

Dell Chassis Management
Controller Firmware
Version 3.1
User Guide



Notes and Cautions



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



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

Information in this publication is subject to change without notice.

© 2010 Dell Inc. All rights reserved.

Reproduction of these materials in any manner whatsoever without the written permission of Dell Inc. is strictly forbidden. Trademarks used in this text: Dell™, the DELL logo, FlexAddress™, OpenManage™, PowerEdge™, and PowerConnect™ are trademarks of Dell Inc. Microsoft®, Active Directory®, Internet Explorer®, Windows®, Windows Server®, and Windows Vista® are either trademarks or registered trademarks of Microsoft Corporation in the United States and other countries. Red Hat® and Red Hat Enterprise Linux® are registered trademarks of Red Hat, Inc. in the United States and other countries. Novell® is a registered trademark and SUSE™ is a trademark of Novell Inc. in the United States and other countries. Intel® is a registered trademark of Intel Corporation. UNIX® is a registered trademark of The Open Group in the United States and other countries. Avocent® is a trademark of Avocent Corporation. OSCAR® is a registered trademark of Avocent Corporation or its affiliates.

Copyright 1998-2006 The OpenLDAP Foundation. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted only as authorized by the OpenLDAP Public License. A copy of this license is available in the file LICENSE in the top-level directory of the distribution or, alternatively, at <http://www.OpenLDAP.org/license.html>. OpenLDAP is a registered trademark of the OpenLDAP Foundation. Individual files and/or contributed packages may be copyrighted by other parties and subject to additional restrictions. This work is derived from the University of Michigan LDAP v3.3 distribution. This work also contains materials derived from public sources. Information about OpenLDAP can be obtained at <http://www.openldap.org/>. Portions Copyright 1998-2004 Kurt D. Zeilenga. Portions Copyright 1998-2004 Net Boolean Incorporated. Portions Copyright 2001-2004 IBM Corporation. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted only as authorized by the OpenLDAP Public License. Portions Copyright 1999-2003 Howard Y.H. Chu. Portions Copyright 1999-2003 Symas Corporation. Portions Copyright 1998-2003 Hallvard B. Furuseth. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that this notice is preserved. The names of the copyright holders may not be used to endorse or promote products derived from this software without their specific prior written permission. This software is provided "as is" without express or implied warranty. Portions Copyright (c) 1992-1996 Regents of the University of Michigan. All rights reserved. Redistribution and use in source and binary forms are permitted provided that this notice is preserved and that due credit is given to the University of Michigan at Ann Arbor. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. This software is provided "as is" without express or implied warranty.

Other trademarks and trade names may be used in this publication to refer to either the entities claiming the marks and names or their products. Dell Inc. disclaims any proprietary interest in trademarks and trade names other than its own.

December 2010

Contents

1	Overview	19
	What's New For This Release	19
	CMC Management Features	20
	Security Features	21
	Chassis Overview	22
	Hardware Specifications	23
	TCP/IP Ports	23
	Supported Remote Access Connections	24
	Supported Platforms	24
	Supported Web Browsers	25
	Supported Management Console Applications	25
	WS-Management Support	25
	Other Documents You May Need	27
2	Installing and Setting Up the CMC	29
	Before You Begin	29
	Installing the CMC Hardware	29
	Checklist for Integration of a Chassis	30

Basic CMC Network Connection	30
Daisy-chain CMC Network Connection	31
Installing Remote Access Software on a Management Station	35
Installing RACADM on a Linux Management Station	35
Uninstalling RACADM From a Linux Management Station	36
Configuring a Web Browser	36
Proxy Server	37
Microsoft Phishing Filter	38
Certificate Revocation List (CRL) Fetching	38
Downloading Files From CMC With Internet Explorer	39
Allow Animations in Internet Explorer	39
Setting Up Initial Access to the CMC	39
Configuring the CMC Network	40
Configuring Networking Using the LCD Configuration Wizard	41
Accessing the CMC Through a Network	48
Installing or Updating the CMC Firmware	49
Downloading the CMC Firmware	49
Updating CMC Firmware Using the Web Interface	50
Updating the CMC Firmware Using RACADM	50
Configuring CMC Properties	51
Configuring Power Budgeting	51
Configuring CMC Network Settings	51
Adding and Configuring Users	52

Adding SNMP and E-mail Alerts	52
Configuring Remote Syslog	52
Understanding the Redundant CMC Environment.	53
About the Standby CMC	53
Active CMC Election Process	54
Obtaining Health Status of Redundant CMC	54
3 Configuring CMC to Use Command Line Consoles	55
Command Line Console Features on the CMC	55
Using a Serial, Telnet, or SSH Console	56
Using a Telnet Console With the CMC	56
Using SSH With the CMC	56
Enabling SSH on the CMC	57
Changing the SSH Port	57
Enabling the Front Panel to iKVM Connection	58
Configuring Terminal Emulation Software	59
Configuring Linux Minicom	59
Connecting to Servers or I/O Modules With the Connect Command.	61
Configuring the Managed Server BIOS for Serial Console Redirection	62
Configuring Windows for Serial Console Redirection	63
Configuring Linux for Server Serial Console Redirection During Boot	63
Configuring Linux for Server Serial Console Redirection After Boot	65

4	Using the RACADM Command Line Interface	69
	Using a Serial, Telnet, or SSH Console	69
	Logging in to the CMC	70
	Starting a Text Console	70
	Using RACADM.	70
	RACADM Subcommands	71
	Accessing RACADM Remotely	74
	Enabling and Disabling the RACADM Remote Capability.	76
	Using RACADM Remotely.	76
	RACADM Error Messages	77
	Using RACADM to Configure the CMC.	78
	Configuring CMC Network Properties.	78
	Setting Up Initial Access to the CMC.	78
	Viewing Current Network Settings	79
	Configuring the Network LAN Settings.	80
	Configuring the Network Security Settings (IPv4 Only)	86
	Using RACADM to Configure Users	87
	Before You Begin	87
	Adding a CMC User.	88
	Using RACADM to Configure Public Key Authentication over SSH.	89
	Before You Begin	89
	Generating Public Keys for Windows.	90
	Generating Public Keys for Linux	91
	RACADM Syntax Notes for CMC	91
	Viewing the Public