Smart Card login. Kerberos validates your credentials based on the Fully Qualified Domain Name (FQDN).

Before you log in as a Active Directory user using Smart Card, make sure to:

- Upload a Trusted Certificate Authority (CA) certificate (CA-signed Active Directory certificate) to CMC
- Configure the DNS server.
- Enable Active Directory login.
- Enable Smart Card login.

To log in to CMC as an Active Directory user using smart card:

1. Log in to CMC using the link `https://<cmcname.domain-name>`.

   The **CMC Login** page is displayed prompting you to insert the smart card.

   NOTE: If you changed the default HTTPS port number (port 80), access the CMC Web page using `<cmcname.domain-name>:<port number>`, where cmcname is the CMC host name for CMC, **domain-name** is the domain name, and **port number** is the HTTPS port number.

2. Insert the smart card and click **Login**.

   The PIN pop-up is displayed.

3. Enter the PIN and click **Submit**.

   NOTE: If the smart card user is present in Active Directory, an Active Directory password is not required.

   You are logged in to CMC with your Active Directory credentials.

Related Links

Configuring CMC SSO Or Smart Card Login For Active Directory Users

Logging Into CMC Using Single Sign-on

When Single Sign-On (SSO) is enabled, you can log in to CMC without entering your domain user authentication credentials, such as user name and password.

NOTE: You cannot use the IP address to log into the Single Sign-On. Kerberos validates your credentials against the Fully Qualified Domain Name (FQDN).

Before logging in to CMC using Single Sign-on, make sure that:

- You have logged into your system using a valid Active Directory user account.
- Single Sign-On option is enabled during Active Directory configuration.

To log in to CMC using Single Sign-on:

1. Log into the client system using your network account.
2. Access the CMC Web interface using: `https://<cmcname.domain-name>`

   For example, **cmc-6G2WXF1.cmcad.lab,** where **cmc-6G2WXF1** is the cmc-name and **cmcad.lab** is the domain-name.

   NOTE: If you have changed the default HTTPS port number (port 80), access the CMC Web interface using `<cmcname.domain-name>:<port number>`, where the **cmcname** is the CMC host name for CMC, **domain-name** is the domain name, and **port number** is the HTTPS port number.

   CMC logs you in, using the Kerberos credentials that were cached by your browser when you logged in using your valid Active Directory account. If the login fails, the browser is redirected to the normal CMC login page.

   NOTE: If you did not log in to the Active Directory domain and are using a browser other then Internet Explorer, the login fails and the browser only displays a blank page.

Related Links

Configuring CMC SSO Or Smart Card Login For Active Directory Users

Logging In to CMC Using Serial, Telnet, or SSH Console

You can log in to CMC through a serial, Telnet, or SSH connection, or through Dell CMC console on iKVM.

After you have configured your management station terminal emulator software and managed node BIOS, perform the following steps to log in to CMC:

1. Connect to the CMC using your management station terminal emulation software.
2. Type your CMC user name and password, and press <Enter>.

   You are logged in to the CMC.

Related Links

Configuring CMC to Use Command Line Consoles

Enabling Access to iKVM from the Dell CMC Console

Accessing CMC Using RACADM

RACADM provides a set of commands that allow you to configure and manage the CMC through a text-based interface. RACADM can be accessed using a Telnet/SSH or serial connection, using the Dell CMC console on the iKVM, or remotely using the RACADM command line interface installed on a management station.

The RACADM interface is classified as follows:

NOTE: Remote RACADM is included on the Dell Systems Management Tools and Documentation DVD and is installed on a management station.

- Remote RACADM — Allows you to run RACADM commands on a management station with the -r option and the DNS name or IP address of the CMC.
- Firmware RACADM — Allows you to log in to the CMC using Telnet, SSH, a serial connection, or the iKVM. With Firmware RACADM, you run the RACADM implementation that is part of the CMC firmware.

You can use remote RACADM commands in scripts to configure multiple CMCs. CMC does not have support for scripting, so you cannot run the scripts directly on the CMC.

For more information about RACADM, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC*.

For more information about configuring multiple CMCs, see Configuring Multiple CMCs Using RACADM.

Logging in to CMC Using Public Key Authentication

You can log into the CMC over SSH without entering a password. You can also send 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.

Before logging in to CMC over SSH, make sure that the public keys are uploaded.

For example:

- **Logging in:** `ssh service@<domain>` or `ssh service@<IP_address>` where IP_address is the CMC IP address.
- **Sending RACADM commands:** `ssh service@<domain> racadm getversion` and `ssh service@<domain> racadm getsel`

When you log in using the service account, if a passphrase was set up when creating the public or private key pair, you may be prompted to enter that passphrase again. If a passphrase is used with the keys, both Windows and Linux clients provide methods to automate that as well. For Windows clients, you can use the Pageant application. It runs in the background and makes entering the passphrase transparent. For Linux clients, you can use the sshagent. For setting up and using either of these applications, see the documentation provided from that application.

Related Links

Configure Public Key Authentication over SSH

Multiple CMC Sessions

The following table provides the list of multiple CMC sessions that are possible using the various interfaces.

Table 5. Multiple CMC Sessions

Interface	Number of Sessions
CMC Web Interface	4
RACADM	4
Telnet	4
SSH	4

4

Updating Firmware

You can update firmware for the following:

- CMC - active and standby
- iKVM
- IOMs

You can update firmware for the following server components:

- iDRAC - iDRACs earlier than iDRAC6 must be updated using the recovery interface. iDRAC6 firmware can also be updated with the recovery interface, but is deprecated for iDRAC6 and future versions.
- BIOS
- Unified Server Configurator
- 32-Bit Diagnostics
- OS-Drivers Pack
- Network Interface Controllers
- RAID Controllers

Related Links

Downloading CMC Firmware
Viewing Currently Installed Firmware Versions
Updating CMC Firmware
Updating iKVM Firmware
Updating IOM Infrastructure Device Firmware
Updating Server iDRAC Firmware
Updating Server Component Firmware
Recovering iDRAC Firmware Using CMC

Downloading CMC Firmware

Before beginning the firmware update, download the latest firmware version from **support.dell.com**, and save it to your local system.

The following software components are included with the CMC firmware package:

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

Viewing Currently Installed Firmware Versions

You can view the currently installed firmware versions using the CMC Web interface or RACADM.

Viewing Currently Installed Firmware Versions Using CMC Web Interface

In the CMC Web interface, go to any of the following pages to view the current firmware versions:

- **Chassis Overview → Update**
- **Chassis Overview → Chassis Controller → Update**
- **Chassis Overview → Server Overview → Update**
- **Chassis Overview → I/O Module Overview → Update**
- **Chassis Overview → iKVM → Update**

The **Firmware Update** page displays the current version of the firmware for each listed component and allows you to update the firmware to the latest revision.

If the chassis contains an earlier generation server whose iDRAC is in recovery mode or if CMC detects that iDRAC has corrupted firmware, then the earlier generation iDRAC is also listed on the Firmware Update page.

Viewing Currently Installed Firmware Versions Using RACADM

To view the currently installed firmware versions using RACADM, use the **getkvminfo** subcommand. For more information, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC*.

Updating CMC Firmware

You can update CMC firmware using Web interface or RACADM. The firmware update, by default, retains the current CMC settings. During the update process, you can reset CMC configuration settings back to the factory default settings.

NOTE: To update firmware on CMC, you must have Chassis Configuration Administrator privilege.

If a Web user interface session is used to update system component firmware, the Idle Timeout setting must be set high enough to accommodate the file transfer time. In some cases, the firmware file transfer time may be as high as 30 minutes. To set the Idle Timeout value, see Configuring Services.

During updates of CMC firmware, it is normal for some or all of the fan units in the chassis to spin at 100%.

If you have redundant CMCs installed in the chassis, it is recommended to update both the CMCs to the same firmware version at the same time with a single operation. If CMCs have different firmware and a failover occurs, unexpected results may occur.

The Active CMC resets and becomes temporarily unavailable after the firmware has been uploaded successfully. If a standby CMC is present, the standby and active roles swap. The standby CMC becomes the active CMC. If an update is applied only to the active CMC, after the reset is complete the active CMC does not run the updated image, only the standby CMC has that image. In general, it is highly recommended to maintain identical firmware versions for the active and standby CMCs.

When the standby CMC has been updated, swap the CMCs' roles so that the newly updated CMC becomes the active CMC and CMC with the older firmware becomes the standby. See the `cmcchangeover` command section in the *RACADM Command Line Reference Guide for iDRAC7 and CMC* for

information about swapping roles. This allows you to verify that the update has succeeded and that the new firmware is working properly, before you update the firmware in the second CMC. When both CMCs are updated, you can use the `cmcchangeover` command to restore the CMCs to their previous roles. CMC Firmware revision 2.x updates both the primary CMC and the redundant CMC without using the `cmcchangeover` command.

To avoid disconnecting other users during a reset, notify authorized users who may log in to CMC and check for active sessions in the Sessions page. To open the **Sessions** page, select **Chassis** in the tree, click the **Network** tab, and then click the **Sessions** subtab.

When transferring files to and from CMC, the file transfer icon spins during the transfer. If your icon is animated, make sure that your browser is configured to allow animations. For instructions, see Allow Animations in Internet Explorer.

If you experience problems downloading files from CMC using Internet Explorer, enable the Do not save encrypted pages to disk option. For instructions, see Downloading Files From CMC With Internet Explorer.

Related Links

Downloading CMC Firmware
Viewing Currently Installed Firmware Versions

Updating CMC Firmware Using Web Interface

To update the CMC firmware using the CMC Web interface:

1. Go to any of the following pages:

   – **Chassis Overview** → **Update**
   – **Chassis Overview** → **Chassis Controller** → **Update**
   – **Chassis Overview** → **I/O Module Overview** → **Update**
   – **Chassis Overview** → **iKVM** → **Update**

   The **Firmware Update** page is displayed.
2. In the **CMC Firmware** section, select the checkbox(s) in the **Update Targets** column for the CMC or CMCs (if standby CMC is present) you want to update the firmware and click **Apply CMC Update**.
3. In the **Firmware Image** field, enter the path to the firmware image file on the management station or shared network, or click **Browse** to navigate to the file location. The default CMC firmware image name is `firmimg.cmc`.
4. Click **Begin Firmware Update** and then click **Yes** to continue. The **Firmware Update Progress** section provides firmware update status information. A status indicator displays on the page while the image file uploads. File transfer time varies based on connection speed. When the internal update process begins, the page automatically refreshes and the Firmware update timer is displayed.
5. Additional instructions:

   – Do not click the **Refresh** icon or navigate to another page during the file transfer.
   – To cancel the process, click **Cancel File Transfer and Update**. This option is available only during file transfer.
   – The **Update State** field displays the firmware update status.

   NOTE: The update may take several minutes for CMC.
6. For a standby CMC, when the update is complete the **Update State** field displays **Done**. For an active CMC, during the final phases of the firmware update process, the browser session and connection with CMC is lost temporarily as the active CMC is taken offline. You must log in again after a few minutes, when the active CMC has rebooted. After CMC resets, the new firmware is displayed on the **Firmware Update** page.

   NOTE: After the firmware update, clear the Web browser cache. For instructions on how to clear the browser cache, see your Web browser's online help.

Updating CMC Firmware Using RACADM

To update CMC firmware using RACADM, use the fwupdate subcommand For more information, see *RACADM Command Line Reference Guide for iDRAC7 and CMC*.

Updating iKVM Firmware

The iKVM resets and becomes temporarily unavailable after the firmware is successfully uploaded.
Related Links

Downloading CMC Firmware
Viewing Currently Installed Firmware Versions

Updating iKVM Firmware Using CMC Web Interface

To update the iKVM firmware using in the CMC Web interface:

1. Go to any of the following pages:

   - **Chassis Overview → Update**
   - **Chassis Overview → Chassis Controller → Update**
   - **Chassis Overview → I/O Module Overview → Update**
   - **Chassis Overview → iKVM → Update**

   The **Firmware Update** page is displayed.
2. In the **iKVM Firmware** section, select the checkbox in the **Update Targets** column for the **iKVM** you want to update the firmware and click **Apply iKVM Update**.
3. In the **Firmware Image** field, enter the path to the firmware image file on the management station or shared network, or click **Browse** to navigate to the file location. The default iKVM firmware image name is **iKVM.bin**.
4. Click **Begin Firmware Update** and then click **Yes** to continue.

   The **Firmware Update Progress** section provides firmware update status information. A status indicator displays on the page while the image file uploads. File transfer time varies based on connection speed. When the internal update process begins, the page automatically refreshes and the Firmware update timer is displayed.
5. Additional instructions to follow:

   - Do not click the **Refresh** icon or navigate to another page during the file transfer.
   - To cancel the process, click **Cancel File Transfer and Update**. This option is available only during file transfer.
   - The **Update State** field displays the firmware update status.

   NOTE: The update may take up to two minutes for iKVM.

   When the update is complete, iKVM resets and the new firmware is displayed on the **Firmware Update** page.

Updating iKVM Firmware Using RACADM

To update iKVM firmware using RACADM, use the `fwupdate` subcommand. For more information, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC*.

Updating IOM Infrastructure Device Firmware

By performing this update, the firmware for a component of the IOM device is updated, but not the firmware of the IOM device itself; the component is the interface circuitry between the IOM device and CMC. The update image for the component resides in the CMC file system, and the component displays as an updatable device on the CMC Web interface only if the current revision on the component and the component image on CMC do not match.

Before updating IOM infrastructure device firmware, make sure the CMC firmware is updated.

CMC allows IOM infrastructure device firmware (IOMINF) updates only if it detects that the IOMINF firmware is out-of-date with the image contained in CMC file system. If the IOMINF firmware is up-to-date, CMC prevents IOMINF updates.Up-to-date IOMINF devices are not listed as updatable devices.

Related Links

Downloading CMC Firmware
Viewing Currently Installed Firmware Versions

Updating IOM Firmware Using CMC Web Interface

To update the IOM Infrastructure device firmware, in the CMC Web interface:

1. Go to any of the following pages:
   - **Chassis Overview** → **Update**
   - **Chassis Overview** → **Chassis Controller** → **Update**
   - **Chassis Overview** → **I/O Module Overview** → **Update**
   - **Chassis Overview** → **iKV** → **Update**

   The **Firmware Update** page is displayed.
2. In the **IOM Firmware** section, select the checkbox in the **Update Targets** column for the IOM you want to update the firmware and click **Apply IOM** Update.

   The **Firmware Image** field does not display for an IOM infrastructure device (IOMINF) target because the required image resides on CMC.
3. Click **Begin Firmware Update** and then click **Yes** to continue.

   The **Firmware Update Progress** section provides firmware update status information. A status indicator displays on the page while the image file uploads. File transfer time varies based on connection speed. When the internal update process begins, the page automatically refreshes and the Firmware update timer is displayed.
4. Additional instructions to follow:
   - Do not click the **Refresh** icon or navigate to another page during the file transfer.
   - The **Update State** field displays the firmware update status.

   NOTE: The file transfer timer is not displayed when updating IOMINF firmware.

   When the update is complete, there is a brief loss of connectivity to the IOM device since it resets and the new firmware is displayed on the **Firmware Update** page.

Updating IOM Firmware Using RACADM

To update IOM infrastructure device firmware using RACADM, use the fwupdate subcommand For more information, see *RACADM Command Line Reference Guide for iDRAC7 and CMC*.

Updating Server iDRAC Firmware

You can update firmware for iDRAC6 and iDRAC7.

The iDRAC firmware must be at version 1.4 or later for servers with iDRAC, or 2.0 or later for servers with iDRAC6 Enterprise. If updating iDRAC firmware to 3.0 or later from an iDRAC version less than 2.3, the iDRAC firmware must first be updated to version 2.3 before updating to version 3.0 or greater.

The iDRAC (on a Server) resets and become temporarily unavailable after firmware updates is successfully uploaded.

Related Links

[Downloading CMC Firmware]

[Viewing Currently Installed Firmware Versions]

Updating Server iDRAC Firmware Using Web Interface

To update the iDRAC firmware in the server using in the CMC Web interface:

1. Go to any of the following pages:

   – **Chassis Overview** → **Update**
   – **Chassis Overview** → **Chassis Controller** → **Update**
   – **Chassis Overview** → **I/O Module Overview** → **Update**
   – **Chassis Overview** → **iKVM** → **Update**

   The Firmware Update page is displayed.

   You can also update server iDRAC firmware at **Chassis Overview** → **Server Overview** → **Update** . For more information, see the Updating Server Component Firmware.
2. To update iDRAC6 firmware, in the **iDRAC6 Enterprise Firmware** section, select the checkbox in the **Update Targets** column for the iKVM you want to update the firmware and click **Apply iDRAC6 Enterprise Update** and go to step 4.
3. To update iDRAC7 firmware, in the **iDRAC7 Enterprise Firmware** section, click the **Update** link for the server for which you want to update the firmware.

   The **Server Component Update** page is displayed. To continue, see the Updating Server Component Firmware section.
4. In the **Firmware Image** field, enter the path to the firmware image file on the management station or shared network, or click **Browse** to navigate to the file location. The default iDRAC firmware image name is **firming.imc**.
5. Click **Begin Firmware Update** and then click **Yes** to continue.

   The **Firmware Update Progress** section provides firmware update status information. A status indicator displays on the page while the image file uploads. File transfer time varies based on connection speed. When the internal update process begins, the page automatically refreshes and the Firmware update timer is displayed.
6. Additional instructions to follow:

   – Do not click the **Refresh** icon or navigate to another page during the file transfer.
   – To cancel the process, click **Cancel File Transfer and Update**. This option is available only during file transfer.
   – The **Update State** field displays the firmware update status.

   NOTE: It may take up to 10 minutes to update the iDRAC firmware.

   When the update is complete, iKVM resets and the new firmware is displayed on the **Firmware Update** page.

Updating Server iDRAC Firmware Using RACADM

To update iDRAC firmware using RACADM, use the fwupdate subcommand For more information, see *RACADM Command Line Reference Guide for iDRAC7 and CMC*.

Updating Server Component Firmware

The Lifecycle Controller service available on each server and is facilitated by iDRAC. You can manage the firmware of the components and devices on the servers using the Lifecycle Controller service. The Lifecycle controller uses an optimization algorithm to update the firmware that reduces the number of reboots efficiently.

Dell Update Packages (DUPs) are used to perform the firmware updates using Lifecycle Controller. The default CMC configuration has a 48MB limit on the size of the DUP. The OS-Driver Pack component DUP exceeds this limit and must be updated separately using the Extended Storage feature.

The Lifecycle Controller provides module update support for iDRAC6 and later servers. The iDRAC firmware must be at version 2.3 or later to update firmware using Lifecycle Controller.

Before using the Lifecycle Controller based update feature, server firmware versions must be updated.

You must update the CMC firmware before updating the server component firmware modules.

Always update the server component firmware modules in the following order:

- BIOS
- Lifecycle Controller
- iDRAC

In the CMC Web interface, you can update the server component firmware on the **Chassis Overview** → **Server Overview** → **Update** → **Server Component Update** page.

If the server does not support the Lifecycle Controller service, the **Component/Device Firmware Inventory** section displays **Not Supported**. For the latest generation servers, install the Lifecycle Controller firmware and update the iDRAC firmware to enable the Lifecycle Controller service on the server. For earlier generation servers, this upgrade may not be possible.

Normally, the Lifecycle Controller firmware is installed using an appropriate installation package that is executed on the server operating system. For supported servers, a special repair or installation package with .usc file extension is available. This enables you to install the Lifecycle Controller firmware through the firmware update facility available on the native iDRAC Web-Browser interface.

You can also install Lifecycle Controller firmware through an appropriate installation package executed on the server OS. For more information, see the *Dell Lifecycle Controller User's Guide*.

If Lifecycle Controller service is disabled on the server, the **Component/Device Firmware Inventory** section displays *Lifecycle Controller may not be enabled*.

Related Links

Enabling Lifecycle Controller
Filtering Components for Firmware Updates
Viewing Firmware Inventory
Lifecycle Controller Job Operations

Enabling Lifecycle Controller

You can enable the Lifecycle Controller service during the server boot process:

- For iDRAC6 servers, on the boot console, when prompted with the message `Press <CTRL-E> for Remote Access Setup within 5 sec.`, press <CTRL-E>. Then, on the setup screen, enable **System Services**.
- For iDRAC7 servers, on the boot console, select F2 for System Setup. On the setup screen, select **iDRAC Settings** and then select **System Services**.

Cancelling System Services enables you to cancel all scheduled jobs that are pending and remove them from the queue.

For more information on the Lifecycle Controller and Server Component, and Device Firmware Management, see:

- *Lifecycle Controller Remote Services User’s Guide*.
- **delltechcenter.com/page/Lifecycle+Controller**.

The **Server Component Update** page enables you to update various firmware components on your system. To use the features and functions on this page, you must have:

- For CMC: **Server Administrator** privilege.
- For iDRAC: **Configure iDRAC** privilege and **Log in to iDRAC** privilege.

In case of insufficient privileges, you can only view the firmware inventory of components and devices on the server. You cannot select any components or devices for any kind of Lifecycle Controller operation on the server.

Filtering Components for Firmware Updates

Information for all the components and devices across all servers is retrieved at one time. To manage this large amount of information, the Lifecycle Controller provides various filtering mechanisms. These filters enable you to:

- Select one or more categories of components or devices for easy viewing.
- Compare firmware versions of components and devices across the server.
- Filter the selected components and devices automatically, to narrow the category of a particular component or device based on types or models.

  NOTE: Automatic filtering feature is important while using the Dell Update Package (DUP). The update programming of a DUP can be based on the type or model of a component or device. The automatic filtering behavior is designed to minimize the subsequent selection decisions after an initial selection is made.

Examples

Following are some examples where the filtering mechanisms are applied:

- If the BIOS filter is selected, only the BIOS inventory for all servers is displayed. If the set of servers consists of a number of server models, and a server is selected for BIOS update, the automatic filtering logic automatically removes all the other servers that do not match with the model of the selected server. This ensures that the selection of the BIOS firmware update image (DUP) is compatible with the correct model of the server.

  Sometimes, a BIOS firmware update image may be compatible across a number of server models. Such optimizations are ignored in case this compatibility is no longer true in the future.
- Automatic filtering is important for firmware updates of Network Interface Controllers (NIC) and RAID Controllers. These device categories have different types and models. Similarly, the firmware update images (DUP) may be available in optimized forms where a single DUP may be programmed to update multiple types or models of devices of a given category.

Filtering Components for Firmware Updates Using CMC Web Interface

To filter the devices:

1. In the system tree go to **Server Overview**, and then click **Update** → **Server Component Update** .

   The **Server Component Update** page is displayed.
2. In the **Component/Device Update Filter** section, select one or more of the following:

   – BIOS
   – iDRAC

- Lifecycle Controller
- 32-Bit Diagnostics
- OS Driver Pack
- Network I/F Controller
- RAID Controller

The **Firmware Inventory** section is displays only the associated components or devices across all servers present in the chassis. The filter is a pass filter; this means that it only permits components or devices associated with the filter and excludes all others.

After the filtered set of components and devices is displayed in the inventory section, further filtering may occur when a component or device is selected for update. For example, if the BIOS filter is selected, then the inventory section displays all the servers with only their BIOS component. If a BIOS component on one of the servers is selected, the inventory is further filtered to display the servers that match the model name of the selected server.

If no filter is selected and a selection for update of a component or device is made on the inventory section, then the filter associated with that selection is automatically enabled. Further filtering may occur where the inventory section displays all the servers that have a match for the selected component in terms of model, type or some form of identity. For example, if a BIOS component on one of the servers is selected for update, the filter is set to the BIOS automatically and the inventory section displays the servers that match the model name of the selected server.

Filtering Components for Firmware Updates Using RACADM

To filter components for Firmware Updates using RACADM, use the getversion command:

```
racadm getversion -l [-m <module>] [-f <filter>]
```

For more information, see the RACADM Command Line Reference Guide for iDRAC7 and CMC available at **support.dell.com/manuals**.

Viewing Firmware Inventory

You can view the summary of the firmware versions for all components and devices for all servers currently present in the chassis along with their status.

Viewing Firmware Inventory Using CMC Web Interface

To view the firmware inventory:

1. In the system tree, go to **Server Overview**, and then click **Update** → **Server Component Update** .

   The **Server Component Update** page is displayed.
2. View the firmware inventory details in the **Component/Device Firmware Inventory** section. Table provides

   - Servers that currently do not support the Lifecycle Controller service are listed as **Not Supported**. A hyperlink is provided to an alternative page where you can directly update only the iDRAC firmware. This page supports only iDRAC firmware update and not any other component and device on the server. iDRAC firmware update is not dependent on the Lifecycle Controller service.
   - If the server is listed as **Not Ready**, it indicates that when the firmware inventory was retrieved, the iDRAC on the server was still initializing. Wait for the iDRAC to be fully operational and then refresh the page for the firmware inventory to be retrieved again.
   - If the inventory of components and devices does not reflect what is physically installed on the server, you must invoke the Lifecycle Controller when the server is in the boot process. This helps to refresh the internal components and devices information and allows you to verify the currently installed components and devices. This occurs when:

        - * The server iDRAC firmware is updated to newly introduce the Lifecycle Controller functionality to the server management.
          * The new devices are inserted into the server.

        To automate this action, iDRAC Configuration Utility (for iDRAC6) or the iDRAC Settings Utility (for iDRAC7) provides an option that can be accessed through the boot console:

          * For iDRAC6 servers, on the boot console, when prompted with the message `Press <CTRL-E> for Remote Access Setup within 5 sec.`, press `<CTRL-E>`. Then, on the setup screen, enable **Collect System Inventory on Restart**.
          * For iDRAC7 servers, on the boot console, select F2 for System Setup. On the setup screen, select iDRAC Settings, and then select System Services (USC). On the setup screen, enable **Collect System Inventory on Restart**.

    – Options to perform the various Lifecycle Controller operations such as Update, Rollback, Reinstall, and Job Deletion are available. Only one type of operation can be performed at a time. Components and devices that are not supported may be listed as part of the inventory, but do not permit Lifecycle Controller operations.

The following table displays the component and devices information on the server:

Table 6. : Component and Devices Information

Field	Description
Slot	Displays the slot occupied by the server in the chassis. Slot numbers are sequential IDs, from 1 to 16 (for the 16 available slots in the chassis), that help to identify the location of the server in the chassis. When there are less than 16 servers occupying slots, only those slots populated by servers are displayed.
Name	Displays the name of the server in each slot.
Model	Displays the model of the server.
Component/Device	Displays a description of the component or device on the server. If the column width is too narrow the mouse-over tool provides a view of the description.
Current Version	Displays the current version of component or device on the server.
Rollback Version	Displays the rollback version of component or device on the server.
Job Status	Displays the job status of any operations that are scheduled on the server. The job status is continuously updated dynamically. If a job completion with state completed is detected, then the firmware versions for the components and devices on that server are automatically refreshed in case there has been a change of firmware version on any of the components or devices. An information icon is also presented adjacent to the current state, which provides additional information of the current job status. This information can be viewed by clicking or hovering over the icon.
Update	Selects the component or device for firmware update on the server.

Viewing Firmware Inventory Using RACADM

To view Firmware Inventory using RACADM, use the getversion command:

```
racadm getversion -l [-m <module>] [-f <filter>]
```

For more information, see the RACADM Command Line Reference Guide for iDRAC7 and CMC available at **support.dell.com/manuals**.

Lifecycle Controller Job Operations

You can perform Lifecycle Controller operations such as:

- Re-install
- Rollback
- Update
- Delete Jobs

Only one type of operation can be performed at a time. Components and devices that are not supported may be listed as part of the inventory, but do not permit Lifecycle Controller operations.

To perform the Lifecycle Controller operations, you must have:

- For CMC: Server Administrator privilege.
- For iDRAC: Configure iDRAC privilege and Log in to iDRAC privilege.

A Lifecycle Controller operation scheduled on a server may take 10 to 15 minutes to complete. The process involves several server reboots during which the firmware installation is performed, which also includes a firmware verification stage. You can view the progress of this process using the server console. If there are several components or devices that need to be updated on a server, you can consolidate all the updates into one scheduled operation thus minimizing the number of reboots required.

Sometimes, when an operation is in the process of being submitted for scheduling through another session or context, another operation is attempted. In this case, a confirmation popup message is displayed indicating the situation and the operation must not be submitted. Wait for the operation in process to complete and then submit the operation again.

Do not navigate away from the page after an operation is submitted for scheduling. If an attempt is made, a confirmation popup message is displayed allowing the intended navigation to be cancelled. Otherwise, the operation is interrupted. An interruption, especially during an Update operation may cause the firmware image file upload to be terminated before proper completion. After an operation has been submitted for scheduling, ensure that the confirmation popup message indicating that the operation has been successfully scheduled is acknowledged.

Related Links

Re-installing Server Component Firmware
Rolling Back Server Component Firmware
Upgrading Server Component Firmware
Deleting Scheduled Server Component Firmware Jobs

Re-installing Server Component Firmware

You can re-install the firmware image of the currently installed firmware for selected components or devices across one or more servers. The firmware image is available within the Lifecycle Controller.

Re-installing Server Component Firmware Using Web Interface

To re-install Server Component Firmware:

1. In the system tree, go to **Server Overview**, and then **Click** → **Update** → **Server Component Update**.

   The **Server Component Update** page is displayed.
2. Filter the component or device (optional).
3. In the **Current Version** column, select the checkbox for the component or device for which you want to re-install the firmware.
4. Select one of the following options:

   – **Reboot Now** - Reboot immediately.

- **On Next Reboot** - Manually reboot the server at a later time.

5. Click **Reinstall**. The firmware version is re-installed for the selected component or device.

Rolling Back Server Component Firmware

You can install the firmware image of the previously installed firmware for selected components or devices across one or more servers. The firmware image is available within the Lifecycle Controller for a rollback operation. The availability is subject to the version compatibility logic of the Lifecycle Controller. It also assumes the previous update was facilitated by the Lifecycle Controller.

Rolling Back Server Component Firmware Using CMC Web Interface

To rollback the server component firmware version to an earlier version:

1. In the CMC Web interface, expand the system tree, go to **Server Overview** and then click **Update** → **Server Component Update** .

   The **Server Component Update** page is displayed.
2. Filter the component or device (optional).
3. In the **Rollback Version** column, select the checkbox for the component or device for which you want to roll back the firmware.
4. Select one of the following options:
   - **Reboot Now** - Reboot immediately.
   - **On Next Reboot** - Manually reboot the server at a later time.
5. Click **Rollback**. The previously installed firmware version is re-installed for the selected component or device.

Upgrading Server Component Firmware

You can install the next version of the firmware image for selected components or devices across one or more servers. The firmware image is available within the Lifecycle Controller for a rollback operation.

NOTE: For iDRAC and OS Driver packs firmware update, make sure the Extended Storage feature is enabled.

It is recommended to clear the job queue before initializing a server component firmware update. A list of all jobs on the server(s) is available on the Lifecycle Controller Jobs page. This page enables deletion of single or multiple jobs or purging of all jobs on the server. See the Troubleshooting section, "Managing Lifecycle Controller jobs on a remote system" .

BIOS updates are specific to the model of the server. The selection logic is based on this behavior. Sometimes, even though a single Network Interface Controller (NIC) device is selected for firmware update on a server, the update may get applied to all the NIC devices on the server. This behavior is inherent in the lifecycle controller functionality and particularly the programming contained with the Dell Update Package (DUP). Currently, Dell Update Packages (DUP) that are less than 48MB in size are supported.

If the update file image size is greater, the job status indicates that the download has failed. If multiple server component updates are attempted on a server, the combined size of all the firmware update files may also exceed 48MB. In such a case, one of the component updates fails as its update file is truncated. To update multiple components on a server, it is recommended to update the Lifecycle Controller and 32-Bit Diagnostics components together first. These do not require a server reboot and are relatively quick to complete. The other components can then be updated together.

All Lifecycle Controller updates are scheduled for immediate execution. However, the system services can delay this execution sometimes. In such situations, the update fails as a result of the remote share that is hosted by the CMC being no longer available.

Upgrading Server Component Firmware Using CMC Web Interface

To upgrade the firmware version to the next version:

1. In the CMC Web interface, in the system tree, go to **Server Overview** and then click **Update** → **Server Component Update** .

   The **Server Component Update** page is displayed.

2. Filter the component or device (optional).

3. In the **Update** column, select the checkbox(es) for the component or device for which you want to update the firmware to the next version. Use the CRTL key shortcut to select a type of component or device for update across all the applicable servers. Pressing and holding the CRTL key highlights all the components in yellow. While the CRTL key is pressed down, select the required component or device by enabling the associated check box in the **Update** column.

   A second table is displayed that lists the selected type of component or device and a selector for the firmware image file. For each type of component, one selector for the firmware image file is displayed.

   Few devices such as Network Interface Controllers (NICs) and RAID Controllers contain many types and models. The update selection logic automatically filters the relevant device type or model based on the initially selected devices. The primary reason for this automatic filtering behavior is that only one firmware image file for the category can be specified.

   NOTE: The update size limitation of either a single DUP or combined DUPs can be ignored if the Extended Storage feature is installed and enabled. For information on enabling extended storage, see Configuring CMC Extended Storage Card.

4. Specify the firmware image file for the selected component(s) or devic(es). This is a Microsoft Windows Dell Update Package (DUP) file.

5. Select one of the following options:

   - **Reboot Now** - Reboot immediately.
   - **On Next Reboot** - Manually reboot the server at a later time.

   NOTE: This step is not valid for Lifecycle Controller and 32-bit Diagnostics firmware update. A server reboot is performed immediatly for these devices.

6. Click **Update**. The firmware version is updated for the selected component or device.

Deleting Scheduled Server Component Firmware Jobs

You can delete jobs scheduled for the selected components and/or devices across one or more servers.

Deleting Scheduled Server Component Firmware Jobs Using Web Interface

To delete scheduled server component firmware jobs:

1. In the CMC Web interface, in the system tree, go to **Server Overview** and then click **Update** → **Server Component Update** .

   The **Server Component Update** page is displayed.

2. Filter the component or device (optional).

3. In the **Job Status** column, if a check box is displayed next to the job status, this indicates a Lifecycle Controller job is in progress and currently is in the indicated state. It can be selected for a job deletion operation.

4. Click **Job Deletion**. The jobs are deleted for the selected component(s) or device(s).

Recovering iDRAC Firmware Using CMC

iDRAC firmware is typically updated using iDRAC interfaces such as the iDRAC Web interface, the SM-CLP command line interface, or operating system specific update packages downloaded from **support.dell.com**. For more information, see the iDRAC User’s Guide.

Early generations of servers can have corrupted firmware recovered using the new update iDRAC firmware process. When CMC detects corrupted iDRAC firmware, it lists the server on the **Firmware Update** page. Perform the steps as mentioned for updating firmware.

5

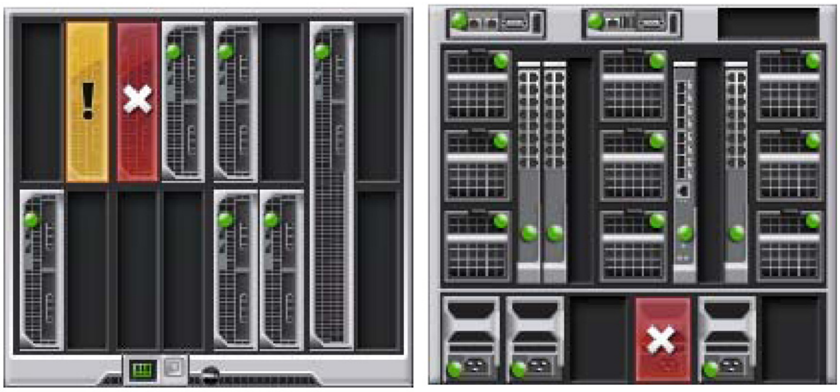
Viewing Chassis Information and Monitoring Chassis and Component Health

You can view information and monitor the health for the following:

- Active and standby CMCs
- All severs and individual servers
- Storage arrays
- All IO Modules (IOMs) and individual IOMs
- Fans
- iKVM
- Power supplies (PSUs)
- Temperature sensors
- LCD assembly

Viewing Chassis and Component Summaries

When you log in to the CMC Web interface, the Chassis Health page allows you to view the health of the chassis and its components. It displays a live graphical view of the chassis and its components. It is dynamically updated, and the component subgraphic overlays and text hints are automatically changed to reflect the current state.



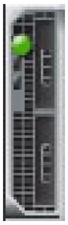
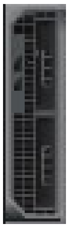
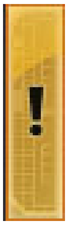
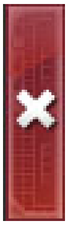
To view the chassis health, go to **Chassis Overview** → **Properties** → **Health** . It displays the overall health status for the chassis, active and standby CMCs, sever modules, IO Modules (IOMs), fans, iKVM, power supplies (PSUs), temperature sensors, and LCD assembly. Detailed information for each component is displayed when you click on that component. In addition, the latest events in the CMC Hardware Log are also displayed. For more information, see the *CMC Online Help*.

If your chassis is configured as a Group Lead, the **Group Health** page is displayed after login. It displays the chassis level information and alerts. All active critical and non-critical alerts are displayed.

Chassis Graphics

The chassis is represented by front and back views (the upper and lower images, respectively). Servers and the LCD are shown in the front view and the remaining components are shown in the back view. Component selection is indicated by a blue cast and is controlled by clicking the image of the required component. When a component is present in the chassis, an icon of that component type is shown in the graphics in the position (slot) where the component has been installed. Empty positions are shown with a charcoal gray background. The component icon visually indicates the state of the component. Other components display icons that visually represent the physical component. Icons for servers and IOMs span multiple slots when a double size component is installed. Hovering over a component displays a tooltip with additional information about that component.

Table 7. : Server Icon States

Icon	Description
	Server is powered on and is operating normally.
	Server is off.
	Server is reporting a non-critical error.
	Server is reporting a critical error.

Icon	Description
▮	No server is present.

Selected Component Information

Information for the selected component is displayed in three independent sections:

- Health and Performance and Properties — Displays the active critical and non-critical events as shown by the hardware logs and the performance data that vary with time.
- Properties — Displays the component properties that do not vary with time or change only infrequently.
- Quick Links — Provides links to navigate to the most frequently accessed pages, and also the most frequently performed actions. Only links applicable to the selected component are displayed in this section.

Viewing Server Model Name and Service Tag

You can view the model name and service tag of each server instantly using the following steps:

1. Expanding Servers in the System tree. All the servers (1-16) appear in the expanded Servers list. A slot without a server has its name grayed out.
2. Using the cursor to hover over the slot name or slot number of a server; a tool tip is displayed with the server's model name and service tag (if available).

Viewing Chassis Summary

You can view the summary of the installed components in the chassis.

To view the chassis summary information, in the CMC Web interface, go to **Chassis Overview** → **Properties** → **Summary** .

The **Chassis Summary** page is displayed. For more information, see the *CMC Online Help*.

Viewing Chassis Controller Information and Status

To view the chassis controller information and status, in the CMC Web interface, go to **Chassis Overview** → **Chassis Controller** → **Properties** → **Status**.

The **Chassis Controller Status** page is displayed. For more information, see the *CMC Online Help*.

Viewing Information and Health Status of All Servers

To view the health status of all the servers, do any of the following:

1. Go to **Chassis Overview** → **Properties** → **Health** .

   The Chassis Health page is displays a graphical overview of all the servers installed in the chassis. Server health status is indicated by the overlay of the server subgraphic. For more information, see the *CMC Online Help*.

2. Go to **Chassis Overview** → **Server Overview** → **Properties** → **Status**.

The Servers Status page provides overviews of the servers in the chassis. For more information, see the *CMC Online Help*.

Viewing Health Status and Information for Individual Server

To view health status for individual servers, do any of the following:

1. Go to **Chassis Overview** → **Properties** → **Health** .

   The **Chassis Health** page displays a graphical overview of all the servers installed in the chassis. Server health status is indicated by the overlay of the server subgraphic. Move the cursor to hover over an individual server subgraphic. A corresponding text hint or screen tip provides additional information for that server. Click the server subgraphic to view the IOM information on the right. For more information, see the *CMC Online Help*.

2. Go to **Chassis Overview** and **expand Server Overview** in the system tree. All the servers (1–16) appear in the expanded list. Click the server (slot) you want to view.

   The **Server Status** page (separate from the **Servers Status** page) provides the health status of the server in the chassis and a launch point to the iDRAC Web interface, which is the firmware used to manage the server. For more information, see the *CMC Online Help*.

   NOTE: To use the iDRAC Web interface, you must have an iDRAC user name and password. For more information about iDRAC and the using the iDRAC Web interface, see the *Integrated Dell Remote Access Controller User's Guide*.

Viewing Storage Array Status

To view health status for storage servers, do any of the following:

1. Go to **Chassis Overview** → **Properties** → **Health** .

   The **Chassis Health** page displays a graphical overview of all the servers installed in the chassis. Server health status is indicated by the overlay of the server subgraphic. Move the cursor to hover over an individual server subgraphic. A corresponding text hint or screen tip provides additional information for that server. Click the server subgraphic to view the IOM information on the right. For more information, see the *CMC Online Help*.

2. Go to **Chassis Overview** and expand **Server Overview** in the system tree. All the slots (1–16) appear in the expanded list. Click the slot where the storage array is inserted.

   The Storage Array Status page provides the health status and properties of the storage array. For more information, see the *CMC Online Help*.

Viewing Information and Health Status of All IOMs

To view health status of the IOMs, in the CMC Web interface, do any of the following:

1. Go to **Chassis Overview** → **Properties** → **Health** .

   The **Chassis Health** page is displayed. The lower section of **Chassis Graphics** depicts the rear view of the chassis and contains the health status for the IOMs. IOM health status is indicated by the overlay of the IOM subgraphic. Move the cursor to hover over the individual IOM subgraphic. The text hint provides additional information on that IOM. Click the IOM subgraphic to view the IOM information on the right.

2. Go to **Chassis Overview** → **I/O Module Overview** → **Properties** → **Status**.

   The **I/O Module Status** page provides overviews of all IOMs associated with the chassis. For more information, see the *CMC Online Help*.

Viewing Information and Health Status For Individual IOM

To view health status of the individual IOMs, in the CMC Web interface, do any of the following:

1. Go to **Chassis Overview** → **Properties** → **Health** .

   The **Chassis Health** page is displayed. The lower section of Chassis Graphics depicts the rear view of the chassis and contains the health status for the IOMs. IOM health status is indicated by the overlay of the IOM subgraphic. Move the cursor to hover over the individual IOM subgraphic. The text hint provides additional information on that IOM. Click the IOM subgraphic to view the IOM information on the right.
2. Go to **Chassis Overview** and expand **I/O Module Overview** in the system tree. All the IOMs (1–6) appear in the expanded list. Click the IOM (slot) you want to view.

   The **I/O Module Status** page (separate from the overall **I/O Module Status** page) specific to the IOM slot is displayed. For more information, see the *CMC Online Help*.

Viewing Information and Health Status of Fans

CMC, which controls fan speeds, automatically increases or decreases fan speeds based on system wide events. CMC generates an alert and increases the fan speeds when the following events occur:

- CMC ambient temperature threshold is exceeded.
- A fan fails.
- A fan is removed from the chassis.

NOTE: During updates of CMC or iDRAC firmware on a server, some or all of the fan units in the chassis spin at 100%. This is normal.

To view the health status of the fans, in the CMC Web interface, do any of the following:

1. Go to **Chassis Overview** → **Properties** → **Health** .

   The **Chassis Health** page is displayed. The lower section of chassis graphics provides the rear view of the chassis and contains the health status of the fan. Fan health status is indicated by the overlay of the fan subgraphic. Move the cursor over the fan subgraphic. The text hint provides additional information on the fan. Click the fan subgraphic to view the fan information on the right.
2. Go to **Chassis Overview** → **Fans** → **Properties** .

   The **Fans Status** page provides the status and speed measurements in revolutions per minute, or RPMs, of the fans in the chassis. There can be one or more fans.

   NOTE: In the event of a communication failure between CMC and the fan unit, CMC cannot obtain or display health status for the fan unit.

   For more information, see the *CMC Online Help*.

Viewing iKVM Information and Health Status

The local access KVM module for the Dell M1000e server chassis is called the Avocent Integrated KVM Switch Module, or iKVM.

To view the health status of the iKVMs associated with the chassis, do any of the following:

1. Go to **Chassis Overview** → **Properties** → **Health** .

   The **Chassis Health** page is displayed. The lower section of chassis graphics provides the rear view of the chassis and contains the health status of the iKVM. iKVM health status is indicated by the overlay of the iKVM subgraphic.

Move the cursor over an iKVM subgraphic and a corresponding text hint or screen tip is displayed. The text hint provides additional information for the iKVM. Click the iKVM subgraphic to view the iKVM information on the right.

2. Go to **Chassis Overview** → **iKVM** → **Properties** .

   The **iKVM Status** page displays the status and readings of the iKVM associated with the chassis. For more information, see the *CMC Online Help*.

Viewing PSU Information and Health Status

To view the health status of the Power Supply Units (PSUs) associated with the chassis, do any of the following:

1. Go to **Chassis Overview** → **Properties** → **Health** .

   The **Chassis Health** page is displayed. The lower section of chassis graphics provides the rear view of the chassis and contains the health status of all PSUs. PSU health status is indicated by the overlay of the PSU subgraphic. Use the cursor to hover over an individual PSU subgraphic and a corresponding text hint or screen tip is displayed. The text hint provides additional information on that PSU. Click the PSU subgraphic to view the PSU information on the right.
2. Go to **Chassis Overview** → **Power Supplies**.

   The **Power Supply Status** page displays the status and readings of the PSUs associated with the chassis. It provides the overall power health, system power status, and the power supply redundancy status. For more information, see the *CMC Online Help*.

Viewing Information and Health Status of Temperature Sensors

To view the health status of the temperature sensors:

Go to **Chassis Overview** → **Temperature Sensors**.

The **Temperature Sensors Status** page displays the status and readings of the temperature probes on the entire chassis (chassis and servers). For more information, see the *CMC Online Help*.

NOTE: The temperature probes value cannot be edited. Any change beyond the threshold generates an alert that causes the fan speed to vary. For example, if the CMC ambient temperature probe exceeds threshold, the speed of the fans on the chassis increases.

Viewing LCD Information and Health

To view the health status for the LCD:

1. In the CMC Web interface, in the system tree go to **Chassis Overview**, and then click **Properties** → **Health**.

   The **Chassis Health** page is displayed. The top section of Chassis Graphics depicts the front view of the chassis. LCD health status is indicated by the overlay of the LCD subgraphic.
2. Move the cursor over the LCD subgraphic. The corresponding text hint or screen tip provides additional information on the LCD.
3. Click the LCD subgraphic to view the LCD information on the right. For more information, see the *CMC Online Help*.

6

Configuring CMC

CMC enables you to configure CMC properties, set up users, and set up alerts to perform remote management tasks.

Before you begin configuring the CMC, you must first configure the CMC network settings to allow the CMC to be managed remotely. This initial configuration assigns the TCP/IP networking parameters that enable access to the CMC. For more information, see Setting Up Initial Access to CMC.

You can configure CMC using Web interface or RACADM.

NOTE: When you configure CMC for the first time, you must be logged in as root user to execute RACADM commands on a remote system. Another user can be created with privileges to configure CMC.

After setting up the CMC and performing the basic configuration, you can do the following:

- Modify the network settings if required.
- Configure interfaces to access CMC.
- Configure LED display.
- Setup Chassis Groups if required.
- Configure Servers, IOMs, or iKVM.
- Configure VLAN Settings.
- Obtain the required certificates.
- Add and configure CMC users with privileges.
- Configure and enable e-mail alerts and SNMP traps.
- Set the power cap policy if required.

Related Links

Logging In to CMC
Viewing and Modifying CMC Network LAN Settings
Configuring Network Security Settings
Configuring Virtual LAN Tag Properties for CMC
Configuring Services
Configuring LEDs to Identify Components on the Chassis
Setting Up Chassis Group
Configuring Server
Managing I/O Fabric
Configuring and Using iKVM
Obtaining Certificates
Configuring User Accounts and Privileges
Configuring CMC To Send Alerts
Managing and Monitoring Power
Configuring Multiple CMCs Using RACADM

Viewing and Modifying CMC Network LAN Settings

The LAN settings, such as community string and SMTP server IP address, affect both the CMC and the external settings of the chassis.

If you have two CMCs (active and standby) on the chassis, and they are connected to the network, the standby CMC automatically assumes the network settings of the active CMC in the event of failover.

When IPv6 is enabled at boot time, three router solicitations are sent every four seconds. If external network switches are running the Spanning Tree Protocol (SPT), the external switch ports may be blocked for more than twelve seconds in which the IPv6 router solicitations are sent. In such cases, there may be a period when IPv6 connectivity is limited, until router advertisements are gratuitously sent by the IPv6 routers.

NOTE: Changing the CMC network settings may disconnect your current network connection.

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

Viewing and Modifying CMC Network LAN Settings Using CMC Web Interface

To view and modify the CMC LAN network settings using CMC Web interface:

1. In the system tree, go to **Chassis Overview** and click **Network** → **Network**. The **Network Configuration** page displays the current network settings.
2. Modify the general, IPv4 or IPv6 settings as required. For more information, see the *CMC Online Help*.
3. Click **Apply Changes** for each section to apply the settings.

Viewing and Modifying CMC Network LAN Settings Using RACADM

To view IPv4 settings, use the following subcommands and objects:

- `getniccfg`
- `getconfig`
- cfgCurrentLanNetworking

To view IPv6 settings, use the following subcommands and objects:

- `getconfig`
- cfgIpv6LanNetworking

To view IPv4 and IPv6 addressing information for the chassis, use `getsysinfo` subcommand.

For more information about the subcommands and objects, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC*.

Enabling the CMC Network Interface

To enable/disable the CMC Network Interface for both IPv4 and IPv6, type:

```
racadm config -g cfgLanNetworking -o cfgNicEnable 1
racadm config -g cfgLanNetworking -o cfgNicEnable 0
```

NOTE: The CMC NIC is enabled by default.

To enable/disable the CMC IPv4 addressing, type:

```
racadm config -g cfgLanNetworking -o cfgNicIPv4Enable
1
racadm config -g cfgLanNetworking -o cfgNicIPv4Enable
0
```

NOTE: The CMC IPv4 addressing is enabled by default.

To enable/disable the CMC IPv6 addressing, type:

```
racadm config -g cfgIpv6LanNetworking -o cfgIPv6Enable
1
racadm config -g cfgIpv6LanNetworking -o cfgIPv6Enable
0
```

NOTE: The CMC IPv6 addressing is disabled by default.

By default, for IPv4, the CMC requests and obtains a CMC IP address from the Dynamic Host Configuration Protocol (DHCP) server automatically. You can disable the DHCP feature and specify static CMC IP address, gateway, and subnet mask.

For an IPv4 network, to disable DHCP and specify static CMC IP address, gateway, and subnet mask, type:

```
racadm config -g cfgLanNetworking -o cfgNicUseDHCP 0
racadm config -g cfgLanNetworking -o cfgNicIpAddress <static IP address>
racadm config -g cfgLanNetworking -o cfgNicGateway <static gateway>
racadm config -g cfgLanNetworking -o cfgNicNetmask <static subnet mask>
```

By default, for IPv6, the CMC requests and obtains a CMC IP address from the IPv6 Autoconfiguration mechanism automatically.

For an IPv6 network, to disable the Autoconfiguration feature and specify a static CMC IPv6 address, gateway, and prefix length, type:

```
racadm config -g cfgIPv6LanNetworking -o
cfgIPv6AutoConfig 0
racadm config -g cfgIPv6LanNetworking -o
cfgIPv6Address <IPv6 address>
racadm config -g cfgIPv6LanNetworking -o
cfgIPv6PrefixLength 64
racadm config -g cfgIPv6LanNetworking -o
cfgIPv6Gateway <IPv6 address>
```

Enabling or Disabling DHCP for the CMC Network Interface Address

When enabled, the CMC’s DHCP for NIC address feature requests and obtains an IP address from the Dynamic Host Configuration Protocol (DHCP) server automatically. This feature is enabled by default.

You can disable the DHCP for NIC address feature and specify a static IP address, subnet mask, and gateway. For more information, see Setting Up Initial Access to CMC.

Enabling or Disabling DHCP for DNS IP Addresses

By default, the CMC’s DHCP for DNS address feature is disabled. When enabled, this feature obtains the primary and secondary DNS server addresses from the DHCP server. While using this feature, you do not have to configure static DNS server IP addresses.

To disable the DHCP for DNS address feature and specify static preferred and alternate DNS server addresses, type:

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

To disable the DHCP for DNS address feature for IPv6 and specify static preferred and alternate DNS server addresses, type:

```
racadm config -g cfgIPv6LanNetworking -o
cfgIPv6DNSServersFromDHCP6 0
```

Setting Static DNS IP addresses

NOTE: The Static DNS IP addresses settings are not valid unless the DCHP for DNS address feature is disabled.

For IPv4, to set the preferred primary and secondary DNS IP server addresses, type:

```
racadm config -g cfgLanNetworking -o cfgDNSServer1 <IP-address>
racadm config -g cfgLanNetworking -o cfgDNSServer2 <IPv4-address>
```

For IPv6, to set the preferred and secondary DNS IP Server addresses, type:

```
racadm config -g cfgIPv6LanNetworking -o
cfgIPv6DNSServer1 <IPv6-address>
racadm config -g cfgIPv6LanNetworking -o
cfgIPv6DNSServer2 <IPv6-address>
```

Configuring DNS Settings (IPv4 and IPv6)

- **CMC Registration** — To register the CMC on the DNS server, type:

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

  NOTE: Some DNS servers only register names of 31 characters or fewer. Make sure the designated name is within the DNS required limit.

  NOTE: The following settings are valid only if you have registered the CMC on the DNS server by setting **cfgDNSRegisterRac** to 1.
- **CMC Name** — By default, the CMC name on the DNS server is cmc-<*service tag*>. To change the CMC name on the DNS server, type:

  ```
  racadm config -g cfgLanNetworking -o cfgDNSRacName <name>
  ```

  where `<name>` is a string of up to 63 alphanumeric characters and hyphens. For example: cmc-1, d-345.
- **DNS Domain Name** — The default DNS domain name is a single blank character. To set a DNS domain name, type:

  ```
  racadm config -g cfgLanNetworking -o
  cfgDNSDomainName <name>
  ```

  where `<name>` is a string of up to 254 alphanumeric characters and hyphens. For example: p45, a-tz-1, r-id-001.

Configuring Auto Negotiation, Duplex Mode, and Network Speed (IPv4 and IPv6)

When enabled, the auto negotiation feature determines whether the CMC automatically sets the duplex mode and network speed by communicating with the nearest router or switch. Auto negotiation is enabled by default.

You can disable auto negotiation and specify the duplex mode and network speed by typing:

```
racadm config -g cfgNetTuning -o cfgNetTuningNicAutoneg 0
racadm config -g cfgNetTuning -o cfgNetTuningNicFullDuplex <duplex mode>
```

where:

`<duplex mode>` is 0 (half duplex) or 1 (full duplex, default)

```
racadm config -g cfgNetTuning -o cfgNetTuningNicSpeed <speed>
```

where:

`<speed>` is 10 or 100 (default).

Setting the Maximum Transmission Unit (MTU) (IPv4 and IPv6)

The MTU property allows you to set a limit for the largest packet that can be passed through the interface. To set the MTU, type:

```
racadm config -g cfgNetTuning -o cfgNetTuningMtu <mtu>
```

where `<mtu>` is a value between 576–1500 (inclusive; default is 1500).

NOTE: IPv6 requires a minimum MTU of 1280. If IPv6 is enabled, and `cfgNetTuningMtu` is set to a lower value, the CMC uses an MTU of 1280.

Configuring Network Security Settings

You can configure the network security settings for IPv4 only.

Configuring Network Security Settings Using CMC Web Interface

NOTE: To perform the following steps, you must have **Chassis Configuration Administrator** privilege.

To configure the network security settings using CMC Web interface:

1. In the system tree, go to **Chassis Overview** and click **Network** → **Network**. The **Network Configuration** page is displayed.
2. In the IPv4 Settings section, click **Advanced Settings**. The **Network Security** page is displayed.
3. Specify the IP range and IP blocking values. For more information, see the *CMC Online Help*.
4. Click **Apply** to save your settings.

Configuring CMC Network Security Settings Using RACADM

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**

A login from the incoming IP address is allowed only if both the following are identical:

- **cfgRacTuneIpRangeMask** bit-wise and with incoming IP address
- **cfgRacTuneIpRangeMask** bit-wise and with **cfgRacTuneIpRangeAddr**

Configuring Virtual LAN Tag Properties for CMC

VLANs are used to allow multiple virtual LANs to co-exist on the same physical network cable and to segregate the network traffic for security or load management purposes. When you enable the VLAN functionality, each network packet is assigned a VLAN tag.

Configuring Virtual LAN Tag Properties for CMC Using Web Interface

To configure VLAN for CMC using the CMC Web interface:

1. Go to any of the following pages:

   – In the system tree, go to **Chassis Overview** and click **Network** → **VLAN**.
   – In the system tree, go to **Chassis Overview** → **Server Overview** and click **Network** → **VLAN**.

   The **VLAN Tag Settings** page is displayed. VLAN tags are chassis properties. They remain with the chassis even when a component is removed.

2. In the **CMC** section, enable VLAN for CMC, set the priority and assign the ID. For more information about the fields, see the *CMC Online Help*.

3. Click Apply. The VLAN tag settings are saved.
   You can also access this page from the **Chassis Overview** → **Servers** → **Setup** → **VLAN** subtab.

Configuring Virtual LAN Tag Properties for CMC Using RACADM

1. Enable the VLAN capabilities of the external chassis management network:

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

2. Specify the VLAN ID for the external chassis management network:

   ```
   racadm config -g cfgLanNetworking -o cfgNicVlanID <VLAN id>
   ```

   The valid values for `<VLAN id>` are 1– 4000 and 4021– 4094. Default is 1.

   For example:

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

3. Then, specify the VLAN priority for the external chassis management network:

   ```
   racadm config -g cfgLanNetworking -o
   cfgNicVLanPriority <VLAN priority>
   ```

   The valid values for `<VLAN priority>` are 0–7. Default is 0.

   For example:

   ```
   racadm config -g cfgLanNetworking -o
   cfgNicVLanPriority 7
   ```

   You can also specify both the VLAN ID and the VLAN priority with a single command:

   ```
   racadm setniccfg -v <VLAN id> <VLAN priority>
   ```

   For example:

   ```
   racadm setniccfg -v 1 7
   ```

4. To remove the CMC VLAN, disable the VLAN capabilities of the external chassis management network:

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

   You can also remove the CMC VLAN using the following command:

   ```
   racadm setniccfg -v
   ```

Configuring Services

You can configure and enable the following services on CMC:

- CMC Serial console — Enable access to CMC using the serial console.
- Web Server — Enable access to CMC Web interface. If you disable the option, use local RACADM to re-enable the Web Server, since disabling the Web Server also disables remote RACADM.
- SSH — Enable access to CMC through firmware RACADM.
- Telnet — Enable access to CMC through firmware RACADM
- RACADM — Enable access to CMC using RACADM.
- SNMP — Enable CMC to send SNMP traps for events.
- Remote Syslog — Enable CMC to log events to a remote server.

CMC includes a Web server that is configured to use the industry-standard SSL security protocol to accept and transfer encrypted data from and to clients over the Internet. The Web server includes a Dell self-signed SSL digital certificate (Server ID) and is responsible for accepting and responding to secure HTTP requests from clients. This service is required by the Web interface and remote RACADM CLI tool for communicating with CMC.

If the Web server resets, wait at least one minute for the services to become available again. A Web server reset usually happens as a result of any of the following events:

- Network configuration or network security properties are changed through the CMC Web user interface or RACADM.
- Web Server port configuration is changed through the Web user interface or RACADM.
- CMC is reset.
- A new SSL server certificate is uploaded.

NOTE: To modify Service settings, you must have **Chassis Configuration Administrator** privilege.

Remote syslog is an additional log target for CMC. After you configure the remote syslog, each new log entry generated by CMC is forwarded to the destination(s).

NOTE: Since the network transport for the forwarded log entries is UDP, there is no guaranteed delivery of log entries, nor is there any feedback to CMC whether the log entries were received successfully.

Configuring Services Using CMC Web Interface

To configure CMC services using CMC Web interface:

1. In the system tree, go to **Chassis Overview**, and then click **Network** → **Services**. The **Services** page is displayed.
2. Configure the following services as required:
   - CMC serial console
   - Web server
   - SSH
   - Telnet
   - Remote RACADM
   - SNMP
   - Remote Syslog

   For information about the fields, see *CMC Online Help*.

3. Click **Apply**, and then update all default time outs and maximum time out limits.

Configuring Services Using RACADM

To enable and configure the various services, use the following RACADM objects:

- `cfgRacTuning`
- `cfgRacTuneRemoteRacadmEnable`

For more information about these objects, see *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at **support.dell.com/manuals**.

If the firmware on the server does not support a feature, configuring a property related to that feature displays an error. For example, using RACADM to enable remote syslog on an unsupported iDRAC displays an error message.

Similarly, when displaying the iDRAC properties using the RACADM getconfig command, the property values are displayed as N/A for an unsupported feature on the server.

For example:

```
$ racadm getconfig -g cfgSessionManagement -m server-1
# cfgSsnMgtWebServerMaxSessions=N/A
# cfgSsnMgtWebServerActiveSessions=N/A
# cfgSsnMgtWebServerTimeout=N/A
# cfgSsnMgtSSHMaxSessions=N/A
# cfgSsnMgtSSHActiveSessions=N/A
# cfgSsnMgtSSHTimeout=N/A
# cfgSsnMgtTelnetMaxSessions=N/A
# cfgSsnMgtTelnetActiveSessions=N/A
# cfgSsnMgtTelnetTimeout=N/A
```

Configuring CMC Extended Storage Card

You can enable or repair the optional Removable Flash Media for use as an extended non-volatile storage. Some CMC features depend on extended nonvolatile storage for their operation.

To enable or repair the Removable Flash Media using the CMC Web interface:

1. In the System tree, go to **Chassis Overview**, and then click **Chassis Controller** → **Flash Media**. The Removable Flash Media page is displayed.
2. From the drop-down menu, select one of the following as required:

   – Use flash media for storing chassis data
   – Repair active controller media
   – Begin replicating data between media
   – Stop replicating data between media
   – Stop using flash media for storing chassis data

   For more information about these options, see the *CMC Online Help*.
3. Click **Apply** to apply the selected option.

   If two CMCs are present in the chassis, both CMCs must contain flash media. CMC features which depend on flash media (except for Flexaddress) do not function properly until the Dell-authorized media is installed and enabled on this page.

Setting Up Chassis Group

CMC enables you to monitor multiple chassis from a single lead chassis. When a Chassis Group is enabled, CMC in the lead chassis generates a graphical display of the status of the lead chassis and all member chassis within the Chassis Group.

The Chassis group features are:

- The **Chassis Group** page displays images portraying the front and back of each chassis, a set for the leader and a set for each member.
- Health concerns for the leader and members of a group are recognized by red or yellow overlays and an X or an ! on the component with the symptoms. Details are visible below the chassis image when you click the chassis image or **Details**.
- Quick Launch links are available for opening member chassis's or server's web pages.
- A blade and Input/Output inventory is available for a group.
- A selectable option is available to synchronize a new member's properties to the leader's properties when the new member is added to the group.

A Chassis Group may contain a maximum of eight members. Also, a leader or member can only participate in one group. You cannot join a chassis, either as a leader or member, that is part of a group to another group. You can delete the chassis from a group and add it later to a different group.

To set up the Chassis Group using the CMC Web interface:

1. Log in with chassis administrator privileges to the chassis planned as the leader.
2. Click **Setup** → **Group Administration**. The **Chassis Group** page is displayed.
3. In the **Chassis Group** page, under **Role**, select **Leader**. A field to add the group name is displayed.
4. Enter the group name in the **Group Name** field, and then click **Apply**.

   NOTE: The same rules that apply for a domain name apply to the group name.

   When the Chassis Group is created, the GUI automatically switches to the **Chassis Group** page. The system tree indicates the group by the Group Name and the lead chassis and the unpopulated member chassis appear in the system tree.

Related Links

Adding Members to Chassis Group
Removing a Member from the Leader
Disbanding a Chassis Group
Disabling an Individual Member at the Member Chassis
Launching a Member Chassis's or Server's Web page
Synchronizing a New Member With Leader Chassis Properties

Adding Members to Chassis Group

After the Chassis Group is setup, you can add members to the group:.

1. Login with chassis administrator privileges to the leader chassis.
2. Select the Lead chassis in the tree.
3. Click **Setup** → **Group Administration**.
4. Under **Group Management**, enter the member's IP address or DNS name in the **Hostname/IP Address** field.
5. Enter a user name with chassis administrator privileges on the member chassis, in the **Username** field.

6. Enter the corresponding password in the **Password** field.
7. Optionally, select **Sync New Member with Leader Properties** to push leader properties to the member. For more information, see Synchronizing a New Member With Leader Chassis Properties.
8. Click **Apply**.
9. Repeat step 4 through step 8 to add a maximum of eight members. The new members' Chassis Names appear in the **Members** dialog box.

   The status of the new member is displayed by selecting the Group in the tree. Details are available by clicking on the chassis image or the details button.

   NOTE: The credentials entered for a member are passed securely to the member chassis, to establish a trust relationship between the member and lead chassis. The credentials are not persisted on either chassis, and are never exchanged again after the initial trust relationship is established.

Removing a Member from the Leader

You can remove a member from the group from the lead chassis. To remove a member:

1. Login with chassis administrator privileges to the leader chassis.
2. Select the Lead chassis in the tree.
3. Click **Setup** → **Group Administration**.
4. From the **Remove Members** list, select the member's name or names to be deleted, and then click **Apply**.

   The lead chassis then communicates to the member or members, if more than one is selected, that it has been removed from the group. The member name is removed. The member chassis may not receive the message, if a network issue prevents contact between the leader and the member. In this case, disable the member from the member chassis to complete the removal.

Related Links

Disabling an Individual Member at the Member Chassis

Disbanding a Chassis Group

To disband a chassis group from the lead chassis:

1. Login with administrator privileges to the leader chassis.
2. Select the Lead chassis in the tree.
3. Click **Setup** → **Group Administration**.
4. In the **Chassis Group** page, under **Role**, select **None**, and then click **Apply**.

   The lead chassis then communicates to all the members that they have been removed from the group. Finally the lead chassis discontinues its role. It can now be assigned as a member or a leader of another group.

   The member chassis may not receive the message, if a network issue prevents contact between the leader and the member. In this case, disable the member from the member chassis to complete the removal.

Disabling an Individual Member at the Member Chassis

Sometimes a member cannot be removed from a group by the lead chassis. This can happen if network connectivity to the member is lost. To remove a member from a group at the member chassis:

1. Login with chassis administrator privileges to the member chassis.
2. Click **Setup** → **Group Administration**.

3. Select **None**, and then click **Apply**.

Launching a Member Chassis's or Server's Web page

Links to a member chassis's Web page, a server's Remote Console or the server iDRAC's Web page within the group are available through the lead chassis's group page. You can use the same user name and password that was used to log in to the lead chassis, to log in to the member device. If the member device has the same login credentials then no additional login is required. Otherwise, the user is directed to the member device's login page.

To navigate to member devices:

1. Login to the lead chassis.
2. Select **Group: name** in the tree.
3. If a member CMC is the required destination, select **Launch CMC** for the required chassis.

   If a server in a chassis is the required destination:

   a) Select the image of the destination chassis.
   b) In the chassis image that appears under the **Health and Alerts** pane, select the server.
   c) In the box labeled **Quick Links**, select the destination device. A new window is displayed with the destination page or login screen.

Synchronizing a New Member With Leader Chassis Properties

You can apply the properties from the leader to a newly added member chassis of a group. To synchronize a new member with the leader properties:

1. Login with administrator privileges to the leader chassis.
2. Select the Lead chassis in the tree.
3. Click **Setup** → **Group Administration**.
4. While adding a new member to the group, in the **Chassis Group** page, select **Sync New Member with Leader Properties**.
5. Click **Apply**. The member takes on the properties of the leader.

The following configuration service properties of several systems within the chassis are affected after synchronization:

Table 8. : Configuration Service Properties

Property	Navigation
SNMP Configuration	In the system tree, go to **Chassis Overview** and click **Network** → **Services** → **SNMP**for details.
Chassis remote logging	In the system tree, go to **Chassis Overview** and click **Network** → **Services** → **Remote Syslog** for details.
User authentication using LDAP and Active Directory services	In the system tree, go to **Chassis Overview** and click **User Authentication** → **Directory Services** for details.
Chassis alerts	In the system tree, go to **Chassis Overview** and click **Alerts** for details.

Server Inventory for MCM group

The Chassis Group Health page displays all the member chassis and allows you to save the server inventory report to a file, using standard browser download capability. The report contains data for:

- All servers currently in all the group chassis (including the leader.)
- Empty slots and extension slots (including full height and double width blades.)

Saving Server Inventory Report

To save the server inventory report using CMC Web interface:

1. In the system tree, select the **Group**. The **Chassis Group Health** page is displayed.
2. Click **Save Inventory Report**. The **File Download** dialog box is displayed prompting you to open or save the file.
3. Click **Save** and specify the path and file name for the blade inventory report.

   NOTE: The Chassis Group leader and Chassis Group member chassis, and the blades in the associated chassis, must be On to get the most accurate blade inventory report.

Exported Data

The server inventory report contains data that was most recently returned by each Chassis Group member during the Chassis Group leader's normal polling (once every 30s.)

To get the most accurate server inventory report:

- The Chassis Group leader chassis and all Chassis Group member chassis must be in **Chassis Power State On**.
- All servers in the associated chassis must be powered on.

The inventory data for the associated chassis and servers may be missing in inventory report, if a subset of the Chassis Group member chassis are:

- In **Chassis Power State Off**
- Powered off

  NOTE: If a server is inserted while the chassis is powered off, the model number is not displayed anywhere in the Web interface until the chassis is powered back.

The following table lists the specific data fields and specific requirements for fields to be reported for each server:

Table 9. : Blade Inventory Field Descriptions

Data Field	Example
Chassis Name	Data Center Chassis Leader
Chassis IP Address	192.168.0.1
Slot Location	1
Slot Name	SLOT-01
Host Name	Corporate Webserver **NOTE:** Requires a Server Administrator agent running on the Server; otherwise shown as blank.

Data Field	Example
Operating System	Windows Server 2008 **NOTE:** Requires a Server Administrator agent running on the Server; otherwise shown as blank.
Model	PowerEdgeM610
Service Tag	1PB8VF1
Total System Memory	4.0 GB **NOTE:** Requires CMC 4.0 (or higher) on member; otherwise shown as blank.
# of CPUs	2 **NOTE:** Requires CMC 4.0 (or higher) on member; otherwise shown as blank.
CPU Info	Intel (R) Xeon (R) CPU E5502 @1.87GHzn **NOTE:** Requires CMC 4.0 (or higher) on member; otherwise shown as blank.

Data Format

The inventory report is generated in a **.CSV** file format such that it can be imported to various tools, such as Microsoft Excel. The inventory report **.CSV** file can be imported into the template by selecting the **Data** → **From Text** in MS Excel. After the inventory report is imported into MS Excel, and if a message is displayed prompting for additional information, select comma-delimited to import the file into MS Excel.

Obtaining Certificates

The following table lists the types of certificates based on the login type.

Table 10. : Types of Login and Certificate

Login Type	Certificate Type	How to Obtain
Single Sign-on using Active Directory	Trusted CA certificate	Generate a CSR and get it signed from a Certificate Authority
Smart Card login as Active Directory user	• User certificate • Trusted CA certificate	• User Certificate — Export the smart card user certificate as Base64-encoded file using the card management software provided by the smart card vendor. • Trusted CA certificate — This certificate is issued by a CA.
Active Directory user login	Trusted CA certificate	This certificate is issued by a CA.
Local User login	SSL Certificate	Generate a CSR and get it signed from a trusted CA

Login Type	Certificate Type	How to Obtain
		NOTE: CMC ships with a default self-signed SSL server certificate. The CMC Web server and Virtual Console use this certificate.

Related Links

Secure Sockets Layer (SSL) Server Certificates

Secure Sockets Layer (SSL) Server Certificates

CMC 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.

SSL allows an SSL-enabled system to 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.

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

The CMC Web server includes a Dell self-signed SSL digital certificate (Server ID). To ensure high security over the Internet, replace the Web server SSL certificate by submitting a request to CMC to generate a new Certificate Signing Request (CSR).

Certificate Signing Request (CSR)

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

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 certificate authority receives your CSR, they review and verify the information the CSR contains. If the applicant meets the certificate authority’s security standards, the certificate authority issues a certificate to the applicant that uniquely identifies that applicant for transactions over networks and on the Internet.

After the certificate authority approves the CSR and sends you a certificate, you must upload the certificate to the CMC firmware. The CSR information stored on the CMC firmware must match the information contained in the certificate.

NOTE: To configure SSL settings for CMC, you must have **Chassis Configuration Administrator** privilege.

NOTE: Any server certificate you upload must be current (not expired) and signed by a certificate authority.

Related Links

Generating a New Certificate Signing Request

Uploading Server Certificate

Viewing Server Certificate

Generating a New Certificate Signing Request

To ensure security, it is strongly recommended that you obtain and upload a secure server certificate to CMC. Secure server certificates ensure the identity of a remote system and that information exchanged with the remote system cannot be viewed or changed by others. Without a secure server certificate, CMC is vulnerable to access from unauthorized users.

To obtain a secure server certificate for CMC, you must submit a Certificate Signing Request (CSR) to a certificate authority of your choice. A CSR is a digital request for a signed, secure server certificate containing information about your organization and a unique, identifying key.

After generating the CSR, you are prompted to save a copy to your management station or shared network, and the unique information used to generate the CSR is stored on CMC. This information is used later to authenticate the server certificate you receive from the certificate authority. After you receive the server certificate from the certificate authority, you must then upload it to CMC.

NOTE: For CMC to accept the server certificate returned by the certificate authority, authentication information contained in the new certificate must match the information that was stored on CMC when the CSR was generated.

CAUTION: When a new CSR is generated, it overwrites any previous CSR on CMC. If a pending CSR is overwritten before its server certificate is granted from a certificate authority, CMC does not accept the server certificate because the information it uses to authenticate the certificate has been lost. Take caution when generating a CSR to prevent overwriting any pending CSR.

Generating a New Certificate Signing Request Using Web Interface

To generate a CSR using the CMC Web interface:

1. In the system tree, go to **Chassis Overview**, and then click **Network** → **SSL**. The **SSL Main Menu** is displayed.
2. Select **Generate a New Certificate Signing Request (CSR)** and click **Next**. The **Generate Certificate Signing Request (CSR)** page is displayed.
3. Type a value for each CSR attribute value.
4. Click **Generate**. A **File Download** dialog box appears.
5. Save the **csr.txt** file to your management station or shared network. (You may also open the file at this time and save it later.) You must later submit this file to a certificate authority.

Generating CSR Using RACADM

To generate a CSR, use the objects in `cfgRacSecurityData` group to specify the values and use the `sslcsrgen` command to generate the CSR. For more information, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at **support.dell.com/manuals**.

Uploading Server Certificate

After generating a CSR, you can upload the signed SSL server certificate to the CMC firmware. CMC resets after the certificate is uploaded. CMC accepts only X509, Base 64 encoded Web server certificates.

CAUTION: During the certificate upload process, CMC is not available.

Uploading Server Certificate Using CMC Web Interface

To upload a server certificate using the CMC Web interface:

1. In the system tree, go to **Chassis Overview**, and then click **Network** → **SSL**. The **SSL Main Menu** is displayed.
2. Select **Upload Server Certificate Based on Generated CSR** option and click **Next**.
3. Click **Choose File** and specify the certificate file.
4. Click **Apply**. If the certificate is invalid, an error message is displayed.

   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.

Uploading Server Certificate Using RACADM

To upload the SSL server certificate, use the `sslcertupload` command. For more information, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at **support.dell.com/manuals**.

Uploading Webserver Key and Certificate

You can upload a Web server key and a server certificate for the Web server key. The server certificate is issued by the Certificate Authority (CA).

The Web server certificate is an essential component used by the SSL encryption process. It authenticates itself to an SSL-enabled client, and allows the client to authenticate itself to the server, thereby enabling both the systems to establish an encrypted connection.

NOTE: To upload a Web server key and server certificate, you must have **Chassis Configuration Administrator** privileges.

Uploading Webserver Key and Certificate Using CMC Web Interface

To upload a webserver key and certificate using the CMC Web interface:

1. In the system tree, go to **Chassis Overview** and click **Network** → **SSL**. The **SSL Main Menu** is displayed.
2. Select **Upload Web Key and Certificate** option and click **Next**.
3. Specify the Private Key File and the Certificate File by clicking **Choose File**.
4. After both the files are uploaded, click **Apply**. If the Web server key and certificate do not match, an error message is displayed.

   NOTE: Only X509, Base-64 encoded certificates are accepted by CMC. Certificates using other encoding schemes such as DER, are not accepted. Uploading a new certificate replaces the default certificate you received with your CMC.

   CMC resets and becomes temporarily unavailable after the certificate has been uploaded successfully. To avoid disconnecting other users during a reset, notify authorized users who might log into CMC and check for active sessions in the **Sessions** page under the **Network** tab.

Uploading Webserver Key and Certificate Using RACADM

To upload SSL key from the client to iDRAC, type the following command:

```
racadm sslkeyupload -t <type> -f <filename>
```

For more information, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at **support.dell.com/manuals**.

Viewing Server Certificate

You can view the SSL server certificate that is currently being used in CMC.

Viewing Server Certificate Using Web Interface

In the CMC Web interface, go to **Chassis Overview** → **Network** → **SSL** , select **View Server Certificate** and click Next. The View Server Certificate page displays the SSL server certificate currently in use. For more information, see CMC Online Help.

Viewing Server Certificate Using RACADM

To view the SSL server certificate, use the `sslcertview` command. For more information, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at **support.dell.com/manuals**.

Configuring Multiple CMCs Using RACADM

Using RACADM, you can configure one or more CMCs with identical properties.

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

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

1. Use RACADM to query the target CMC that contains the desired configuration.

   NOTE: The generated configuration file is **myfile.cfg**. You can rename the file. The **.cfg** file does not contain user passwords. When the **.cfg** file is uploaded to the new CMC, you must re-add all passwords.
2. Open a Telnet/SSH text console to the CMC, log in, and type:

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

   NOTE: Redirecting the CMC configuration to a file using `getconfig -f` is only supported with the remote RACADM interface.
3. Modify the configuration file using a plain-text editor (optional). Any special formatting characters in the configuration file may corrupt the RACADM database.
4. Use the newly created configuration file to modify a target CMC. At the command prompt, type:

   ```
   racadm config -f myfile.cfg
   ```
5. Reset the target CMC that was configured. At the command prompt, type:

   ```
   racadm reset
   ```

   The `getconfig -f myfile.cfg` subcommand (step 1) requests the CMC configuration for the active CMC and generates the **myfile.cfg** file. If required, you can rename the file or save it to a different location.

   You can use the getconfig command 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 other CMCs. The Server Administrator uses the `config` command to synchronize the user and password database.

Related Links

Creating a CMC Configuration File

Creating a CMC Configuration File

The CMC configuration file, **<filename>.cfg**, is used with the `racadm config -f <filename>.cfg`command to create a simple text file. The command allows you to build a configuration file (similar to a **.ini** file) and configure the CMC from this file.

You may use any file name, and the file does not require a **.cfg** extension (although it is referred to by that designation in this subsection).

NOTE: For more information about the `getconfig` subcommand, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC*.

RACADM parses the **.cfg** file when it is first loaded onto the CMC 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 message explains the problem. The entire file is parsed for correctness, and all errors display. Write commands are not transmitted to the CMC if an error is found in the **.cfg** file. You must correct all errors before any configuration can take place.

To check for errors before you create the configuration file, use the `–c` option with the `config` subcommand. With the `–c` option, `config` only verifies syntax and does not write to the CMC.

Follow these guidelines when you create a **.cfg** file:

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

  The parser reads in all of the indexes from the CMC for that group. Any objects within that group are modifications when the CMC is configured. If a modified object represents a new index, the index is created on the CMC during configuration.

- You cannot specify a desired index in a **.cfg** file.

  Indexes may be created and deleted. Over time the group may become fragmented with used and unused indexes. If an index is present, it is modified. If an index is not present, the first available index is used.

  This method allows flexibility when adding indexed entries where you do not need to make exact index matches between all the CMCs being managed. New users are added to the first available index. A **.cfg** file that parses and runs correctly on one CMC may not run correctly on another if all indexes are full and you must add a new user.

- Use the `racresetcfg` subcommand to configure both CMCs with identical properties.

  Use the `racresetcfg` subcommand to reset the CMC to original defaults, and then run the `racadm config -f <filename>.cfg` command. Ensure that the **.cfg** file includes all desired objects, users, indexes, and other parameters. For a complete list of objects and groups, see the database property chapter of the *RACADM Command Line Reference Guide for iDRAC6 and CMC*.

  CAUTION: Use the `racresetcfg` subcommand to reset the database and the CMC Network Interface 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.

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

Related Links

Parsing Rules

Parsing Rules

- Lines that start with a hash character (#) 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 their strings. 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 CMC, without adding escape characters.

  For example:

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

- All group entries must be surrounded by open- and close-brackets ([and]).

  The starting [character that denotes a group name must be 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 database property chapter of the *RACADM Command Line Reference Guide for iDRAC6 and CMC*. The following example displays a group name, object, and the object's property value:

  ```
  [cfgLanNetworking] -{group name}
  cfgNicIpAddress=143.154.133.121 {object name}
  {object value}
  ```

- 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 = (for example, a second =, a #, [,], and so on) is taken as-is. These characters are valid modem chat script characters.

  ```
  [cfgLanNetworking] -{group name}
  cfgNicIpAddress=143.154.133.121 {object value}
  ```

- The **.cfg** parser ignores an index object entry.

  You cannot specify which index is used. If the index already exists, it is either used or the new entry is created in the first available index for that group.

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

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

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

- The line for an indexed group cannot be deleted from a **.cfg** file. If you do delete the line with a text editor, RACADM stops when it parses the configuration file and alert you of the error.

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

  ```
  racadm config -g <groupname>  -o <objectname> -i <index 1-16> ""
  ```

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

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

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

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

  ```
  [cfgUserAdmin]
  cfgUserAdminUserName= <USER_NAME>
  ```

- When using remote RACADM to capture the configuration groups into a file, if a key property within a group is not set, the configuration group is not saved as part of the configuration file. If these configuration groups are needed to be cloned onto other CMCs, the key property must be set before executing the `getconfig -f` command. Alternatively, you can manually enter the missing properties into the configuration file after running the `getconfig -f` command. This is true for all the racadm indexed groups.

  This is the list of the indexed groups that exhibit this behavior and their corresponding key properties:

  - cfgUserAdmin — cfgUserAdminUserName
  - cfgEmailAlert — cfgEmailAlertAddress
  - cfgTraps — cfgTrapsAlertDestIPAddr
  - cfgStandardSchema — cfgSSADRoleGroupName
  - cfgServerInfo — cfgServerBmcMacAddress

Modifying the CMC IP Address

When you modify the CMC 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.

Example:

```
#
# Object Group "cfgLanNetworking"
#
[cfgLanNetworking]
cfgNicIpAddress=10.35.10.110
cfgNicGateway=10.35.10.1
```

This file is 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 updates 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 with the command, `racadm getconfig -f <myfile> .cfg`.

NOTE: *Anchor* is a reserved word and should not be used in the **.cfg** file.

Viewing and Terminating CMC Sessions

You can view the number of users currently logged in to iDRAC7 and terminate the user sessions.

NOTE: To terminate a session, you must have **Chassis Configuration Administrator** privilege.

Viewing and Terminating CMC Sessions Using Web Interface

To view or terminate a session using Web interface:

1. In the system tree, go to **Chassis Overview**. and click **Network** → **Sessions**.

   The **Sessions** page is displays the session ID, username, IP address, and session type. For more information about these properties, see the *CMC Online Help*.
2. To terminate the session, click **Terminate** for a session.

Viewing and Terminating CMC Sessions Using RACADM

You must have administrator privileges to terminate CMC sessions using RACADM.

To view the current user sessions, use the `getssninfo` command.

To terminate a user session, use the `closessn` command.

For more information about these commands, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at **support.dell.com/manuals**.

7

Configuring Server

You can do the following for the server:

- Configuring Slot Names
- Configuring iDRAC Network Settings
- Configuring iDRAC VLAN Tag Settings
- Setting First Boot Device
- Configuring Server FlexAddress
- Configuring Remote File Share
- Configuring BIOS Settings Using Server Clone

Configuring Slot Names

Slot names are used to identify individual servers. When choosing slot names, the following rules apply:

- Names may contain a **maximum of 15** non-extended ASCII characters (ASCII codes 32 through 126).
- Slot names must be unique within the chassis. No two slots may have the same name.
- Strings are not case-sensitive. `Server-1, server-1, and SERVER-1` are equivalent names.
- Slot names must not begin with the following strings:
  - `Switch-`
  - `Fan-`
  - `PS-`
  - `KVM`
  - `DRAC-`
  - `MC-`
  - `Chassis`
  - `Housing-Left`
  - `Housing-Right`
  - `Housing-Center`
- The strings `Server-1` through `Server-16` may be used, but only for the corresponding slot. For example, `Server-3` is a valid name for slot 3, but not for slot 4. Note that `Server-03` is a valid name for any slot.

  NOTE: To change a slot name, you must have **Chassis Configuration Administrator** privilege.

The slot name setting in the Web interface resides on CMC only. If a server is removed from the chassis, the slot name setting does not remain with the server.

The slot name setting does not extend to the optional iKVM. The slot name information is available through the iKVM FRU.

The slot name setting in the CMC Web interface always overrides any change you make to the display name in the iDRAC interface.

To edit a slot name using the CMC Web interface:

1. In the system tree, go to **Chassis Overview** → **Server Overview** and then click **Setup** → **Slot Names**. The **Slot Names** page is displayed.
2. In the **Slot Name** field, edit the slot name. Repeat this step for each slot you want to rename.
3. To use the server's host name as slot name, select **Use Host Name** for the **Slot Name** option. This override the static slot names with the server's Host Name (or system name), if it is available. This requires the OMSA agent to be installed on the server. For more details on the OMSA agent, see the *Dell OpenManage Server Administrator User's Guide*.
4. Click **Apply** to save the settings.
5. To restore the default slot name (**SLOT-01** to **SLOT-16**, based on the server's slot position) to the server, click **Restore Default Value**.

Configuring iDRAC Network Settings

You can configure installed or newly inserted server's iDRAC network configuration settings. A user can configure one or more installed iDRAC devices. The user can also configure the default iDRAC network configuration settings and root password for severs that are installed later; these default settings are the iDRAC QuickDeploy settings.

For more information about iDRAC, see the *iDRAC7 User's Guide* at **support.dell.com/manuals**.

Related Links

Configuring iDRAC QuickDeploy Network Settings
Modifying iDRAC Network Settings for Individual Server iDRAC
Modifying iDRAC Network Settings Using RACADM

Configuring iDRAC QuickDeploy Network Settings

Use the QuickDeploy Settings to configure the network settings for newly inserted servers. After enabling QuickDeploy, the QuickDeploy settings are applied to servers when that server is installed.

To enable and set the iDRAC QuickDeploy settings using the CMC Web interface:

1. In the system tree, go to **Server Overview**, and then click **Setup** → **iDRAC**. The **Deploy iDRAC** page is displayed.
2. In the **QuickDeploy Settings** section, specify the settings mentioned in the following table.

Table 11. : QuickDeploy Settings

Setting	Description
QuickDeploy Enabled	Enables or disables the **QuickDeploy** feature that automatically applies the iDRAC settings configured on this page to newly inserted servers; the auto configuration must be confirmed locally on the LCD panel. **NOTE:** This includes the root user password if the **Set iDRAC Root Password on Server Insertion** box is checked. By default, this option is disabled.
Set iDRAC Root Password on Server Insertion	Specifies whether a server's iDRAC root password must be changed to the value provided in the **iDRAC Root Password** field when the server is inserted.
iDRAC Root Password	When **Set iDRAC Root Password on Server Insertion** and **QuickDeploy Enabled** options are selected, this

Setting	Description
	password value is assigned to a server's iDRAC root user password when the server is inserted into chassis. The password can have 1 to 20 printable (including spaces) characters.
Confirm iDRAC Root Password	Verifies the password entered into the **iDRAC Root Password** field.
Enable iDRAC LAN	Enables or disables the iDRAC LAN channel. By default, this option is disabled.
Enable iDRAC IPv4	Enables or disables IPv4 on iDRAC. By default, this option is enabled.
Enable iDRAC IPMI over LAN	Enables or disables the IPMI over LAN channel for each iDRAC present in the chassis.By default, it is disabled.
Enable iDRAC DHCP	Enables or disables DHCP for each iDRAC present in the chassis. If this option is enabled, the fields **QuickDeploy IP**, **QuickDeploy Subnet Mask**, and **QuickDeploy Gateway** are disabled, and cannot be modified since DHCP is used to automatically assign these settings for each iDRAC. By default, this option is disabled.
Starting iDRAC IPv4 Address (Slot 1)	Specifies the static IP address of iDRAC in the server, in slot 1 of the enclosure. The IP address of each subsequent iDRAC is incremented by 1 for each slot from slot 1's static IP address. In the case where the IP address plus the slot number is greater than the subnet mask, an error message is displayed. **NOTE:** The subnet mask and the gateway are not incremented like the IP address. For example, if the starting IP address is `192.168.0.250` and the subnet mask is `255.255.0.0` then the QuickDeploy IP address for slot 15 is `192.168.0.265`. If the subnet mask were `255.255.255.0`, the `QuickDeploy IP address range is not fully within QuickDeploy Subnet` error message is displayed when you click the **Save QuickDeploy Settings** or **Auto-Populate Using QuickDeploy Settings**.
iDRAC IPv4 Netmask	Specifies the QuickDeploy subnet mask that is assigned to all newly inserted servers.
iDRAC IPv4 Gateway	Specifies the QuickDeploy default gateway that is assigned to all iDRAC present in the chassis.
Enable iDRAC IPv6	Enables IPv6 addressing for each iDRAC present in the chassis that is IPv6 capable.
Enable iDRAC IPv6 Autoconfiguration	Enables the iDRAC to obtain IPv6 settings (address and prefix length) from a DHCPv6 server and also enables

Setting	Description
	stateless address auto configuration. By default, this option is enabled.
iDRAC IPv6 Gateway	Specifies the default IPv6 gateway to be assigned to the iDRACs. The default value is "::".
iDRAC IPv6 Prefix Length	Specifies the prefix length to be assigned for the IPv6 addresses on the iDRAC. The default value is 64.

3. Click **Save QuickDeploy Settings** to save the settings. If you have made changes to the iDRAC network setting, click **Apply iDRAC Network Settings** to deploy the settings to the iDRAC.

   The QuickDeploy feature only executes when it is enabled, and a server is inserted in the chassis. If **Set iDRAC Root Password on Server Insertion** and **QuickDeploy Enabled** are enabled, the user is prompted using the LCD interface to allow or not allow the password change. If there are network configuration settings that differ from the current iDRAC settings, the user is prompted to either accept or not accept the changes.

   NOTE: When there is a LAN or IPMI over LAN difference, the user is prompted to accept the QuickDeploy IP address setting. If the difference is the DHCP setting, the user is prompted to accept the DHCP QuickDeploy setting.

   To copy the QuickDeploy settings into the **iDRAC Network Settings** section, click **Auto-Populate Using QuickDeploy Settings**. The QuickDeploy network configurations settings are copied into the corresponding fields in the **iDRAC Network Configuration Settings** table.

   NOTE: Changes made to QuickDeploy fields are immediate, but changes made to one or more iDRAC server network configuration settings may require a couple of minutes to propagate from CMC to iDRAC. Clicking **Refresh** too soon may display only partially correct data for one or more iDRAC servers.

Modifying iDRAC Network Settings for Individual Server iDRAC

Using this table you can configure the iDRAC network configurations settings for each installed server. The initial values displayed for each of the fields are the current values read from the iDRAC.

To modify the iDRAC Network Settings using the CMC Web interface:

1. In the system tree, go to **Server Overview**, and then click **Setup** → **iDRAC**. The **Deploy iDRAC** page is displayed. The **iDRAC Network Settings** section lists all installed server's iDRAC IPv4 and IPv6 network configuration settings.

2. Modify the iDRAC network settings as required for the server(s).

   NOTE: You must select the **Enable LAN** option to specify the IPv4 or IPv6 settings. For information about the fields, see CMC Online Help.

3. To deploy the setting to iDRAC, click **Apply iDRAC Network Settings**. If you made changes to the QuickDeploy settings, they are also saved.

   The **iDRAC Network Settings** table reflects future network configuration settings; the values shown for installed servers may or may not be the same as the currently installed iDRAC network configuration settings. Click **Refresh** to update the **iDRAC Deploy** page with each installed iDRAC network configuration settings after changes are made.

   NOTE: Changes made to QuickDeploy fields are immediate, but changes made to one or more iDRAC server network configuration settings may require a couple of minutes to propagate from CMC to iDRAC. Clicking **Refresh** too soon may display only partially correct data for a one or more iDRAC servers.

Modifying iDRAC Network Settings Using RACADM

RACADM `config` or `getconfig` commands support the `-m <module>` option for the following configuration groups:

- `cfgLanNetworking`
- `cfgIPv6LanNetworking`
- `cfgRacTuning`
- `cfgRemoteHosts`
- `cfgSerial`
- `cfgSessionManagement`

For more information on the property default values and ranges, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC*.

Configuring iDRAC VLAN Tag Settings

VLANs are used to allow multiple virtual LANs to co-exist on the same physical network cable and to segregate the network traffic for security or load management purposes. When you enable the VLAN functionality, each network packet is assigned a VLAN tag. VLAN tags are chassis properties. They remain with the chassis even when a component is removed.

Configuring iDRAC VLAN Tag Settings Using Web Interface

To configure VLAN for server using the CMC Web interface:

1. Go to any of the following pages:
   - In the system tree, go to **Chassis Overview** and click **Network** → **VLAN**.
   - In the system tree, go to **Chassis Overview** → **Server Overview** and click **Network** → **VLAN**. The **VLAN Tag Settings** page is displayed.
2. In the **iDRAC** section, enable VLAN for the server(s), set the priority and enter the ID. For more information about the fields, see the *CMC Online Help*.
3. Click **Apply** to save the settings.

Configuring iDRAC VLAN Tag Settings Using RACADM

- Specify the VLAN ID and priority of a particular server with the following command:

  ```
  racadm setniccfg -m server-<n> -v <VLAN id> <VLAN priority>
  ```

  The valid values for `<n>` are 1 – 16.

  The valid values for `<VLAN>` are 1 – 4000 and 4021 – 4094. Default is 1.

  The valid values for `<VLAN priority>` are 0 – 7. Default is 0.

  For example:

  ```
  racadm setniccfg -m server-1 -v 1 7
  ```

  For example:

- To remove a server VLAN, disable the VLAN capabilities of the specified server's network:

  ```
  racadm setniccfg -m server-<n> -v
  ```

  The valid values for `<n>` are 1-16.

  For example:

  ```
  racadm setniccfg -m server-1 -v
  ```

Setting First Boot Device

You can specify the CMC first boot device for each server. This may not be the actual first boot device for the server or even represent a device present in that server; instead it represents a device sent by CMC to the server and used as its first boot device in regard to that server.

You can set the default boot device and set a one-time boot device so that you can boot a image to perform tasks such as running diagnostics or reinstalling an operating system.

You can set the first boot device for the next boot only or for all subsequent reboots. Based on this selection, you can set the first boot device for the server. 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 CMC Web interface or from the BIOS boot sequence.

NOTE: The first boot device setting in CMC Web Interface overrides the System BIOS boot settings.

The boot device that you specify must exist and contain bootable media.

You can set the following devices for first boot.

Table 12. : Boot Devices

Boot Device	Description
PXE	Boot from a Preboot Execution Environment (PXE) protocol on the network interface card.
Hard Drive	Boot from the hard drive on the server.
Local CD/DVD	Boot from a CD/DVD drive on the server.
Virtual Floppy	Boot from the virtual floppy drive. The floppy drive (or a floppy disk image) is on another computer on the management network, and is attached using the iDRAC GUI console viewer.
Virtual CD/DVD	Boot from a virtual CD/DVD drive or CD/DVD ISO image. The optical drive or ISO image file is located on another computer or disk available on the management network and is attached using the iDRAC GUI console viewer.
iSCSI	Boot from an Internet Small Computer System Interface (iSCSI) device.
Local SD Card	Boot from the local SD (Secure Digital) card - for servers that support iDRAC6 and iDRAC7 systems only.
Floppy	Boot from a floppy disk in the local floppy disk drive.
RFS	Boot from a Remote File Share (RFS) image. The image file is attached using the iDRAC GUI console viewer.

Related Links

Setting First Boot Device For Multiple Servers Using CMC Web Interface
Setting First Boot Device For Individual Server Using CMC Web Interface

Setting First Boot Device Using RACADM

Setting First Boot Device For Multiple Servers Using CMC Web Interface

NOTE: To set the first boot device for servers, you must have **Server Administrator** privileges or **Chassis Configuration Administrator** privileges and **iDRAC login** privileges.

To set the first boot device for multiple servers using the CMC Web interface:

1. In the system tree, go to **Server Overview**, and then click **Setup** → **First Boot Device**. A list of servers is displayed.
2. In the **First Boot Device** column, from the drop-down menu, select the boot device you want to use for each server.
3. If you want the server to boot from the selected device every time it boots, clear the **Boot Once** option for the server. If you want the server to boot from the selected device only on the next boot cycle, select the **Boot Once** option for the server.
4. Click **Apply** to save the settings.

Setting First Boot Device For Individual Server Using CMC Web Interface

To set the first boot device for servers, you must have **Server Administrator** privileges or **Chassis Configuration Administrator** privileges and **iDRAC login** privileges.

To set the first boot device for individual server using the CMC Web interface:

1. In the system go to **Server Overview**, and then click the server for which you want to set the first boot device.
2. Go to **Setup** → **First Boot Device**. The **First Boot Device** page is displayed.
3. From the **First Boot Device** drop-down menu, select the boot device you want to use for each server.
4. If you want the server to boot from the selected device every time it boots, clear the **Boot Once** option for the server. If you want the server to boot from the selected device only on the next boot cycle, select the **Boot Once** option for the server
5. Click **Apply** to save the settings.

Setting First Boot Device Using RACADM

To set the first boot device, use the `cfgServerFirstBootDevice` object.

To enable boot once for a device, use the `cfgServerBootOnce` object.

For more information about these objects, see the *RACADM Command Line Reference Guide for iDRAC and CMC* available at **support.dell.com/manuals**.

Configuring Server FlexAddress

For information to configure FlexAddress for servers, see Configuring FlexAddress for Server-Level Slots.

Configuring Remote File Share

The Remote Virtual Media File Share feature maps a file from a share drive on the network to one or more servers through CMC to deploy or update an operating system. When connected, the remote file is accessible as if it is on the local system. Two types of media are supported: floppy drives and CD/DVD drives.

To perform a remote file share operation (connect, disconnect, or deploy), you must have Chassis Configuration Administrator or Server Administrator privileges.

To configure the remote file share using CMC Web interface:

1. In the system tree, go to **Server Overview**, and then click **Setup** → **Remote File Sharing**. The **Deploy Remote File Share** page is displayed.

   Enter the result of your step here (optional).
2. Specify the required settings. For more information, see the *CMC Online Help*.
3. Click **Connect** to connect to a remote file share. To connect a remote file share, you must provide the path, user name, and password. A successful operation allows access to the media.

   Click **Disconnect** to disconnect a previously connected remote file share.

   Click **Deploy** to deploy the media device.

   NOTE: Save all working files before executing the `Deploy` command because this action causes the server to be restarted.

   This command involves these actions:

   - The remote file share is connected.
   - The file is selected as the first boot device for the servers.
   - The server is restarted.
   - Power is applied to the server if the server is turned off.

Configuring BIOS Settings Using Server Clone

The server cloning feature allows you to apply all BIOS settings from a specified server to one or more servers. BIOS settings that can be cloned are those BIOS settings, which can be modified and are intended to be replicated across servers.

The server cloning feature supports iDRAC6 and iDRAC7 Servers. Earlier generation RAC servers are listed, but are greyed out on the main page, and are not enabled to use this feature.

To use the server cloning feature:

- iDRAC must have the minimum version that is required. iDRAC6 servers require a minimum version of 3.2 and iDRAC7 servers require version 1.00.00.
- Server must have supported generation of iDRAC.
- Server must be powered on.

The source and target servers need not belong to the same generation. Only the available cloneable settings are applied from one server profile to other servers.

You can:

- Copy the BIOS settings of one server to another.
- Save a profile from a server.
- Apply a profile to other servers.
- View BIOS settings from a server or from a saved profile.
- Display the log activity for recent BIOS profile tasks.

Related Links

Accessing BIOS Profile Page
Adding Profile
Managing Stored Profiles
Applying Profile
Viewing BIOS Settings

Viewing Profile Log
Completion Status and Troubleshooting

Accessing BIOS Profile Page

You can add, manage, and apply BIOS profiles to one or more servers using the **BIOS Profile** page.

To access the BIOS Profile page using the CMC Web interface, in the system tree, go to **Chassis Overview** → **Server Overview** and click **Setup** → **Profiles**. The **BIOS Profiles** page is displayed.

Related Links

Adding Profile
Managing Stored Profiles
Applying Profile
Viewing BIOS Settings
Viewing Profile Log
Completion Status and Troubleshooting

Adding Profile

Before root cloning the BIOS properties of a server, you must first capture the properties to a Stored Profile.

When you create a Stored Profile, you provide a name and optional description for each profile. You can save a maximum of 16 Stored Profiles on the CMC non-volatile extended storage media.

Removing or disabling the non-volatile extended storage media prevents access to Stored Profiles, and disables the Server Cloning feature.

To add a profile:

1. In the **BIOS Profile** page, click **Add Profile**. The **Add BIOS Profile** page is displayed.
2. Enter the profile name and description (optional), select the server from where the profile must be captured, and click **Save**. CMC communicates with the LC to get the available BIOS settings and store them as a named profile.

Managing Stored Profiles

You can edit, view, or delete BIOS profiles.

To manage the stored profiles on the CMC:

1. In the **BIOS Profile** page, in the **Apply Profile** section, click **Manage Profiles**. The **Manage BIOS Profiles** page is displayed.
2. To edit a profile, click **Edit**.
3. To view BIOS settings, click **View**.
4. To delete a profile, click **Delete**.

   For more information, see the *CMC Online Help*.

Applying Profile

When stored profiles are available in the non-volatile media on the CMC, to initiate a server cloning operation, you can apply a Stored Profile to one or more servers.

The operation status, slot number, slot name, and model name is displayed for each server in the **Apply Profile** table.

NOTE: If a server does not support Lifecycle Controller or the chassis is powered off, you cannot apply a profile to the server.

To apply a profile to one or more server(s):

1. In the **BIOS Profiles** page, in the **Apply Profile** section, from the **Select Profile** drop-down menu, select the profile that you want to apply.
2. From the **Select the Target Server(s)** section, select the servers for which you want to apply the profile. For more information, see the *CMC Online Help*.
3. Click **Apply**. The selected profile is applied to the server(s) and the server(s) is rebooted immediately.

Viewing BIOS Settings

To view BIOS settings for a selected server, in the **BIOS Profiles** page, in the **Apply Profile** section, click **View** in the BIOS settings column for the profile for which you want to view the BIOS settings information. The **View Settings** page is displayed.

Only BIOS settings on the server which may be modified by applying a profile (cloneable settings) are displayed. The settings are partitioned into groups in the same way they are displayed in the iDRAC BIOS Setup screen.

NOTE: The CMC Server Cloning application retrieves and displays the correct BIOS and Boot settings for a specific server, only if the Control System Inventory on Restart (CSIOR) option is enabled.

To enable CSIOR on:

- 11th generation servers — After rebooting the server, from the **Ctrl-E** setup, select **System Services**, enable **CSIOR** and save the changes.
- 12th generation servers — After rebooting the server, from the **F2** setup, select **iDRAC Settings** → **Lifecycle Controller□** , enable **CSIOR** and save the changes.

Viewing Profile Log

To view the profile log, in the **BIOS Profiles** page, see the **Recent Profile Log** section that lists the 10 latest profile log entries directly from server cloning operations. Each recent profile log displays the severity, the time and date when server cloning operation was submitted, and the description of the cloning log message. The log entries are also available in the RAC log. To view the other available entries, click **Go to Profile Log**. The **Profile Log** page is displayed.

Completion Status and Troubleshooting

To check the completion status of an applied BIOS profile:

1. In the **BIOS Profiles** page, note down the Job ID (JID) of the submitted job from the **Recent Profile Log** section.
2. In the system tree, go to **Server Overview** and click **Troubleshooting** → **Lifecycle Controller Jobs**. Look up the same JID in the **Jobs** table.

Launching iDRAC using Single Sign-On

CMC provides limited management of individual chassis components, such as servers. For complete management of these individual components, CMC provides a launch point for the server's management controller (iDRAC) Web-based interface.

A user may be able to launch iDRAC Web interface without having to login a second time, as this feature utilizes single sign-on. Single sign-on policies are:

- A CMC user who has server administrative privilege, is automatically logged into iDRAC using single sign-on. Once on the iDRAC site, this user is automatically granted Administrator privileges. This is true even if the same user does not have an account on iDRAC, or if the account does not have the Administrator's privileges.
- A CMC user who does **NOT** have the server administrative privilege, but has the same account on iDRAC is automatically logged into iDRAC using single sign-on. Once on the iDRAC site, this user is granted the privileges that were created for the iDRAC account.
- A CMC user who does not have the server administrative privilege, or the same account on the iDRAC, does **NOT** automatically logged into iDRAC using single sign-on. This user is directed to the iDRAC login page when the **Launch iDRAC GUI** is clicked.

  NOTE: The term "the same account" in this context means that the user has the same login name with a matching password for CMC and for iDRAC. The user who has the same login name without a matching password, is considered to have the same account.

  NOTE: Users may be prompted to log in to iDRAC (see the third Single Sign-on policy bullet above).

  NOTE: If the iDRAC network LAN is disabled (LAN Enabled = No), single sign-on is not available.

If the server is removed from the chassis, the iDRAC IP address is changed, or the iDRAC network connection experiences a problem, then clicking Launch iDRAC GUI may display an error page.

Related Links

Launching iDRAC from Servers Status Page
Launching iDRAC from Server Status Page

Launching iDRAC from Servers Status Page

To launch the iDRAC management console from the **Servers Status** page:

1. In the system tree, click **Server Overview**. The **Servers Status** page is displayed.
2. Click **Launch iDRAC** for the server you want to launch the iDRAC Web interface.

Launching iDRAC from Server Status Page

To launch the iDRAC management console for an individual server:

1. In the system tree, expand **Server Overview**. All of the servers (1–16) appear in the expanded **Servers** list.
2. Click the server for which you want to launch the iDRAC Web interface. The **Server Status** page is displayed.
3. Click **Launch iDRAC GUI**. The iDRAC Web interface is displayed.

Launching Remote Console from CMC Web Interface

You can launch a Keyboard-Video-Mouse (KVM) session directly on the server. The remote console feature is supported only when all of the following conditions are met:

- The chassis power is on.
- Servers that support iDRAC6 and iDRAC7.
- The LAN interface on the server is enabled.
- The iDRAC version is 2.20 or later.
- The host system is installed with JRE (Java Runtime Environment) 6 Update 16 or later.
- The browser on host system allows pop-up windows (pop-up blocking is disabled).

Remote Console can also be launched from the iDRAC Web interface. For more details, see *iDRAC User's Guide*.

Related Links

Launching Remote Console from Chassis Health Page
Launching Remote Console from Server Status Page

Launching Remote Console from Servers Status Page

Launching Remote Console from Chassis Health Page

To launch a remote console from the CMC Web interface, do any of the following:

1. In the system tree, go to **Chassis Overview**, and then click **Properties** → **Health**. The **Chassis Health** page is displayed.
2. Click on the specified server in the chassis graphic.
3. In the **Quicklinks** section, click the **Launch Remote Console** link to launch the remote console.

Launching Remote Console from Server Status Page

To launch a remote console for an individual server:

1. In the system tree, expand **Server Overview**. All servers (1–16) appear in the expanded servers list.
2. Click the server for which you want to launch the remote console. The **Server Status** page appears.
3. Click **Launch Remote Console**.

Launching Remote Console from Servers Status Page

To launch a remote console from the **Servers Status** page:

1. In the system tree, go to **Server Overview**, and then click **Properties** → **Status**. The **Servers Status** page is displayed.
2. Click **Launch Remote Console** for the required server.

8

Configuring CMC To Send Alerts

You can set alerts and actions for certain events that occur on the managed system. An event occurs when the status of a system component is greater than the pre-defined condition. If an event matches an event filter and you have configured this filter to generate an alert (e-mail alert or SNMP trap), then an alert is sent to one or more configured destinations.

To configure CMC to send alerts:

1. Enable the global chassis event alerts.
2. Optionally, you can select the events for which alerts must be generated.
3. Configure the e-mail alert or SNMP trap settings.

Related Links

Enabling Or Disabling Alerts
Configuring Alert Destinations

Enabling Or Disabling Alerts

To send alerts to configured destinations, you must enable the global alerting option. This property overrides the individual alert setting.

Make sure that the SNMP or e-mail alert destinations are configured to receive the alerts.

Enabling Or Disabling Alerts Using CMC Web Interface

To enable or disable generating alerts:

1. In the system tree, go to **Chassis Overview**, and then click **Alerts** → **Chassis Events**.
   The **Chassis Events** page is displayed.
2. Under **Chassis Event Filters Configuration** section, select **Enable Chassis Event Alerts** option to enable alert generation. Else, clear this option.
3. Under the **Chassis Event List** section, do one of the following:
   - Select individual events for which alerts must be generated.
   - Select the **Enable Alert** option on the column header to generate alerts for all events. Else, clear this option.
4. Click **Apply** to save the setting.

Enabling Or Disabling Alerts Using RACADM

To enable or disable generating alerts, use the **cfgIpmiLanAlertEnable** RACAM object. For more information, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC*.

Configuring Alert Destinations

The management station uses Simple Network Management Protocol (SNMP) to receive data from CMC.

You can configure the IPv4 and IPv6 alert destinations, e-mail settings, and SMTP server settings, and test these settings.

Before configuring the e-mail alert or SNMP trap settings, make sure that you have **Chassis Configuration Administrator** privilege.

Related Links

Configuring SNMP Trap Alert Destinations
Configuring E-Mail Alert Settings

Configuring SNMP Trap Alert Destinations

You can configure the IPv6 or IPv4 addresses to receive the SNMP traps.

Configuring SNMP Trap Alert Destinations Using CMC Web Interface

To configure IPv4 or IPv6 alert destination settings using CMC Web interface:

1. In the system tree, go to **Chassis Overview** , and then click **Alerts** → **Trap Settings** .

   The **Chassis Event Alert Destinations** page is displayed.
2. Enter the following:

   – In the **Destination** field, enter a valid IP address. Use the quad-dot IPv4 format, standard IPv6 address notation, or FQDN. For example: **123.123.123.123** or **2001:db8:85a3::8a2e:370:7334** or **dell.com** .

     Choose a format that is consistent with the networking technology or infrastructure. The Test Trap functionality cannot detect incorrect choices based on the current network configuration (example, use of an IPv6 destination in an IPv4-only environment).

   – In the **Community String** field, enter a valid community string to which the destination management station belongs.

     This community string differs from the community string on the **Chassis** → **Network** → **Services** page. The SNMP traps community string is the community that CMC uses for outbound traps destined to management stations. The community string on the **Chassis** → **Network** → **Services** page is the community string that management stations use to query the SNMP daemon on CMC.

   – Under **Enabled** , select the check box corresponding to the destination IP to enable the IP address to receive the traps. You can specify up to four IP addresses.
3. Click **Apply** to save the settings.
4. To test whether the IP address is receiving the SNMP traps, click **Send** in the **Test SNMP Trap** column.

   The IP alert destinations are configured.

Configuring SNMP Trap Alert Destinations Using RACADM

To configure IP alert destination using RACADM:

1. Open a serial/Telnet/SSH text console to CMC and log in.

   NOTE: Only one filter mask may be set for both SNMP and e-mail alerting. You can skip step 2 if you have already selected filter mask.
2. Enable alert generation:

```
racadm config -g cfgAlerting -o cfgAlertingEnable 1
```

3. Specify the events for which alerts must be generated:

   ```
   racadm config -g cfgAlerting -o cfgAlertingFilterMask <mask value>
   ```

   where `<mask value>` is a hex value between 0x0 and 0xffffffff.

   To obtain the mask value, use a scientific calculator in hex mode and add the second values of the individual masks (1, 2, 4, and so on) using the <OR> key.

   For example, to enable trap alerts for Battery Probe Warning (0x2) , Power Supply Failure (0x1000) , and KVM failure (0x80000) , key 2 <OR> 1000 <OR> 200000 and press the <=> key.

   The resulting hex value is 208002, and the mask value for the RACADM command is 0x208002.

   Table 13. Event Traps Filter Masks

Event	Filter Mask Value
Fan Probe Failure	0x1
Battery Probe Warning	0x2
Temperature Probe Warning	0x8
Temperature Probe Failure	0x10
Redundancy Degraded	0x40
Redundancy Lost	0x80
Power Supply Warning	0x800
Power Supply Failure	0x1000
Power Supply Absent	0x2000
Hardware Log Failure	0x4000
Hardware Log Warning	0x8000
Server Absent	0x10000
Server Failure	0x20000
KVM Absent	0x40000
KVM Failure	0x80000
IOM Absent	0x100000
IOM Failure	0x200000
Firmware Version Mismatch	0x400000
Chassis Power Threshold Error	0x1000000
SDCARD Absent	0x2000000
SDCARD Error	0x4000000
Chassis Group Error	0x8000000
Server Sleeve Absent	0x10000000
Fabric Mismatch	0x20000000

4. Enable traps alerts:

   ```
   racadm config -g cfgTraps -o cfgTrapsEnable 1 -i <index>
   ```

where`<index>` is a value between 1–4. CMC uses the index number to distinguish up to four configurable destinations for traps alerts. Destinations may be specified as appropriately formatted numeric addresses (IPv6 or IPv4), or Fully-Qualified Domain Names (FQDNs).

5. Specify a destination IP address to receive the traps alert:

   ```
   racadm config -g cfgTraps -o cfgTrapsAlertDestIPAddr <IP address> -i <index>
   ```

   where`<IP address>` is a valid destination, and `<index>` is the index value specified in step 4.

6. Specify the community name:

   ```
   racadm config -g cfgTraps -o cfgTrapsCommunityName <community name> -i
   <index>
   ```

   where `<community name>` is the SNMP community to which the chassis belongs, and `<index>` is the index value specified in steps 4 and 5.

   You can configure up to four destinations to receive traps alerts. To add more destinations, repeat steps 2–6.

   NOTE: The commands in steps 2–6 overwrites any existing settings configured for the index specified (1–4). To determine whether an index has previously configured values, type: `racadm getconfig -g cfgTraps -i <index>`. If the index is configured, values appear for the **cfgTrapsAlertDestIPAddr** and **cfgTrapsCommunityName** objects.

7. To test an event trap for an alert destination, type:

   ```
   racadm testtrap -i <index>
   ```

   where `<index>` is a value 1–4 representing the alert destination you want to test.

   If you are not sure of the index number, use:

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

Configuring E-Mail Alert Settings

When CMC detects a chassis event, such as an environmental warning or a component failure, it can be configured to send an e-mail alert to one or more e-mail addresses.

You must configure the SMTP e-mail server to accept relayed emails from the CMC IP address, a feature which is normally turned off in most mail servers due to security concerns. For instructions to do this in a secure manner, see the documentation that was provided with the SMTP server.

NOTE: If your mail server is Microsoft Exchange Server 2007, make sure that iDRAC7 domain name is configured for the mail server to receive the email alerts from iDRAC7.

NOTE: E-mail alerts support both IPv4 and IPv6 addresses. The DRAC DNS Domain Name must be specified when using IPv6.

If your network has an SMTP server that releases and renews IP address leases periodically, and the addresses are different, then there is a duration when this property setting does not work due to change in the specified SMTP server IP address. In such cases, use the DNS name.

Configuring E-Mail Alert Settings Using CMC Web Interface

To configure the e-mail alert settings using Web interface:

1. In the system tree, go to **Chassis Overview** , and then click **Alerts** → **E-mail Alert Settings** .
2. Specify the SMTP e-mail server settings and the e-mail address(es) to receive the alerts. For information about the fields, see the *CMC Online Help*.
3. Click **Apply** to save the settings.
4. Click **Send** under **Test E-mail** to send a test e-mail to the specified e-mail alert destination.

Configuring E-Mail Alert Settings Using RACADM

To send a test e-mail to an e-mail alert destination using RACADM :

1. Open a serial/Telnet/SSH text console to CMC and log in.

2. Enable alert generation:

   ```
   racadm config -g cfgAlerting -o cfgAlertingEnable 1
   ```

   NOTE: Only one filter mask may be set by both SNMP and e-mail alerting. You may skip step 3 if you have already set a filter mask.

3. Specify the events for which alerts must be generated:

   ```
   racadm config -g cfgAlerting -o cfgAlertingFilterMask <mask value>
   ```

   where `<mask value>` is a hexadecimal value between 0x0 and 0xffffffff and must be expressed with the leading 0x characters. Table Event Traps Filter Masks provides filter masks for each event type. For instructions on calculating the hex value for the filter mask you want to enable, see step 3 in Configuring SNMP Trap Alert Destinations Using RACADM.

4. Enable e-mail alert generation:

   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertEnable 1 -i <index>
   ```

   where `<index>` is a value between 1–4. CMC uses the index number to distinguish up to four configurable destination e-mail addresses.

5. Specify a destination e-mail address to receive the e-mail alerts:

   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertAddress <email address> -i
   <index>
   ```

   where`<email address>` is a valid e-mail address, and `<index>` is the index value you specified in step 4.

6. Specify the name of the person receiving the e-mail alert:

   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertEmailName <email name> -i
   <index>
   ```

   where `<email name>` is the name of the person or group receiving the e-mail alert, and `<index>` is the index value specified in step 4 and step 5. The e-mail name can contain up to 32 alphanumeric characters, dashes, underscores, and periods. Spaces are not valid.

7. Setup the SMTP host:

   ```
   racadm config -g cfgRemoteHosts -o cfgRhostsSmtpServerIpAddr host.domain
   ```

   where `host.domain` is the FQDN.

   You can configure up to four destination e-mail addresses to receive e-mail alerts. To add more e-mail addresses, repeat step 2 – step 6.

   NOTE: The commands in steps 2–6 overwrite any existing settings configured for the index you specify (1–4). To determine whether an index has previously configured values, type:x`racadm getconfig -g cfgEmailAlert — I` *`<index>`*. If the index is configured, values appear for the **cfgEmailAlertAddress** and **cfgEmailAlertEmailName** objects.

   For more information, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at **support.dell.com/manuals**.

9

Configuring User Accounts and Privileges

You can setup user accounts with specific privileges (*role-based authority*) to manage your system with CMC and maintain system security. By default CMC is configured with a local administrator account. This default user name is *root* and the password is *calvin*. As an administrator, you can setup user accounts to allow other users to access CMC.

You can setup up to 16 local users or use directory services such as Microsoft Active Directory or LDAP to setup additional user accounts. Using a directory service provides a central location for managing authorized user accounts.

CMC supports role-based access to users with a set of associated privileges. The roles are administrator, operator, read only, or none. The role defines the maximum privileges available.

Related Links

Types of Users
Configuring Local Users
Configuring Active Directory Users
Configuring Generic LDAP Users
Modifying Root User Administrator Account Settings

Types of Users

There are two types of users:

- CMC users or chassis users
- iDRAC users or server users (since the iDRAC resides on a server)

CMC and iDRAC users can be local or directory service users.

Except where a CMC user has **Server Administrator** privilege, privileges granted to a CMC user are not automatically transferred to the same user on a server, because server users are created independently from CMC users. In other words, CMC Active Directory users and iDRAC Active Directory users reside on two different branches in the Active Directory tree. To create a local server user, the Configure Users must log in to the server directly. The Configure Users cannot create a server user from CMC or vice versa. This rule protects the security and integrity of the servers.

Table 14. : User Types

Privilege	Description
CMC Login User	User can log in to CMC and view all the CMC data, but cannot add or modify data or execute commands. It is possible for a user to have other privileges without the CMC Login User privilege. This feature is useful when a user is temporarily not allowed to login. When that user’s CMC Login User privilege is restored, the user retains all the other privileges previously granted.
Chassis Configuration Administrator	User can add or change data that: • Identifies the chassis, such as chassis name and chassis location. • Is assigned specifically to the chassis, such as IP mode (static or DHCP), static IP address, static gateway, and static subnet mask.

Privilege	Description
	• Provides services to the chassis, such as date and time, firmware update, and CMC reset. • Is associated with the chassis, such as slot name and slot priority. Although these properties apply to the servers, they are strictly chassis properties relating to the slots rather than the servers themselves. For this reason, slot names and slot priorities can be added or changed whether or not servers are present in the slots. When a server is moved to a different chassis, it inherits the slot name and priority assigned to the slot it occupies in the new chassis. Its previous slot name and priority remain with the previous chassis. **NOTE:** CMC users with the **Chassis Configuration Administrator** privilege can configure power settings. However, the **Chassis Control Administrator** privilege is needed to perform chassis power operations, including power on, power off, and power cycle.
User Configuration Administrator	User can: • Add a new user. • Change a user's password. • Change a user's privileges. • Enable or disable a user's login privilege but retain the user's name and other privileges in the database.
Clear Logs Administrator	User can clear the hardware log and CMC log.
Chassis Control Administrator (Power Commands)	CMC users with the **Chassis Power Administrator** privilege can perform all power-related operations. They can control chassis power operations, including power on, power off, and power cycle. **NOTE:** To configure power settings, the **Chassis Configuration Administrator** privilege is needed.
Server Administrator	This is a blanket privilege, granting a CMC user all rights to perform any operation on any servers present in the chassis. When a user with **Server Administrator** privilege issues an action to be performed on a server, the CMC firmware sends the command to the targeted server without checking the user's privileges on the server. In other words, the **Server Administrator** privilege overrides any lack of administrator privileges on the server. Without the **Server Administrator** privilege, a user created on the chassis can only execute a command on a server when all of the following conditions are true: • The same user name exists on the server. • The same user name must have the same password on the server. • The user must have the privilege to execute the command. When a CMC user who does not have **Server Administrator** privilege issues an action to be performed on a server, CMC sends a command to the targeted server with the user’s login name and password. If the user does not exist on the server, or if the password does not match, the user is denied the ability to perform the action. If the user exists on the target server and the password matches, the server responds with the privileges of which the user was granted on the server.

Privilege	Description
	Based on the privileges responding from the server, CMC firmware decides if the user has the right to perform the action. Listed below are the privileges and the actions on the server to which the Server Administrator is entitled. These rights are applied only when the chassis user does not have the Server Administrative privilege on the chassis. Server Configuration Administrator: • Set IP address • Set gateway • Set subnet mask • Set first boot device Configure Users: • Set iDRAC root password • iDRAC reset Server Control Administrator: • Power on • Power off • Power cycle • Graceful shutdown • Server Reboot
Test Alert User	User can send test alert messages.
Debug Command Administrator	User can execute system diagnostic commands.
Fabric A Administrator	User can set and configure the Fabric A IOM, which resides in either slot A1 or slot A2 of the I/O slots.
Fabric B Administrator	User can set and configure the Fabric B IOM, which resides in either slot B1 or slot B2 of the I/O slots.
Fabric C Administrator	User can set and configure the Fabric C IOM, which resides in either slot C1 or slot C2 of the I/O slots.

The CMC user groups provide a series of user groups that have pre-assigned user privileges.

NOTE: If you select Administrator, Power User, or Guest User, and then add or remove a privilege from the predefined set, the CMC Group automatically changes to Custom.

Table 15. : CMC Group Privileges

User Group	Privileges Granted
Administrator	• CMC Login User • Chassis Configuration Administrator • User Configuration Administrator • Clear Logs Administrator • Server Administrator • Test Alert User

User Group	Privileges Granted
	• Debug Command Administrator • Fabric A Administrator • Fabric B Administrator • Fabric C Administrator
Power User	• Login • Clear Logs Administrator • Chassis Control Administrator (Power commands) • Server Administrator • Test Alert User • Fabric A Administrator • Fabric B Administrator • Fabric C Administrator
Guest User	Login
Custom	Select any combination of the following permissions: • CMC Login User • Chassis Configuration Administrator • User Configuration Administrator • Clear Logs Administrator • Chassis Control Administrator (Power commands) • Server Administrator • Test Alert User • Debug Command Administrator • Fabric A Administrator • Fabric B Administrator • Fabric C Administrator
None	No assigned permissions

Table 16. : Comparison of Privileges Between CMC Administrators, Power Users, and Guest Users

Privilege Set	Administrator Permissions	Power User Permissions	Guest User Permissions
CMC Login User	Yes	Yes	Yes
Chassis Configuration Administrator	Yes	No	No
User Configuration Administrator	Yes	No	No
Clear Logs Administrator	Yes	Yes	No
Chassis Control Administrator (Power commands)	Yes	Yes	No
Server Administrator	Yes	Yes	No
Test Alert User	Yes	Yes	No

Privilege Set	Administrator Permissions	Power User Permissions	Guest User Permissions
Debug Command Administrator	Yes	No	No
Fabric A Administrator	Yes	Yes	No
Fabric B Administrator	Yes	Yes	No
Fabric C Administrator	Yes	Yes	No

Modifying Root User Administrator Account Settings

For added security, it is strongly recommended that you change the default password of the root (User 1) account. The root account is the default administrative account that ships with CMC.

To change the default password for the root account using the CMC Web interface:

1. In the system tree, go to **Chassis Overview**, and then click **User Authentication** → **Local Users**. The **Users** page is displayed.
2. In the **User ID** column, click a user ID 1.

   NOTE: User ID 1 is the root user account that is shipped by default with CMC. This cannot be changed.

   The **User Configuration** page is displayed.
3. Select **Change Password** check box.
4. Type the new password in the **Password** and **Confirm Password** fields.
5. Click **Apply**. The password is changed for user ID 1.

Configuring Local Users

You can configure up to 16 local users in CMC with specific access permissions. Before you create a CMC local user, verify if any current users exist. You can set user names, passwords, and roles with the privileges for these users. The user names and passwords can be changed using any of the CMC secured interfaces (that is, Web interface, RACADM or WS-MAN).

Configure Local Users Using CMC Web Interface

To add and configure local CMC users:

NOTE: You must have **Configure Users** permission to create a CMC user.

1. In the system tree, go to **Chassis Overview**, and then click **User Authentication** → **Local Users**. The **Users** page is displayed.
2. In the **User ID** column, click a user ID number. The **User Configuration** page is displayed.

   NOTE: User ID 1 is the root user account that is shipped by default with CMC. This cannot be changed.
3. Enable the user ID and specify the user name, password, and access privileges for the user. For more information about the options, see the *CMC Online Help*.
4. Click **Apply**. The user is created with the required privileges.

Configure Local Users Using RACADM

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

You can configure up to 16 users in the CMC property database. Before you manually enable a CMC user, verify if any current users exist.

If you are configuring a new CMC or if you have used the racadm `racresetcfg` command, the only current user is `root` with the password `calvin`. The `racresetcfg` subcommand resets all configuration parameters to the original defaults. Any previous changes are lost.

NOTE: Users can be enabled and disabled over time, and disabling a user does not delete the user from the database.

To verify if a user exists, open a Telnet/SSH text console to the CMC, log in, and 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 CMC configuration parameters.

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

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. It indicates that it is a read-only object. 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 a second CMC with the same settings as the main CMC.

Adding CMC User Using RACADM

To add a new user to the CMC configuration, perform the following:

1. Set the user name.
2. Set the password.
3. Set the user privileges. For information about user privileges, see Types of Users.
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 CMC.

NOTE: See the *RACADM Command Line Reference Guide for iDRAC7 and CMC* for a list of valid bit mask values for specific user privileges. The default privilege value is 0, which indicates the user has no privileges enabled.

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

To verify that the user was added successfully with the correct privileges, use the following commands:

```
racadm getconfig –g cfgUserAdmin –i 2
```

For more information on the RACADM commands, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at **support.dell.com/manuals**.

Disabling CMC User

When using RACADM, users must be disabled manually and on an individual basis. Users cannot be deleted using a configuration file.

To delete a CMC user, the command syntax is:

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName
-i <index>""
racadm config -g cfgUserAdmin -i 2 -o
cfgUserAdminPrivilege 0x0
```

A null string of double quote characters ("") instructs CMC to remove the user configuration at the specified index and reset the user configuration to the original factory defaults.

Enabling CMC User With Permissions

To enable a user with specific administrative permissions (role-based authority):

1. Locate an available user index using the command syntax:

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

2. Type the following commands with the new user name and password.

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

   NOTE: For a list of valid bit mask values for specific user privileges, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at **support.dell.com/manuals**. The default privilege value is 0, which indicates the user has no privileges enabled.

Configuring Active Directory Users

If your company uses the Microsoft Active Directory software, you can configure the software to provide access to CMC, allowing you to add and control CMC user privileges to your existing users in your directory service. This is a licensed feature.

NOTE: Using Active Directory to recognize CMC users is supported on the Microsoft Windows 2000 and Windows Server 2003 operating systems. Active Directory over IPv6 and IPv4 is supported on Windows 2008.

You can configure user authentication through Active Directory to log in to the CMC. You can also provide role-based authority, which enables an administrator to configure specific privileges for each user.

Supported Active Directory Authentication Mechanisms

You can use Active Directory to define CMC user access using two methods:

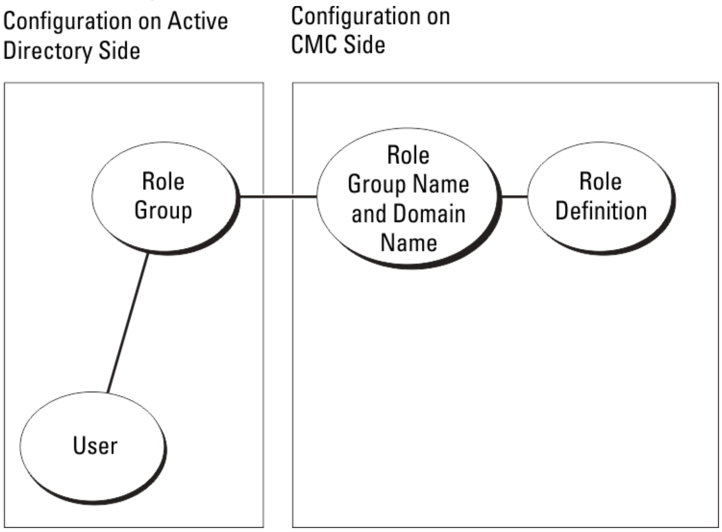
- *Standard schema* solution that uses Microsoft's default Active Directory group objects only.
- *Extended schema* solution that has customized Active Directory objects provided by Dell. All the access control objects are maintained in Active Directory. It provides maximum flexibility to configure user access on different CMCs with varying privilege levels.

Related Links

Standard Schema Active Directory Overview
Extended Schema Active Directory Overview

Standard Schema Active Directory Overview

As shown in the following figure, using standard schema for Active Directory integration requires configuration on both Active Directory and CMC.


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

In Active Directory, a standard group object is used as a role group. A user who has CMC access is a member of the role group. To give this user access to a specific CMC card, the role group name and its domain name need to be configured on the specific CMC card. The role and the privilege level is defined on each CMC card and not in the Active Directory. You can configure up to five role groups in each CMC. The following table shows the default role group privileges.

Table 17. : Default Role Group Privileges

Role Group	Default Privilege Level	Permissions Granted	Bit Mask
1	None	• CMC Login User • Chassis Configuration Administrator • User Configuration Administrator • Clear Logs Administrator	0x00000fff

Role Group	Default Privilege Level	Permissions Granted	Bit Mask
		• Chassis Control Administrator (Power Commands) • Server Administrator • Test Alert User • Debug Command Administrator • Fabric A Administrator • Fabric B Administrator • Fabric C Administrator	
2	None	• CMC Login User • Clear Logs Administrator • Chassis Control Administrator (Power Commands) • Server Administrator • Test Alert User • Fabric A Administrator • Fabric B Administrator • Fabric C Administrator	0x00000ed9
3	None	CMC Login User	0x00000001
4	None	No assigned permissions	0x00000000
5	None	No assigned permissions	0x00000000

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

NOTE: For more information about user privileges, see Types of Users.

Configuring Standard Schema Active Directory

To configure CMC for a Active Directory login access:

1. On an Active Directory server (domain controller), open the **Active Directory Users and Computers Snap-in**.
2. Using the CMC Web interface or RACADM:
   a) Create a group or select an existing group.
   b) Configure the role privileges.
3. Add the Active Directory user as a member of the Active Directory group to access CMC.

Configuring Active Directory With Standard Schema Using CMC Web Interface

NOTE: For information about the various fields, see the *CMC Online Help*.

1. In the system tree, go to **Chassis Overview**, and then click **User Authentication** → **Directory Services**. The **Directory Services** page is displayed.
2. Select **Microsoft Active Directory (Standard Schema)**. The settings to be configured for standard schema is displayed on the same page.
3. Specify the following:

   – Enable Active Directory, enter the root domain name, and the timeout value.

   – If you want the directed call to search the domain controller and global catalog, select the **Search AD Server to search (Optional)** option and specify the domain controller and global catalog details.
4. Click **Apply** to save the settings.

   NOTE: You must apply the settings before continuing. If you do not apply the settings, the settings are lost when you navigate to the next page.
5. In the **Standard Schema Setting**s section, click a **Role Group**. The **Configure Role Group** page is displayed.
6. Specify the group name, domain, and privileges for a role group.
7. Click **Apply** to save the role group settings and then click **Go Back To Configuration** page.
8. If you have enabled certificate validation, you must upload the domain forest root certificate authority-signed certificate to CMC. In the **Manage Certificates** section, type the file path of the certificate or browse to the certificate file. Click **Upload** to upload the file to CMC.

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

   The SSL certificates for the domain controllers must be signed by the root certificate authority-signed certificate. The root certificate authority-signed certificate must be available on the management station accessing CMC.
9. If you have enabled Single Sign-On (SSO), in the **Kerberos Keytab** section, click **Browse**, specify the keytab file and click **Upload**. When the upload is complete, a message is displayed indicating a successful or failed upload.
10. Click **Apply**. The CMC Web server automatically restarts after you click **Apply**.
11. Log out and then log in to CMC to complete the CMC Active Directory configuration.
12. Select **Chassis** in the system tree, and navigate to the **Network** tab. The **Network Configuration** page appears.
13. Under **Network Settings**, if **Use DHCP (for CMC Network Interface IP Address)** is selected, select **Use DHCP to obtain DNS server address**.

    To manually enter a DNS server IP address, clear Use **DHCP to obtain DNS server addresses** and type the primary and alternate DNS server IP addresses.
14. Click **Apply Changes**.

    The CMC Standard Schema Active Directory feature configuration is complete.

Configuring Active Directory With Standard Schema Using RACADM

To configure CMC Active Directory with Standard Schema using the RACADM:

1. Open a serial/Telnet/SSH text console to the CMC, and type:

```
racadm config -g cfgActiveDirectory -o cfgADEnable 1
racadm config -g cfgActiveDirectory -o cfgADType 2
racadm config -g cfgActiveDirectory -o
cfgADRootDomain <fully qualified root domain name>
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>
racadm sslcertupload -t 0x2 -f <ADS root CA
certificate>
racadm sslcertdownload -t 0x1 -f <RAC SSL
certificate>
```

NOTE: For bit mask number values, see the database property chapter of the *RACADM Command Line Reference Guide for iDRAC7 and CMC*

2. Specify a DNS server using one of the following options:

   – If DHCP is enabled on CMC and you want to use the DNS address obtained automatically by the DHCP server, type the following command:

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

   – If DHCP is disabled on CMC or you want manually to input your DNS IP address, type the following commands:

   ```
   racadm config -g cfgLanNetworking -o
   cfgDNSServersFromDHCP 0
   racadm config -g cfgLanNetworking -o
   cfgDNSServer1 <primary DNS IP address>
   racadm config -g cfgLanNetworking -o
   cfgDNSServer2 <secondary DNS IP address>
   ```

Extended Schema Active Directory Overview

Using the extended schema solution requires the Active Directory schema extension.

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. One example of a class that is stored in the database is the user class. Some example user class attributes can include the user’s first name, last name, phone number, and so on.

You can extend the Active Directory database by adding your own unique *attributes* and *classes* for specific requirements. Dell has extended the schema to include the necessary changes to support remote management authentication and authorization using Active Directory.

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 Schema Extensions

Dell has extended the schema to include an *Association*, *Device*, and *Privilege* property. The *Association* property is used to link together the users or groups with a specific set of privileges to one or more RAC devices. This model provides an administrator maximum flexibility over the different combinations of users, RAC privileges, and RAC devices on the network without much complexity.

When there are two CMCs on the network that you want to integrate with Active Directory for authentication and authorization, create at least one association object and one RAC device object for each CMC. You can create multiple association objects, and each association object can be linked to as many users, groups of users, or RAC device objects as required. The users and RAC device objects can be members of any domain in the enterprise.

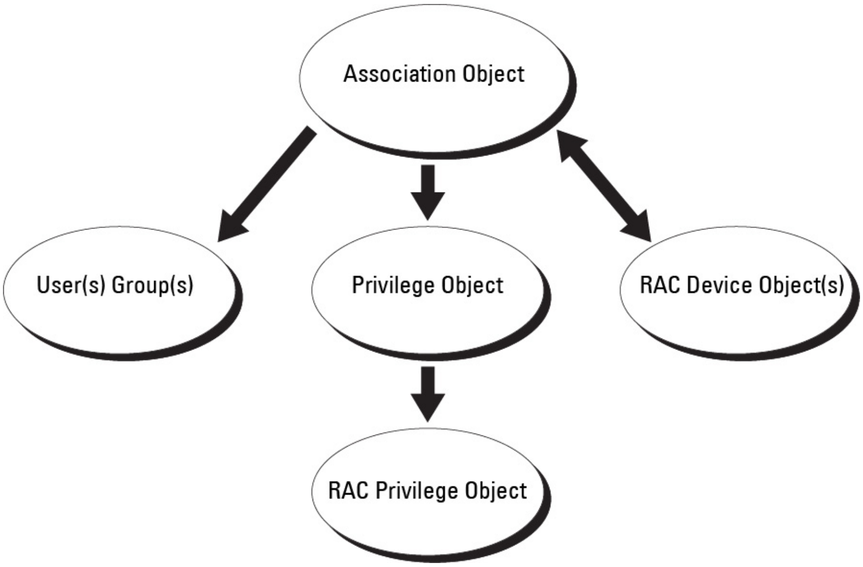
However, each association object can be linked (or, may link users, groups of users, or RAC device objects) to only one privilege object. This example allows an administrator to control each user's privileges on specific CMCs.

The RAC device object is the link to RAC firmware for querying Active Directory for authentication and authorization. When a RAC is added to the network, the administrator must configure the RAC and its device object with its Active Directory name so that users can perform authentication and authorization with Active Directory. Additionally, the administrator must add the RAC to at least one association object for users to authenticate.

The following figure shows that the association object provides the connection that is needed for the authentication and authorization.

NOTE: The RAC privilege object applies to DRAC 4, DRAC 5, and CMC.

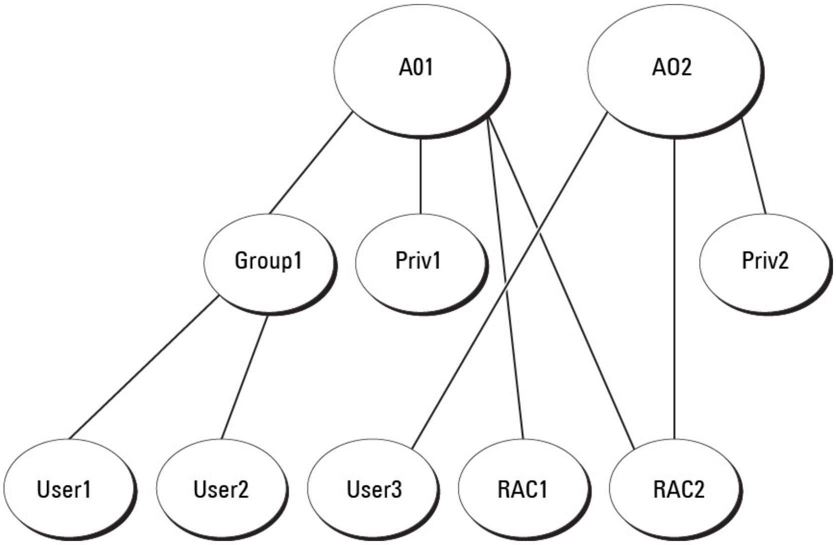
You can create as many or as few association objects as required. However, you must create at least one Association Object, and you must have one RAC device object for each RAC (CMC) on the network that you want to integrate with Active Directory.



The Association Object allows as many or as few users and/or groups as well as RAC Device Objects. However, the Association Object only includes one Privilege Object per Association Object. The Association Object connects the *Users* who have *Privileges* on RACs (CMCs).

Additionally, you can configure Active Directory objects in a single domain or in multiple domains. For example, you have two CMCs (RAC1 and RAC2) and three existing Active Directory users (user1, user2, and user3). You want to give user1 and user2 an administrator privilege to both CMCs and give user3 a login privilege to the RAC2 card. The following figure illustrates how you set up the Active Directory objects in this scenario.

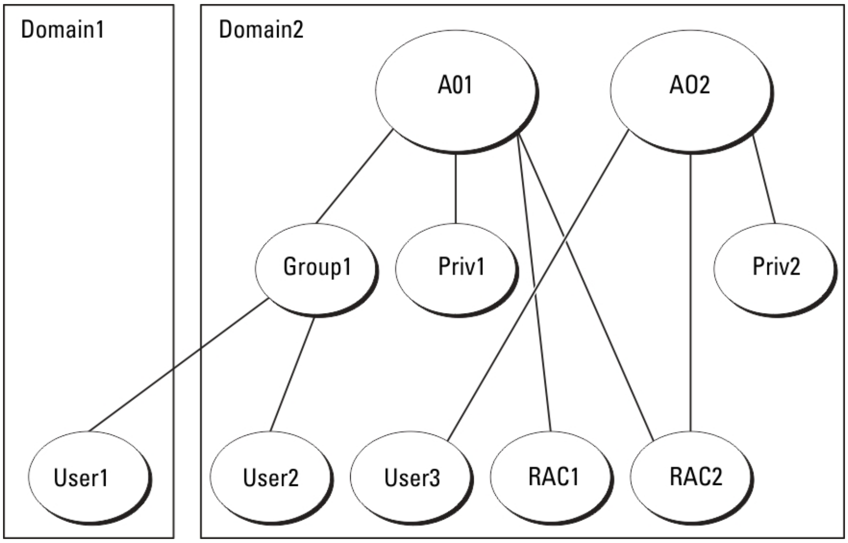
When adding Universal Groups from separate domains, create an Association Object with Universal Scope. The Default Association objects created by the Dell Schema Extender Utility are Domain Local Groups and does not work with Universal Groups from other domains.



To configure the objects for the single domain scenario:

1. Create two Association Objects.
2. Create two RAC Device Objects, RAC1 and RAC2, to represent the two CMCs.
3. Create two Privilege Objects, Priv1 and Priv2, in which Priv1 has all privileges (administrator) and Priv2 has login privilege.
4. Group user1 and user2 into Group1.
5. Add Group1 as Members in Association Object 1 (A01), Priv1 as Privilege Objects in A01, and RAC1, RAC2 as RAC Devices in A01.
6. Add User3 as Members in Association Object 2 (A02), Priv2 as Privilege Objects in A02, and RAC2 as RAC Devices in A02.

The following figure provides an example of Active Directory objects in multiple domains. In this scenario, you have two CMCs (RAC1 and RAC2) and three existing Active Directory users (user1, user2, and user3). User1 is in Domain1, and user2 and user 3 are in Domain2. In this scenario, configure user1 and user 2 with administrator privileges to both CMCs and configure user3 with login privileges to the RAC2 card.



To configure the objects for the multiple domain scenario:

1. Ensure that the domain forest function is in Native or Windows 2003 mode.
2. Create two Association Objects, A01 (of Universal scope) and A02, in any domain. The figure Setting Up Active Directory Objects in Multiple Domains shows the objects in Domain2.
3. Create two RAC Device Objects, RAC1 and RAC2, to represent the two CMCs.
4. Create two Privilege Objects, Priv1 and Priv2, in which Priv1 has all privileges (administrator) and Priv2 has login privilege.
5. Group user1 and user2 into Group1. The group scope of Group1 must be Universal.
6. Add Group1 as Members in Association Object 1 (A01), Priv1 as Privilege Objects in A01, and RAC1, RAC2 as RAC Devices in A01.
7. Add User3 as Members in Association Object 2 (A02), Priv2 as Privilege Objects in A02, and RAC2 as RAC Devices in A02.

Configuring Extended Schema Active Directory

To configure Active Directory to access CMC:

1. Extend the Active Directory schema.
2. Extend the Active Directory Users and Computers Snap-in.
3. Add CMC users and their privileges to Active Directory.
4. Enable SSL on each of your domain controllers.
5. Configure CMC Active Directory properties using CMC Web interface or RACADM.

Related Links

Extending Active Directory Schema
Installing Dell Extension to the Active Directory Users and Computers Snap-In
Adding CMC Users and Privileges to Active Directory
Configuring Active Directory With Extended Schema Using CMC Web Interface
Configuring Active Directory With Extended Schema Using RACADM

Extending Active Directory Schema

Extending your Active Directory schema adds a Dell organizational unit, schema classes and attributes, and example privileges and association objects to the Active Directory schema. Before you extend the schema, make sure 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 is not 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:

- **DVDdrive:\SYSMGMT\ManagementStation\support\OMActiveDirectory_T ools \Remote_Management_Advanced\LDIF_Files**
- **<DVDdrive>:\SYSMGMT\ManagementStation\support\OMActiveDirector y_Tools \Remote_Management_Advanced\Schema Extender**

To use the LDIF files, see the instructions in the readme included in the **LDIF_Files** directory.

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

Using Dell Schema Extender

⚠ **CAUTION: The Dell Schema Extender uses the SchemaExtenderOem.ini file. To make sure 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 classes and attributes exist. For more information on classes and attributes, see Classes and Attributes. See the Microsoft documentation for details about using the MMC and the Active Directory Schema Snap-in.

Classes and Attributes

Table 18. : 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 19. : dellRacDevice Class

OID	1.2.840.113556.1.8000.1280.1.7.1.1
Description	Represents the Dell RAC device. The RAC must be configured as delliDRACDevice in Active Directory. This configuration enables CMC to send Lightweight Directory Access Protocol (LDAP) queries to Active Directory.
Class Type	Structural Class
SuperClasses	dellProduct
Attributes	dellSchemaVersion dellRacType

Table 20. : 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

OID	1.2.840.113556.1.8000.1280.1.7.1.2
Attributes	dellProductMembers dellPrivilegeMember

Table 21. : dellRAC4Privileges Class

OID	1.2.840.113556.1.8000.1280.1.1.1.3
Description	Defines the privileges (Authorization Rights) for CMC device.
Class Type	Auxiliary Class
SuperClasses	None
Attributes	dellIsLoginUser dellIsCardConfigAdmin dellIsUserConfigAdmin dellIsLogClearAdmin dellIsServerResetUser dellIsTestAlertUser dellIsDebugCommandAdmin dellPermissionMask1 dellPermissionMask2

Table 22. : 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 23. : 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 24. : List of Attributes Added to the Active Directory Schema

Assigned OID/Syntax Object Identifier	Single Valued
Attribute: `dellPrivilegeMember` **Description**: List of `dellPrivilege` objects that belong to this attribute.	FALSE

Assigned OID/Syntax Object Identifier	Single Valued
OID: 1.2.840.113556.1.8000.1280.1.1.2.1 **Distinguished Name**: (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	
Attribute: `dellProductMembers` **Description**: List of `dellRacDevices` objects that belong to this role. This attribute is the forward link to the `dellAssociationMembers` backward link. **Link ID**: 12070 **OID**: 1.2.840.113556.1.8000.1280.1.1.2.2 **Distinguished Name**: (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
Attribute: `dellIsCardConfigAdmin` **Description**: TRUE if the user has Card Configuration rights on the device. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.4 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
Attribute: `dellIsLoginUser` **Description**: TRUE if the user has Login rights on the device. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.3 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
Attribute: `dellIsUserConfigAdmin` **Description**: TRUE if the user has User Configuration Administrator rights on the device. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.5 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
Attribute: `delIsLogClearAdmin` **Description**: TRUE if the user has Clear Logs Administrator rights on the device. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.6 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
Attribute: `dellIsServerResetUser` **Description**: TRUE if the user has Server Reset rights on the device. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.7 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
Attribute: `dellIsTestAlertUser` **Description**: TRUE if the user has Test Alert User rights on the device. **OID**: 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
Attribute: `dellIsDebugCommandAdmin` **Description**: TRUE if the user has Debug Command Admin rights on the device.	TRUE

Assigned OID/Syntax Object Identifier	Single Valued
OID: 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)	
Attribute: `dellSchemaVersion` **Description**: The Current Schema Version is used to update the schema. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.12 Case Ignore String(LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
Attribute: `dellRacType` **Description**: This attribute is the Current Rac Type for the dellRacDevice object and the backward link to the dellAssociationObjectMembers forward link. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.13 Case Ignore String(LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
Attribute: `dellAssociationMembers` **Description**: List of dellAssociationObjectMembers that belong to this Product. This attribute is the backward link to the dellProductMembers Linked attribute. **Link ID**: 12071 **OID**: 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
Attribute: `dellPermissionsMask1` **OID**: 1.2.840.113556.1.8000.1280.1.6.2.1 Integer (LDAPTYPE_INTEGER)	
Attribute: `dellPermissionsMask2` **OID**: 1.2.840.113556.1.8000.1280.1.6.2.2 Integer (LDAPTYPE_INTEGER)	

Installing Dell Extension to the Active Directory Users and Computers Snap-In

When you extend the schema in Active Directory, you must also extend the Active Directory Users and Computers Snap-in so the administrator can manage RAC (CMC) devices, users and user groups, RAC associations, and RAC privileges.

When you install your systems management software using the *Dell Systems Management Tools and Documentation* DVD, you can extend 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 64-bit Windows Operating Systems, the Snap-in installer is located under:**<DVDdrive>:\SYSMGMT\ManagementStation\support\OMActiveDirect ory_SnapIn64**

For more information about the Active Directory Users and Computers Snap-in, see Microsoft documentation.

Adding CMC Users and Privileges to Active Directory

Using the Dell-extended Active Directory Users and Computers Snap-in, you can add CMC users and privileges by creating RAC device, association, and privilege objects. To add each object, perform the following:

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

Related Links

- Adding Objects to Association Object
- Creating RAC Device Object
- Creating Privilege Object
- Creating Association Object

Creating RAC Device Object

To create RAC 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. Enter a name for the new object. The name must be identical to the CMC name that you enter in "Configuring Active Directory With Extended Schema Using CMC Web Interface".
4. Select **RAC Device Object** and click **OK**.

Creating Privilege Object

To create prvivlege object:

NOTE: You must create a privilege object 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. Enter a name for the new object.
4. Select **Privilege Object** and click **OK**.
5. Right-click the privilege object that you created, and select **Properties**.
6. Click the **RAC Privileges** tab and assign the privileges for the user or group. For more information about CMC user privileges, see Types of Users.

Creating Association Object

The Association Object is derived from a Group and must contain a Group Type. The Association Scope specifies the Security Group Type for the Association Object. When you create an Association Object, choose the Association Scope that applies to the type of objects you intend to add. For example, if you select Universal, the association objects are only available when the Active Directory Domain is functioning in Native Mode or above.

To create association object:

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. Enter a name for the new object and select **Association Object**.
4. Select the scope for the **Association Object** and click **OK**.

Adding Objects to Association Object

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

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

Related Links

- Adding Users or User Groups
- Adding Privileges

[Adding RAC Devices or RAC Device Groups](#)

Adding Users or User Groups

To add users or user groups:

1. Right-click the **Association Object** and select **Properties**.
2. Select the **Users** tab and click **Add**.
3. Enter the user or user group name and click **OK**.

Adding Privileges

To add privileges:

1. Select the **Privileges Object** tab and click **Add**.
2. Enter the privilege object 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 RAC device. Only one privilege object can be added to an Association Object.

Adding RAC Devices or RAC Device Groups

To add RAC devices or RAC device groups:

1. Select the **Products** tab and click **Add**.
2. Enter RAC devices or RAC device group name and click **OK**.
3. In the **Properties** window, click **Apply** and click **OK**.

   Click the **Products** tab to add one or more RAC devices to the association. The associated devices specify the RAC devices connected to the network that are available for the defined users or user groups. Multiple RAC devices can be added to an Association Object.

Configuring Active Directory With Extended Schema Using CMC Web Interface

To configure Active Directory with extended schema using CMC Web interface:

NOTE: For information about the various fields, see the *CMC Online Help*.

1. In the system tree, go to **Chassis Overview**, and then click **User Authentication** → **Directory Services**.
2. Select **Microsoft Active Directory (Extended Schema)**. The settings to be configured for extended schema is displayed on the same page.
3. Specify the following:

   - Enable Active Directory, enter the root domain name, and the timeout value.
   - If you want the directed call to search the domain controller and global catalog, select the **Search AD Server to search (Optional)** option and specify the domain controller and global catalog details.

     NOTE: Setting the IP address as 0.0.0.0 disables CMC from searching for a server.

     NOTE: You can specify a list of domain controller or global catalog servers separated by commas. CMC allows you to specify up to three IP addresses or host names.

     NOTE: Domain controller and global catalog servers that are not correctly configured for all domains and applications may produce unexpected results during the functioning of the existing applications/domains.
4. Click **Apply** to save the settings.

   NOTE: You must apply the settings before continuing. If you do not apply the settings, the settings are lost when you navigate to the next page.

5. In the **Extended Schema Settings** section, enter the CMC device name and the domain name.
6. If you have enabled certificate validation, you must upload the domain forest root certificate authority-signed certificate to CMC. In the **Manage Certificates** section, type the file path of the certificate or browse to the certificate file. Click **Upload** to upload the file to CMC.

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

   The SSL certificates for the domain controllers must be signed by the root certificate authority-signed certificate. The root certificate authority-signed certificate must be available on the management station accessing CMC.

   CAUTION: SSL certificate validation is required by default. Disabling this certificate is risky.

7. If you have enabled Single Sign-On (SSO), in the Kerberos Keytab section, click **Browse**, specify the keytab file and click **Upload**. When the upload is complete, a message is displayed indicating a successful or failed upload.
8. Click **Apply**. The CMC Web server automatically restarts after you click **Apply**.
9. Log in to the CMC Web interface.
10. Select **Chassis** in the system tree, click the **Network** tab, then click the **Network** subtab. The **Network Configuration** page is displayed.
11. If **Use DHCP** for CMC Network Interface IP Address, is enabled, do one of the following:

    – Select **Use DHCP to Obtain DNS Server Addresses**to enable the DNS server addresses to be obtained automatically by the DHCP server.

    – Manually configure a DNS server IP address by leaving the **Use DHCP to Obtain DNS Server Addresses** check box unchecked and then typing your primary and alternate DNS server IP addresses in the fields provided.

12. Click **Apply Changes**. The Active Directory settings for extended schema is configured.

Configuring Active Directory With Extended Schema Using RACADM

To configure the CMC Active Directory with Extended Schema using the RACADM:

1. Open a serial/Telnet/SSH text console to CMC, log in, and type:

   ```
   racadm config -g cfgActiveDirectory -o cfgADEnable 1
   racadm config -g cfgActiveDirectory -o cfgADType 1
   racadm config -g cfgActiveDirectory -o
   cfgADRacDomain <fully qualified CMC domain name>
   racadm config -g cfgActiveDirectory -o
   cfgADRootDomain <fully qualified root domain name>
   racadm config -g cfgActiveDirectory -o
   cfgADRacName <CMC common name>
   racadm sslcertupload -t 0x2 -f <ADS root CA
   certificate> -r
   racadm sslcertdownload -t 0x1 -f <CMC SSL certificate>
   ```

   NOTE: You can use this command through remote RACADM only. For more information on remote RACADM, see *RACADM Command Line Reference Guide for iDRAC7 and CMC*.

   Optional: If you want to specify an LDAP or Global Catalog server instead of using the servers returned by the DNS server to search for a user name, type the following command to enable the **Specify Server** option:

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

   NOTE: When you use the **Specify Server** option, the host name in the certificate authority-signed certificate is not matched against the name of the specified server. This is particularly useful if you are a CMC administrator, because it enables you to enter a host name as well as an IP address.

After you enable the **Specify Server** option, you can specify an LDAP server and global catalog with IP addresses or fully qualified domain names (FQDNs) of the servers. The FQDNs consist of the host names and the domain names of the servers.

To specify an LDAP server, type:

```
racadm config -g cfgActiveDirectory -o
cfgADDomainController <AD domain controller IP address>
```

To specify a Global Catalog server, type:

```
racadm config -g cfgActiveDirectory -o
cfgADGlobalCatalog <AD global catalog IP address>
```

NOTE: Setting the IP address as 0.0.0.0 disables CMC from searching for a server.

NOTE: You can specify a list of LDAP or global catalog servers separated by commas. CMC allows you to specify up to three IP addresses or host names.

NOTE: LDAP or LDAPs that are not correctly configured for all domains and applications may produce unexpected results during the functioning of the existing applications/domains.

2. Specify a DNS server using one of the following options:

   – If DHCP is enabled on CMC and you want to use the DNS address obtained automatically by the DHCP server, type the following command:

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

   – If DHCP is disabled on CMC, or if DHCP is enabled but you want to specify your DNS IP address manually, type following commands:

   ```
   racadm config -g cfgLanNetworking -o
   cfgDNSServersFromDHCP 0
   racadm config -g cfgLanNetworking -o
   cfgDNSServer1 <primary DNS IP address>
   racadm config -g cfgLanNetworking -o
   cfgDNSServer2 <secondary DNS IP address>
   ```

   The Extended Schema feature configuration is complete.

Configuring Generic LDAP Users

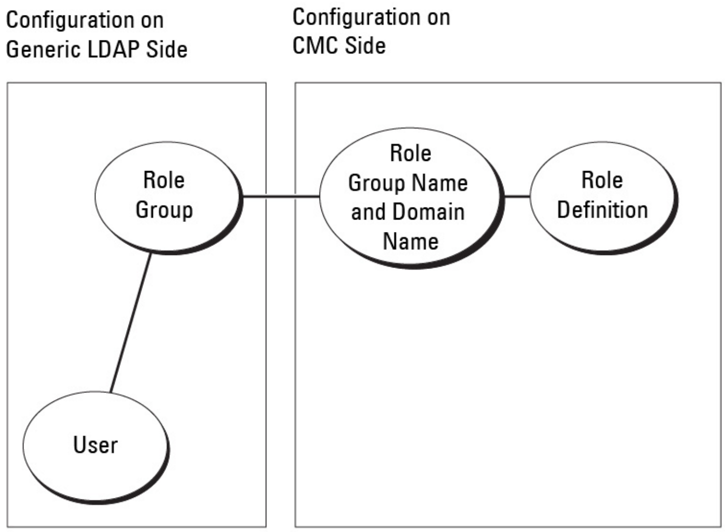
CMC provides a generic solution to support Lightweight Directory Access Protocol (LDAP)-based authentication. This feature does not require any schema extension on your directory services.

A CMC administrator can now integrate the LDAP server user logins with CMC. This integration requires configuration on both LDAP server and CMC. On the LDAP server, a standard group object is used as a role group. A user who has CMC access becomes a member of the role group. Privileges are still stored on CMC for authorization similar to the working of the Standard Schema setup with Active Directory support.

To enable the LDAP user to access a specific CMC card, the role group name and its domain name must be configured on the specific CMC card. You can configure a maximum of five role groups in each CMC. A user has the option to be added to multiple groups within the directory service. If a user is a member of multiple groups, then the user obtains the privileges of all their groups.

For information about the privileges level of the role groups and the default role group settings, see Types of Users.

The following figure illustrates configuration of CMC with Generic LDAP.


Configuration on
Generic LDAP Side
Configuration on
CMC Side
Role
Group
User
Role
Group Name
and Domain
Name
Role
Definition

Configuring the Generic LDAP Directory to Access CMC

The CMC's Generic LDAP implementation uses two phases in granting access to a user—user authentication and then user authorization.

Authentication of LDAP Users

Some directory servers require a bind before any searches can be performed against a specific LDAP server.

To authenticate a user:

1. Optionally bind to the Directory Service. The default is an anonymous bind.
2. Search for the user based upon their user login. The default attribute is `uid`.
3. If more than one object is found, then the process returns an error.
4. Unbind and perform a bind with the user's DN and password.
5. If the bind fails, then the login fails.

   If these steps succeed, the user is authenticated.

Authorization of LDAP Users

To authorize a user:

1. Search each configured group for the user's domain name within the `member or uniqueMember` attributes. An administrator can configure this field.
2. For every group the user is a member of, add their privileges together.

Configuring Generic LDAP Directory Service Using CMC Web-Based Interface

To configure the generic LDAP directory service using Web interface:

NOTE: You must have **Chassis Configuration Administrator** privilege.

1. In the system tree, go to **Chassis Overview**, and then click **User Authentication** → **Directory Services**.
2. Select Generic **LDAP**. The settings to be configured for standard schema is displayed on the same page.
3. Specify the following:

   NOTE: For information about the various fields, see the *CMC Online Help*.

   – Common Settings
   – Server to use with LDAP:

     * Static server — Specify the FQDN or IP address and the LDAP port number.
     * DNS server — Specify the DNS server to retrieve a list of LDAP servers by looking up their SRV record within the DNS.

       The following DNS query is performed for SRV records:

       ```
       _[Service Name]._tcp.[Search Domain]
       ```

       where <`Search Domain`> is the root level domain to use within the query and <`Service Name`> is the service name to use within the query.

       For example:

       ```
       _ldap._tcp.dell.com
       ```

       where `ldap` is the service name and `dell.com` is the search domain.

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

   NOTE: You must apply the settings before continuing. If you do not apply the settings, the settings are lost when you navigate to the next page.

5. In the **Group Settings** section, click a **Role Group**. The **Configure LDAP Role Group** page is displayed.
6. Specify the group domain name and privileges for the role group.
7. Click **Apply** to save the role group settings, click **Go Back To Configuration page**, and then select **Generic LDAP**.
8. If you have selected **Certificate Validation Enabled** option, then in the **Manage Certificates** section, specify the CA certificate to validate the LDAP server certificate during SSL handshake and click **Upload**. The certificate is uploaded to CMC and the details are displayed.
9. Click **Apply**. The generic LDAP directory service is configured.

Configuring Generic LDAP Directory Service Using RACADM

To configure the LDAP directory service, use the objects in `cfgLdap` and `cfgLdapRoleGroup` RACADM groups.

There are many options to configure LDAP logins. In most of the cases, some options can be used with their default settings.

NOTE: It is highly recommended to use the racadm `testfeature -f LDAP` command to test the LDAP settings for first time setups. This feature supports both IPv4 and IPv6.

The required property changes include enabling LDAP logins, setting the server FQDN or IP, and configuring the base DN of the LDAP server.

- `$ racadm config -g cfgLDAP -o cfgLDAPEnable 1`
- `$ racadm config -g cfgLDAP -o cfgLDAPServer 192.168.0.1`
- `$ racadm config -g cfgLDAP -o cfgLDAPBaseDN dc=company,dc=com`

CMC can be configured to optionally query a DNS server for SRV records. If the `cfgLDAPSRVLookupEnable` property is enabled the `cfgLDAPServer` property is ignored. The following query is used to search the DNS for SRV records:

```
_ldap._tcp.domainname.com
```

`ldap` in the above query is the `cfgLDAPSRVLookupServiceName` property.

`cfgLDAPSRVLookupDomainName` is configured to be **domainname.com**.

For more information about the RACADM objects, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at **support.dell.com/manuals**.

10

Configuring CMC For Single Sign-On Or Smart Card Login

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

Starting with CMC version 2.10, CMC supports Kerberos based Active Directory authentication to support Smart Card and SSO logins.

SSO uses kerberos as an authentication method allowing users who have signed in to the domain an automatic or single sign-on to subsequent applications such as Exchange. For single sign-on login, CMC uses the client system's credentials, which are cached by the operating system after you log in using a valid Active Directory account.

Two-factor-authentication, provides a higher-level of security by requiring users to have a password or PIN and a physical card containing a private key or digital certificate. Kerberos uses this two-factor authentication mechanism allowing systems to prove their authenticity.

NOTE: Selecting a login method does not set policy attributes with respect to other login interfaces, for example, SSH. You must set other policy attributes for other login interfaces as well. If you want to disable all other login interfaces, navigate to the **Services** page and disable all (or some) login interfaces.

Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows 7, and Windows Server 2008 can use Kerberos as the authentication mechanism for SSO and smart card login.

For information on Kerberos, see the Microsoft website.

Related Links

System Requirements

Prerequisites For Single Sign-On Or Smart Card Login

Configuring CMC SSO Or Smart Card Login For Active Directory Users

System Requirements

To use the Kerberos authentication, the network must include:

- DNS server
- Microsoft Active Directory Server

  NOTE: If you are using Active Directory on Windows 2003, make sure that you have the latest service packs and patched installed on the client system. If you are using Active Directory on Windows 2008, make sure that you have installed SP1 along with the following hot fixes:

  Windows6.0-KB951191-x86.msu for the KTPASS utility. Without this patch the utility generates bad keytab files.

  Windows6.0-KB957072-x86.msu for using GSS_API and SSL transactions during an LDAP bind.
- Kerberos Key Distribution Center (packaged with the Active Directory Server software).
- DHCP server (recommended).
- The DNS server reverse zone must have an entry for the Active Directory server and CMC.

Client Systems

- For only Smart Card login, the client system must have the Microsoft Visual C++ 2005 redistributable. For more information see **www.microsoft.com/downloads/details.aspx?FamilyID= 32BC1BEEA3F9-4C13-9C99-220B62A191EE&displaylang=en**
- For Single Sign-On or smart card login, the client system must be a part of the Active Directory domain and Kerberos Realm.

CMC

- CMC must have firmware version 2.10 or later.
- Each CMC must have an Active Directory account.
- CMC must be a part of the Active Directory domain and Kerberos Realm.

Prerequisites For Single Sign-On Or Smart Card Login

The pre-requisites to configure SSO or Smart Card logins are:

- Setup the kerberos realm and Key Distribution Center (KDC) for Active Directory (ksetup).
- A robust NTP and DNS infrastructure to avoid issues with clock drift and reverse lookup.
- Configure CMC with Active Directory standard schema role group with authorized members.
- For smart card, create Active Directory users for each CMC, configured to use Kerberos DES encryption but not pre-authentication.
- Configure the browser for SSO or smart card login.
- Register the CMC users to the Key Distribution Center with Ktpass (this also outputs a key to upload to CMC).

Related Links

Configuring Standard Schema Active Directory
Configuring Extended Schema Active Directory
Configuring Browser For SSO Login
Generating Kerberos Keytab File
Configuring Browser For Smart Card Login

Generating Kerberos Keytab File

To support the SSO and smart card login authentication, CMC supports Windows Kerberos network. The ktpass tool (available from 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. For more information on the ktpass utility, see the Microsoft website.

Before generating a keytab file, you must create an Active Directory user account for use with the **-mapuser** option of the ktpass command. You must use the same name as the CMC DNS name, to which you upload the generated keytab file.

To generate a keytab file using the ktpass tool:

1. Run the *ktpass* utility on the domain controller (Active Directory server) where you want to map CMC to a user account in Active Directory.
2. Use the following `ktpass` command to create the Kerberos keytab file:

   ```
   C:\>ktpass -princ HTTP/cmcname.domain_name.com@REALM_NAME.COM - mapuser
   dracname -crypto DES-CBC-MD5 -ptype KRB5_NT_PRINCIPAL -pass * -out c:
   \krbkeytab
   ```

   NOTE: The `cmcname.domainname.com` must be lower case as required by RFC and the `@REALM_NAME` must be uppercase. In addition, CMC supports the DES-CBC-MD5 type of cryptography for Kerberos authentication.

   A keytab file is generated that must be uploaded to CMC.

   NOTE: The keytab contains an encryption key and must be kept secure. For more information on the *ktpass* utility, see the **Microsoft** website.

Configuring CMC For Active Directory Schema

For information to configure CMC for Active Directory standard schema, see Configuring Standard Schema Active Directory.

For information to configure CMC for Extended Schema Active Directory, see Extended Schema Active Directory Overview.

Configuring Browser For SSO Login

Single Sign-On (SSO) is supported on Internet Explorer versions 6.0 and later and Firefox versions 3.0 and later.

NOTE: The following instructions are applicable only if CMC uses Single Sign-On with Kerberos authentication.

Internet Explorer

To configure Internet Explorer for Single Sign-On:

1. In the Internet Explorer, select **Tools** → **Internet Options**.
2. On the **Security** tab, under **Select a zone to view or change security settings**, select **Local Intranet**.
3. Click **Sites**.

   The **Local Intranet** dialog box is displayed.
4. Click **Advanced** .

   The **Local Intranet Advance Settings** dialog box is displayed.
5. In the **Add this site to the zone**, type the name of CMC and the domain it belongs to and click **Add**.

   NOTE: You can use a wildcard (*) to specify all devices or users in that domain.

Mozilla Firefox

1. In Firefox, type **about:config** in the Address bar.

   NOTE: If the browser displays the **This might void your warranty warning**, click **I'll be careful. I promise**.
2. In the **Filter** text box, type **negotiate**.

   The browser displays a list of preference names limited to those containing the word negotiate.
3. From the list, double-click **network.negotiate-auth.trusted-uris**.
4. In the **Enter string value** dialog box, type the CMC's domain name and click **OK**.

Configuring Browser For Smart Card Login

Mozilla Firefox — CMC 2.10 does not support Smart Card login through the Firefox browser.

Internet Explorer — Ensure that the Internet Browser is configured to download Active-X plug-ins.

Configuring CMC SSO Or Smart Card Login For Active Directory Users

You can use CMC Web interface or RACADM to configure CMC SSO or smart card login.

Related Links

Prerequisites For Single Sign-On Or Smart Card Login
Uploading Keytab File

Configuring CMC SSO Or Smart Card Login For Active Directory Users Using Web Interface

To configure Active Directory SSO or smart card login for CMC:

NOTE: For information about the options, see the *CMC Online Help*.

1. While configuring Active Directory to setup a user account, perform the following additional steps:
   - Upload the keytab file
   - To enable SSO, select **Enable Single Sign-On** option.
   - To enable smart card login, select **Enable Smart-Card Login** option.

     NOTE: All command line out-of-band interfaces including secure shell (SSH), Telnet, Serial, and remote RACADM remain unchanged if this option is selected.
2. Click **Apply**.

   The settings are saved.

   You can test the Active Directory using Kerberos authentication using the RACADM command:

   ```
   testfeature -f adkrb -u <user>@<domain>
   ```

   where `<user>` is a valid Active Directory user account.

   A command success indicates that CMC is able to acquire Kerberos credentials and access the user's Active Directory account. If the command is not successful, resolve the error and run the command again. For more information, see RACADM *Command Line Reference Guide for iDRAC7 and CMC* on **support.dell.com/manuals**.

Uploading Keytab File

The Kerberos keytab file serves as the CMC's user name and password credentials to the Kerberos Data Center (KDC), which in turns allows access to the Active Directory. Each CMC in the Kerberos realm must be registered with the Active Directory and must have a unique keytab file.

You can upload a Kerberos Keytab generated on the associated Active Directory Server. You can generate the Kerberos Keytab from the Active Directory Server by executing the **ktpass.exe** utility. This keytab establishes a trust relationship between the Active Directory Server and CMC.

To upload the keytab file:

1. In the system tree, go to **Chassis Overview**, and then click **User Authentication** → **Directory Services**.
2. Select **Microsoft Active Directory (Standard Schema)**.

3. In the **Kerberos Keytab** section, click **Browse**, select keytab file, and click **Upload** .

   When the upload is complete, a message is displayed indicating whether the keytab file is successfully uploaded or not.

Configuring CMC SSO Login Or Smart Card Login For Active Directory Users Using RACADM

In addition to the steps performed while configuring Active Directory, run the following command to enable SSO:

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

In addition to the steps performed while configuring Active Directory, use the following objects to enable smart card login:

- `cfgSmartCardLogonEnable`
- `cfgSmartCardCRLEnable`

11

Configuring CMC to Use Command Line Consoles

This section provides information about the CMC command line console (or serial/Telnet/Secure Shell console) features, and explains how to set up the system so that you can perform systems management actions through the console. For information on using the RACADM commands in CMC through the command line console, see *RACADM Command Line Reference Guide for iDRAC7 and CMC*.

Related Links

Logging In to CMC Using Serial, Telnet, or SSH Console

CMC Command Line Console Features

The CMC supports the following serial, Telnet, and SSH console features:

- One serial client connection and up to four simultaneous Telnet client connections.
- Up to four simultaneous Secure Shell (SSH) client connections.
- RACADM command support.
- Built-in connect command connecting to the serial console of servers and I/O modules; also available as `racadm connect`.
- Command Line editing and history.
- Session timeout control on all console interfaces.

CMC Command Line Commands

When you connect to the CMC command line, you can enter these commands:

Table 25. : CMC Command Line Commands

Command	Description
`racadm`	RACADM commands begin with the keyword `racadm`and are followed by a subcommand. For more information, see *RACADM Command Line Reference Guide for iDRAC7 and CMC*.
`connect`	Connects to the serial console of a server or I/O module. For more information, see Connecting to Servers or I/O Modules Using Connect Command . **NOTE:** You can also use the racadm `connect` command.
`exit`, `logout`, and `quit`	All the commands perform the same action. They end the current session and return to a login prompt.

Using Telnet Console With CMC

You can have up to four Telnet sessions with CMC at a time.

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

Using SSH With CMC

SSH is a command line session that includes the same capabilities as a Telnet session, but with session negotiation and encryption to improve security. The CMC supports SSH version 2 with password authentication. SSH is enabled on the CMC by default.

NOTE: The CMC does not support SSH version 1.

When an error occurs during the CMC login, the SSH client issues an error message. The message text is dependent on the client and is not controlled by the CMC. Review the RACLog messages to determine the cause of the failure.

NOTE: `OpenSSH` must be run from a VT100 or ANSI terminal emulator on Windows. You can also run `OpenSSH` using **Putty.exe**. Running `OpenSSH` at the Windows command prompt does not provide full functionality (that is, some keys do not respond and no graphics are displayed). For Linux, run SSH Client Services to connect to CMC with any shell.

Four simultaneous SSH sessions are supported at a time. The session timeout is controlled by the `cfgSsnMgtSshIdleTimeout` property. For more information, see the database property chapter of the *RACADM Command Line Reference Guide for iDRAC7 and CMC*, the **Services Management** page in the Web interface, or see Configuring Services

CMC also supports Public Key Authentication (PKA) over SSH. This authentication method improves SSH scripting automation by removing the need to embed or prompt for user ID/password. For more information, see Configure Public Key Authentication over SSH .

SSH is enabled by default. If SSH is disabled, then you can enable it using any other supported interface.

To configure SSH, see Configuring Services.

Related Links

Configuring Services

Supported SSH Cryptography Schemes

To communicate with CMC using SSH protocol, it supports multiple cryptography schemes listed in the following table.

Table 26. : 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

Scheme Type	Scheme
	• 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

Configure Public Key Authentication over SSH

You can configure up to 6 public keys that can be used with the service username over SSH interface. Before adding or deleting public keys, be sure to use the view command to see what keys are already set up so a key is not accidentally overwritten or deleted. The service username is a special user account that can be used when accessing the CMC through SSH. When the PKA over SSH is set up and used correctly, you need not enter username or passwords to log in to the CMC. This can be very useful to set up automated scripts to perform various functions.

NOTE: There is no GUI support for managing this feature; you can only use RACADM.

When adding new public keys, ensure that the existing keys are not already at the index where the new key is added. CMC 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.

When using the public key comment section of the public key, remember that only the first 16 characters are utilized by the CMC. The public key comment is used by the CMC to distinguish SSH users when using the RACADM `getssninfo` command since all PKA users use the service username to log in.

For example, if two public keys are set up one with comment PC1 and one with comment PC2:

```
racadm getssninfo
Type       User  IP Address  Login
Date/Time
SSH        PC1   x.x.x.x     06/16/2009
09:00:00
SSH        PC2   x.x.x.x     06/16/2009
09:00:00
```

For more information on the `sshpkauth`, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC*.

Related Links

Generating Public Keys for Windows
Generating Public Keys for Linux
RACADM Syntax Notes for CMC
Viewing Public Keys
Adding Public Keys
Deleting Public Keys

Generating Public Keys for Windows

Before adding an account, a public key is required from the system that accesses the CMC over SSH. There are two 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.

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 SSH-2 RSA or SSH-2 DSA for the type of key to generate (SSH-1 is not supported).
2. Enter the number of bits for the key. The number should be between 768 and 4096.

   NOTE: The CMC may not display a message if you add keys less than 768 or greater than 4096, but when you try to log in, these keys it fails.

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 have two options for using the public key:

   – Save the public key to a file to upload later.

   – Copy and paste the text from the **Public key for pasting** window when adding the account using the text option.

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 type:

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

where,

`–t` option must be 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.

The <`passphrase`> is optional. After the command completes, use the public file to pass to the RACADM for uploading the file.

RACADM Syntax Notes for CMC

When using the `racadm sshpkauth` command, ensure the following:

- For the `–i` option, the parameter must be`svcacct`. All other parameters for `–i` fail in CMC. The `svcacct` is a special account for public key authentication over SSH in CMC.
- To log in to the CMC, the user must be service. Users of the other categories do have access to the public keys entered using the `sshpkauth` command.

Viewing Public Keys

To view the public keys that you have added to the CMC, type:

```
racadm sshpkauth –i svcacct –k all –v
```

To view one key at a time, replace`all` with a number from 1 – 6. For example, to view key 2, type:

```
racadm sshpkauth –i svcacct –k 2 –v
```

Adding Public Keys

To add a public key to the CMC using the file upload `-f` option, type:

```
racadm sshpkauth –i svcacct –k 1 –p 0xfff –f <public key file>
```

NOTE: You can only use the file upload option with remote RACADM. For more information, see *RACADM Command Line Reference Guide for iDRAC7 and CMC*.

To add a public key using the text upload option, type:

```
racadm sshpkauth –i svcacct –k 1 –p 0xfff –t "<public key text>"
```

Deleting Public Keys

To delete a public key type:

```
racadm sshpkauth –i svcacct –k 1 –d
```

To delete all public keys type:

```
racadm sshpkauth –i svcacct –k all –d
```

Enabling Front Panel to iKVM Connection

For information and instructions on using the iKVM front panel ports, see Enabling or Disabling Access to iKVM from Front Panel

Configuring Terminal Emulation Software

The CMC supports a serial text console from a management station running one of the following types of terminal emulation software:

- Linux Minicom.
- Hilgraeve's HyperTerminal Private Edition (version 6.3).

Perform the steps in the following subsections to configure the required type of terminal software.

Configuring Linux Minicom

Minicom is a 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. See the information in the Required Minicom Settings section to configure other versions of Minicom.

Configuring Minicom Version 2.0

NOTE: For best results, set the **cfgSerialConsoleColumns** property to match the number of columns. Be aware that the prompt consumes two characters. For example, for an 80-column terminal window:

```
racadm config –g cfgSerial –o
cfgSerialConsoleColumns 80.
```

1. 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 12.
2. At the Linux command prompt, type `minicom -s`.
3. Select **Serial Port Setup** and press <Enter>.
4. Press <a>, and then select the appropriate serial device (for example, `/dev/ttyS0`).

5. Press <e>, and then set the **Bps/Par/Bits** option to **115200 8N1**.
6. Press <f>, and then set **Hardware Flow Control** to **Yes** and set **Software Flow Control** to **No**. To exit the **Serial Port Setup** menu, press <Enter>.
7. Select **Modem and Dialing** and press <Enter>.
8. In the **Modem Dialing and Parameter Setup** menu, press <Backspace> to clear the **init**, **reset**, **connect**, and **hangup** settings so that they are blank, and then press <Enter> to save each blank value.
9. When all specified fields are clear, press <Enter> to exit the **Modem Dialing and Parameter Setup** menu.
10. Select **Exit From Minicom** and press <Enter>.
11. At the command shell prompt, type `minicom <Minicom config file name>`.
12. Press <Ctrl+a>, <x>, <Enter> to exit Minicom.

    Ensure that the Minicom window displays a login prompt. When the login prompt appears, your connection is successful. You are now ready to login and access the CMC command line interface.

Required Minicom Settings

See the following table to configure any version of Minicom.

Table 27. : Minicom Settings

Setting Description	Required Setting
Bps/Par/Bits	115200 8N1
Hardware flow control	Yes
Software flow control	No
Terminal emulation	ANSI
Modem dialing and parameter settings	Clear the **init**, **reset**, **connect**, and **hangup** settings so that they are blank

Connecting to Servers or I/O Modules Using Connect Command

The CMC can establish a connection to redirect the serial console of server or I/O modules.

For servers, serial console redirection can be accomplished using:

- CMC command line and the connect, or racadm connect command. For more information, see *RACADM Command Line Reference Guide for iDRAC7 and CMC*.
- iDRAC Web interface serial console redirection feature.
- iDRAC Serial Over LAN (SOL) functionality.

In a serial, Telnet, SSH console, the CMC supports the connect command to establish a serial connection to server or IOM modules. The server serial console contains both the BIOS boot and setup screens, and the operating system serial console. For I/O modules, the switch serial console is available.

CAUTION: When executed from the CMC serial console, the `connect -b` option stays connected until the CMC resets. This connection is a potential security risk.

NOTE: The `connect` command provides the `-b` (binary) option. The `-b` option passes raw binary data, and `cfgSerialConsoleQuitKey` is not used. Additionally, when connecting to a server using the CMC serial console, transitions in the DTR signal (for example, if the serial cable is removed to connect a debugger) do not cause a logout.

NOTE: If an IOM does not support console redirection, the `connect` command displays an empty console. In that case, to return to the CMC console, type the Escape sequence. The default console escape sequence is <Ctrl>\.

There are up to six IOMs on the managed system.

To connect to an IOM:

```
connect switch-n
```

where `n` is an IOM label A1, A2, B1, B2, C1, and C2.

(See Figure 13-1 for an illustration of the placement of IOMs in the chassis.) When you reference the IOMs in the connect command, the IOMs are mapped to switches as shown in the following table.

Table 28. : Mapping I/O Modules to Switches

I/O Module Label	Switch
A1	switch-a1 or switch- 1
A2	switch-a2 or switch-2
B1	switch-b1 or switch-3
B2	switch-b2 or switch-4
C1	switch-c1 or switch-5
C2	switch-c2 or switch-6

NOTE: There can only be one IOM connection per chassis at a time.

NOTE: You cannot connect to pass-throughs from the serial console.

To connect to a managed server serial console, use the command `connect server-nx`, where `n` is 1-8 and `x` is a,b, c, or d. You can also use the `racadm connect server-n` command. When you connect to a server using the `-b` option, binary communication is assumed and the escape character is disabled. If the iDRAC is not available, you see a `No route to host` error message.

The `connect server-n` command enables the user to access the server's serial port. After this connection is established, the user can see the server's console redirection through CMC's serial port that includes both the BIOS serial console and the operating system serial console.

NOTE: To see the BIOS boot screens, serial redirection has to be enabled in the servers' BIOS Setup. Also, you must set the terminal emulator window to 80x25. Otherwise, the screen is garbled.

NOTE: Not all keys work in the BIOS setup screens, so provide appropriate escape sequences for **CTRL+ALT+DEL**, and other escape sequences. The initial redirection screen displays the necessary escape sequences.

Related Links

Configuring the Managed Server BIOS for Serial Console Redirection
Configuring Windows for Serial Console Redirection
Configuring Linux for Server Serial Console Redirection During Boot
Configuring Linux for Server Serial Console Redirection After Boot

Configuring the Managed Server BIOS for Serial Console Redirection

It is necessary to connect to the managed server using the iKVM (see Managing Servers With iKVM) or establish a Remote Console session from the iDRAC7 Web interface (see the *iDRAC7 User's Guide* on **support.dell.com/manuals**).

Serial communication in the BIOS is OFF by default. To redirect host text console data to Serial over LAN, you must enable console redirection through COM1. To change the BIOS setting:

1. Boot the managed server.
2. Press <F2> to enter the BIOS setup utility during POST.

3. Scroll down to **Serial Communication** and press <Enter> . In the pop-up dialog box, the serial communication list displays these options:

   - off
   - on without console redirection
   - on with console redirection via COM1

   Use the arrow keys to navigate between these options.
4. Ensure that **On with console redirection via COM1** is enabled.
5. Enable **Redirection After Boot** (default value is **disabled**). This option enables BIOS console redirection across subsequent reboots.
6. Save the changes and exit.

   The managed server reboots.

Configuring Windows for Serial Console Redirection

There is no configuration necessary for servers running the Microsoft Windows Server versions, starting with Windows Server 2003. Windows receives information from the BIOS, and enable the Special Administration Console (SAC) console one COM1.

Configuring Linux for Server Serial Console Redirection During Boot

The following steps are specific to the Linux GRand Unified Bootloader (GRUB). Similar changes are necessary for using a different boot loader.

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

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

1. Locate the general setting sections in the file and add the following two new lines:

   ```
   serial --unit=1 --speed=57600
   terminal --timeout=10 serial
   ```
2. Append two options to the kernel line:

   ```
   kernel console=ttyS1,57600
   ```
3. If the **/etc/grub.conf** contains a `splashimage` directive, comment it out.

   The following example shows the changes described in this procedure.

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

```
timeout=10
#splashimage=(hd0,2)/grub/splash.xpm.gz
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=
ttyS1,57600
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
initrd /boot/initrd-2.4.9-e.3.img
```

When you edit the **/etc/grub.conf** file, follow these guidelines:

- Disable GRUB's graphical interface and use the text-based interface; otherwise, the GRUB screen is not displayed in console redirection. To disable the graphical interface, comment out the line starting with `splashimage`.
- To start multiple GRUB options to start console sessions through the serial connection, add the following line to all options:

  ```
  console=ttyS1,57600
  ```

  The example shows `console=ttyS1,57600` added to only the first option.

Configuring Linux for Server Serial Console Redirection 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
```

The following example shows the file with the new line.

```
#
# inittab This file describes how the INIT process
# should set up the system in a certain
# run-level.
#
# Author: Miquel van Smoorenburg
# Modified for RHS Linux by Marc Ewing and
# Donnie Barnes
#
# Default runlevel. The runlevels used by RHS are:
# 0 - halt (Do NOT set initdefault to this)
# 1 - Single user mode
# 2 - Multiuser, without NFS (The same as 3, if you
# do not have networking)
# 3 - Full multiuser mode
# 4 - unused
# 5 - X11
# 6 - reboot (Do NOT set initdefault to this)
#
id:3:initdefault:
# System initialization.
si::sysinit:/etc/rc.d/rc.sysinit
l0:0:wait:/etc/rc.d/rc 0
l1:1:wait:/etc/rc.d/rc 1
l2:2:wait:/etc/rc.d/rc 2
l3:3:wait:/etc/rc.d/rc 3
```

```
l4:4:wait:/etc/rc.d/rc 4
l5:5:wait:/etc/rc.d/rc 5
l6:6:wait:/etc/rc.d/rc 6
# Things to run in every runlevel.
ud::once:/sbin/update
# Trap CTRL-ALT-DELETE
ca::ctrlaltdel:/sbin/shutdown -t3 -r now
# When our UPS tells us power has failed, assume we
have a few
# minutes of power left. Schedule a shutdown for 2
minutes from now.
# This does, of course, assume you have power
installed and your
# UPS is connected and working correctly.
pf::powerfail:/sbin/shutdown -f -h +2 "Power Failure;
System Shutting Down"
# If power was restored before the shutdown kicked in,
cancel it.
pr:12345:powerokwait:/sbin/shutdown -c "Power
Restored; Shutdown Cancelled"
# Run gettys in standard runlevels
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
1:2345:respawn:/sbin/mingetty tty1
2:2345:respawn:/sbin/mingetty tty2
3:2345:respawn:/sbin/mingetty tty3
4:2345:respawn:/sbin/mingetty tty4
5:2345:respawn:/sbin/mingetty tty5
6:2345:respawn:/sbin/mingetty tty6

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

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

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

```
ttyS1
```

The following example shows a sample file with the new line.

```
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
```

12

Using FlexAddress and FlexAdress Plus Cards

This section provides information about FlexAddress and FlexAddress Plus cards, how to configure and use these cards.

Related Links

About FlexAddress
About FlexAddress Plus
FlexAddress and FlexAddress Plus Comparison

About FlexAddress

The FlexAddress feature is an optional upgrade that allows server modules to replace the factory-assigned World Wide Name and Media Access Control (WWN/MAC) network IDs with WWN/MAC IDs provided by the chassis.

Every server module is assigned unique WWN and/or MAC IDs as part of the manufacturing process. Before FlexAddress, if you had to replace one server module with another, the WWN/MAC IDs changes and Ethernet network management tools and SAN resources had to be reconfigured to identify the new server module.

FlexAddress allows CMC to assign WWN/MAC IDs to a particular slot and override the factory IDs. Hence, if the server module is replaced, the slotbased WWN/MAC IDs remain the same. This feature eliminates the need to reconfigure Ethernet network management tools and SAN resources for a new server module.

Additionally, the *override* action only occurs when a server module is inserted in a FlexAddress enabled chassis; no permanent changes are made to the server module. If a server module is moved to a chassis that does not support FlexAddress, the factory-assigned WWN/MAC IDs is used.

The FlexAddress feature card contains a range of MAC addresses. Before installing FlexAddress, you can determine the range of MAC addresses contained on a FlexAddress feature card by inserting the SD card into an USB Memory Card Reader and viewing the **pwwn_mac.xml** file. This clear text XML file on the SD card contains an XML tag *mac_start* that is the first starting hex MAC address that is used for this unique MAC address range. The *mac_count* tag is the total number of MAC addresses that the SD card allocates. The total MAC range allocated can be determined by:

```
<mac_start> + 0xCF (208 - 1) = mac_end
```

where 208 is the *mac_count* and the formula is:

```
<mac_start> + <mac_start>  - 1 = <mac_end>
```

For example:

```
(starting_mac)00188BFFDCFA + 0xCF = (ending_mac)00188BFFDDC9
```

.

NOTE: Lock the SD card prior to inserting in the USB Memory Card Reader to prevent accidently modifying any of the contents. You *must unlock* the SD card before inserting into CMC.

About FlexAddress Plus

The FlexAddress Plus is a new feature added to the feature card version 2.0. It is an upgrade from FlexAddress feature card version 1.0. FlexAddress Plus contains more MAC addresses than the FlexAddress feature. Both features allow the chassis to assign World Wide Name/Media Access Control (WWN/MAC) addresses to Fibre Channel and Ethernet devices. Chassis assigned WWN/MAC addresses are globally unique and specific to a server slot.

FlexAddress and FlexAddress Plus Comparison

FlexAddress has 208 addresses divided into 16 server slots, thus each slot is allocated with 13 MACs.

FlexAddress Plus has 2928 addresses divided into 16 server slots, thus each slot is allocated with 183 MACs.

The following table shows the provision of the MAC addresses in both the features.

	Fabric A	Fabric B	Fabric C	iDRAC Management	Total MACs
FlexAddress	4	4	4	1	13
FlexAddress Plus	60	60	60	3	183

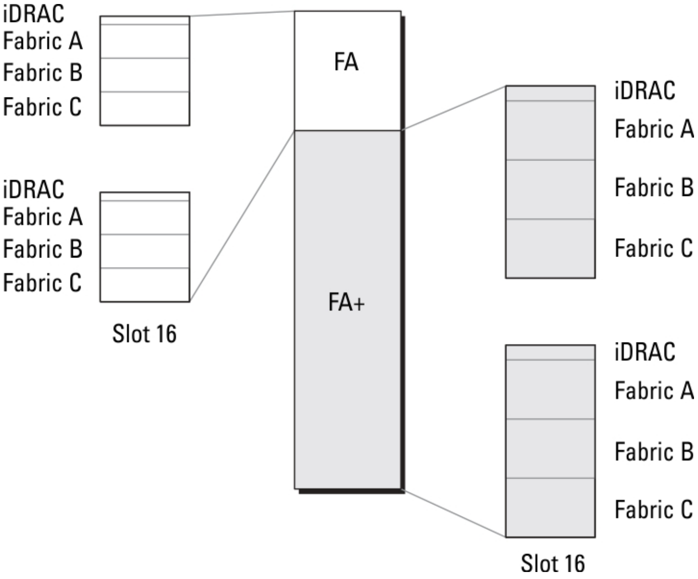


Figure 1. FlexAdress (FA) vs FlexPlusAddress (FA+) Features

Activating FlexAddress

FlexAddress is delivered on a Secure Digital (SD) card that must be inserted into CMC to activate the feature. To activate the FlexAddress feature, software updates may be required; if you are not activating FlexAddress these updates are not required. The updates (listed in the following table) include server module BIOS, I/O mezzanine BIOS or firmware, and CMC firmware. You must apply these updates before you enable FlexAddress. If these updates are not applied, the FlexAddress feature may not function as expected.

Component	Minimum Required Version
Ethernet Mezzanine card - Broadcom M5708t, 5709, 5710	• Boot code firmware 4.4.1 or later • iSCSI boot firmware 2.7.11 or later • PXE firmware 4.4.3 or later
FC Mezzanine card - QLogic QME2472, FC8	BIOS 2.04 or later

Component	Minimum Required Version
FC Mezzanine card - Emulex LPe1105-M4, FC8	BIOS 3.03a3 and firmware 2.72A2 or later
Server Module BIOS	• PowerEdge M600 – BIOS 2.02 or later • PowerEdge M605 – BIOS 2.03 or later • PowerEdge M805 • PowerEdge M905 • PowerEdge M610 • PowerEdge M710 • PowerEdge M710hd
PowerEdgeM600/M605 LAN on motherboard (LOM)	• Boot code firmware 4.4.1 or later • iSCSI boot firmware 2.7.11 or later
iDRAC	• Version 1.50 or later for PowerEdge xx0x systems • Version 2.10 or later for PowerEdge xx1x systems
CMC	Version 1.10 or later

NOTE: Any system ordered after June 2008 has the correct firmware versions.

To make sure proper deployment of the FlexAddress feature, update the BIOS and the firmware in the following order:

1. Update all mezzanine card firmware and BIOS.
2. Update server module BIOS.
3. Update iDRAC firmware on the server module.
4. Update all CMC firmware in the chassis; if redundant CMCs are present, ensure both are updated.
5. Insert the SD card into the passive module for a redundant CMC module system or into the single CMC module for a non-redundant system.

   NOTE: If CMC firmware that supports FlexAddress (version 1.10 or later) is not installed, the feature is not activated.

   See the *Chassis Management Controller (CMC) Secure Digital (SD) Card Technical Specification* document for SD card installation instructions.

   NOTE: The SD card contains a FlexAddress feature. Data contained on the SD card is encrypted and may not be duplicated or altered in any way as it may inhibit system function and cause the system to malfunction.

   NOTE: Your use of the SD card is limited to one chassis only. If you have multiple chassis, you must purchase additional SD cards.

   Activation of the FlexAddress feature is automatic on restart of CMC with the SD feature card installed; this activation causes the feature to bind to the current chassis. If you have the SD card installed on the redundant CMC, activation of the FlexAddress feature does not occur until the redundant CMC is made active. See the *Chassis Management Controller (CMC) Secure Digital (SD) Card Technical Specification* document for information on how to make a redundant CMC active.

   When CMC restarts, verify the activation process. For more information, see Verifying FlexAddress Activation.

Activating FlexAddress Plus

FlexAddress Plus is delivered on the FlexAddress Plus Secure Digital (SD) card along with the FlexAddress feature.

NOTE: The SD card labeled FlexAddress only contains FlexAddress and the card labeled FlexAddress Plus contains FlexAddress and FlexAddress Plus. The card must be inserted into CMC to activate the feature.

Some servers, such as the PowerEdge M710HD, may require more MAC addresses than FA can provide to CMC, depending on how they are configured. For these servers, upgrading to FA+ enables full optimization of the WWN/MACs configuration. Contact Dell to obtain support for the FlexAddress Plus feature.

To activate the FlexAddress Plus feature, the following software updates are required: server BIOS, server iDRAC, and CMC firmware. If these updates are not applied, only FlexAddress feature is available. For information on the minimum required versions of these components, see the *Readme* at **support/dell.com/manuals**.

.

Verifying FlexAddress Activation

Use the following RACADM command to verify the SD feature card and its status:

```
racadm featurecard -s
```

Table 29. Status Messages Returned by featurecard -s Command

Status Message	Actions
No feature card inserted.	Check CMC to verify that the SD card was properly inserted. In a redundant CMC configuration, ensure that the CMC with the SD feature card installed is the active CMC and not the standby CMC.
The feature card inserted is valid and contains the following feature(s) FlexAddress: The feature card is bound to this chassis.	No action required.
The feature card inserted is valid and contains the following feature(s) FlexAddress: The feature card is bound to another chassis, svctag = ABC1234, SD card SN = 01122334455	Remove the SD card; locate and install the SD card for the current chassis.
The feature card inserted is valid and contains the following feature(s) FlexAddress: The feature card is not bound to any chassis.	The feature card can be moved to another chassis or can be reactivated on the current chassis. To reactivate on the current chassis, enter `racadm racreset` until the CMC module with the feature card installed becomes active.

Use the following RACADM command to display all activated features on the chassis:

```
racadm feature -s
```

The command returns the following status message:

```
Feature = FlexAddress
Date Activated = 8 April 2008 - 10:39:40
Feature installed from SD-card SN = 01122334455
```

If there are no active features on the chassis, the command returns a message:

```
racadm feature -s
No features active on the chassis
```

Dell Feature Cards may contain more than one feature. Once any feature included on a Dell Feature Card has been activated on a chassis, any other features that may be included on that Dell Feature Card cannot be activated on a different chassis. In this case, the racadm feature -s command displays the following message for the affected features:

```
ERROR: One or more features on the SD card are active on another chassis
```

For more information on the **feature** and**featurecard** commands, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC.*

Deactivating FlexAddress

The FlexAddress or feature can be deactivated and the SD card returned to a pre-installation state using a RACADM command. There is no deactivation function within the Web interface. Deactivation returns the SD card to its original state where it can be installed and activated on a different chassis. The term FlexAddress, in this context, implies both FlexAddress and FlexAddressPlus.

NOTE: The SD card must be physically installed in CMC, and the chassis must be powered-down before executing the deactivation command.

If you execute the deactivation command with no card installed, or with a card from a different chassis installed, the feature is deactivated and no change is made to the card.

To deactivate the FlexAddress feature and restore the SD card:

```
racadm feature -d -c flexaddress
```

The command returns the following status message if it is successfully deactivated:

```
feature FlexAddress is deactivated on the chassis successfully.
```

If the chassis is not powered-down prior to execution, the command fails with the following error message:

```
ERROR: Unable to deactivate the feature because the chassis is powered ON
```

For further information on the command, see the **feature** command section of the *RACADM Command Line Reference Guide for iDRAC7 and CMC.*

Viewing FlexAddress Information

You can view status information for the entire chassis or for an individual server. The information displayed includes:

- Fabric configuration.
- FlexAddress is active or not active.
- Slot number and name.
- Chassis-assigned and server-assigned addresses.
- Addresses in use.

Related Links

Viewing FlexAddress Information For Chassis
Viewing FlexAddress Information For All Servers
Viewing FlexAddress Information for Individual Servers

Viewing FlexAddress Information For Chassis

FlexAddress status information can be displayed for the entire chassis. The status information includes whether the feature is active and an overview of the FlexAddress status for each server.

To view the chassis FlexAddress status using CMC Web interface, go to **Chassis Overview** → **Setup** → **General**.

The **General Chassis Settings** page is displayed.

The **FlexAddress** has a value **Active** or **Not Active**. The value **Active** indicates the feature is installed on the chassis and **Not Active** indicates the feature is not installed and not in use on the chassis.

Use the following RACADM command to display FlexAddress status for the entire chassis:

```
racadm getflexaddr
```

To display FlexAddress status for a particular slot:

```
racadm getflexaddr [-i <slot#>]
```

where *<slot#>* is a value from 1– 16.

For additional information on **getflexaddr** command, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC.*

Viewing FlexAddress Information For All Servers

To view FlexAddress status for all the servers using CMC Web interface, in the system tree, go to **Server Overview** → **Properties** → **WWN/MAC** .

The **WWN/MAC Summary** page is displayed that provides the WWN configuration and MAC addresses for all the slots in the chassis.

Fabric Configuration

Fabric A, Fabric B, and Fabric C display the type of the Input/Output fabric installed.

iDRAC displays the server management MAC address.

NOTE: If Fabric A is enabled, unpopulated slots display chassis-assigned MAC addresses for Fabric A and MAC or WWNs for Fabrics B and C if they are in use by populated slots.

WWN/MAC Addresses

Displays FlexAddress configuration for each slot in the chassis. Information displayed includes:

- iDRAC management controller is not a fabric but its FlexAddress is treated like one.
- Slot number and location.
- FlexAddress is active or not active.
- Fabric type.
- Server-assigned and chassis-assigned WWN/MAC addresses in use.

A green check mark indicates the active address type, either server-assigned or chassis-assigned.

For information about the fields, see the *CMC Online Help.*

Viewing FlexAddress Information for Individual Servers

To view FlexAddress information for a particular server using the CMC Web interface:

1. In the system tree, expand **Server Overview**.

All the servers (1–16) appear in the expanded **Servers** list.

2. Click the server you want to view. .

   The **Server Status** page is displayed

3. Click the **Setup** tab, and then the **FlexAddress** subtab.

   The **FlexAddress** page is displayed that provides the WWN configuration and MAC addresses for the selected server. For more information, see the *CMC Online Help.*

Configuring FlexAddress

FlexAddress is an optional upgrade that allows server modules to replace the factory-assigned WWN/MAC ID with a WWN/MAC ID provided by the chassis.

NOTE: In this section, the term FlexAddress also indicates FlexAddress Plus.

You must purchase and install the FlexAddress upgrade to configure the FlexAddress. If the upgrade is not purchased and installed, the following text is displayed on the Web interface:

```
Optional feature not installed. See the Dell Chassis Management Controller
Users Guide for information on the chassis-based WWN and MAC address
administration feature. To purchase this feature, please contact Dell at
www.dell.com.
```

If you purchase FlexAddress with your chassis, it is installed and active when you power up your system. If you purchase FlexAddress separately, you must install the SD feature card using the instructions in the *Chassis Management Controller (CMC) Secure Digital (SD) Card Technical Specification* document at **support.dell.com/manuals.**

The server must be turned off before you begin configuration. You can enable or disable FlexAddress on a per fabric basis. Additionally, you can enable or disable the feature on a per slot basis. After you enable the feature on a per-fabric basis, you can then select slots to be enabled. For example, if Fabric-A is enabled, any slots that are enabled have FlexAddress enabled only on Fabric- A. All other fabrics use the factory-assigned WWN/MAC on the server.

Selected slots have FlexAddress enabled for all fabrics that are enabled. For example, it is not possible to enable Fabric-A and B, and have Slot 1 be FlexAddress enabled on Fabric-A but not on Fabric-B.

NOTE: Make sure that the Blade Servers are powered off before changing the fabric level (A, B, C, or DRAC) flex address.

Related Links

Wake-On-LAN with FlexAddress
Configuring FlexAddress for Chassis-Level Fabric and Slots
Configuring FlexAddress for Server-Level Slots
Additional FlexAddress Configuration for Linux

Wake-On-LAN with FlexAddress

When the FlexAddress feature is deployed for the first time on a given server module, it requires a power-down and power-up sequence for FlexAddress to take effect. FlexAddress on Ethernet devices is programmed by the server module BIOS. For the server module BIOS to program the address, it needs to be operational which requires the server module to be powered up. When the power-down and power-up sequences complete, the chassis-assigned MAC IDs are available for Wake-On-LAN (WOL) function.

Configuring FlexAddress for Chassis-Level Fabric and Slots

At the chassis level, you can enable or disable the FlexAddress feature for fabrics and slots. FlexAddress is enabled on a per-fabric basis and then slots are selected for participation in the feature. Both fabrics and slots must be enabled to successfully configure FlexAddress.

Configuring FlexAddress for Chassis-Level Fabric and Slots Using CMC Web Interface

To enable or disable fabrics and slots to use the FlexAddress feature using the CMC Web interface:

1. In the system tree, go to **Server Overview**, and then click **Setup** → **FlexAddress.** .

   The **Deploy FlexAddress** page is displayed.

2. In the **Select Fabrics for Chassis-Assigned WWN/MACs section**, select the fabric type for which you want to enable FlexAddress. To disable, clear the option.

   NOTE: If no fabrics are selected, FlexAddress is not enabled for the selected slots.

   The **Select Slots for Chassis-Assigned WWN/MACs** page is displayed.

3. Select the **Enabled** option for the slot for which you want to enable FlexAddress. To disable, clear the option.

   NOTE: If a server is present in the slot, turn it off before enabling the FlexAddress feature on that slot.

   NOTE: If no slots are selected, FlexAddress is not enabled for the selected fabrics.

4. Click **Apply** to save the changes.

   For more information, see the *CMC Online Help.*

Configuring FlexAddress for Chassis-Level Fabric and Slots Using RACADM

To enable or disable fabrics, use the following RACADM command:

```
racadm setflexaddr [-f <fabricName> <state>
```

where, `<fabricName> = A, B, C, or iDRAC` and `<state> = 0 or 1`

0 is disable and 1 is enable.

To enable or disable slots, use the following RACADM command:

```
racadm setflexaddr [-i <slot#> <state>
```

where, `<slot#> = 1or 16` and `<state> = 0 or 1`

0 is disable and 1 is enable.

For more information on **setflexaddr** command, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC.*

Configuring FlexAddress for Server-Level Slots

At the server level, you can enable or disable the FlexAddress feature for individual slots.

Configuring FlexAddress for Server-Level Slots Using CMC Web Interface

To enable or disable an individual slot to use the FlexAddress feature using the CMC Web interface:

1. In the system tree, expand **Server Overview**.

   All the servers (1–16) appear in the expanded **Servers** list.

2. Click the server you want to view.

The **Server Status** page displays.

3. Click the **Setup** tab, and the **FlexAddress** subtab.

   The **FlexAddress** page is displayed.

4. From the **FlexAddress Enabled** drop-down menu, select **Yes** to enable FlexAddress or select **No** to disable FlexAddress.

5. Click **Apply** to save the changes.

   For more information, see the *CMC Online Help*.

Configuring FlexAddress for Server-Level Slots Using RACADM

To configure the flexaddress for Server-level slots using RACADM:

```
racadm setflexaddr [-i <slot#> <state>] [-f <fabricName> <state>]
```

where, `<slot#> = 1 to 16`

`<fabricName> = A, B, C`

`<state> = 0 or 1`

0 is disable and 1 is enable.

Additional FlexAddress Configuration for Linux

When changing from a server-assigned MAC ID to chassis-assigned MAC ID on Linux-based operating systems, additional configuration steps may be required:

- SUSE Linux Enterprise Server 9 and 10 — You may need to run Yet Another Setup Tool (YAST) on the Linux system to configure the network devices and then restart the network services.
- Red Hat Enterprise Linux 4 and Red Hat Enterprise Linux 5: Run Kudzu, a utility to detect and configure new or changed hardware on the system. Kudzu displays The Hardware Discovery Menu; it detects the MAC address change as hardware was removed and new hardware added.

Viewing World Wide Name/Media Access Control (WWN/MAC) IDs

The **WWN/MAC Summary** page allows you to view the WWN configuration and MAC address of a slot in the chassis.

Fabric Configuration

The **Fabric Configuration** section displays the type of Input/Output fabric that is installed for Fabric A, Fabric B, and Fabric C. A green check mark indicates that the fabric is enabled for FlexAddress. The FlexAddress feature is used to deploy chassis assigned and slot persistent WWN/MAC addresses to various fabrics and slots within the chassis. This feature is enabled on a per fabric and per slot basis.

NOTE: For more information on the FlexAddress feature, see About FlexAddress.

WWN/MAC Addresses

The **WWN/MAC Address** section displays the WWN/MAC information that is assigned to all servers, even if those server slots are currently empty.

- **Location** displays the location of the slot occupied by the Input/Output modules. The six slots are identified by a combination of the group name (A, B, or C) and slot number (1 or 2): slot names A1, A2, B1, B2, C1, or C2. iDRAC is the server's integrated management controller.
- **Fabric** displays the type of the I/O fabric.

- **Server-Assigned** displays the server-assigned WWN/MAC addresses embedded in the controller's hardware.
- **Chassis-Assigned** displays the chassis-assigned WWN/MAC addresses used for the particular slot.

A green check mark in the **Server-Assigned** or in **Chassis-Assigned** columns indicates the type of active addresses. Chassis-assigned addresses are assigned when FlexAddress is activated on the chassis, and represents the slot-persistent addresses. When ChassisaAssigned addresses are checked, those addresses are used even if one server is replaced with another server.

Command Messages

The following table lists the RACADM commands and output for common FlexAddress situations.

Table 30. FlexAddress Commands and Output

Situation	Command	Output

SD card in the active CMC module is bound to another service tag.	`$racadm featurecard -s`	`The feature card inserted is valid and contains the following feature(s)`
		`FlexAddress: The feature card is bound to another chassis, svctag = <Service tag Number> SD card SN = <Valid flex address serial number>`

SD card in the active CMC module that is bound to the same service tag.	`$racadm featurecard -s`	`The feature card inserted is valid and contains the following feature(s)`
		`FlexAddress: The feature card is bound to this chassis`

SD card in the active CMC module that is not bound to any service tag.	`$racadm featurecard -s`	`The feature card inserted is valid and contains the following feature(s)`
		`FlexAddress: The feature card is not bound to any chassis`

FlexAddress feature not active on the chassis for any reason (No SD card inserted/ corrupt SD card/ after feature deactivated /SD card bound to a different chassis)	`$racadm setflexaddr [-f <fabricName> <slotState>]`
	`$racadm setflexaddr [-i <slot#> <slotstate>]`
		`ERROR: Flexaddress feature is not active on the chassis`

Guest user attempts to set FlexAddress on slots/fabrics	`$racadm setflexaddr [-f <fabricName> <slotState>]`
	`$racadm setflexaddr [-i <slot#> <slotstate>]`
		`ERROR: Insufficient user privileges to perform operation`

Deactivating FlexAddress feature with chassis powered ON.	`$racadm feature -d -c flexaddress`	`ERROR: Unable to deactivate the feature because the chassis is powered ON`
Guest user tries to deactivate the feature on the chassis.	`$racadm feature -d -c flexaddress`	`ERROR: Insufficient user privileges to perform operation`

Situation	Command	Output
Changing the slot/fabric FlexAddress settings while the server modules are powered ON.	`$racadm setflexaddr -i 1 1`	`ERROR: Unable to perform the set operation because it affects a powered ON server`

FlexAddress DELL SOFTWARE LICENSE AGREEMENT

This is a legal agreement between you, the user, and Dell Products L.P. or Dell Global B.V. ("Dell"). This agreement covers all software that is distributed with the Dell product, for which there is no separate license agreement between you and the manufacturer or owner of the software (collectively the "Software"). This agreement is not for the sale of Software or any other intellectual property. All title and intellectual property rights in and to Software is owned by the manufacturer or owner of the Software. All rights not expressly granted under this agreement are reserved by the manufacturer or owner of the Software. By opening or breaking the seal on the Software packet(s), installing or downloading the Software, or using the Software that has been preloaded or is embedded in your product, you agree to be bound by the terms of this agreement. If you do not agree to these terms, promptly return all Software items (disks, written materials, and packaging) and delete any preloaded or embedded Software.

You may use one copy of the Software on only one computer at a time. If you have multiple licenses for the Software, you may use as many copies at any time as you have licenses. "Use" means loading the Software in temporary memory or permanent storage on the computer. Installation on a network server solely for distribution to other computers is not "use" if (but only if) you have a separate license for each computer to which the Software is distributed. You must ensure that the number of persons using the Software installed on a network server does not exceed the number of licenses that you have. If the number of users of Software installed on a network server exceeds the number of licenses, you must purchase additional licenses until the number of licenses equals the number of users before allowing additional users to use the Software. If you are a commercial customer of Dell or a Dell affiliate, you hereby grant Dell, or an agent selected by Dell, the right to perform an audit of your use of the Software during normal business hours, you agree to cooperate with Dell in such audit, and you agree to provide Dell with all records reasonably related to your use of the Software. The audit is limited to verification of your compliance with the terms of this agreement.

The Software is protected by United States copyright laws and international treaties. You may make one copy of the Software solely for backup or archival purposes or transfer it to a single hard disk provided you keep the original solely for backup or archival purposes. You may not rent or lease the Software 240 Using FlexAddress and FlexAdress Plus Cards or copy the written materials accompanying the Software, but you may transfer the Software and all accompanying materials on a permanent basis as part of a sale or transfer of the Dell product if you retain no copies and the recipient agrees to the terms hereof. Any transfer must include the most recent update and all prior versions. You may not reverse engineer, decompile or disassemble the Software. If the package accompanying your computer contains compact discs, 3.5" and/or 5.25" disks, you may use only the disks appropriate for your computer. You may not use the disks on another computer or network, or loan, rent, lease, or transfer them to another user except as permitted by this agreement.

LIMITED WARRANTY

Dell warrants that the Software disks is free from defects in materials and workmanship under normal use for ninety (90) days from the date you receive them. This warranty is limited to you and is not transferable. Any implied warranties are limited to ninety (90) days from the date you receive the Software. Some jurisdictions do not allow limits on the duration of an implied warranty, so this limitation may not apply to you. The entire liability of Dell and its suppliers, and your exclusive remedy, shall be (a) return of the price paid for the Software or (b) replacement of any disk not meeting this warranty that is sent with a return authorization number to Dell, at your cost and risk. This limited warranty is void if any disk damage has resulted from accident, abuse, misapplication, or service or modification by someone other than Dell. Any replacement disk is warranted for the remaining original warranty period or thirty (30) days, whichever is longer.

Dell does NOT warrant that the functions of the Software meets your requirements or that operation of the Software is uninterrupted or error free. You assume responsibility for selecting the Software to achieve your intended results and for the use and results obtained from the Software.

DELL, ON BEHALF OF ITSELF AND ITS SUPPLIERS, DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, FOR THE SOFTWARE AND ALL ACCOMPANYING WRITTEN MATERIALS. This limited warranty gives you specific legal rights; you may have others, which vary from jurisdiction to jurisdiction.

IN NO EVENT SHALL DELL OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR OTHER PECUNIARY LOSS) ARISING OUT OF USE OR INABILITY TO USE THE SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Because some jurisdictions do not allow an exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

OPEN SOURCE SOFTWARE

A portion of this CD may contain open source software, which you can use under the terms and conditions of the specific license under which the open source software is distributed.

THIS OPEN SOURCE SOFTWARE IS DISTRIBUTED IN THE HOPE THAT IT WILL BE USEFUL, BUT IS PROVIDED "AS IS" WITHOUT ANY EXPRESSED OR IMPLIED WARRANTY; INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL DELL, THE COPYRIGHT HOLDERS, OR THE CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTUTUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILTIY, WHETHER IN CONTRACT, STRICT LIABITLY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILTIY OF SUCH DAMAGE.

.U.S. GOVERNMENT RESTRICTED RIGHTS

The software and documentation are "commercial items" as that term is defined at 48 C.F.R. 2.101, consisting of "commercial computer software" and "commercial computer software documentation" as such terms are used in 48 C.F.R. 12.212. Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4, all U.S. Government end users acquire the software and documentation with only those rights set forth herein.

Contractor/manufacturer is Dell Products, L.P., One Dell Way, Round Rock, Texas 78682.

GENERAL

This license is effective until terminated. It terminates upon the conditions set forth above or if you fail to comply with any of its terms. Upon termination, you agree that the Software and accompanying materials, and all copies thereof, is destroyed. This agreement is governed by the laws of the State of Texas. Each provision of this agreement is severable. If a provision is found to be unenforceable, this finding does not affect the enforceability of the remaining provisions, terms, or conditions of this agreement. This agreement is binding on successors and assigns. Dell agrees and you agree to waive, to the maximum extent permitted by law, any right to a jury trial with respect to the Software or this agreement. Because this waiver may not be effective in some jurisdictions, this waiver may not apply to you. You acknowledge that you have read this agreement, that you understand it, that you agree to be bound by its terms, and that this is the complete and exclusive statement of the agreement between you and Dell regarding the Software.

13

Managing I/O Fabric

The chassis can have up to six I/O modules (IOMs), where each IOM is a pass-through or switch module. The IOMs are classified into three groups—A, B, and C. Each group has two slots—Slot 1 and Slot 2.

The slots are designated with letters, from left to right, across the back of the chassis: A1 | B1 | C1 | C2 | B2 | A2. Each server has slots for two mezzanine cards (MCs) to connect to the IOMs. The MC and the corresponding IOM must have the same fabric.

Chassis IO is segregated into three discrete data paths: A, B and C. These paths are described as FABRICS and support Ethernet, Fibre Channel, or InfiniBand. These discrete fabric paths are split into two IO Banks, bank one and bank two. Each server IO adapter (Mezzanine Card or LOM) can have either two or four ports depending on the capability. These ports are divided evenly to IOM banks one and two to allow for redundancy. When you deploy the Ethernet, iSCSI, or FibreChannel networks, span their redundant links across banks one and two for maximum availability. The discrete IOM is identified with the fabric identifier and the bank number.

Example: A1 denotes Fabric A in bank 1. C2 denotes Fabric Cin bank 2.

The chassis supports three fabric or protocol types. The IOMs and Mezzanine Cards in a group must have the same or compatible fabric types.

- Group A IOMS are always connected to the servers' on-board Ethernet adapters; the fabric type of Group A is always Ethernet.
- For Group B, the IOM slots are permanently connected to the first MC slot in each server module.
- For Group C, the IOM slots are permanently connected to the second MC in each server module.

NOTE: In the CMC CLI, IOMs are referred to by the convention, switch-n: A1=switch-1, A2=switch-2, B1=switch-3, B2=switch-4, C1=switch-5, and C2= switch-6.

Related Links

Fabric Management Overview
Invalid Configurations
Fresh Power-up Scenario
Monitoring IOM Health
Configuring Network Settings for IOM(s)
Managing VLAN for IOM
Managing Power Control Operation for IOMs
Enabling or Disabling LED Blinking for IOMs
Resetting IOM to Factory Default Settings

Fabric Management Overview

Fabric management helps avoid electrical, configuration, or connectivity related problems due to installation of an IOM or MC that has an incompatible fabric type from the chassis' established fabric type. Invalid hardware configurations can cause electric or functional problems to the chassis or its components. Fabric management prevents invalid configurations from powering on.

The following figure shows the location of IOMs in the chassis. The location of each IOM is indicated by its group number (A, B, or C). These discrete fabric paths are split into two IO Banks, bank one and two. On the chassis, the IOM slot names are marked A1, A2, B1, B2, C1, and C2.

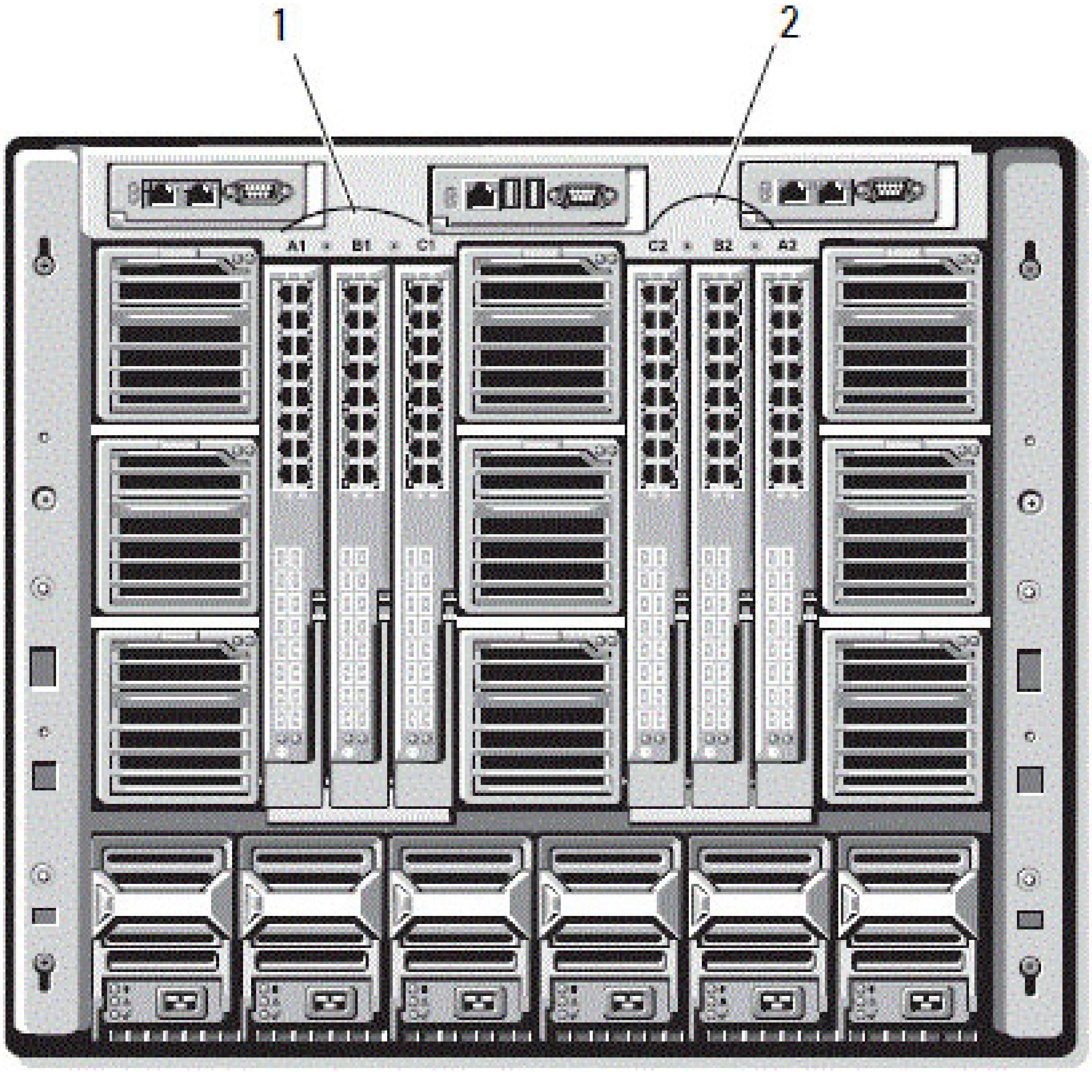


Figure 2. Rear View of a Chassis, Showing the Location of the IOMs

1	Bank 1 (Slots A1, B1, C1)	2	Bank 2 (Slots A2, B2, C2)

CMC creates entries in both the hardware log and CMC logs for invalid hardware configurations.

For example:

- An Ethernet MC connected to a Fibre Channel IOM is an invalid configuration. However, an Ethernet MC connected to both an Ethernet switch and an Ethernet pass-through IOM installed in the same IOM group is a valid connection.
- A Fibre Channel pass-through IOM and a fibre channel switch IOM in slots B1 and B2 is a valid configuration if the first MCs on all of the servers are also fibre channel. In this case, CMC powers-on the IOMs and the servers. However, certain fibre channel redundancy software may not support this configuration; not all valid configurations are necessarily supported configurations.

Fabric verification for server IOMs and MCs is performed only when the chassis is powered on. When the chassis is on standby power, the iDRACs on the server modules remain powered off and thus are unable to report the server's MC fabric type. The MC fabric type may not be reported in the CMC user interface until the iDRAC on the server is powered on. Additionally, if the chassis is powered on, fabric verification is performed when a server or IOM is inserted (optional). If a fabric mismatch is detected, the server or IOM is allowed to power on and the status LED flashes Amber.

Invalid Configurations

There are three types of invalid configurations:

- Invalid MC or LOM configuration, where a newly installed server's fabric type is different from the existing IOM fabric, that is, a single server's LOM or MC is not supported by its corresponding IOM. In this case, all the other servers in the chassis are running, but the server with the mismatched MC card cannot be power on. The power button on the server flashes Amber to alert a fabric mismatch.
- Invalid IOM-MC configuration, where a newly installed IOM's fabric type and the resident MC's fabric types do not match or are incompatible. The mismatched IOM is held in the power-off state. CMC adds an entry to CMC and hardware logs noting the invalid configuration and specifying the IOM name. CMC causes the error LED on the offending IOM to blink. If CMC is configured to send alerts, it sends e-mail and/or SNMP alerts for this event.
- Invalid IOM-IOM configuration, where a newly installed IOM has a different or incompatible fabric type from an IOM already installed in its group. CMC holds the newly installed IOM in powered-off state, causes the IOM's error LED to blink, and logs entries in CMC and hardware logs about the mismatch.

Fresh Power-up Scenario

When the chassis is plugged in and powered up, the I/O modules have priority over the servers. The first IOM in each group is allowed to power up before the others. At this time, verification of their fabric types is not performed. If there is no IOM on the first slot of a group, the module on the second slot of that group powers up. If both slots have IOMs, the module in the second slot is compared for consistency against the one in the first.

After the IOMs power up, the servers power up, and CMC verifies the servers for fabric consistency.

A pass-through module and switch are allowed in the same group if their fabric is identical. Switches and pass-through modules can exist in the same group even if they are manufactured by different vendors.

Monitoring IOM Health

For information about monitoring IOM health, see Viewing Information and Health Status of All IOMs and Viewing Information and Health Status For Individual IOM.

Configuring Network Settings for IOM(s)

You can specify the network settings for the interface used to manage the IOM. For Ethernet switches, the out-of-band management port (IP address) is configured. The in-band management port (that is, VLAN1) is not configured using this interface.

Before configuring the network settings for the IOM(s), make sure the IOM is powered on.

To configure the network setting, you must have:

- Fabric A Administrator privileges to configure IOMs in Group A.
- Fabric B Administrator privileges to configure IOMs in Group B.
- Fabric C Administrator privileges to configure IOMs in Group C.

NOTE: For Ethernet switches, the in-band (VLAN1) and out-of-band management IP addresses cannot be the same or on the same network; this results in the out-of-band IP address not being set. See the IOM documentation for the default in-band management IP address.

NOTE: Do not configure I/O module network settings for Ethernet pass-through and Infiniband switches.

Configuring Network Settings for IOMs Using CMC Web Interface

To configure the network settings for IOM(s) using the CMC Web interface:

1. In the system tree, go to **I/O Module Overview** and click **Setup** or expand **I/O Module Overview** , select the IOM, and click **Setup**.

   The **Deploy I/O Modules** page displays the IOM(s) that are powered on.

2. For the required IOM(s), enable DHCP, enter the IP address, subnet mask, and gateway address.
3. For IOMs that are manageable, enter root password, SNMP RO Community string, and Syslog Server IP Address. For information about the fields, see *CMC Online Help*.

   NOTE: The IP address set on the IOMs from CMC is not saved to the switch's permanent startup configuration. To save the IP address configuration permanently, you must enter the `connect switch-n command`, or `racadm connect switch -n` RACADM command, or use a direct interface to the IOM GUI to save this address to the startup configuration file.

4. Click **Apply**.

   The network settings are configured for the IOM(s).

   NOTE: For IOMs that are manageable, you can reset the VLANs, network properties, and IO ports to default configurations.

Configuring Network Settings for IOMs Using RACADM

To configure the network settings for IOMs using RACADM, set the date and time. See the deploy command section in the *RACADM Command Line Reference Guide for iDRAC7 and CMC*.

You can set the username, password, and SNMP string for an IOM using the RACADM deploy command:

```
racadm deploy -m switch-<n> -u <username> -p <password>

racadm deploy -m switch-<n> -u -p <password> -v SNMPv2 <snmpCommunityString> ro

racadm deploy -a [server|switch] -u <username> -p <password>
```

Resetting IOM to Factory Default Settings

You can reset IOM to the factory default settings using the **Deploy I/O Modules** page.

To reset the selected IOMs to factory default settings using the CMC Web interface:

1. In the system tree, go to **I/O Module Overview** and click **Setup** or expand **I/O Module Overview** in the system tree, select the IOM, and click **Setup**.

   The **Deploy I/O Modules** page displays the IOM(s) that are powered on.

2. For the required IOM(s), click **Reset**.

   A warning message is displayed.

3. Click **OK** to continue.

Managing VLAN for IOM

Virtual LANs (VLANs) for IOMs allow you to separate users into individual network segments for security and other reasons. By using VLANs you can isolate the networks for individual users on a 32 port switch. You can associate selected ports on a switch with selected VLAN and treat these ports as a separate switch.

CMC Web Interface allows you to configure the in-band management ports (VLAN) on the IOMs.

Related Links

Configuring VLAN settings on IOMs Using CMC Web Interface
Viewing the VLAN settings on IOMs Using CMC Web Interface
Viewing the Current VLAN Settings on IOMs Using CMC Web Interface
Adding Tagged VLANs for IOMs Using CMC Web Interface
Removing VLANs for IOMs Using CMC Web Interface
Updating Untagged VLANs for IOMs Using CMC Web Interface
Resetting VLANs for IOMs Using CMC Web Interface

Configuring VLAN settings on IOMs Using CMC Web Interface

NOTE: You can configure VLAN settings only on PowerEdge M I/O Aggregator IOM. Other IOMs including MXL 10/40GbE are not supported.

To configure the VLAN settings on IOM(s) using the CMC Web interface:

1. In the system tree, go to **I/O Module Overview** and click **Setup VLAN Manager**.

   The VLAN Manager page displays the IOM(s) that are powered on and the available ports.

2. In the **Select I/O Module**section, select the configuration type from the drop down list, and then select the required IOM(s).

   For information about the fields, see *CMC Online Help*

3. In the **Specify Port Range** section, select the range of fabric ports to be assigned to the selected IOM(s).

   For information about the fields, see *CMC Online Help*

4. Select the **Select**or **Deselect All** option to apply the changes to all or no IOMs.

   or

   Select the check box for the specific slots to select the required IOMs.

5. In the **Edit VLANs** section, enter the VLAN IDs for the IOMs. Enter VLAN IDs in the range 1-4094. VLAN IDs can be entered as a range or separated by a comma. Example: 1,5,10,100-200.

6. Select one of the following options from the drop-down menu as required:

   – Add Tagged VLANs
   – Remove VLANs
   – Update untagged VLANs
   – Reset to all VLANs
   – Show VLANs

7. Click **Save** to save the new settings made to the **VLAN Manager** page.

   For information about the fields, see *CMC Online Help*

   NOTE: The Summary VLANs of All Ports section displays information about the IOMs present in the Chassis and the assigned VLANs. Click Save to save a csv file of the summary of the current VLAN settings.

   NOTE: The CMC Managed VLANs section displays the summary of all VLANs assigned to the IOMs.

8. Click **Apply**.

   The network settings are configured for the IOM(s).

Viewing the VLAN settings on IOMs Using CMC Web Interface

To view the VLAN settings on IOM(s) using the CMC Web interface:

1. In the system tree, go to **I/O Module Overview** and click **Setup** → **VLAN Manager**.

   The **VLAN Manager** page is displayed.

   The **Summary VLANs of All Ports** section displays information about the current VLAN settings for the IOMs.
2. Click **Save** to save the VLAN settings to a file.

Viewing the Current VLAN Settings on IOMs Using CMC Web Interface

To view the current VLAN settings on IOMs using the CMC Web Interface:

1. In the system tree, go to **I/O Module Overview** and click **Setup** → **VLAN Manager** .

   The **VLAN Manager** page is displayed.
2. In the **Edit VLANs** section, select **Show VLANs** in the drop down list and click **Apply**.

   An Operation Successful message is displayed. The current VLAN settings that are assigned to the IOMs are displayed in the VLAN Assignment Summary field.

Adding Tagged VLANs for IOMs Using CMC Web Interface

To add tagged VLANs for IOM(s) using the CMC Web interface:

1. In the system tree, go to **I/O Module Overview** and click **Setup** → **VLAN Manager**.

   The VLAN Manager page is displayed.
2. In the **Select I/O Module** section, select the required IOMs.
3. In the **Specify Port Range** section, select the range of fabric ports to be assigned to the selected IOM(s).

   For information about the fields, see *CMC Online Help*.
4. Select the **Select**or **Deselect All** option to apply the changes to all or no IOMs.

   or

   Select the check box against the specific slots to select the required IOMs.
5. In the **Edit VLANs** section, select **Add Tagged VLANs** in the drop down list and click **Apply**.

   The tagged VLANs are assigned to the selected IOMs.

   The operation successful message is displayed. The current VLAN settings that are assigned to the IOMs are displayed in the **VLAN Assignment Summary field** .

Removing VLANs for IOMs Using CMC Web Interface

To remove VLANs from IOM(s) using the CMC Web interface:

1. In the system tree, go to **I/O Module Overview** and click **Setup** → **VLAN Manager**.

   The VLAN Manager page is displayed.
2. In the **Select I/O Module** section, select the required IOMs.
3. In the **Edit VLANs** section, select **Remove VLANs** in the drop down list and click **Apply**.

The VLANs assigned to the selected IOMs are removed.

An Operation Successful message is displayed. The current VLAN settings that are assigned to the IOMs are displayed in the **VLAN Assignment Summary** field.

Updating Untagged VLANs for IOMs Using CMC Web Interface

To update untagged VLANs for IOM(s) using the CMC Web interface:

1. In the system tree, go to **I/O Module Overview** and click **Setup** → **VLAN Manager** .

   The **VLAN Manager** page is displayed.
2. In the **Select I/O Module** section, select the required IOMs.
3. In the **Specify Port Range** section, select the range of fabric ports to be assigned to the selected IOM(s).

   For information about the fields, see *CMC Online Help*.
4. Select the **Select/Deselect All** option to apply the changes to all or no IOMs.

   or

   Select the check box against the specific slots to select the required IOMs.
5. In the **Edit VLANs** section, select **Update the Untagged VLANs** in the drop down list and click **Apply**.

   A warning message is displayed that the configurations of the existing untagged VLAN will be overwritten with the configurations of the newly assigned untagged VLAN.
6. Click **OK** to confirm.

   The untagged VLANs are updated with the configurations of the newly assigned untagged VLAN.

   An Operation Successful message is displayed. The current VLAN settings that are assigned to the IOMs are displayed in the VLAN Assignment Summary field.

Resetting VLANs for IOMs Using CMC Web Interface

To reset VLANs for IOM(s) to default configurations using the CMC Web interface:

1. In the system tree, go to **I/O Module Overview** and click **Setup** → **VLAN Manager**.

   The **VLAN Manager** page is displayed.
2. In the **Select I/O Module** section, select the required IOMs.
3. In the **Edit VLANs** section, select **Reset VLANs** in the drop down list and click **Apply**.

   A warning message is displayed indicating that the configurations of the existing VLANs will be overwritten with the default configurations.
4. Click **OK** to confirm.

   The VLANs are assigned to the selected IOMs according to the default configurations.

   An Operation Successful message is displayed. The current VLAN settings that are assigned to the IOMs are displayed in the VLAN Assignment Summary field.

Managing Power Control Operation for IOMs

For information to set the power control operation for IOM(s), see Executing Power Control Operations on an IOM.

Enabling or Disabling LED Blinking for IOMs

For information to enable LED blinking for IOM(s), see Configuring LEDs to Identify Components on the Chassis.

14

Configuring and Using iKVM

The local access KVM module for the Dell M1000e server chassis is called the Avocent Integrated KVM Switch Module, or iKVM. The iKVM is an analog keyboard, video, and mouse switch that plugs into the chassis. It is an optional, hot-pluggable module to the chassis that provides local keyboard, mouse, and video access to the servers in the chassis, and to the active CMC's command line.

Related Links

iKVM User Interface
iKVM Key Features
Physical Connection Interfaces

iKVM User Interface

The iKVM uses the On Screen Configuration and Reporting (OSCAR) graphical user interface, which is activated using a hot key. OSCAR allows you to select one of the servers or the Dell CMC command line you want to access with the local keyboard, display, and mouse. Only one iKVM session per chassis is allowed.

Related Links

Using OSCAR

iKVM Key Features

- Security — Protects the system with a screen saver password. After a userdefined time, the screen saver mode engages, and access is denied until the correct password is entered to reactivate OSCAR.
- Scanning — Allows you to select a list of servers, which are displayed in the order selected while OSCAR is in scan mode.
- Server Identification — CMC assigns unique slot names for all the servers in the chassis. Although, you can assign names to the servers using the OSCAR interface from a tiered connection, CMC assigned names take precedence, and any new names you assign to the servers using OSCAR is overwritten.

  To change slot names using the CMC Web interface, see Configuring Slot Names. To change a slot name using RACADM, see the **setslotname** section in the *RACADM Command Line Reference Guide for iDRAC7 and CMC*.
- Video — The iKVM video connections support video display resolutions ranging from 640 x 480 at 60 Hz up to 1280 x 1024 at 60 Hz.
- Plug and Play — The iKVM supports Display Data Channel (DDC) Plug and Play, which automates video monitor configuration, and is compliant with the VESA DDC2B standard.
- Flash Upgradable — Allows you to update the iKVM firmware using the CMC Web interface or RACADM `fwupdate` command.

Related Links

Using OSCAR
Managing Servers With iKVM
Managing iKVM From CMC
Updating iKVM Firmware

Physical Connection Interfaces

You can connect to a server or the CMC CLI console through the iKVM from the chassis front panel, an Analog Console Interface (ACI), and the chassis rear panel.

NOTE: The ports on the control panel on the front of the chassis are designed specifically for the iKVM, which is optional. If you do not have the iKVM module, you cannot use the front control panel ports.

iKVM Connection Precedences

Only one iKVM connection is available at a time. The iKVM assigns an order of precedence for each type of connection so that when there are multiple connections, only one connection is available while the others are disabled.

The order of precedence for iKVM connections is:

1. Front panel
2. ACI
3. Rear Pane

For example, if you have iKVM connections in the front panel and ACI, the front panel connection remains active while the ACI connection is disabled. If you have ACI and rear connections, the ACI connection takes precedence.

Tiering Through ACI Connection

The iKVM allows tiered connections with servers and the iKVM's CMC command line console, either locally through a Remote Console Switch port or remotely through the Dell RCS software. The iKVM supports ACI connections from the following products:

- 180AS, 2160AS, 2161DS, 2161DS-2, or 4161DS Dell Remote Console Switches
- Avocent AutoView switching system
- Avocent DSR switching system
- Avocent AMX switching system

NOTE: 2161DS does not support the Dell CMC console connection.

NOTE: The iKVM also supports an ACI connection to the Dell 180ES and 2160ES, but the tiering is non-seamless. This connection requires a USB to PS2 SIP.

Using OSCAR

This section provides information to launch, configure, and use the OSCAR interface.

Related Links

Launching OSCAR
Navigation Basics
Configuring Oscar

Launching OSCAR

To launch OSCAR:

1. Press <Print Screen>.

   The Main dialog box is displayed.

   If a password is assigned, the **Password** dialog box appears after clicking <Print Screen>.

2. Type the password and click **OK**.

   The Main dialog box appears.

   NOTE: There are four options for invoking OSCAR. You can enable one, multiple, or all of these key sequences by selecting boxes in the Invoke OSCAR section of the Main dialog box.

Related Links

Setting Console Security

Navigation Basics

Navigation Basics

Table 31. : OSCAR Keyboard and Mouse Navigation

Key or Key Sequence	Result
• <Print Screen>-<Print Screen> • <Shift>-<Shift> • <Alt>-<Alt> • <Ctrl>-<Ctrl>	Any of these key sequences opens OSCAR depending on the **Invoke OSCAR** settings. You can enable two, three, or all of these key sequences by selecting boxes in the **Invoke OSCAR** section of the **Main** dialog box, and then clicking **OK**.
<F1>	Opens the **Help** screen for the current dialog box.
<Esc>	Closes the current dialog box without saving changes and returns to the previous dialog box. In the **Main** dialog box, <Esc> closes the OSCAR interface and returns to selected server. In a message box, it closes the pop-up box and returns to the current dialog box.
<Alt>	Opens dialog boxes, selects or checks options, and executes actions when used in combination with underlined letters or other designated characters.
<Alt> + <X>	Closes the current dialog box and returns to the previous dialog box.
<Alt> + <O>	Selects **OK** and returns to the previous dialog box.
<Enter>	Completes a switch operation in the **Main** dialog box and exits OSCAR.
Single-click, <Enter>	In a text box, selects the text for editing and enables the left-arrow key and right-arrow keys to move the cursor. Press <Enter> again to quit the edit mode.
<Print Screen>, <Backspace>	Toggles back to previous selection if there were no other keystrokes.
<Print Screen>, <Alt> + <0>	Immediately disconnects a user from a server; no server is selected. Status flag displays Free. (This action only applies to the =<0> on the keyboard and not the keypad.)
<Print Screen> <Pause>	Immediately turns on screen saver mode and prevents access to that specific console, if it is password protected.
Up/Down Arrow keys	Moves the cursor from line to line in lists.
Right/Left Arrow keys	Moves the cursor within the columns when editing a text box.

Key or Key Sequence	Result
<Home>/<End>	Moves the cursor to the top (Home) or bottom (End) of a list.
<Delete>	Deletes characters in a text box.
Number Keys	Type from the keyboard or keypad.
<Caps Lock>	Disabled. To change case, use the <Shift> key.

Configuring Oscar

You can configure the OSCAR settings using the **Setup** dialog box.

Accessing Setup Dialog Box

To access the **Setup** dialog box:

1. Press <Print Screen> to launch the OSCAR interface.

   The **Main** dialog box is displayed.

2. Click **Setup**.

   The **Setup** dialog box is displayed.

Feature	Purpose
Menu	Changes the server listing between numerically by slot or alphabetically by name.
Security	– Sets a password to restrict access to servers – Enables a screen saver and set an inactivity time before the screen saver appears and set the screen save mode.
Flag	Changes display, timing, color, or location of the status flag.
Language	Changes the language for all OSCAR screens.
Broadcast	Sets up to simultaneously control multiple servers through keyboard and mouse actions.
Scan	Sets up a custom scan pattern for up to 16 servers.

Related Links

- Changing Display Behavior
- Assigning Key Sequences for OSCAR
- Setting Screen Delay Time for OSCAR
- Setting Status Flag Display

Changing Display Behavior

Use the **Menu** dialog box to change the display order of servers and set a screen delay time for OSCAR.

To change the display behavior:

1. Press <Print Screen> to launch OSCAR.

   The **Main** dialog box is displayed.

2. Click **Setup** and then **Menu.**

   The **Menu** dialog box is displayed.

3. To choose the default display order of servers, do one of the following:
   - Select **Name** to display servers alphabetically based on the name.
   - Select **Slot** to display servers numerically by slot number.
4. Click **OK**.

Assigning Key Sequences for OSCAR

To assign one or more key sequences for OSCAR activation, select a key sequence from the **Invoke OSCAR** menu and click **OK**. The default key to invoke OSCAR is <Print Screen>.

Setting Screen Delay Time for OSCAR

To set a screen delay time for the OSCAR, after you press <Print Screen> enter the number of seconds (0 through 9) to delay the OSCAR display and click **OK**.

Entering <0> launches OSCAR with no delay.

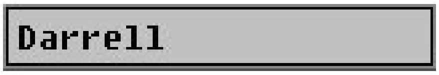
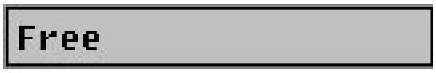
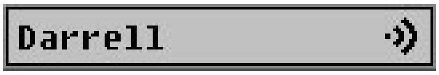
Setting a time to delay display of OSCAR allows you to complete a soft switch.

Related Links

Soft Switching

Setting Status Flag Display

The status flag displays on your desktop and shows the name of the selected server or the status of the selected slot. Use the Flag dialog box to configure the flag to display by server, or to change the flag color, opacity, display time, and location on the desktop.

Flag	Description
 Darrell	Flag type by name.
 Free	Flag indicating that the user is disconnected from all systems.
 Darrell	Flag indicating that Broadcast mode is enabled.

To set the display of the status flag:

1. Press <Print Screen> to launch OSCAR.

   The **Main** dialog box appears.
2. Click **Setup** and then **Flag**.

   The **Flag** dialog box appears.
3. Select **Displayed** to always display the flag or **Displayed** and **Timed** to display the flag for only five seconds after switching.

   NOTE: If you select **Timed** by itself, the flag is not displayed.
4. In the **Display Color** section, select a flag color. Options are black, red, blue, and purple.
5. In **Display Mode**, select **Opaque** for a solid color flag or **Transparent** to see the desktop through the flag.
6. To position the status flag on the desktop, click **Set Position**.

   The **Set Position** Flag is displayed.

7. Left-click on the title bar and drag it to the desired location on the desktop and then right-click to return to the **Flag** dialog box.
8. Click **OK** and again click **OK** to save the settings.

   To exit without saving the changes, click ☒.

Managing Servers With iKVM

The iKVM is an analog switch matrix supporting up to 16 servers. The iKVM switch uses the OSCAR user interface to select and configure the servers. In addition, the iKVM includes a system input to establish a CMC command line console connection to CMC.

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

Related Links

Peripherals Compatibility and Support
Viewing and Selecting Servers

Peripherals Compatibility and Support

The iKVM is compatible with the following peripherals:

- Standard PC USB keyboards with QWERTY, QWERTZ, AZERTY, and Japanese 109 layouts.
- VGA monitors with DDC support.
- Standard USB pointing devices.
- Self-powered USB 1.1 hubs connected to the local USB port on the iKVM.
- Powered USB 2.0 hubs connected to the Dell M1000e chassis' front panel console.

NOTE: You can use multiple keyboards and mice on the iKVM local USB port. The iKVM aggregates the input signals. If there are simultaneous input signals from multiple USB keyboards or mice, it may have unpredictable results.

NOTE: The USB connections are solely for supported keyboard, mouse, and USB hubs. iKVM does not support data transmitted from other USB peripherals.

Viewing and Selecting Servers

When you launch OSCAR, the **Main** dialog box appears. Use the **Main** dialog box to view, configure, and manage servers through the iKVM. You can view the servers by name or by slot. The slot number is the chassis slot number the server occupies. The **Slot** column indicates the slot number in which a server is installed.

NOTE: The Dell CMC command line occupies Slot 17. Selecting this slot displays the CMC command line, where you can execute RACADM commands or connect to the serial console of server or I/O modules.

NOTE: Server names and slot numbers are assigned by CMC.

Related Links

Soft Switching
Viewing Server Status
Selecting Servers

Viewing Server Status

The right columns of the **Main** dialog box indicates the server status in the chassis. The following table describe the status symbols.

Table 32. OSCAR Interface Status Symbols

Symbols	Description
🟢	Server is online.
❌	Server is offline or absent from chassis.
🟡	Server is not available.
A	Server is being accessed by the user channel indicated by the letter: • A=rear panel • B=front panel

Selecting Servers

Use the **Main** dialog box to select the servers. When you select a server, the iKVM reconfigures the keyboard and mouse to the proper settings for that server.

- To select servers, do one of the following:
  - Double-click the server name or the slot number.
  - If the display order of your server list is by slot (that is, the Slot button is depressed), type the slot number and press <Enter>.
  - If the display order of your server list is by name (that is, the Name button is depressed), type the first few characters of the server name, establish it as unique, and press <Enter> twice.
- To select the previous server, press <Print Screen> and then <Backspace>. This key combination toggles between the previous and current connections.
- To disconnect the user from a server, do one of the following:
  - Press <Print Screen> to access OSCAR and then click Disconnect.
  - Press <Print Screen> and then <Alt> <0>. This leaves you in a free state, with no server selected. The status flag on your desktop, if active, displays Free. See **Setting Status Flag Display**

Soft Switching

Soft switching is switching between servers using a hotkey sequence. Press <Print Screen> to soft switch to a server and then type the first few characters of its name or number. If you have previously set a delay time (the number of seconds before the **Main** dialog box is displayed after <Print Screen> is pressed) and if you press the key sequences before that time has elapsed, the OSCAR interface does not display.

Related Links

Configuring Soft Switching

Soft Switching to a Server

Configuring Soft Switching

To configure OSCAR for soft switching:

1. Press <Print Screen> to launch the OSCAR interface.

The **Main** dialog box appears.

2. Click **Setup** and then **Menu**.

   The **Menu** dialog box appears.
3. Select **Name** or **Slot** for the Display/Sort Key.
4. Type the desired delay time in seconds in the **Screen Delay Time** field.
5. Click **OK**.

Soft Switching to a Server

To soft switch to a server:

- To select a server, press <Print Screen>. If the display order of your server list is by slot as per your selection (that is, the Slot button is depressed), type the slot number and press <Enter>

  or

  If the display order of your server list is by name as per your selection (that is, the Name button is depressed), type the first few characters of the name of the server to establish it as unique and press <Enter>.
- To switch back to the previous server, press <Print Screen> then <Backspace>.

Video Connections

The iKVM has video connections on the front and rear panels of the chassis. The front panel connection signals take precedence over that of the rear panel. When a monitor is connected to the front panel, the video connection does not pass through to the rear panel, and an OSCAR message displays stating that the rear panel KVM and ACI connections are disabled. If the monitor is disabled (that is, removed from the front panel or disabled by a CMC command), the ACI connection becomes active while the rear panel KVM remains disabled.

Related Links

iKVM Connection Precedences

Enabling or Disabling Access to iKVM from Front Panel

Preemption Warning

Normally, a user connected to a server console through the iKVM and another user connected to the same server console through the iDRAC Web interface console redirection feature both have access to the console and are able to type simultaneously.

To prevent this scenario, before starting the iDRAC Web interface console redirection, the remote user can disable the local console in the iDRAC Web interface. The local iKVM user sees an OSCAR message that the connection is preempted in a specified amount of time. The local user should finish using the console before the iKVM connection to the server is terminated.

There is no preemption feature available to the iKVM user.

NOTE: If a remote iDRAC user has disabled the local video for a specific server, that server's video, keyboard and mouse is unavailable to the iKVM. The server state is marked with a yellow dot in the OSCAR menu to indicate that it is locked or unavailable for local use see Viewing Server Status.

Related Links

Viewing Server Status

Setting Console Security

OSCAR enables you to configure security settings on the iKVM console. You can setup a screen saver mode that engages after the console remains unused for a specified delay time. Once engaged, the console remains locked until you press any key or move the mouse. Enter the screen saver password to continue.

Use the **Security** dialog box to lock the console with a password, set or change the password, or enable the screen saver.

NOTE: If the iKVM password is lost or forgotten, you can reset it to the iKVM factory default using the CMC Web interface or RACADM.

Related Links

Accessing Security Dialog Box
Setting Password
Password-protecting the Console
Setting Automatic Logout
Removing Password Protection From the Console
Enabling Screen Saver Mode With No Password Protection
Exiting Screen Saver Mode
Clearing Lost or Forgotten Password

Accessing Security Dialog Box

To access the Security dialog box:

1. Press <Print Screen>.

   The **Main** dialog box appears.
2. Click **Setup** and then **Security**.

   The **Security** dialog box appears.

Setting Password

To set the password:

1. Single-click and press <Enter> or double-click in the **New** field.
2. Type the new password and press <Enter>. Passwords are case sensitive and require 5–12 characters. They must include at least one letter and one number. Legal characters are: A–Z, a–z, 0–9, space, and hyphen.
3. In the **Repeat** field, type the password again, and press <Enter>.
4. Click **OK** and close the dialog box.

Password-protecting the Console

To password-protect the console:

1. Set the password as described in Setting Password.
2. Select the **Enable Screen Saver** box.
3. Type the number of minutes of **Inactivity Time** (from 1 through 99) to delay password protection and screen saver activation.
4. For **Mode**: If the monitor is ENERGY STAR compliant, select **Energy**; otherwise select **Screen**.

   – If the mode is set to **Energy**, the appliance puts the monitor into sleep mode. This is normally indicated by the monitor powering off and the amber light replacing the green power LED.

- If the mode is set to **Screen**, the OSCAR flag bounces around the screen for the duration of the test. Before the test starts, a warning popup box displays the following message: "Energy mode may damage a monitor that is not ENERGY STAR compliant. However, once started, the test can be quit immediately via mouse or keyboard interaction."

CAUTION: Monitor damage may result from the use of Energy mode with monitors not compliant with Energy Star.

5. Optional: To activate the screen saver test, click **Test**. The **Screen Saver Test** dialog box displays. Click **OK** to start the test.

   The test takes 10 seconds. After it completes, you are returned to the **Security** dialog box.

Setting Automatic Logout

You can set OSCAR to automatically log out of a server after a period of inactivity.

1. In the **Main** dialog box, click **Setup** and then **Security**.
2. In the **Inactivity Time** field, enter the length of time you want to stay connected to a server before it automatically disconnects you.
3. Click **OK** .

Removing Password Protection From the Console

To remove password protection from your console:

1. In the **Main** dialog box, click **Setup** and then **Security**.
2. In the **Security** dialog box, single-click and press <Enter>, or double-click in the **New field**.
3. Leave the **New field** empty and press <Enter>.
4. Single-click and press <Enter> , or double-click in the **Repeat** field.
5. Leave the **Repeat** field empty and press <Enter>.
6. Click **OK**.

Enabling Screen Saver Mode With No Password Protection

NOTE: If your console is password-protected, you must first remove password protection. Remove the password before enabling screen saver mode with no password protection.

To enable Screen Saver mode without password protection:

1. Select **Enable Screen Saver**.
2. Type the number of minutes (1 through 99) that you want to delay activation of the screen saver.
3. Select **Energy** if your monitor is ENERGY STAR compliant, otherwise select **Screen**.

   CAUTION: Monitor damage may result from the use of Energy mode with monitors not compliant with Energy Star.

4. Optional: To activate the screen saver test, click **Test**. The **Screen Saver Test** dialog box is displayed. Click **OK** to start the test.

   The test takes 10 seconds. After it completes, the **Security** dialog box is displayed.

   NOTE: Enabling **Screen Saver** mode disconnects the user from a server. This means no server is selected. The status flag displays **Free**.

Exiting Screen Saver Mode

To exit screen saver mode and return to the **Main** dialog box, press any key or move your mouse.

To turn off the screen saver, in the **Security** dialog box, clear the **Enable Screen Saver** box and click **OK** .

To immediately turn on the screen saver, press <Print Screen> and then press <Pause>.

Clearing Lost or Forgotten Password

When the iKVM password is lost or forgotten, you can reset it to the iKVM factory default, and then change the password. You can reset the password using either the CMC Web interface or RACADM.

To reset a lost or forgotten iKVM password using the CMC Web interface, in the system tree, go to **Chassis Overview** → **iKVM**, click **Setup** tab, and then click **Restore Default Values**.

You can change the password from the default using OSCAR. For more information see Setting Password.

To reset a lost or forgotten password using RACADM, open a serial/Telnet/SSH text console to CMC, log in, and type:

```
racadm racresetcfg -m kvm
```

NOTE: Using the `racresetcfg` command resets the Front Panel Enable and Dell CMC Console Enable settings, if they are different from the default values.

For more information about the `racresetcfg` subcommand, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC*.

Changing the Language

Use the **Language** dialog box to change the OSCAR text to display in any of the supported languages. The text immediately changes to the selected language on all of the OSCAR screens.

To change the OSCAR language:

1. Press <Print Screen>.

   The **Main** dialog box appears.
2. Click **Setup** and then **Language**.

   The **Language** dialog box appears.
3. Select the required language and click **OK**.

Displaying Version Information

Use the **Version** dialog box to display the iKVM firmware and hardware versions, and to identify the language and keyboard configuration.

To display version information:

1. Press <Print Screen>.

   The **Main** dialog box is displayed.
2. Click **Commands** and then **Display Versions**.

   The **Version** dialog box is displayed. The top half of the **Version** dialog box lists the subsystem versions.
3. Click ☒ or press <Esc> to close the **Version** dialog box.

Scanning the System

In scan mode, the iKVM automatically scans from slot to slot (server to server). You can scan up to 16 servers by specifying the servers you want to scan and the number of seconds each server is displayed.

Related Links

Adding Servers to the Scan List

To add servers to the scan list:

1. Press <Print Screen>.

   The **Main** dialog box is displayed.
2. Click **Setup** and then **Scan**.

   The **Scan** dialog box is displayed listing all servers in the chassis.
3. Perform one of the following functions:

   – Select the servers you want to scan

   – Double-click the server name or slot.

   – Press <Alt> and the number of the servers you want to scan. You can select up to 16 servers.
4. In the **Time** field, enter the number of seconds (3 through 99) that you want iKVM to wait before the scan moves to the next server in the sequence.
5. Click **Add/Remove**, and then click **OK**.

Removing Server from Scan List

To remove a server from the Scan list:

1. In the **Scan** dialog box, do one of the following:

   – Select the server to be removed.

   – Double-click the server name or slot.

   – Click **Clear** to remove all servers from the **Scan** list.
2. Click **Add/Remove** , and then click **OK**.

Starting the Scan Mode

To start the scan mode:

1. Press <Print Screen>.

   The **Main** dialog box is displayed.
2. Click **Commands**.

   The **Command** dialog box is displayed.
3. Select the **Scan Enable** option.
4. Click **OK**.

   A message is displayed indicating that the mouse and keyboard have been reset.
5. Click ☒ to close the message box.

Cancelling Scan Mode

To cancel the scan mode:

1. If OSCAR is open and the **Main** dialog box is displayed, select a server in the list. .

   or

If OSCAR is not open, move the mouse or press any key on the keyboard

The **Main** dialog box is displayed. Select a server in the list.

2. Click **Commands**.

   The **Commands** dialog box is displayed.

3. Clear the **Scan Enable** option and click **OK**.

Broadcasting to Servers

You can simultaneously control more than one server in the system to make sure that all selected servers receive identical input. You can choose to broadcast keystrokes and/or mouse movements independently:

- Broadcasting keystrokes: When using keystrokes, the keyboard state must be identical for all servers receiving a broadcast for the keystrokes to be interpreted identically. Specifically, the <Caps Lock> and <Num Lock> modes must be the same on all keyboards. While the iKVM attempts to send keystrokes to the selected servers simultaneously, some servers may inhibit and thereby delay the transmission
- Broadcasting mouse movements: For the mouse to work accurately, all servers must have identical mouse drivers, desktops (such as identically placed icons), and video resolutions. The mouse also must be in exactly the same place on all screens. Since these conditions are extremely difficult to achieve, broadcasting mouse movements to multiple servers may have unpredictable results.

NOTE: You can broadcast up to 16 servers at a time.

To broadcast to servers:

1. Press <Print Screen>.

   The **Main** dialog box is displayed.

2. Click **Setup** and then **Broadcast**.

   The **Broadcast** dialog box is displayed.

3. Enable mouse and/or keyboard for the servers that are to receive the broadcast commands by selecting the boxes.

   or

   Press the up or down arrow keys to move the cursor to a target server. Then, press <Alt> <K> to select the keyboard box and/or <Alt> <M to select the mouse box. Repeat for additional servers.

4. Click **OK** to save the settings and return to the **Setup** dialog box.

5. Click ☒ or press <Escape> to return to the **Main** dialog box.

6. Click **Commands**.

   The **Commands** dialog box is displayed.

7. Click the **Broadcast Enable** box to activate broadcasting.

   The **Broadcast Warning** dialog box is displayed.

8. Click **OK** to enable the broadcast. To cancel and return to the **Commands** dialog box, click ☒ or press <Esc

9. If broadcasting is enabled, type the information and/or perform the mouse movements you want to broadcast from the management station. Only servers in the list are accessible.

Managing iKVM From CMC

You can do the following:

- View iKVM status and properties

- Update iKVM Firmware
- Enable or disable access to iKVM from front panel
- Enable or disable access to iKVM from the Dell CMC console

Related Links

Updating iKVM Firmware
Enabling or Disabling Access to iKVM from Front Panel
Viewing iKVM Information and Health Status
Enabling Access to iKVM from the Dell CMC Console

Enabling or Disabling Access to iKVM from Front Panel

You can enable or disable access to iKVM from the front panel using the CMC Web interface or RACADM.

Enabling or Disabling Access to iKVM From Front Panel Using Web Interface

To enable or disable access to the iKVM from the front panel using the CMC Web interface:

1. In the system tree, go to **Chassis Overview** → **iKVM** and click **Setup** tab.
   The **iKVM Configuration** page displays.
2. To enable, select the **Front Panel USB/Video Enabled** option. To disable, clear the **Front Panel USB/Video Enabled** option.
3. Click **Apply** to save the setting.

Enabling or Disabling Access to iKVM From Front Panel Using RACADM

To enable or disable access to the iKVM from the front panel using RACADM, open a serial/Telnet/SSH text console to CMC, log in, and type:

```
racadm config -g cfgKVMInfo -o cfgKVMFrontPanelEnable <value>
```

where <value> is 1 (enable) or 0 (disable). For more information about the

`config`

subcommand, see *RACADM Command Line Reference Guide for iDRAC7 and CMC.*

Enabling Access to iKVM from the Dell CMC Console

To enable access to the CMC CLI from iKVM using the CMC Web interface, in the system tree, go to **Chassis Overview** → **iKVM** and click **Setup** tab. Select the **Allow access to CMC CLI from iKVM** option, and click **Apply** to save the setting.

To enable access to the CMC CLI from iKVM using RACADM, open a serial/Telnet/SSH text console to CMC, log in, and type:

```
racadm config -g cfgKVMInfo -o cfgKVMAccessToCMCEnable 1
```

Related Links

Logging In to CMC Using Serial, Telnet, or SSH Console

15

Managing and Monitoring Power

The Dell PowerEdge M1000e server enclosure is the most power-efficient modular server enclosure. It is designed to include highly-efficient power supplies and fans, has an optimized layout for the air ro flow more easily through the system, and contains power-optimized components throughout the enclosure. The optimized hardware design is coupled with sophisticated power management capabilities built into the Chassis Management Controller (CMC), power supplies, and iDRAC to allow you to further enhance power efficiency and to have full control over your power environment.

The Power Management features of the M1000e help administrators configure the enclosure to reduce power consumption and to adjust the power as required specific to the environment.

The PowerEdge M1000e modular enclosure consumes AC power and distributes the load across all active internal power supply units (PSUs). The system can deliver up to 16685 Watts of AC power that is allocated to server modules and the associated enclosure infrastructure.

The PowerEdge M1000e enclosure can be configured for any of three redundancy policies that affect PSU behavior and determine how chassis Redundancy state is reported to administrators.

You can also control Power management through the **Power Measure, Mitigate, and Manage Console (PM3)**. When PM3 controls power externally, CMC continues to maintain:

- Redundancy Policy
- Remote Power Logging
- Server Performance Over Power Redundancy
- Dynamic Power Supply Engagement
- 110 VAC Operation

PM3 then manages:

- Server power
- Server priority
- System Input Power Capacity
- Maximum Power Conservation Mode

NOTE: Actual power delivery is based on configuration and workload.

You can use the CMC Web interface or RACADM to manage and configure power controls on CMC:

- View power allocations, consumption, and status for the chassis, servers, and PSUs.
- Configure power budget and redundancy policy for the chassis.
- Execute power control operations (power-on, power-off, system reset, power-cycle) for the chassis.

Related Links

Redundancy Policies
Dynamic Power Supply Engagement
Default Redundancy Configuration
Power Budgeting For Hardware Modules
Server Slot Power Priority Settings

Viewing Power Consumption Status
Viewing Power Budget Status
Redundancy Status and Overall Power Health
Configuring Power Budget and Redundancy
Executing Power Control Operations
You can execute the following power control operation for the chassis, servers, and IOMs.

Redundancy Policies

Redundancy policy is a configurable set of properties that determine how CMC manages power to the chassis. The following redundancy policies are configurable with or without dynamic PSU engagement:

- AC Redundancy
- Power Supply Redundancy
- No Redundancy

AC Redundancy Policy

The purpose of the AC redundancy policy is to enable a modular enclosure system to operate in a mode in which it can tolerate AC power failures. These failures may originate in the AC power grid, the cabling and delivery, or a PSU itself.

When you configure a system for AC redundancy, the PSUs are divided into grids: PSUs in slots 1, 2, and 3 are in the first grid while PSUs in slots 4, 5, and 6 are in the second grid. CMC manages power so that if there is a failure of either grid the system continues to operate without any degradation. AC redundancy also tolerates failures of individual PSUs.

NOTE: Since one role of AC redundancy is to provide seamless server operation despite failure of a whole power grid, the most power is available to maintain AC redundancy when the capacities of the two grids are approximately equal.

NOTE: AC redundancy is only met when the load requirements do not exceed the capacity of the weakest power grid.

AC Redundancy Levels

One PSU in each grid is the minimum configuration necessary for use as AC redundant. Additional configurations are possible with every combination that has at least one PSU in each grid. However, to make the maximum power available for use, the total power of the PSUs in each leg should be as close to equal as practical. The upper limit of power while maintaining AC redundancy is the power available on the weakest of the two grids. The following figure illustrates 2 PSUs per grid and a power failure on grid 1.

If for some reason CMC is unable to maintain AC redundancy, an e-mail and/or SNMP alerts are sent to administrators if the Redundancy Lost event is configured for alerting.

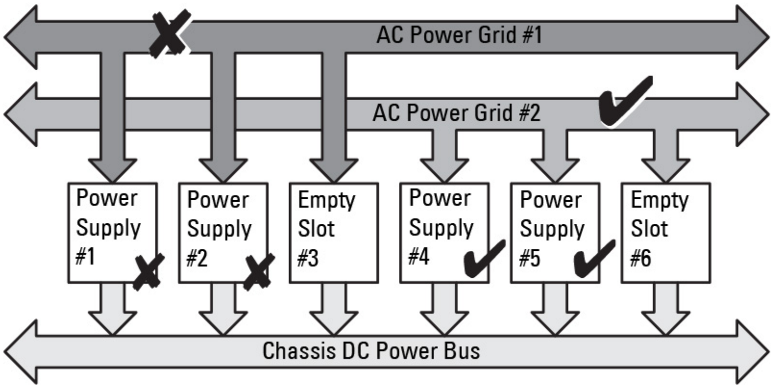


Figure 3. PSUs per grid and a power failure on grid 1

In the event of a single PSU failure in this configuration, the remaining PSUs in the failing grid are marked as Online. In this state, any of the remaining PSUs can fail without interrupting operation of the system. If a PSU fails, the chassis health is marked non-critical. If the smaller grid cannot support the total chassis power allocations, then AC redundancy status is reported as **No Redundancy** and Chassis health is displayed as **Critical**.

Power Supply Redundancy Policy

The power supply redundancy policy is useful when redundant power grids are not available, but you may want to be protected against a single PSU failure bringing down your servers in a modular enclosure. The highest capacity PSU is kept in online reserve for this purpose. This forms a Power Supply redundancy pool. The figure below illustrates power supply redundancy mode.

PSUs beyond those required for power and redundancy are still available and is added to the pool in the event of a failure.

Unlike AC redundancy, when power supply redundancy is selected CMC does not require the PSU units to be present in any specific PSU slot positions.

NOTE: Dynamic Power Supply Engagement (DPSE) allows PSUs to be placed in standby. The standby state indicates a physical state, that of not supplying power. When you enable DPSE, the extra PSUs may be placed in Standby mode to increase efficiency and save power.

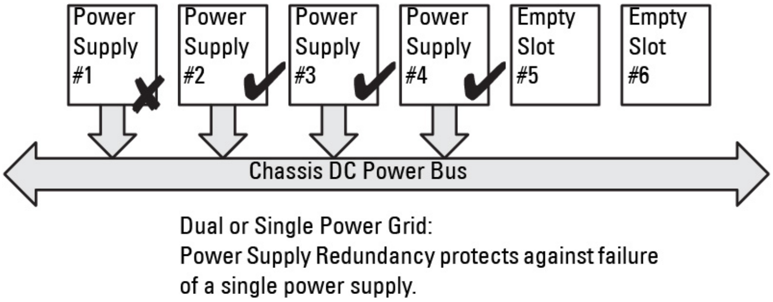


Figure 4. Power Supply Redundancy: Totally 4 PSUs with a failure of one PSU

No Redundancy Policy

The no redundancy mode is the factory default setting for three PSU configuration and indicates that the chassis does not have any power redundancy configured. In this configuration, the overall redundancy status of the chassis always indicates no redundancy. The figure below illustrates no redundancy mode is the factory default setting for three PSU configuration.

CMC does not require the PSU units to be present in any specific PSU slot positions when **No Redundancy** is configured.

NOTE: All PSUs in the chassis are **Online** if DPSE is disabled when in **No Redundancy** mode. When DPSE is enabled all active PSUs in the chassis are listed as **Online** and additional PSUs may be turned to **Standby** to increase the system's power efficiency.

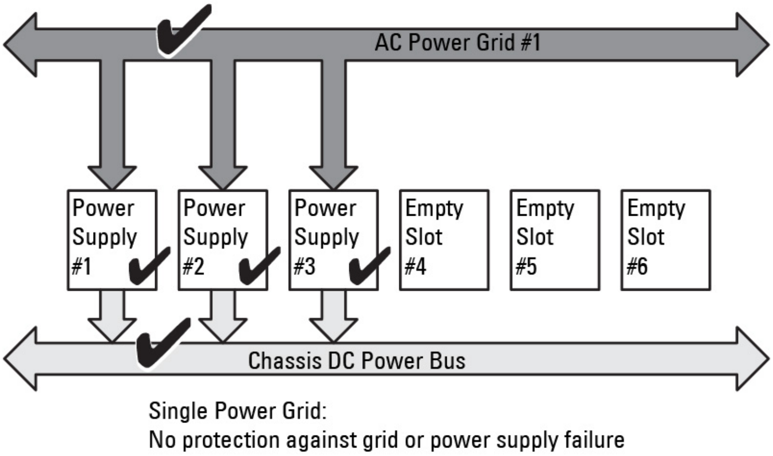


Figure 5. No Redundancy with three PSUs in the chassis

A PSU failure brings other PSUs out of Standby mode, as needed, to support the chassis power allocations. If you have four PSUs, and require only three, then in the event that one fails, the fourth PSU is brought online. A chassis can have all six PSUs online.

When you enable DPSE, the extra PSUs may be placed in Standby mode to increase efficiency and save power. For more information, see Default Redundancy Configuration.

Dynamic Power Supply Engagement

Dynamic Power Supply Engagement (DPSE) mode is disabled by default. DPSE saves power by optimizing the power efficiency of the PSU’s supplying power to the chassis. This also results in increased PSU life, and reduced heat generation.

CMC monitors total enclosure power allocation, and moves the PSUs into Standby state, causing the total power allocation of the chassis to be delivered through fewer PSUs. Since the online PSUs are more efficient when running at higher utilization, this improves their efficiency while also improving longevity of the standby PSUs.

To operate remaining PSUs at their maximum efficiency:

- **No Redundancy** mode with DPSE is highly power efficient, with optimal PSUs online. PSUs that are not needed are placed in standby mode.
- **PSU Redundancy** mode with DPSE also provides power efficiency. At least two supplies are online, with one PSU required to power the configuration and one to provide redundancy in case of PSU failure. PSU Redundancy mode offers protection against the failure of any one PSU, but offers no protection in the event of an AC grid loss.
- **AC Redundancy** mode with DPSE, where at least two of the supplies are active, one on each power grid, provides a good balance between efficiency and maximum availability for a partially-loaded modular enclosure configuration.
- Disabling DPSE provides the lowest efficiency as all six supplies are active and share the load, resulting in lower utilization of each power supply.

DPSE can be enabled for all three power supply redundancy configurations explained above — **No Redundancy**, **Power Supply Redundancy**, and **AC Redundancy**.

- In a **No Redundancy** configuration with DPSE, the M1000e can have up to five power supply units in **Standby** state. In a six PSU configuration, some PSU units are placed in **Standby** and stay unutilized to improve power efficiency. Removal or failure of an online PSU in this configuration cause a PSU in **Standby** state to become **Online**; however, standby PSUs can take up to two seconds to become active, so some server modules may lose power during the transition in the **No Redundancy** configuration.

  NOTE: In a three PSU configuration, server load may prevent any PSUs from transitioning to Standby
- In a **Power Supply Redundancy** configuration, the enclosure always keeps an additional PSU powered on and marked **Online** in addition to the PSUs required to power the enclosure. Power utilization is monitored and up to 284 Managing and Monitoring Power four PSUs could be moved to Standby state depending on the overall system load. In a six PSU configuration, a minimum of two power supply units are always powered on.

  Since an enclosure in the **Power Supply Redundancy** configuration always has an extra PSU engaged, the enclosure can tolerate the loss of one online PSU and still have enough power for the installed server modules. The loss of the online PSU causes a standby PSU to come online. Simultaneous failure of multiple PSUs may result in the loss of power to some server modules while the standby PSUs are powering up.
- In **AC Redundancy** configuration, all power supplies are engaged at chassis power up. Power utilization is monitored, and if system configuration and power utilization allows, PSUs are moved to the **Standby** state. Since the **Online** status of PSUs in a grid mirrors that of the other grid, the enclosure can sustain the loss of power to an entire grid with no interruption of power to the enclosure.

  An increase in power demand in the **AC Redundancy** configuration cause the engagement of PSUs from the **Standby** state. This maintains the mirrored configuration needed for dual-grid redundancy.

  NOTE: With DPSE Enabled, the Standby PSUs are brought **Online** to reclaim power if power demand increases in all three Power Redundancy policy modes.

Default Redundancy Configuration

The default redundancy configuration for a chassis depends on the number of PSUs it contains, as shown in the following table.

Table 33. Default Redundancy Configuration

PSU Configuration	Default Redundancy Policy	Default Dynamic PSU Engagement Setting
Six PSUs	AC Redundancy	Disabled
Three PSUs	No Redundancy	Disabled

AC Redundancy

In AC Redundancy mode with six PSUs, all six PSUs are active. The three PSUs on the left must connect to one AC power grid, while the three PSUs on the right connect to another AC power grid.

CAUTION: To avoid a system failure and for AC Redundancy to work effectively, there must be a balanced set of PSU properly cabled to separate AC grids.

If one AC grid fails, the PSUs on the functioning AC grid take over without interruption to the servers or infrastructure.

CAUTION: In AC redundancy mode, you must have balanced sets of PSUs (at least one PSU in each grid). If this condition is not met, AC redundancy may not be possible.

Power Supply Redundancy

When power supply redundancy is enabled, a PSU in the chassis is kept as a spare, ensuring that the failure of any one PSU does not cause the servers or chassis to power-down. Power Supply Redundancy mode requires up to four PSUs.

Additional PSUs, if present, are utilized to improve power efficiency of the system if DPSE is enabled. Subsequent failures after loss of redundancy may cause the servers in the chassis to power down.

No Redundancy

Power in excess of what is necessary to power the chassis is available, even on a failure, to continue to power the chassis.

CAUTION: The No Redundancy mode uses optimum PSUs when DPSE is enabled for the requirements of the chassis. Failure of a single PSU could cause servers to lose power and data in this mode.

Power Budgeting For Hardware Modules

CMC offers a power budgeting service that allows you to configure power budget, redundancy, and dynamic power for the chassis.

The power management service enables optimization of power consumption and re-allocation of power to different modules based on demand.

The following figure illustrates a chassis that contains a six-PSU configuration. The PSUs are numbers 1-6, starting on the left-side of the enclosure.

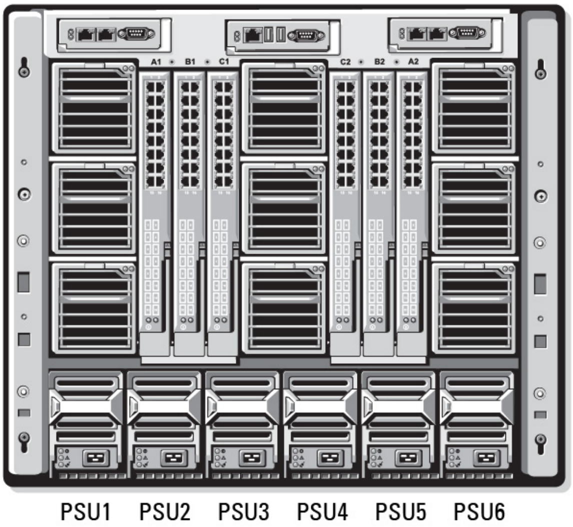


Figure 6. Chassis With Six-PSU Configuration

CMC maintains a power budget for the enclosure that reserves the necessary wattage for all installed servers and components.

CMC allocates power to the CMC infrastructure and the servers in the chassis. CMC infrastructure consists of components in the chassis, such as fans, I/O modules, and iKVM (if present). The chassis may have up to 16 servers that communicate to the chassis through the iDRAC. For more information, see the *iDRAC7 User's Guide* at **support.dell.com/manuals**.

iDRAC provides CMC with its power envelope requirements before powering up the server. The power envelope consists of the maximum and minimum power requirements necessary to keep the server operating. iDRAC's initial estimate is based on its initial understanding of components in the server. After operation commences and further components are discovered, iDRAC may increase or decrease its initial power requirements.

When a server is powered-up in an enclosure, the iDRAC software re-estimates the power requirements and requests a subsequent change in the power envelope.

CMC grants the requested power to the server, and the allocated wattage is subtracted from the available budget. Once the server is granted a power request, the server's iDRAC software continuously monitors the actual power consumption. Depending on the actual power requirements, the iDRAC power envelope may change over time. iDRAC requests a power step-up only if the servers are fully consuming the allocated power.

Under heavy load the performance of the server’s processors may be degraded to ensure power consumption stays lower than the user-configured *System Input Power Cap*.

The PowerEdge M1000e enclosure can supply enough power for peak performance of most server configurations, but many available server configurations do not consume the maximum power that the enclosure can supply. To help data centers provision power for their enclosures, the M1000e allows you to specify a *System Input Power Cap* to ensure that the overall chassis AC power draw stays under a given threshold. CMC first ensures enough power is available to run the fans, IO Modules, iKVM (if present), and CMC itself. This power allocation is called the *Input Power Allocated to Chassis Infrastructure*. Following Chassis Infrastructure, the servers in an enclosure are powered up. Any attempt to set a *System Input Power Cap* less than the actual consumption fails.

If necessary for the total power budget to stay below the value of the *System Input Power Cap*, CMC allocates servers a value less than their maximum requested power. Servers are allocated power based on their *Server Priority* setting, with higher priority servers getting maximum power, priority 2 servers getting power after priority 1 servers, and so on. Lower priority servers may get less power than priority 1 servers based on *System Input Max Power Capacity* and the user-configured setting of *System Input Power Cap*.

Configuration changes, such as an additional server in the chassis, may require the *System Input Power Cap* to be increased. Power needs in a modular enclosure also increase when thermal conditions change and the fans are required to run at higher speed, which causes them to consume additional power. Insertion of I/O modules and iKVM also increases the power needs of the modular enclosure. A fairly small amount of power is consumed by servers even when they are powered down to keep the management controller powered up.

Additional servers can be powered up in the modular enclosure only if sufficient power is available. The *System Input Power Cap* can be increased any time up to a maximum value of 16685 watts to allow the power up of additional servers.

Changes in the modular enclosure that reduce the power allocation are:

- Server power off
- Server
- I/O module
- iKVM removal
- Transition of the chassis to a powered off state

You can reconfigure the *System Input Power Cap* when chassis is either ON or OFF.

NOTE:

Server Slot Power Priority Settings

CMC allows you to set a power priority for each of the sixteen server slots in an enclosure. The priority settings are 1 (highest) through 9 (lowest). These settings are assigned to slots in the chassis, and the slot's priority is inherited by any server inserted in that slot. CMC uses slot priority to preferentially budget power to the highest priority servers in the enclosure.

According to the default server slot priority setting, power is equally apportioned to all slots. Changing the slot priorities allows administrators to prioritize the servers that are given preference for power allocations. If the more critical server modules are left at their default slot priority of 1, and the less critical server modules are changed to lower priority value of 2 or higher, the priority 1 server modules is powered on first. These higher priority servers get their maximum power allocation, while lower priority servers may be not be allocated enough power to run at their maximum performance or they may not even power on at all, depending on how low the system input power cap is set and the server power requirements.

If an administrator manually powers on the low priority server modules before the higher priority ones, then the low priority server modules are the first modules to have their power allocation lowered down to the minimum value, in order to accommodate the higher priority servers. Therefore, after the available power for allocation is exhausted, then CMC reclaims power from lower or equal priority servers until they are at their minimum power level.

NOTE: I/O modules, fans, and iKVM (if present) are given the highest priority. CMC reclaims power only from lower priority devices to meet the power needs of a higher priority module or server.

Assigning Priority Levels to Servers

Server priority levels determine which servers the CMC draws power from when additional power is required.

NOTE: The priority you assign to a server is linked to its slot and not to the server itself. If you move the server to a new slot, you must re-configure the priority for the new slot location.

NOTE: To perform power management actions, you must have **Chassis Configuration Administrator** privilege.

Assigning Priority Levels to Servers Using CMC Web Interface

To assign priority levels using the CMC Web interface:

1. In the system tree go to **Server Overview**, and then click **Power** → **Priority**.

   The **Server Priority** page lists all the servers in the chassis.

2. Select a priority level (1–9, where 1 is the highest priority) for one, multiple, or all servers. The default value is 1. You can assign the same priority level to multiple servers.

3. Click **Apply** to save your changes.

Assigning Priority Levels to Servers Using RACADM

Open a serial/Telnet/SSH text console to CMC, log in, and type:

```
racadm config -g cfgServerInfo -o cfgServerPriority -i <slot number> <priority
level>
```

where <*slot number*> (1–16) refers to the location of the server, and <*priority level*> is a value between 1–9

For example, to set the priority level to 1 for the server in slot 5, type the following command:

```
racadm config -g cfgServerInfo -o cfgServerPriority -i 5 1
```

Viewing Power Consumption Status

CMC provides the actual input power consumption for the entire system.

Viewing Power Consumption Status Using CMC Web Interface

To view power consumption status using the CMC Web interface, in the system tree go to **Chassis Overview** and click **Power** → **Power Monitoring** . The Power Monitoring page displays the power health, system power status, real-time power statistics, and real-time energy statistics. For more information, see the *CMC Online Help*.

NOTE: You can also view the power redundancy status under Power Supplies in the **System tree** → **Status tab** .

Viewing Power Consumption Status Using RACADM

To view power consumption status using RACADM:

Open a serial/Telnet/SSH text console to CMC, log in, and type:

```
racadm getpminfo
```

Viewing Power Budget Status

You can view the power budget status using the CMC Web interface or RACADM.

Viewing Power Budget Status Using CMC Web Interface

To view power budget status using CMC Web interface, in the system tree go to **Chassis Overview** and click **Power** → **Budget Status**. The **Power Budget Status** page displays the system power policy configuration, power budget details, budget allocated for server modules, and chassis power supply details. For more information, see the *CMC Online Help*.

Viewing Power Budget Status Using RACADM

Open a serial/Telnet/SSH text console to CMC, log in, and type:

```
racadm getpbinfo
```

For more information about **getpbinfo**, including output details, see the **getpbinfo** command section in the *RACADM Command Line Reference Guide for iDRAC6 and CMC*.

Redundancy Status and Overall Power Health

The redundancy status is a factor in determining the overall power health. When the power redundancy policy is set, for example, to AC Redundancy and the redundancy status indicates that the system is operating with redundancy, the overall power health is typically **OK**. However, if the conditions for operating with AC redundancy cannot be met, the redundancy status is **No**, and the overall power health is **Critical**. This is because the system is not able to operate in accordance with the configured redundancy policy.

NOTE: CMC does not perform a pre-check of these conditions when you change the redundancy policy to or from AC redundancy. So, configuring the redundancy policy may immediately result in redundancy lost or a regained condition.

Related Links

- PSU Failure With Degraded or No Redundancy Policy
- PSU Removals With Degraded or No Redundancy Policy
- New Server Engagement Policy
- Power Supply and Redundancy Policy Changes in System Event Log

PSU Failure With Degraded or No Redundancy Policy

CMC decreases power to servers when an insufficient power event occurs, such as a PSU failure. After decreasing power on servers, CMC re-evaluates the power needs of the chassis. If power requirements are still not met, CMC powers off lower priority servers.

Power for higher priority servers is restored incrementally while power needs remain within the power budget. To set the redundancy policy, see Configuring Power Budget and Redundancy.

PSU Removals With Degraded or No Redundancy Policy

CMC may begin conserving power when you remove a PSU or a PSU AC cord. CMC decreases power to the lower priority servers until power allocation is supported by the remaining PSUs in the chassis. If you remove more than one PSU, CMC evaluates power needs again when the second PSU is removed to determine the firmware response. If power requirements are still not met, CMC may power off the lower priority servers.

Limits

- CMC does not support *automated* power-down of a lower priority server to allow power up of a higher priority server; however, you can perform user-initiated power-downs.
- Changes to the PSU redundancy policy are limited by the number of PSUs in the chassis. You can select any of the three PSU redundancy configuration settings listed in Default Redundancy Configuration.

New Server Engagement Policy

When a new server is powered on, CMC may need to decrease power to lower priority servers to allow more power for the new server if adding the new server exceeds the power available for the chassis. This could happen if the administrator has configured a power limit for the chassis that is below what would be required for full power allocation to the servers, or if insufficient power is available for the worst-case power need of all servers in the chassis. If enough power cannot be freed by reducing the allocated power of the lower priority servers, the new server may not be allowed to power up.

The highest amount of sustained power required to run the chassis and all of the servers, including the new one, at full power is the worst-case power requirement. If that amount of power is available, then no servers are allocated power that is less than the worst-case power needed and the new server is allowed to power up.

If the worst-case power requirement cannot be met, power is reduced to the lower priority servers until enough power is freed to power up the new server.

The following table provides the actions taken by CMC when a new server is powered on in the scenario described earlier.

Table 34. CMC Response When a Server Power-On is Attempted

Worst Case Power is Available	CMC Response	Server Power On
Yes	No power conservation is required	Allowed
No	Perform power conservation: • Power required for new server is available • Power required for new server is not available	Allowed Disallowed

If a PSU fails, it results in a non-critical health state and a PSU failure event is generated. The removal of a PSU results in a PSU removal event.

If either event results in a loss of redundancy, based on power allocations, a *loss of redundancy* event is generated.

If the subsequent power capacity or the user power capacity is greater than the server allocations, servers have degraded performance or, in a worse case, servers may be powered down. Both conditions are in reverse-priority order, that is, the lower priority servers are powered down first.

The following table provides the firmware response to a PSU power down or removal as it applies to various PSU redundancy configurations.

Table 35. Chassis Impact from PSU Failure or Removal

PSU Configuration	Dynamic PSU Engagement	Firmware Response
AC Redundancy	Disabled	CMC alerts you of loss of AC Redundancy.
Power Supply Redundancy	Disabled	CMC alerts you of loss of Power Supply Redundancy.
No Redundancy	Disabled	Decrease power to low priority servers, if needed.
AC Redundancy	Enabled	CMC alerts you of loss of AC Redundancy. PSUs in standby mode (if any) are turned on to compensate for power budget lost from the PSU failure or removal.
Power Supply Redundancy	Enabled	CMC alerts you of loss of Power Supply Redundancy. PSUs in standby mode (if any) are turned on to compensate for power budget lost from PSU failure or removal.
No Redundancy	Enabled	Decrease power to low priority servers, if needed.

Power Supply and Redundancy Policy Changes in System Event Log

Changes in the power supply state and power redundancy policy are recorded as events. Events related to the power supply that record entries in the system event log (SEL) are power supply insertion and removal, power supply input insertion and removal, and power supply output assertion and de-assertion.

The following table lists the SEL entries that are related to power supply changes:

Table 36. SEL Events for Power Supply Changes

Power Supply Event	System Event Log (SEL) Entry
Insertion	Power supply presence was asserted
Removal	Power supply presence was de-asserted
AC input received	Power supply input lost was de-asserted
AC input lost	Power supply input lost was asserted
DC output produced	Power supply failure was de-asserted
DC output lost	Power supply failure was asserted
Unacknowledged 110V operation detected	Power supply low input voltage (110) was asserted
110V operation acknowledged	Power supply low input voltage (110) was de-asserted

Events related to changes in the power redundancy status that record entries in the SEL are redundancy loss and redundancy regain for the modular enclosure that is configured for either an **AC Redundancy** power policy or **Power Supply Redundancy** power policy. The following table lists the SEL entries that are related to power redundancy policy changes.

Power Policy Event	System Event Log (SEL) Entry
Redundancy lost	Redundancy lost was asserted
Redundancy regained	Redundancy lost was de-asserted

Configuring Power Budget and Redundancy

You can configure the power budget, redundancy, and dynamic power of the entire chassis (chassis, servers, I/O modules, iKVM, CMC, and power supplies), which uses six power supply units (PSUs). The power management service optimizes power consumption and re-allocates power to different modules based on the requirement.

You can configure the following:

- System Input Power Cap
- Redundancy Policy
- Server Performance Over Power Redundancy
- Enable Dynamic Power Supply Engagement
- Disable Chassis Power Button
- Allow 110 VAC Operation
- Max Power Conservation Mode
- Remote Power Logging
- Remote Power Logging Interval
- Server Based Power Management

Related Links

Power Conservation and Power Budget
Maximum Power Conservation Mode
Server Power Reduction to Maintain Power Budget
110V PSUs AC Operation
Server Performance Over Power Redundancy

Remote Logging
External Power Management
Configuring Power Budget and Redundancy Using CMC Web Interface
Configuring Power Budget and Redundancy Using RACADM

Power Conservation and Power Budget

CMC performs power conservation when the user-configured maximum power limit is reached. When the demand for power exceeds the user configured System Input Power Cap, CMC reduces power to servers in reverse-priority order to free power for higher priority servers and other modules in the chassis.

If all or multiple slots in the chassis are configured with the same priority level, CMC decreases power to servers in increasing slot number order. For example, if the servers in slots 1 and 2 have the same priority level, the power for the server in slot 1 is decreased before that of the server in slot 2.

NOTE: You can assign a priority level to each server in the chassis assigning a number from 1 through 9 for each server. The default priority level for all servers is 1. The lower the number, the higher the priority level.

The power budget is limited to a maximum of which ever set of three PSUs that is the weakest. If you attempt to set an AC power budget value that exceeds the *System Input Power Cap* value, CMC displays a failure message. The power budget is limited to 16685 Watts.

Maximum Power Conservation Mode

CMC performs maximum power conservation when:

- Maximum conservation mode is enabled
- An automated command line script, issued by a UPS device, enables maximum conservation mode.

In maximum power conservation mode, all servers start functioning at their minimum power levels, and all subsequent server power allocation requests are denied. In this mode, the performance of powered on servers may be degraded. Additional servers cannot be powered on, regardless of server priority.

The system is restored to full performance when the maximum conservation mode is cleared.

Server Power Reduction to Maintain Power Budget

CMC reduces power allocations of lower priority servers when additional power is needed to maintain the system power consumption within the user-configured *System Input Power Cap*. For example, Managing and Monitoring Power 297 when a new server is engaged, CMC may decrease power to low priority servers to allow more power for the new server. If the amount of power is still insufficient after reducing power allocations of the lower priority servers, CMC lowers the performance of servers until sufficient power is freed to power the new server.

CMC reduces server power allocation in two cases:

- Overall power consumption exceeds the configurable *System Input Power Cap*.
- A power failure occurs in a non-redundant configuration.

110V PSUs AC Operation

Some PSUs support operation with 110V AC input. This input can exceed the allowed limit for the branch circuit. If any PSUs are connected to 110V AC, the user needs to set CMC for normal operation of the enclosure. If it is not set and 110V PSUs are detected, all subsequent server power allocation requests are denied. In this case, additional servers cannot be powered on, regardless of their priority. You can set CMC to use 110 V PSUs using the Web interface or RACADM.

Power supply entries are logged to the SEL log:

- When 110V power supplies are detected or removed.
- When the 110V AC input operation is enabled or disabled.

The overall power health is at least in Non-Critical state when the chassis is operating in 110V mode and the user has not enabled the 110V operation. The "Warning" icon is displayed on the Web interface main page when in Non-Critical state.

Mixed 110V and 220V operation is not supported. If CMC detects that both voltages are in use, then one voltage is selected and those power supplies connected to the other voltage are powered off and marked as failed.

Server Performance Over Power Redundancy

When enabled, this option favors server performance and server powerup, over maintaining power redundancy. When disabled, the system favors power redundancy over server performance. When disabled, then if the power 298 Managing and Monitoring Power supplies in the chassis do not provide sufficient power, both for redundancy, as well as full performance, then to preserve redundancy, some servers may not be:

- Granted sufficient power for full performance
- Powered on

Remote Logging

Power consumption can be reported to a remote syslog server. Total chassis power consumption, minimum, maximum, and average power consumption over a collection period can be logged. For more information on enabling this feature and configuring the collection/logging interval, see related sections below.

External Power Management

CMC Power management is optionally controlled by the Power Measure, Mitigate, and Manage Console (PM3). For more information, see the *PM3 User's Guide*.

When external power management is enabled, PM3 manages:

- Server Power of 12th generation servers
- Server Priority of 12th generation servers
- System Input Power Capacity
- Maximum Power Conservation Mode

The CMC continues to maintain or manage:

- Redundancy Policy
- Remote Power Logging
- Server Performance over Power Redundancy
- Dynamic Power Supply Engagement
- Server Power of 11th generation and earlier servers

PM3 then manages prioritization and power of 12th generation blade servers in the chassis from the budget available after allocation of power to chassis infrastructure and prior generation blade servers. Remote power logging is unaffected by external power management.

After the Server Based Power Management Mode is enabled, the chassis is prepared for PM3 management. All 12th generation server priorities are set to 1 (High). PM3 manages the server power and priorities directly. Since PM3 controls compatible server power allocations, CMC no longer controls the Maximum Power Conservation Mode. Hence, this selection is disabled.

When the Maximum Power Conservation Mode is enabled, the CMC sets the System Input Power Capacity to the maximum that the chassis can handle. CMC does not allow power to exceed the highest capacity. However, PM3 handles all other power capacity limitations.

When PM3 management of power is disabled, the CMC reverts to the server priority settings before the external management was enabled.

NOTE: When PM3 management is disabled, CMC does not revert to the earlier setting of the maximum chassis power. See the **CMC log** for the earlier setting to manually restore the value.

Configuring Power Budget and Redundancy Using CMC Web Interface

NOTE: To perform power management actions, you must have **Chassis Configuration Administrator** privilege.

To configure power budget using the Web interface:

1. In the system tree, go to **Chassis Overview,** and then click **Power** → **Configuration**

The **Budget/Redundancy Configuration** page is displayed.

2. Select any or all of the following properties as required. For information about each of the fields, see *CMC Online Help*.
   - Enable Server Based Power Management
   - System Input Power Cap
   - Redundancy Policy
   - Server Performance Over Power Redundancy
   - Enable Dynamic Power Supply Engagement
   - Disable Chassis Power Button
   - Allow 110 VAC Operation
   - Max Power Conservation Mode
   - Enable Remote Power Logging 300 Managing and Monitoring Power
   - Remote Power Logging Interval
3. Click **Apply** to save the changes.

Configuring Power Budget and Redundancy Using RACADM

NOTE: To perform power management actions, you must have **Chassis Configuration Administrator** privilege.

To enable and set the redundancy policy:

1. Open a serial/Telnet/SSH text console to CMC and log in.
2. Set properties as needed:
   - To select a redundancy policy, type:

     ```
     racadm config -g cfgChassisPower -o
     cfgChassisRedundancyPolicy <value>
     ```

     where <value> is 0 (No Redundancy), 1 (AC Redundancy), 2 (Power Supply Redundancy). The default is 0.

     For example, the following command sets the redundancy policy to 1:

     ```
     racadm config -g cfgChassisPower -o
     cfgChassisRedundancyPolicy 1
     ```
   - To set the power budget value, type:

     ```
     racadm config -g cfgChassisPower -o
     cfgChassisPowerCap <value>
     ```

     where <*value*> is a number between 2715–16685 representing the maximum power limit in watts. The default is 16685.

     For example, the following command sets the maximum power budget to 5400 watts:

     ```
     racadm config -g cfgChassisPower -o
     cfgChassisPowerCap 5400
     ```

     .
   - To enable or disable dynamic PSU engagement, type:

     ```
     racadm config -g cfgChassisPower -o
     cfgChassisDynamicPSUEngagementEnable <value>
     ```

     where <value> is 0 (disable), 1 (enable). The default is 0.

     For example, the following command disables dynamic PSU engagement:

     ```
     racadm config -g cfgChassisPower -o
     cfgChassisDynamicPSUEngagementEnable 0
     ```

.

- To enable the maximum power consumption mode, type:

  ```
  racadm config -g cfgChassisPower -o
  cfgChassisMaxPowerConservationMode 1
  ```

- To restore normal operation, type:

  ```
  racadm config -g cfgChassisPower -o
  cfgChassisMaxPowerConservationMode 0
  ```

- Enable 110 VAC PSUs:

  ```
  racadm config -g cfgChassisPower -o
  cfgChassisAllow110VACOperation 1
  ```

- Enable Server Performance Over Power Redundancy:

  ```
  racadm config -g cfgChassisPower -o
  cfgChassisPerformanceOverRedundancy 1
  ```

- Disable Server Performance Over Power Redundancy:

  ```
  racadm config -g cfgChassisPower -o
  cfgChassisPerformanceOverRedundancy 0
  ```

- To enable the power remote logging feature, enter the following command:

  ```
  racadm config -g cfgRemoteHosts -o
  cfgRhostsSyslogPowerLoggingEnabled 1
  ```

- To specify the desired logging interval, enter the following command:

  ```
  racadm config -g cfgRemoteHosts -o
  cfgRhostsSyslogPowerLoggingInterval n
  ```

  where n is 1-1440 minutes.

- To determine if the power remote logging feature is enabled, enter the following command:

  ```
  racadm getconfig -g cfgRemoteHosts -o
  cfgRhostsSyslogPowerLoggingEnabled
  ```

- To determine the power remote logging interval, enter the following command:

  ```
  racadm getconfig -g cfgRemoteHosts -o
  cfgRhostsSyslogPowerLoggingInterval
  ```

  The power remote logging feature is dependent on remote syslog hosts having been previously configured. Logging to one or more remote syslog hosts must be enabled, otherwise power consumption is logged. This can be done either through the web GUI or the RACADM CLI. For more information, see the remote syslog configuration instructions.

- To enable remote power management by PM3, type:

  ```
  racadm config -g cfgChassisPower -o
  cfgChassisServerBasedPowerMgmtMode 1
  ```

- To restore CMC power management, type:

  ```
  racadm config -g cfgChassisPower -o
  cfgChassisServerBasedPowerMgmtMode 0
  ```

For information about RACADM commands for chassis power, see the **config**, **getconfig**, **getpbinfo**, and **cfgChassisPower** sections in the *RACADM Command Line Reference Guide for iDRAC7 and CMC*.

Executing Power Control Operations

You can execute the following power control operation for the chassis, servers, and IOMs.

NOTE: Power control operations affect the entire chassis.

Related Links

Executing Power Control Operations on the Chassis

[Executing Power Control Operations on a Server](#)
[Executing Power Control Operations on an IOM](#)

Executing Power Control Operations on the Chassis

CMC enables you to remotely perform several power management actions, such as an orderly shutdown, on the entire chassis (chassis, servers, IOMs, iKVM, and PSUs).

NOTE: To perform power management actions, you must have **Chassis Configuration Administrator** privilege.

Executing Power Control Operations on the Chassis Using Web Interface

To execute power control operations on the chassis using the CMC Web interface:

1. In the system tree, go to **Chassis Overview** and click **Power** → **Control** .

   The **Chassis Power Control** page is displayed.
2. Select one of the following power control operations.

   For information about each option, see the *CMC Online Help*.

   - Power On System
   - Power Off System
   - Power Cycle System (cold boot)
   - Reset CMC (warm boot)
   - Non-Graceful Shutdown
3. Click **Apply**.

   A dialog box appears requesting confirmation.
4. Click **OK** to perform the power management action (for example, cause the system to reset).

Executing Power Control Operations on the Chassis Using RACADM

Open a serial/Telnet/SSH text console to CMC, log in, and type:

```
racadm chassisaction -m chassis <action>
```

where <*action*> is powerup, powerdown, powercycle, nongraceshutdown or reset.

Executing Power Control Operations on a Server

You can remotely perform power management actions for multiple servers at a time or an individual server in the chassis.

NOTE: To perform power management actions, you must have **Chassis Configuration Administrator** privilege.

Executing Power Control Operations for Multiple Servers Using CMC Web Interface

To execute power control operation for multiple servers using the Web interface:

1. In the system tree, go to **Server Overview** and click **Power** → **Control** .

   The **Power Control** page is displayed.
2. In the **Operations** column, from the drop-down menu, select one of the following power control operation for the required servers:

   - No Operation
   - Power On Server

- Power Off Server
- Graceful Shutdow n
- Reset Server (warm boot
- Power Cycle Server (cold boot)

For information about the options, see the *CMC Online Help*.

3. Click **Apply**.

   A dialog box appears requesting confirmation.

4. Click **OK** to perform the power management action (for example, cause the server to reset).

Executing Power Control Operations on a Server Using CMC Web Interface

To execute power control operation for an individual server using the CMC Web interface:

1. In the system tree, go to **Chassis Overview** and click **Server Overview**.
2. Click on the server for which you want to execute the power control operation, and then click the **Power** tab.

   The **Server Power Management** page is displayed.

3. Select one of the following power control operation:

   - Power On Server
   - Power Off Server
   - Reset Server (warm boot)
   - Power Cycle Server (cold boot)

   For information about the options, see the *CMC Online Help*.

4. Click **Apply**.

   A dialog box appears requesting confirmation.

5. Click **OK** to perform the power management action (for example, cause the server to reset).

Executing Power Control Operations on a Server Using RACADM

To execute power control operations on a server using RACADM, open a serial/Telnet/SSH text console to CMC, log in, and type:

```
racadm serveraction -m <module> <action>
```

where <*module*> specifies the server by its slot number (server-1 through server-16) in the chassis, and <*action*> is the operation you want to execute:

```
powerup, powerdown, powercycle, graceshutdown, or hardreset.
```

Executing Power Control Operations on an IOM

You can remotely execute a reset or power cycle on an individual IOM.

NOTE: To perform power management actions, you must have **Chassis Configuration Administrator** privilege.

Executing Power Control Operations on IOMs Using CMC Web Interface

To execute power control operations on an IOM using the CMC Web interface:

1. In the system tree, go to **Chassis Overview** → **I/O Module Overview** and click **Power**.

   The **Power Control** page is displayed.

2. For the IOM in the list, from the drop-down menu, select the operation you want to execute (reset or power cycle).

3. Click **Apply**.

   A dialog box appears requesting confirmation.

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

Executing Power Control Operations on IOMs Using RACADM

To execute power control operations on an IOM using RACADM, open a serial/Telnet/SSH text console to CMC, log in, and type:

```
racadm chassisaction -m switch-<n><action>
```

where <*n*> is a number 1-6 and specifies the IOM (A1, A2, B1, B2, C1, C2), and <action> indicates the operation you want to execute: powercycle or reset.

16

Troubleshooting and Recovery

This section explains how to perform tasks related to recovering and troubleshooting problems on the remote system using the CMC Web interface.

- Viewing chassis information.
- Viewing the event logs.
- Gathering Configuration information, error status and error logs.
- Using the Diagnostic Console.
- Managing power on a remote system.
- Managing Lifecycle Controller jobs on a remote system.
- Reset Components.
- Troubleshooting Network Time Protocol (NTP) problems.
- Troubleshooting network problems.
- Troubleshooting alerting problems.
- Resetting forgotten administrator password.
- Saving and restoring Chassis configuration settings and certificates.
- Error codes and logs.

Gathering Configuration Information and Chassis Status and Logs Using RACDUMP

The `racdump` subcommand provides a single command to get comprehensive chassis status, configuration state information, and the historic event logs.

The `racdump` subcommand displays the following information:

- General system/RAC information
- CMC information
- Chassis information
- Session information
- Sensor information
- Firmware build information

Supported Interfaces

- CLI RACADM
- Remote RACADM
- Telnet RACADM

Racdump includes the following subsystems and aggregates the following RACADM commands. For more information on racdump, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC.*

Subsystem	RACADM Command
General System/RAC information	`getsysinfo`
Session information	`getssinfo`
Sensor information	`getsensorinfo`
Switches information (IO Module)	`getioinfo`
Mezzanine card information (Daughter card)	`getdcinfo`
All modules information	`getmodinfo`
Power budget information	`getpbinfo`
KVM information	`getkvminfo`
NIC information (CMC module)	`getniccfg`
Redundancy information	`getredundancymode`
Trace log information	`gettracelog`
RAC event log	`gettraclog`
System event log	`getsel`

Downloading SNMP Management Information Base (MIB) File

The CMC SNMP MIB File defines chassis types, events, and indicators. CMC enables you to download the MIB file using the Web Interface.

To download the CMC's SNMP Management Information Base (MIB) file using the CMC Web interface:

1. In the system tree, go to **Chassis Overview** and click **Network** → **Services** → **SNMP**.

   The **SNMP Configuration** section is displayed.
2. Click **Save** to download the CMC **MIB** file to your local system.

   For more information on the SNMP **MIB** file, see the *Dell OpenManage Server Administrator SNMP Reference Guide* at **support.dell.com/manuals.**

First Steps to Troubleshooting a Remote System

The following questions are commonly used to troubleshoot high-level problems in the managed system:

- Is the system powered on or off?
- If powered on, is the operating system functioning, crashed, or frozen?
- If powered off, did the power turn off unexpectedly?

Power Troubleshooting

The following information helps you to troubleshoot power supply and power-related issues:

- **Problem:** Configured the **Power Redundancy Policy** to **AC Redundancy**, and a Power Supply Redundancy Lost event was raised.
  - **Resolution A:** This configuration requires at least one power supply in side 1 (the left three slots) and one power supply in side 2 (the right three slots) to be present and functional in the modular enclosure.

Additionally the capacity of each side must be enough to support the total power allocations for the chassis to maintain **AC redundancy**. (For full AC Redundancy operation, ensure that a full PSU configuration of six power supplies is available.)

  - **Resolution B:** Check if all power supplies are properly connected to the two AC grids; power supplies in side 1 need to be connected to one AC grid, those in side 2 need to be connected to the other AC grid, and both AC grids need to be working. **AC Redundancy** is lost when one of the AC grids is not functioning.

- **Problem:** The PSU state is displayed as **Failed (No AC)**, even when an AC cord is connected and the power distribution unit is producing good AC output.

  - **Resolution A:** Check and replace the AC cord. Check and confirm that the power distribution unit providing power to the power supply is operating as expected. If the failure still persists, call Dell customer service for replacement of the power supply.
  - **Resolution B:** Check that the PSU is connected to the same voltage as the other PSUs. If CMC detects a PSU operating at a different voltage, the PSU is turned off and marked Failed.

- **Problem:** Dynamic Power Supply Engagement is enabled, but none of the power supplies display in the **Standby** state.

  - **Resolution A:** There is insufficient surplus power. One or more power supplies are moved into the Standby state only when the surplus power available in the enclosure exceeds the capacity of at least one power supply.
  - **Resolution B:** Dynamic Power Supply Engagement cannot be fully supported with the power supply units present in the enclosure. To check if this is the case, use the Web interface to turn Dynamic Power Supply Engagement off, and then on again. A message is displayed if Dynamic Power Supply Engagement cannot be fully supported.

- **Problem:** Inserted a new server into the enclosure with sufficient power supplies, but the server does not power on.

  - **Resolution A:** Check the system input power cap setting - it might be configured too low to allow any additional servers to be powered up.
  - **Resolution B:** Check for 110V operation. If any power supplies are connected to 110V branch circuits, you must acknowledge this as a valid configuration before servers are allowed to power on. For more details, see the power configuration settings.
  - **Resolution C:** Check the maximum power conservation setting. If this is set then servers are allowed to power on. For more details, see the power configuration settings.
  - **Resolution D:** Check the server slot power priority of the slot associated with the newly inserted server, and ensure it is not lower than any other server slot power priority.

- **Problem:** Available power keeps changing, even when the modular enclosure configuration hasn't changed

  - **Resolution:** CMC 1.2 and higher versions have dynamic fan power management that reduces server allocations briefly if the enclosure is operating near the peak user configured power cap; it causes the fans to be allocated power by reducing server performance to keep the input power draw below **System Input Power Cap**. This is normal behavior.

- **Problem:** 2000 W is reported as the **Surplus for Peak Performance.**

  - **Resolution:** The enclosure has 2000 W of surplus power available in the current configuration, and the **System Input Power Cap** can be safely reduced by this amount being reported without impacting server performance.

- **Problem:** A subset of servers lost power after an AC Grid failure, even when the chassis was operating in the **AC Redundancy** configuration with six power supplies.

  - **Resolution:** This can occur if the power supplies are improperly connected to the redundant AC grids at the time the AC grid failure occurs. The **AC Redundancy** policy requires that the left three power supplies to be connected to one AC Grid, and right three power supplies to be connected to other AC Grid. If two PSU are improperly connected, such as PSU3 and PSU4 are connected to the wrong AC grids, an AC grid failure cause loss of power to the least priority servers.

- **Problem:** The least priority servers lost power after a PSU failure.
  - **Resolution:** This is expected behavior if the enclosure power policy was configured to **No Redundancy.** To avoid a future power supply failure causing servers to power off, ensure that the chassis has at least four power supplies and is configured for the **Power Supply Redundancy** policy to prevent PSU failure from impacting server operation.
- **Problem:** Overall server performance decreases when the ambient temperature increases in the data center.
  - **Resolution:** This can occur if the **System Input Power Cap** has been configured to a value that results in an increased power need by fans having to be made up by reduction in the power allocation to the servers. User can increase the **System Input Power Cap** to a higher value that allow for additional power allocation to the fans without an impact on server performance.

Troubleshooting Alerts

Use the CMC log and the trace log to troubleshoot CMC alerts. The success or failure of each e-mail and/or SNMP trap delivery attempt is logged into the CMC log. Additional information describing the particular error is logged in the trace log. However, since SNMP does not confirm delivery of traps, use a network analyzer or a tool such as Microsoft's snmputil to trace the packets on the managed system.

Related Links

Configuring CMC To Send Alerts

Viewing Event Logs

You can view hardware and CMC logs for information on system-critical events that occur on the managed system.

Related Links

Viewing Hardware Log
Viewing CMC Log

Viewing Hardware Log

CMC generates a hardware log of events that occur on the chassis. You can view the hardware log using the Web interface and remote RACADM.

NOTE: To clear the hardware log, you must have **Clear Logs Administrator** privilege.

NOTE: You can configure CMC to send e-mail or SNMP traps when specific events occur. For information on configuring CMC to send alerts, see Configuring CMC to Send Alerts.

Examples of hardware log entries

```
critical System Software event: redundancy lost
Wed May 09 15:26:28 2007 normal System Software
event: log cleared was asserted
Wed May 09 16:06:00 2007 warning System Software
event: predictive failure was asserted
Wed May 09 15:26:31 2007 critical System Software
event: log full was asserted
Wed May 09 15:47:23 2007 unknown System Software
event: unknown event
```

Related Links

Viewing Event Logs

Viewing Hardware Logs Using CMC Web Interface

You can view, save, and clear the hardware log. You can sort the log entries based on Severity, Date/Time, or Description by clicking the column heading. Subsequent clicks on the column headings reverse the sort.

To view the hardware logs using CMC Web interface, in the system tree, go to **Chassis Overview** and click **Logs** → **Hardware Log** . The **Hardware Log** page is displayed. To save a copy of the hardware log to your managed station or network, click **Save Log** and then specify a location for a text file of the log.

NOTE: Since the log is saved as a text file, the graphical images used to indicate severity in the user interface do not appear. In the text file, severity is indicated with the words OK, Informational, Unknown, Warning, and Severe. The date and time entries appear in ascending order. If <SYSTEM BOOT> appears in the **Date/Time** column, it means that the event occurred during shut down or start up of any of the modules, when no date or time is available.

To clear the hardware log, click **Clear Log.**

NOTE: CMC creates a new log entry indicating that the log was cleared.

Viewing Hardware Logs Using RACADM

To view the hardware log using RACADM, open a serial/Telnet/SSH text console to CMC, log in, and type:

```
racadm getsel
```

To clear the hardware log, type:

```
racadm clrsel
```

Viewing CMC Log

CMC generates a log of the chassis-related events.

NOTE: To clear the CMC log, you must have **Clear Logs Administrator** privilege.

Related Links

Viewing Event Logs

Viewing CMC Logs Using the Web Interface

You can view, save, and clear the CMC log. You can sort the log entries based on Source, Date/Time, or Description by clicking the column heading. Subsequent clicks on the column headings reverse the sort.

To view the CMC log using the CMC Web interface, in the system tree, go to **Chassis Overview** and click **Logs** → **CMC Log**. The **CMC Log** page is displayed.

To save a copy of the CMC log to your managed station or network, click **Save Log** and then specify a location save the log file.

Viewing CMC Logs Using RACADM

To view the CMC log information using RACADM, open a serial, Telnet, SSH text console to CMC, log in, and type:

```
racadm getraclog
```

To clear the hardware log, type:

```
racadm clrraclog
```

Using Diagnostic Console

You can diagnose issues related to the chassis hardware using CLI commands if you an advanced user or a user under the direction of technical support.

NOTE: To modify these settings, you must have **Debug Command Administrator** privilege.

To access the Diagnostic Console using the CMC Web interface:

1. In the system tree, go to **Chassis Overview** and click **Troubleshooting** → **Diagnostics**.

   The **Diagnostic Console** page displays.

2. In the **Command** text box, enter a command and click **Submit.** .

   For information about the commands, see the *CMC Online Help.*

   A diagnostic results page appears.

Resetting Components

You can reset the active CMC, or to virtually reseat servers causing them to behave as if they were removed and reinserted. If the chassis has a standby CMC, resetting the active CMC causes a failover and the standby CMC becomes active.

NOTE: To reset components, you must have **Debug Command Administrator** privilege.

To reset the components using the CMC Web interface,

1. In the system tree, go to **Chassis Overview,** and click **Troubleshooting** → **Reset Components.** .

   The **Reset Components** page is displayed.

2. To reset the active CMC, in the **CMC Status** section, click **Reset/Failover CMC**. If a standby CMC is present and a chassis is fully redundant, a failover occurs causing the standby CMC to become active.

3. To virtually reseat the server, in the **Virtual Reseat Server** section, select servers to reseat, and click **Apply Selections**.

   For more information, see the *CMC Online Help*.

   This operation causes the servers to behave as if they were removed and reinserted.

Saving or Restoring Chassis Configuration

To save or restore a backup of the Chassis configuration using the CMC Web interface:

1. In the system tree, go to **Chassis Overview**, and then click **Setup** → **Chassis Backup.** . The **Chassis Backup** page is displayed.

2. To save the chassis configuration, click **Save**. Override the default file path (optional) and click **OK** to save the file.

   NOTE: The default backup file name contains the Chassis' service tag. This backup file can be used later, to restore the settings and certificates for this chassis only.

3. To restore the chassis configuration, click **Choose File**, specify the backup file, and click **Restore**.

   NOTE: CMC does not reset upon restoring configuration, however CMC services may take some time to effectively impose any changed or new configuration. After successful completion, all current sessions are closed.

Troubleshooting Network Time Protocol (NTP) Errors

After configuring CMC to synchronize its clock with a remote time server over the network, it may take 2-3 minutes before a change in the date and time occurs. If after this time there is still no change, it may be necessary to troubleshoot a problem. CMC may not be able to synchronize its clock for the following reasons:

- Problem with the NTP Server 1, NTP Server 2, and NTP Server 3 settings.
- Invalid host name or IP address may have been accidentally entered.
- Network connectivity problem that prevents CMC from communicating with any of the configured NTP servers.
- DNS problem, preventing any of the NTP server host names from being resolved.

To troubleshoot these problems, check the information in the CMC Trace Log. This log contains an error message for NTP related failures. If CMC is not able to synchronize with any of the configured remote NTP servers, then CMC time is synchronized to the local system clock and the trace log contains an entry similar to the following:

```
Jan 8 20:02:40 cmc ntpd[1423]: synchronized to LOCAL(0), stratum 10
```

You can also check the ntpd status by typing the following racadm command:

```
racadm getractime –n
```

If the '*' is not displayed for one of the configured servers, the settings may not be configured correctly. The output of this command contains detailed NTP statistics that may be useful in debugging the problem.

If you attempt to configure a Windows-based NTP server, it may help to increase the `MaxDist` parameter for `ntpd`. Before changing this parameter, understand all the implications, since the default setting must be large enough to work with most NTP servers.

To modify the parameter, type the following command:

```
racadm config –g cfgRemoteHosts –o cfgRhostsNtpMaxDist 32
```

After making the change, disable NTP, wait for 5-10 seconds, then enable NTP again:

NOTE: NTP may take an additional three minutes to synchronize again.

To disable NTP, type:

```
racadm config –g cfgRemoteHosts –o cfgRhostsNtpEnable 0
```

To enable NTP, type:

```
racadm config –g cfgRemoteHosts –o cfgRhostsNtpEnable 1
```

If the NTP servers are configured correctly and this entry is present in the trace log, then this confirms that CMC is not able to synchronize with any of the configured NTP servers.

If the NTP server IP address is not configured, you may see a trace log entry similar to the following:

```
Jan 8 19:59:24 cmc ntpd[1423]: Cannot find existing interface for address
1.2.3.4 Jan 8 19:59:24 cmc ntpd[1423]: configuration of 1.2.3.4 failed
```

If an NTP server setting was configured with an invalid host name, you may see a trace log entry as follows:

```
Aug 21 14:34:27 cmc ntpd_initres[1298]: host name not found: blabla Aug 21
14:34:27 cmc ntpd_initres[1298]: couldn't resolve `blabla', giving up on it
```

For information on how to enter the `gettracelog` command to review the trace log using the CMC Web interface, see Using Diagnostic Console.

Interpreting LED Colors and Blinking Patterns

The LEDs on the chassis provide the component status as per the following:

- Steadily glowing, green LEDs indicate that the component is powered on. If the green LED is blinking, it indicates a critical but routine event, such as a firmware upload, during which the unit is not operational. It does not indicate a fault.
- A blinking amber LED on a module indicates a fault on that module.
- Blue, blinking LEDs are configurable by the user and used for identification (see Downloading SNMP Management Information Base (MIB) File).

Table 37. LED Color and Blinking Patterns

Component	LED Color, Blinking Pattern	Meaning
CMC	Green, glowing steadily	Powered on
	Green, blinking	Firmware is being uploaded
	Green, dark	Powered off
	Blue, glowing steadily	Active
	Blue, blinking	User-enabled module identifier
	Amber, glowing steadily	Not used
	Amber, blinking	Fault
	Blue, dark	Standby
iKVM	Green, glowing steadily	Powered on
	Green, blinking	Firmware is being uploaded
	Green, dark	Powered off
	Amber, glowing steadily	Not used
	Amber, blinking	Fault
	Amber, dark	No fault
Server	Green, glowing steadily	Powered on
	Green, blinking	Firmware is being uploaded
	Green, dark	Powered off
	Blue, glowing steadily	Normal
	Blue, blinking	User-enabled module identifier
	Amber, glowing steadily	Not used
	Amber, blinking	Fault
	Blue, dark	No fault
IOM (Common)	Green, glowing steadily	Powered on
	Green, blinking	Firmware is being uploaded

Component	LED Color, Blinking Pattern	Meaning
	Green, dark	Powered off
	Blue, glowing steadily	Normal/stack master
	Blue, blinking	User-enabled module identifier
	Amber, glowing steadily	Not used
	Amber, blinking	Fault
	Blue, dark	No fault/stack slave
IOM (Pass through)	Green, glowing steadily	Powered on
	Green, blinking	Not used
	Green, dark	Powered off
	Blue, glowing steadily	Normal
	Blue, blinking	User-enabled module identifier
	Amber, glowing steadily	Not used
	Amber, blinking	Fault
	Blue, dark	No fault
Fan	Green, glowing steadily	Fan working
	Green, blinking	Not used
	Green, dark	Powered off
	Amber, glowing steadily	Fan type not recognized, update CMC firmware
	Amber, blinking	Fan fault; tachometer out of range
	Amber, dark	Not used
PSU	(Oval) Green, glowing steadily	AC OK
	(Oval) Green, blinking	Not used
	(Oval) Green, dark	AC Not OK
	Amber, glowing steadily	Not used
	Amber, blinking	Fault
	Amber, dark	No fault
	(Circle) Green, glowing steadily	DC OK
	(Circle) Green, dark	DC Not OK

Troubleshooting Non-responsive CMC

If you cannot log in to CMC using any of the interfaces (the Web interface, Telnet, SSH, remote RACADM, or serial), you can verify the CMC functionality observing the LEDs on CMC, obtaining recovery information using the DB-9 serial port, or recovering the CMC firmware image.

NOTE: It is not possible to log in to the standby CMC using a serial console.

Observing LEDs to Isolate the Problem

Facing the front of CMC as it is installed in the chassis, there are two LEDs on the left side of the card:

- Top LED — The top green LED indicates power. If it is not on:
  - Verify that you have AC present to at least one power supply.
  - Verify that the CMC card is seated properly. You can release or pull the ejector handle, remove CMC, reinstall CMC making sure the board is inserted all the way and the latch closes correctly.
- Bottom LED — The bottom LED is multi-colored. When CMC is active and running, and there are no problems, the bottom LED is blue. If it is amber, a fault was detected. The fault may be caused by any of the following three events:
  - A core failure. In this case, the CMC board must be replaced.
  - A self-test failure. In this case, the CMC board must be replaced.
  - An image corruption. In this case, upload the CMC firmware image to recover the CMC.

  NOTE: A normal CMC boot or reset takes over a minute to fully boot into its operating system and be available for login. The blue LED is enabled on the active CMC. In a redundant, two-CMC configuration, only the top green LED is enabled on the standby CMC.

Obtain Recovery Information From DB-9 Serial Port

If the bottom LED is amber, recovery information is available from the DB-9 serial port located on the front of CMC.

To obtain recovery information:

1. Install a NULL modem cable between CMC and a client machine.
2. Open a terminal emulator of your choice (such as HyperTerminal or Minicom). Set up: 8 bits, no parity, no flow control, baud rate 115200.

   A core memory failure displays an error message every 5 seconds.
3. Press <Enter>.

   If a recovery prompt appears, additional information is available. The prompt indicates the CMC slot number and failure type.

   To display failure reason and syntax for a few commands, type `recover` and then press <Enter>.

   Sample prompts:

   ```
   recover1[self test] CMC 1 self test failure
   ```

   ```
   recover2[Bad FW images] CMC2 has corrupted images
   ```

   - If the prompt indicates a self test failure, there are no serviceable components on CMC. CMC is bad and must be returned to Dell.
   - If the prompt indicates **Bad FW Images**, then follow the steps in Recovering Firmware Image to fix the problem.

Recovering Firmware Image

CMC enters recover mode when a normal CMC operating boot is not possible. In recover mode, a small subset of commands are available that allow you to reprogram the flash devices by uploading the firmware update file,

firmimg.cmc. This is the same firmware image file used for normal firmware updates. The recovery process displays its current activity and boots to the CMC OS upon completion.

When you type recover and then press <Enter> at the recovery prompt, the recover reason and available sub-commands display. An example recover sequence may be:

```
recover getniccfg
recover setniccfg 192.168.0.120 255.255.255.0
192.168.0.1
recover ping 192.168.0.100
recover fwupdate -g -a 192.168.0.100
```

NOTE: Connect the network cable to the left most RJ45.

NOTE: In recover mode, you cannot ping CMC normally because there is no active network stack. The `recover ping <TFTP server IP>` command allows you to ping to the TFTP server to verify the LAN connection. You may need to use the `recover reset` command after `setniccfg` on some systems.

Troubleshooting Network Problems

The internal CMC trace log allows you to debug CMC alerts and networking. You can access the trace log using the CMC Web interface or RACADM. See the `gettracelog` command section in the *RACADM Command Line Reference Guide for iDRAC7 and CMC*.

The trace log tracks the following information:

- DHCP — Traces packets sent to and received from a DHCP server.
- DDNS — Traces dynamic DNS update requests and responses.
- Configuration changes to the network interfaces.

The trace log may also contain CMC firmware-specific error codes that are related to the internal CMC firmware, not the managed system's operating system.

Resetting Administrator Password

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

To perform management actions, a user with **Administrator** privileges is required. The CMC software has a user account password protection security feature that may be disabled if the administrator account password is forgotten. If the administrator account password is forgotten, it can be recovered using the PASSWORD_RSET jumper on the CMC board.

The CMC board has a two-pin password reset connector as shown in the following figure. If a jumper is installed in the reset connector, the default administrator account and password is enabled and set to the default values of `username: root` and `password: calvin`. The administrator account is reset regardless if the account has been removed, or if the password was changed.

NOTE: Make sure the CMC module is in a passive state before you begin.

To perform management actions, a user with **Administrator** privileges is required. If the administrator account password is forgotten, it can be reset using the PASSWORD_RST jumper on the CMC board.

The PASSWORD_RST jumper uses a two-pin connector as shown in the following figure.

While the PASSWORD_RST jumper is installed, the default administrator account and password is enabled and set to the following default values:

```
username: root
password: calvin
```

The administrator account is temporarily reset regardless if the administrator account was removed, or if the password was changed.

NOTE: When the PASSWORD_RST jumper is installed, a default serial console configuration is used (rather than configuration property values), as follows:

```
cfgSerialBaudRate=115200
cfgSerialConsoleEnable=1
cfgSerialConsoleQuitKey=^\
cfgSerialConsoleIdleTimeout=0
cfgSerialConsoleNoAuth=0
cfgSerialConsoleCommand=""
cfgSerialConsoleColumns=0
```

1. Press the CMC release latch on the handle and move the handle away from the module front panel. Slide the CMC module out of the enclosure.

   NOTE: Electrostatic discharge (ESD) events can damage CMC. Under certain conditions, ESD may build up on your body or an object, and then discharge into your CMC. To prevent ESD damage, you must take precautions to discharge static electricity from your body while handling and accessing CMC outside the Chassis.

2. Remove the jumper plug from the password reset connector, and insert a 2-pin jumper to enable the default administrator account. To locate the password jumper on the CMC board, see the following figure.

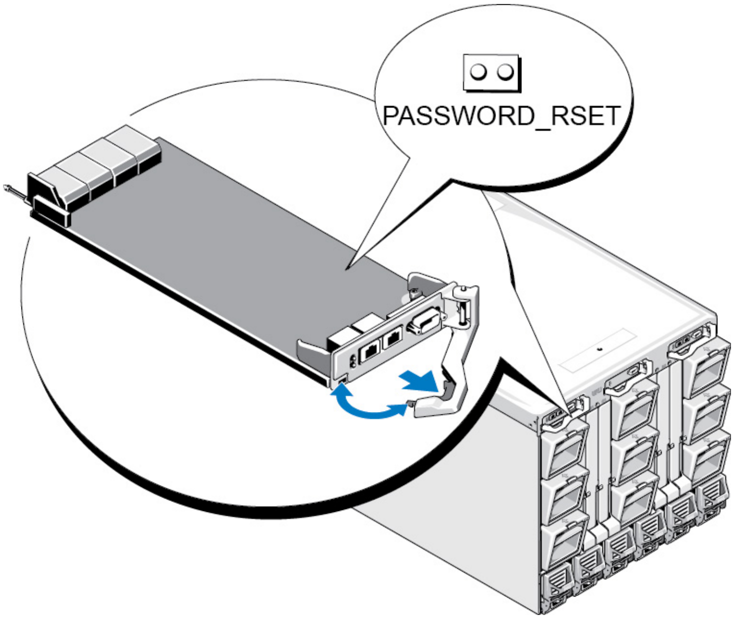
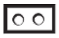
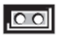


Figure 7. Password Reset Jumper Location

Table 38. CMC Password Jumper Settings

PASSWORD_RSET		(default)	The password reset feature is disabled.
			The password reset feature is enabled.

3. Slide the CMC module into the enclosure. Reattach any cables that were disconnected.

   NOTE: Make sure that the CMC module becomes the active CMC, and remains the active CMC until the remaining steps are completed.

4. If the jumpered CMC module is the only CMC, then wait for it to finish rebooting. If there is a redundant CMCs in the chassis, then initiate a changeover to make the jumpered CMC module active. In the Web interface, in the system tree, go to **Chassis Overview** and click **Power** → **Control**, select the **Reset CMC (warm boot)**, and click **Apply**.

   CMC automatically fails over to the redundant module, and that module now becomes active.

5. Log into the active CMC using the default administrator username:root and password: calvin, and restore any necessary user account settings. The existing accounts and passwords are not disabled and are still active.
6. Perform the required management actions, including creating a new administrator password.
7. Remove the 2-pin PASSWORD_RST jumper and replace the jumper plug.
   a) Press in the CMC release latch on the handle and move the handle away from the module front panel. Slide the CMC module out of the enclosure.
   b) Remove the 2-pin jumper and replace the jumper plug.
   c) Slide the CMC module into the enclosure. Reattach any cables that were disconnected. Repeat step 4 to make the unjumpered CMC module the active CMC.

17

Using LCD Panel Interface

You can use the LCD panel on the chassis to perform configuration and diagnostics, and to obtain status information about the chassis and its contents.

The following figure illustrates the LCD panel. The LCD screen displays menus, icons, pictures, and messages.

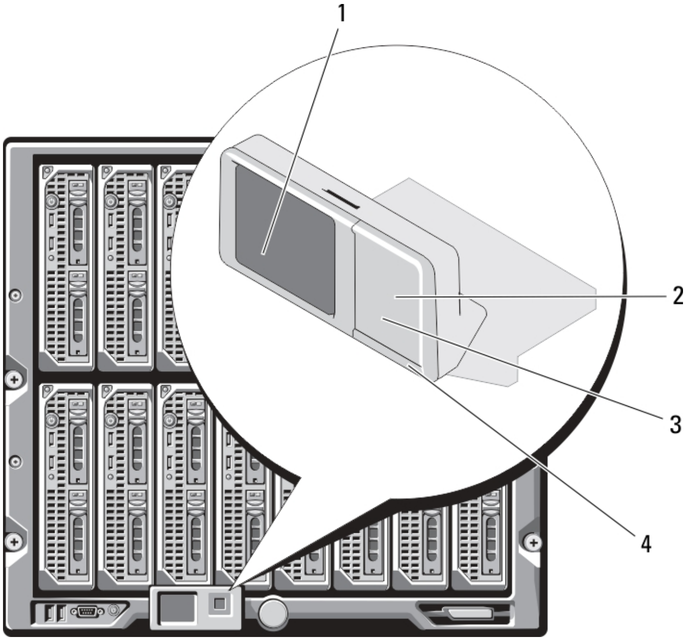


Figure 8. LCD Display

1	LCD screen	2	selection ("check") button
3	scroll buttons (4)	4	status indicator LED

Related Links

- LCD Navigation
- Diagnostics
- LCD Hardware Troubleshooting
- Front Panel LCD Messages
- LCD Error Messages
- LCD Module and Server Status Information

LCD Navigation

The right side of the LCD panel contains five buttons: four arrow buttons (up, down, left, and right) and a center button.

- *To move between screens, use the right (next) and left (previous) arrow buttons. At any time while using the panel, you can return to a previous screen.*

- *To scroll through options on a screen, use the down and up arrow buttons.*
- *To select and save an item on a screen and move to the next screen, use the center button.*

The up, down, left, and right arrow buttons change the selected menu items or icons on the screen. The selected item is shown with a light blue background or border.

When messages displayed on the LCD screen are longer than what fits on the screen, use the left and right arrow buttons to scroll the text left and right.

The icons described in the following table are used to navigate between LCD screens.

Table 39. LCD Panel Navigational Icons

Icon Normal	Icon Highlighted	Icon Name and Description
◀	◀	**Back** — Highlight and press the center button to return to the previous screen.
✓	✓	**Accept/Yes** — Highlight and press the center button to accept a change and return to the previous screen.
▶	▶	**Skip/Next** — Highlight and press the center button to skip any changes and go to the next screen.
✗		**No** — Highlight and press the center button to answer "No" to a question and go to the next screen.
⟳ ⟳	⟳	**Rotate** — Highlight and press the center button to switch between the front and rear graphical views of the chassis. **NOTE:** The amber background indicates that the opposite view has errors.
ℹ	ℹ	**Component Identify** — Blinks the blue LED on a component. **NOTE:** There is a blinking blue rectangle around this icon when Component Identify is enabled.

A status indicator LED on the LCD panel provides an indication of the overall health of the chassis and its components.

- Solid blue indicates good health.
- Blinking amber indicates that at least one component has a fault condition.
- Blinking blue is an ID signal, used to identify one chassis in a group of chassis.

Related Links

Main Menu
LCD Setup Menu
Language Setup Screen
Default Screen

Graphical Server Status Screen
Graphical Module Status Screen
Enclosure Menu Screen
Module Status Screen
Enclosure Status Screen
IP Summary Screen

Main Menu

From the **Main** menu, you can navigate to one of the following screens:

- **LCD Setup Menu** — select the language to use and the LCD screen that displays when no one is using the LCD.
- **Server** — displays status information for servers.
- **Enclosure** — displays status information for the chassis.

Use the up and down arrow buttons to highlight an item.

Press the center button to activate your selection.

LCD Setup Menu

The **LCD Setup** menu displays a menu of items that can be configured:

- **Language Setup** — choose the language you want to use for LCD screen text and messages.
- **Default Screen** — choose the screen that displays when there is no activity on the LCD panel.

Use the up and down arrow buttons to highlight an item in the menu or highlight the **Back** icon if you want to return to the **Main** menu.

Press the center button to activate your selection.

Language Setup Screen

The **Language Setup** screen allows you to select the language used for LCD panel messages. The currently active language is highlighted with a light blue background.

1. Use the up, down, left, and right arrow buttons to highlight the desired language.
2. Press the center button. The **Accept** icon appears and is highlighted.
3. Press the center button to confirm the change. The **LCD Setup** menu is displayed.

Default Screen

The **Default Screen** allows you to change the screen that the LCD panel displays when there is no activity at the panel. The factory default screen is the **Main Menu.** You can choose from the following screens to display:

- **Main Menu**
- **Server Status** (front graphical view of the chassis)
- **Module Status** (rear graphical view of the chassis)
- **Custom** (Dell logo with chassis name)

The currently active default screen is highlighted in light blue.

1. Use the up and down arrow buttons to highlight the screen you want to set to the default.
2. Press the center button. The **Accept** icon is highlighted.
3. Press the center button again to confirm the change. The **Default Screen** is displayed.

Graphical Server Status Screen

The **Graphical Server Status** screen displays icons for each server installed in the chassis and indicates the general health status for each server. The server health is indicated by the color of the server icon:

- Gray — server is off with no errors
- Green — server is on with no errors
- Yellow — server has one or more non-critical errors
- Red — server has one or more critical errors
- Black — server is not present

A blinking light blue rectangle around a server icon indicates that the server is highlighted.

To view the **Graphical Module Status** screen, highlight the rotate icon, and press the center button.

To view the status screen for a server, use the arrow buttons to highlight the desired server, and press the center button. The **Server Status** screen displays.

To return to the Main Menu, use the arrow buttons to highlight the **Back** icon, and press the center button.

Graphical Module Status Screen

The **Graphical Module Status** screen displays all modules installed in the rear of the chassis and provides summary health information for each module. Module health is indicated by the color of each module icon as follows:

- Gray — module is off or on standby with no errors
- Green — module is on with no errors
- Yellow — module has one or more non-critical errors
- Red — server has one or more critical errors
- Black — module is not present

A blinking light blue rectangle around a module icon indicates that the module is highlighted.

To view the **Graphical Server Status** screen, highlight the rotate icon, and press the center button.

To view the status screen for a module, use the up, down, left, and right arrow buttons to highlight the desired module, and press the center button. The **Module Status** screen displays.

To return to the **Main Menu,** use the arrow buttons to highlight the Back icon, press the center button. The **Main Menu** displays.

Enclosure Menu Screen

From this screen, you can navigate to the following screens:

- **Module Status screen**
- **Enclosure Status screen**
- **IP Summary screen**
- **Main Menu**

Use the navigation buttons to highlight the desired item (highlight the **Back** icon to return to the **Main Menu**) and press the center button. The selected screen displays.

Module Status Screen

The **Module Status** screen displays information and error messages about a module. For messages that can appear on this screen, see LCD Module and Server Status Information and LCD Error Messages.

Use the up and down arrow keys to move through messages. Use the left and right arrow keys to scroll messages that do not fit on the screen.

Highlight the **Back** icon and press the center button to return to the **Graphical Module Status** screen.

Enclosure Status Screen

The **Enclosure Status** screen displays information and error messages about the enclosure. For messages that can appear on this screen, see LCD Error Messages. Use the up and down arrow keys to move through messages.

Use the left and right arrow keys to scroll messages that do not fit on the screen.

Highlight the **Back** icon and press the center button to return to the **Enclosure Status** screen.

IP Summary Screen

The **IP Summary** screen shows IP information for CMC and iDRAC of each installed server.

Use the up and down arrow buttons to scroll through the list. Use the left and right arrow buttons to scroll selected messages that are longer than the screen.

Use the up and down arrow buttons to select the **Back** icon and press the center button to return to the **Enclosure** menu.

Diagnostics

The LCD panel helps you to diagnose problems with any server or module in the chassis. If there is a problem or fault with the chassis or any server or other module in the chassis, the LCD panel status indicator blinks amber. On the Main Menu an icon with an amber background displays next to the menu item—Server or Enclosure—that leads to the faulty server or module.

By following the amber icons through the LCD menu system, you can display the status screen and error messages for the item that has the problem.

Error messages on the LCD panel can be removed by removing the module or server that is the cause of the problem or by clearing the hardware log for the module or server. For server errors, use the iDRAC Web interface or command line interface to clear the server's System Event Log (SEL). For chassis errors, use the CMC Web interface or command line interface to clear the hardware log.

LCD Hardware Troubleshooting

If you are experiencing issues with the LCD in relation to your use of CMC, use the following hardware troubleshooting items to determine if there is an LCD hardware or connection issue.

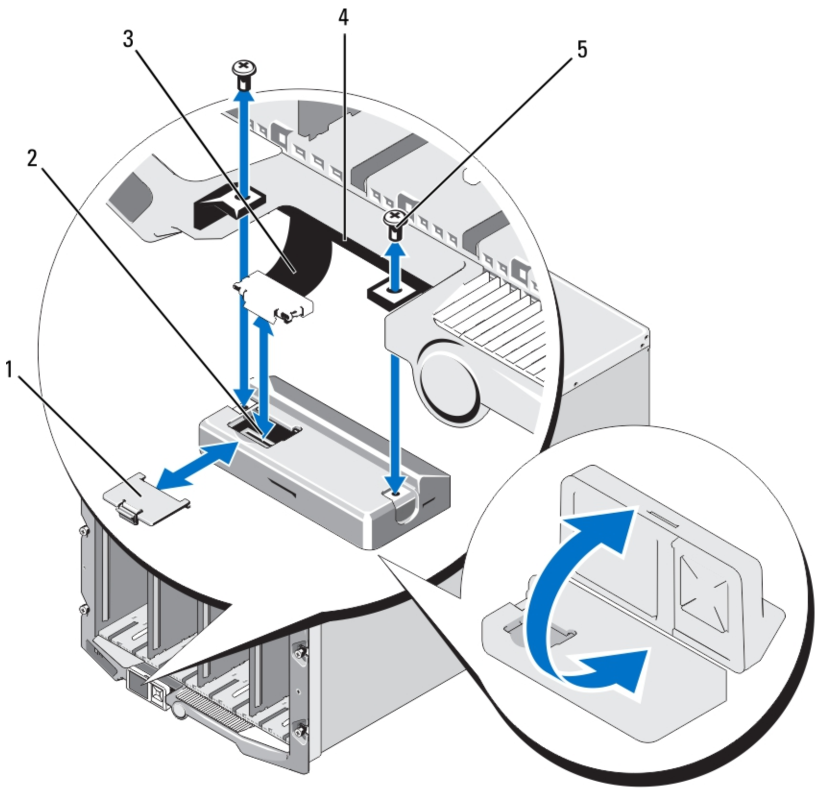


Figure 9. Removing and Installing LCD Module

1	cable cover	2	LCD module
3	ribbon cable	4	hinges (2)
5	screws (2)		

Table 40. LCD Hardware Troubleshooting Items

Symptom	Issue	Recovery Action
Alert screen message `CMC Not Responding` and LED is blinking amber.	Loss of communication from CMC to the LCD front panel.	Check that CMC is booting; then, reset CMC using GUI or RACADM commands.
Alert screen message `CMC Not Responding` and LED is solid amber or is off.	LCD module communications is stuck during a CMC fail-over or reboots.	Review the hardware log using the GUI or RACADM commands. Look for a message that states: `Can not communicate with LCD controller.` Reseat the LCD module ribbon cable.
Screen text is scrambled.	Defective LCD screen.	Replace the LCD module.
LED and LCD is off.	The LCD cable is not connected properly or is faulty; or the LCD module is faulty.	Review the hardware log using the GUI or RACADM commands. Look for a message that states: • `The LCD module cable is not connected, or is improperly connected.`

		• `The control panel cable is not connected, or is improperly connected.` Reseat cables.
LCD screen message `No CMC Found.`	No CMC is present in the chassis.	Insert a CMC into the chassis or reseat existing CMC if present.

Front Panel LCD Messages

This section contains two subsections that list error and status information that is displayed on the front panel LCD.

Error messages on the LCD have a format that is similar to the System Event Log (SEL) viewed from the CLI or Web interface.

The tables in the error section list the error and warning messages that are displayed on the various LCD screens and the possible cause of the message. Text enclosed in angled brackets (< >) indicates that the text may vary.

Status information on the LCD includes descriptive information about the modules in the chassis. The tables in this section describe the information that is displayed for each component.

LCD Error Messages

Table 41. CMC Status Screens

Severity	Message	Cause
Critical	The CMC <number> battery failed.	CMC CMOS battery is missing or has no voltage.
Critical	CMC <number> LAN heartbeat was lost.	The CMC NIC connection has been removed or is not connected.
Warning	A firmware or software incompatibility detected between iDRAC in slot <number> and CMC.	Firmware between the two devices does not match in order to support one or more features.
Warning	A firmware or software incompatibility detected between system BIOS in slot <number> and CMC.	Firmware between the two devices does not match in order to support one or more features.
Warning	A firmware or software incompatibility detected between CMC 1 and CMC 2.	Firmware between the two devices does not match in order to support one or more features.

Table 42. Enclosure/Chassis Status Screen

Severity	Message	Cause
Critical	Fan <number> is removed.	This fan is required for proper cooling of the enclosure/chassis.
Warning	Power supply redundancy is degraded.	One or more PSU have failed or removed and the system can no longer support full PSU redundancy.
Critical	Power supply redundancy is lost.	One or more PSU have failed or removed and the system is no longer redundant.

Critical	The power supplies are not redundant. Insufficient resources to maintain normal operations.	One or more PSU have failed or removed and the system lacks sufficient power to maintain normal operations. This could cause servers to power down.
Warning	The control panel ambient temperature is greater than the upper warning threshold.	Chassis/Enclosure intake temperature exceeded the warning threshold.
Critical	The control panel ambient temperature is greater than the upper warning threshold.	Chassis/Enclosure intake temperature exceeded the warning threshold.
Critical	CMC redundancy is lost.	CMC no longer redundant. This happens if the standby CMC is removed.
Critical	All event logging is disabled.	The Chassis/Enclosure cannot store events to the logs. This usually indicates a problem with the control panel or control panel cable.
Warning	Log is full.	Chassis has detected that only one more entry can be added to the CEL (hardware log) before it is full.
Warning	Log is almost full.	Chassis event log is 75% full.

Table 43. Fan Status Screens

Severity	Message	Cause
Critical	Fan <number> RPM is operating less than the lower critical threshold.	The speed of the specified fan is not sufficient to provide enough cooling to the system.
Critical	Fan <number> RPM is operating greater than the upper critical threshold.	The speed of the specified fan is too high, usually due to a broken fan blade.

Table 44. IOM Status Screens

Severity	Message	Cause
Warning	A fabric mismatch detected on I/O module <number>.	The IO module fabric does not match that of the server or the redundant I/O module.
Warning	A link tuning failure detected on I/O module <number>.	The IO module could not be set to correctly use the NIC on one or more servers.
Critical	A failure is detected on I/O module <number>.	The I/O module has a fault. The same error can also happen if the I/O module is thermal-tripped.

Table 45. iKVM Status Screen

Severity	Message	Cause
Warning	Console is not available for Local KVM.	Minor failure, such as corrupted firmware.
Critical	Local KVM can not detect any hosts.	USB host enumeration failure.
Critical	OSCAR, on screen display is not functional for the Local KVM.	OSCAR failure.
Non-Recoverable	Local KVM is not functional, and is powered off.	Serial RIP failure or USB host chip failure.

Table 46. PSU Status Screens

Severity	Message	Cause
Critical	Power supply <number> failed.	The PSU has failed.
Critical	The power input for power supply <number> is lost.	Loss of AC power or AC cord unplugged.
Warning	Power supply <number> is operating at 110 volts, and could cause a circuit breaker fault.	Power supply is plug into a 110 volt source.

Table 47. Server Status Screen

Severity	Message	Cause
Warning	The system board ambient temperature is less than the lower warning threshold.	Server temperature is getting cool.
Critical	The system board ambient temperature is less than the lower critical threshold.	Server temperature is getting cold.
Warning	The system board ambient temperature is greater than the upper warning threshold.	Server temperature is getting warm.
Critical	The system board ambient temperature is greater than the upper critical threshold.	Server temperature is getting too hot.
Critical	The system board Current Latch current is outside of the allowable range	Current crossed a failing threshold.
Critical	The system board battery failed.	CMOS battery is not present or has no voltage.
Warning	The storage battery is low.	ROMB battery is low.
Critical	The storage battery failed.	CMOS battery is not present or has no voltage.
Critical	The CPU <number> <voltage sensor name > voltage is outside of the allowable range.	
Critical	The system board<voltage sensor name > voltage is outside of the allowable range.	
Critical	The mezzanine card <number> <voltage sensor name > voltage is outside of the allowable range.	
Critical	The storage <voltage sensor name > voltage is outside of the allowable range.	
Critical	CPU <number> has an internal error (IERR).	CPU failure.
Critical	CPU <number> has a thermal trip (over-temperature) event.	CPU overheated.
Critica	CPU <number> configuration is unsupported.	Incorrect processor type or in wrong location.
Critical	CPU <number> is absent.	Required CPU is missing or not present.
Critical	Mezz B<slot number> Status: Add-in Card sensor for Mezz B<slot number>, install error was asserted.	Incorrect Mezzanine card installed for IO fabric.

Critical	Mezz C<slot number> Status: Add-in Card sensor for Mezz C<slot number>, install error was asserted.	Incorrect Mezzanine card installed for IO fabric.
Critical	Drive <number> is removed.	Storage Drive was removed.
Critical	Fault detected on Drive <number>.	Storage Drive failed.
Critical	The system board fail-safe voltage is outside of the allowable range.	This event is generated when the system board voltages are not at normal levels.
Critical	The watchdog timer expired.	The iDRAC watchdog timer expires and no action is set.
Critical	The watchdog timer reset the system.	The iDRAC watchdog detected that the system has crashed (timer expired because no response was received from Host) and the action is set to reboot.
Critical	The watchdog timer powered off the system.	The iDRAC watchdog detected that the system has crashed (timer expired because no response was received from Host) and the action is set to power off.
Critical	The watchdog timer power cycled the system.	The iDRAC watchdog detected that the system has crashed (timer expired because no response was received from Host) and the action is set to power cycle.
Critical	Log is full.	The SEL device detects that only one entry can be added to the SEL before it is full.
Warning	Persistent correctable memory errors detected on a memory device at location <location>.	
Warning	Persistent correctable memory error rate has increased for a memory device at location <location>.	Correctable ECC errors reach a critical rate.
Critical	Multi-bit memory errors detected on a memory device at location <location>.	An uncorrectable ECC error was detected.
Critical	An I/O channel check NMI was detected on a component at bus <number> device <number> function <number>.	A critical interrupt is generated in the I/O Channel.
Critical	An I/O channel check NMI wa detected on a component at slot <number>.	A critical interrupt is generated in the I/O Channel.
Critical	A PCI parity error was detected on a component at bus <number> device <number> function <number>.	Parity error was detected on the PCI bus.
Critical	A PCI parity error was detected on a component at slot <number>.	Parity error was detected on the PCI bus.
Critical	A PCI system error was detected on a component at bus <number> device <number> function <number>.	PCI error detected by device.

Critical	A PCI system error was detected on a component at slot <number>.	PCI error detected by device.
Critical	Persistent correctable memory error logging disabled for a memory device at location <location>.	Single bit error logging is disable when too many SBE get logged for a memory device.
Critical	All event logging is disabled.	
Non-Recoverable	CPU protocol error detected.	The processor protocol entered a non-recoverable state.
Non-Recoverable	CPU bus parity error detected.	The processor bus PERR entered a non-recoverable state.
Non-Recoverable	CPU initialization error detected.	The processor initialization entered a non-recoverable state.
Non-Recoverable	CPU machine check detected.	The processor machine check entered a non-recoverable state.
Critical	Memory redundancy is lost.	
Critical	A bus fatal error was detected on a component at bus <number> device <number> function <number>.	Fatal error is detected on the PCIe bus.
Critical	A software NMI was detected on a component at bus <number> device <number> function <number>.	Chip error is detected.
Critical	Failed to program virtual MAC address on a component at bus <number> device <number> function <number>.	Flex address could be programmed for this device.
Critical	Device option ROM on mezzanine card <number> failed to support Link Tuning or FlexAddress.	Option ROM does not support Flex address or linking tuning.
Critical	Failed to get Link Tuning or FlexAddress data from iDRAC.	

NOTE: For information on other server related LCD messages, see "Server User Guide".

LCD Module and Server Status Information

The tables in this section describe status items that are displayed on the front panel LCD for each type of component in the chassis.

Table 48. CMC Status

Item	Description
Example: CMC1, CMC2	Name/Location.
No Errors	If no error occurs then “No Errors” is displayed, else lists error messages.
Firmware Version	Only displays on an active CMC. Displays Standby for the standby CMC.
IP4 <enabled, disabled>	Displays current IPv4 enabled state only on an active CMC.
IP4 Address: <address, acquiring>	Only displays if IPv4 is enabled only on an active CMC.
IP6 <enabled, disabled>	Displays current IPv6 enabled state only on an active CMC.
IP6 Local Address: <address>	Only displays if IPv6 is enabled only on an active CMC.
IP6 Global Address: <address>	Only displays if IPv6 is enabled only on an active CMC.

Table 49. Chassis/Enclosure Status

Item	Description
User Define Name	Example: “Dell Rack System”. This is settable via CMC CLI or Web GUI.
Error Messages	If no errors occur then No Errors is displayed; otherwise error messages are listed, critical errors first, then warnings.
Model Number	Example "PowerEdgeM1000".
Power Consumption	Current power consumption in watts.
Peak Power	Peak power consumed in watts.
Minimum Power	Minimum power consumed in watts.
Ambient Temperature	Current ambient temperature in degrees Celsius.
Service Tag	The factory-assigned service tag.
CMC redundancy mode	Non-Redundant or Redundant.
PSU redundancy mode	Non-Redundant, AC Redundant, or DC Redundant.

Table 50. Fan Status

Item	Description
Name/Location	Example: Fan1, Fan2, etc.
Error Messages	If no error then "No Errors" is shown; otherwise error messages are listed, critical errors first, then warnings.
RPM	Current fan speed in RPM.

Table 51. PSU Status

Item	Description
Name/Location	Example: PSU1, PSU2, etc.
Error Messages	If no error then "No Errors" is shown; otherwise error messages are listed, critical errors first, then warnings.
Status	Offline, Online, or Standby.
Maximum Wattage	Maximum Wattage that PSU can supply to the system.

Table 52. IOM Status

Item	Description
Name/Location	Example: IOM A1, IOM B1. etc.
Error Messages	If no error then "No Errors" is shown; otherwise error messages are listed, critical errors first, then warnings.
Status	Off or On.
Model	Model of the IOM.
Fabric Type	Networking type.
IP address	Only shows if IOM is On. This value is zero for a pass through type IOM.
Service Tag	The factory-assigned service tag.

Table 53. iKVM Status

Item	Description
Name	iKVM.
No Error	If there are no errors, then No Errors is displayed; otherwise error messages are listed. The critical errors are listed first, and then the warnings. For more information see "LCD Error Messages".
Status	Off or On.
Model/Manufacture	A description of the iKVM model.
Service Tag	The factory-assigned service tag.
Part Number	The Manufacturer part number.
Firmware Version	iKVM firmware version.
Hardware Version	iKVM hardware version.

NOTE: This information is dynamically updated

Table 54. Server Status

Item	Description
Example: Server 1, Server 2, etc.	Name/Location.
No Errors	If there are no errors, then No Errors is displayed; otherwise error messages are listed. The critical errors are listed first, and then the warnings. For more information, see "LCD Error Messages".
Slot Name	Chassis slot name. For example, SLOT-01. **NOTE:** You can set this table through the CMC CLI or Web GUI.
Name	Name of the server, which the user can set through Dell OpenManage. The name is displayed only if iDRAC has finished booting, and the server supports this feature, else iDRAC booting messages are displayed.
Model Number	Displays if iDRAC finished booting.
Service Tag	Displays if iDRAC finished booting.
BIOS Version	Server BIOS firmware version.
Last POST Code	Displays the last server BIOS POST code messages string.
iDRAC Firmware Version	Displays if iDRAC finished booting. **NOTE:** iDRAC version 1.01 is displayed as 1.1. There is no iDRAC version 1.10.
IP4 <enabled, disabled>	Displays the current IPv4 enabled state.
IP4 Address: <address, acquiring>	Only displays if IPv4 is enabled.
IP6 <enabled, disabled>	Only displays if iDRAC supports IPv6. Displays current IPv6-enabled state.
IP6 Local Address: <address>	Only displays if iDRAC supports IPv6 and IPv6 is enabled.
IP6 Global Address: <address>	Only displays if iDRAC supports IPv6 and IPv6 is enabled.
FlexAddress enabled on Fabrics	Only displays if the feature is installed. Lists the fabrics enabled for this server (that is, A, B, C).

The information in Table 17-16 is dynamically updated. If the server does not support this feature, then the following information does not appear, else Server Administrator options are as follows:

- Option “None” = No strings must be displayed on the LCD.
- Option “Default” = No Effect.
- Option “Custom” = Allows you to enter a string name for the server.

The information is displayed only if iDRAC has completed booting. For more information on this feature, see the *RACADM Command Line Reference Guide for iDRAC7 and CMC*.

18

Frequently Asked Questions

This section lists the frequently asked questions for the following:

- RACADM
- Managing and Recovering a Remote System
- Active Directory
- FlexAddress and FlexAddressPlus
- iKVM
- IOM

RACADM

After performing a CMC reset (using the RACADM racreset subcommand), when a command is entered, the following message is displayed:

```
racadm <subcommand> Transport: ERROR: (RC=-1)
```

What does this message mean?

Another command must be issued only after CMC completes the reset.

Using the RACADM subcommands sometimes displays one or more of the following errors:

- Local error messages — Problems such as syntax, typographical errors, and incorrect names.
  Example:`ERROR: <message>`

Use the RACADM help subcommand to display correct syntax and usage information.

CMC-related error messages — Problems where the CMC is unable to perform an action. Also might say "racadm command failed."

Type `racadm gettracelog` for debugging information.

While using remote RACADM, the prompt changes to a ">" and the "$" prompt is not displayed again.

If a non-matched double quotation mark (") or a non-matched single quotation (') is used in the command, the CLI changes to the ">" prompt and queue all commands.

To return to the $ prompt, type <Ctrl>–d.

An error message "Not Found" is displayed, while using the `$ logout` and `$ quit` commands.

The logout and quit commands are not supported in the CMC RACADM interface.

Managing and Recovering a Remote System

When accessing the CMC Web interface, a security warning stating that the host name of the SSL certificate does not match the host name of CMC is displayed.

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

To address this security concern, upload a CMC server certificate issued to the IP address of CMC. 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 of CMC (for example, 192.168.0.120) or the registered DNS CMC name.

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

1. In the System tree, click **Chassis Overview.**
2. Click the **Network** tab, and then click **Network.**

   The Network Configuration page appears.
3. Select the **Register CMC** on **DNS** option.
4. Enter the CMC name in the **DNS CMC Name** field.
5. Click **Apply** Changes.

   For more information about generating CSRs and issuing certificates, see Obtaining Certificates.

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

   It may take a minute for the remote RACADM services and the Web interface to become available after the CMC Web server resets.

   The CMC Web server is reset after the following occurrences:

   - Changing the network configuration or network security properties using the CMC Web user interface.
   - The cfgRacTuneHttpsPort property is changed (including when a config -f <config file> changes it).
   - `racresetcfg` is used or a chassis configuration backup is restored.
   - CMC is reset.
   - A new SSL server certificate is uploaded.

   Why doesn't my DNS server register my CMC?

   Some DNS servers only register names with a maximum of 31 characters.

   When accessing the CMC Web interface, a security warning stating that the SSL certificate was issued by a certificate authority that is not trusted is displayed.

   CMC includes a default CMC server certificate to ensure network security for the Web interface and remote RACADM features. This certificate is not issued by a trusted certificate authority. To address this security concern, upload a CMC server certificate issued by a trusted certificate authority (such as Thawte or Verisign). For more information about certificates, see Obtaining Certificates.

   Why is the following message displayed for unknown reasons?

   `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, the **get community name = public** and the **set community name = private.** By default, the community name for the CMC agent is public. When IT Assistant sends out a set request, the CMC agent generates the SNMP authentication error because it only accepts requests from **community = public.**

   Change the CMC community name using RACADM. To see the CMC community name, use the following command:

   ```
   racadm getconfig -g cfgOobSnmp
   ```

   To set the CMC community name, use the following command:

   ```
   racadm config -g cfgOobSnmp -o cfgOobSnmpAgentCommunity <community name>
   ```

   To prevent SNMP authentication traps from being generated, enter input community names that are accepted by the agent. Since CMC only allows one community name, enter the same get and set community name for IT Assistant discovery setup.

Enter an example that illustrates the current task (optional).

Enter the tasks the user should do after finishing this task (optional).

Active Directory

Does Active Directory support CMC login across multiple trees?

Yes. The CMC's Active Directory querying algorithm supports multiple trees in a single forest.

Does the login to CMC using Active Directory work in mixed mode (that is, the domain controllers in the forest run different operating systems, such as Microsoft Windows 2000 or Windows Server 2003)?

Yes. In mixed mode, all objects used by the CMC querying process (among user, RAC Device Object, and Association Object) must be in the same domain.

The Dell-extended Active Directory Users and Computers Snap-In checks the mode and limits users in order to create objects across domains if in mixed mode.

Does using CMC with Active Directory support multiple domain environments?

Yes. The domain forest function level must be in Native mode or Windows 2003 mode. In addition, the groups among Association Object, RAC user objects, and RAC Device Objects (including Association Object) must be universal groups.

Can these Dell-extended objects (Dell Association Object, Dell RAC Device, and Dell Privilege Object) be in different domains?

The Association Object and the Privilege Object must be in the same domain. The Dell-extended Active Directory Users and Computers Snap-In allows to create these two objects in the same domain only. Other objects can be in different domains.

Are there any restrictions on Domain Controller SSL configuration?

Yes. All SSL certificates for Active Directory servers in the forest must be signed by the same root certificate authority-signed certificate, because CMC only allows upload of one trusted certificate authority-signed SSL certificate.

The Web interface does not launch after a new RAC certificate is created and uploaded.

If Microsoft Certificate Services is used to generate the RAC certificate, the User Certificate option may have been used instead of Web Certificate when creating the certificate.

To recover, generate a CSR, create a new Web certificate from Microsoft Certificate Services, and upload it using the following RACADM commands:

```
racadm sslcsrgen [-g] [-f {filename}]
```

```
racadm sslcertupload -t 1 -f {web_sslcert}
```

FlexAddress and FlexAddressPlus

What happens if a feature card is removed?

There is no visible change is a feature card is removed. Feature cards can be removed and stored or may be left in place.

What happens if a feature card that was used in one chassis is removed and put into another chassis?

The Web interface displays the following error message:

```
This feature card was activated with a different chassis. It must be removed
before accessing the FlexAddress feature.
```

```
Current Chassis Service Tag = XXXXXXXX
```

```
Feature Card Chassis Service Tag = YYYYYYYY
```

```
An entry is added to the CMC log that states:
```

```
cmc <date timestamp> : feature 'FlexAddress@YYYYYYYY' not activated; chassis
ID='XXXXXXXX'
```

What happens if the feature card is removed and a non-FlexAddress card is installed?

No activation or modifications to the card should occur. The card is ignored by CMC. In this situation, the **$racadm featurecard -s** command returns the following message:

```
No feature card inserted
ERROR: can't open file
```

If the chassis service tag is reprogrammed, what happens if there is a feature card bound to that chassis?

- If the original feature card is present in the active CMC on that or any other chassis, the Web interface displays the following error message:

  ```
  This feature card was activated with a different chassis. It must be
  removed before accessing the FlexAddress feature.
  Current Chassis Service Tag = XXXXXXXX
  Feature Card Chassis Service Tag = YYYYYYYY
  ```

  The original feature card is no longer eligible for deactivation on that or any other chassis, unless Dell Service re-programs the original chassis service tag back into a chassis, and CMC that has the original feature card is made active on that chassis.
- The FlexAddress feature remains activated on the originally bound chassis. The *binding* of that chassis feature is updated to reflect the new service tag.

Is an error message displayed if two feature cards installed in the redundant CMC system?

The feature card in the active CMC is active and installed in the chassis. The second card is ignored by CMC.

Does the SD card have a write protection lock on it?

Yes it does. Before installing the SD card into the CMC module, verify the write protection latch is in the unlock position. The FlexAddress feature cannot be activated if the SD card is write protected. In this situation, the **$racadm feature -s** command returns this message:

```
No features active on the chassis. ERROR: read only file system
```

What happens if there isn’t an SD card in the active CMC module?

The **$racadm featurecard -s** command returns this message:

```
No feature card inserted.
```

What happens to FlexAddress feature if the server BIOS is updated from version 1.xx to version 2.xx?

The server module needs to be powered down before it can be used with FlexAddress. After the server BIOS update is complete, the server module does not get chassis-assigned addresses until the server has been power cycled.

What happens if a chassis with a single CMC is downgraded with firmware prior to 1.10?

- The FlexAddress feature and configuration is removed from the chassis.
- The feature card used to activate the feature on this chassis is unchanged, and remains bound to the chassis. When this chassis’s CMC firmware is subsequently upgraded to 1.10 or later, the FlexAddress feature is reactivated by reinserting the original feature card (if necessary), resetting CMC (if feature card was inserted after firmware upgrade was completed), and reconfiguring the feature.

What happens if a CMC unit is replaced with one that has firmware prior to 1.10 in a chassis with redundant CMCs?

In a chassis with redundant CMCs, if a CMC unit is replaced with one that has firmware prior to 1.10, the following procedure must be used to ensure the current FlexAddress feature and configuration is NOT removed:

- Ensure the active CMC firmware is always version 1.10 or later.
- Remove the standby CMC and insert the new CMC in its place.
- From the Active CMC, upgrade the standby CMC firmware to 1.10 or later.

NOTE: If the standby CMC firmware is not updated to 1.10 or later and a failover occurs, the FlexAddress feature is not configured. The feature must be reactivated and reconfigured again.

How can a SD card be recovered if the SD card was not in the chassis when the deactivation command was executed on the FlexAddress?

The issue is that the SD card cannot be used to install FlexAddress on another chassis if it was not in CMC when FlexAddress was deactivated. To recover use of the card, insert the card back into a CMC in the chassis that it is bound to, reinstall FlexAddress, and then deactivate FlexAddress, again.

The SD card is properly installed and all the firmware/software updates are installed. The FlexAddress is active, the server deployment screen does not display the options to deploy it? What is wrong?

This is a browser caching issue. Shut down the browser and relaunch.

What happens to FlexAddress if I need to reset my chassis configuration using the RACADM command, `racresetcfg`?

The FlexAddress feature will still be activated and ready to use. All fabrics and slots are selected as default.

NOTE: It is highly recommended that you power down your chassis before issuing the RACADM command `racresetcfg`.

After disabling only the FlexAddressPlus feature (leaving FlexAddress still activated), why does the `racadm setflexaddr` command on the (stillactive) CMC fail?

If the CMC subsequently becomes active, with the FlexAddressPlus feature card still in its cardslot, the FlexAddressPlus feature gets re-activated, and slot or fabric flexaddress configuration changes can resume.

iKVM

The message "User has been disabled by CMC control" appears on the monitor connected to the front panel. Why?

The front panel connection has been disabled by CMC. Enable the front panel using either the CMC Web interface or RACADM.

To enable the front panel using the CMC Web interface, go to**iKVM** → **Setup** tab, select the **Front Panel USB/Video Enabled** option, and click **Apply** to save the setting.

To enable the front panel using RACADM, open a serial/Telnet/SSH text console to CMC, log in, and type:

```
racadm config -g cfgKVMInfo -o cfgKVMAccesToCMCEnable 1
```

The rear panel access does not work. Why?

The front panel setting is enabled by CMC, and a monitor is currently connected to the front panel.

Only one connection is allowed at a time. The front panel connection has precedence over ACI and the rear panel. For more information about connection precedence, see iKVM Connection Precedences.

The message "User has been disabled as another appliance is currently tiered" appears on the monitor connected to the rear panel. Why?

A network cable is connected to the iKVM ACI port connector and to a secondary KVM appliance.

Only one connection is allowed at a time. The ACI tiering connection has precedence over the rear panel monitor connection. The precedence order is front panel, ACI, and then rear panel.

The iKVM's amber LED is blinking. Why?

There are three possible causes:

- **There is problem with the iKVM,** for which the iKVM requires reprogramming. To fix the problem, follow the instructions for updating iKVM firmware.
- **The iKVM is reprogramming the CMC Console Interface.** In this case, the CMC Console is temporarily unavailable and represented by a yellow dot in the OSCAR interface. This process takes up to 15 minutes.
- **The iKVM firmware has detected a hardware error.** For additional information, view the iKVM status.

The iKVM is tiered through the ACI port to an external KVM switch, but all of the entries for the ACI connections are unavailable.

All of the states are showing a yellow dot in the OSCAR interface.

The front panel connection is enabled and has a monitor connected. Because the front panel has precedence over all other iKVM connections, the ACI and rear panel connectors are disabled.

To enable your ACI port connection, you must first disable front panel access or remove the monitor connected to the front panel. The external KVM switch OSCAR entries become active and accessible.

To disable the front panel using the Web interface, go to **iKVM** → **Setup** tab, clear the **Front Panel USB/Video Enabled** option, and click Apply.

To disable the front panel using RACADM, open a serial/Telnet/SSH text console to CMC, log in, and type:

```
racadm config -g cfgKVMInfo -o cfgKVMFrontPanelEnable 0
```

In the OSCAR menu, the Dell CMC connection displays a red X, and it is not possible to connect to CMC. Why?

There are two possible causes:

- **The Dell CMC console has been disabled.** In this case, enable it using either the CMC Web interface or RACADM.
- **CMC is unavailable because it is initializing, switching over to the standby CMC, or reprogramming.** In this case, simply wait until CMC finishes initializing.

The slot name for a server is displayed as "Initializing" in OSCAR, and it cannot be selected it. Why?

Either the server is initializing or the iDRAC on that server failed initialization.

Initially, wait for 60 seconds. If the server is still initializing, the slot name appears as soon as initialization is complete, and the server can be selected.

If, after 60 seconds, OSCAR still indicates that the slot is initializing, remove and then re-insert the server in the chassis. This action allows iDRAC to reinitialize.

IOM

After a configuration change, sometimes CMC displays the IP address as 0.0.0.0.

Click the Refresh icon to see if the IP address is set correctly on the switch. If an error is made in setting the IP/mask/gateway, the switch does not set the IP address and returns a 0.0.0.0 in all fields.

Common errors are:

- Setting the out-of-band IP address to be the same as, or on the same network as, the in-band management IP address.
- Entering an invalid subnet mask.
- Setting the default gateway to an address that is not on a network that is directly connected to the switch.

For more information on IOM network settings, see the *Dell PowerConnect M6220 Switch Important Information* document and the *Dell PowerConnect 6220 Series Port Aggregator White Paper.*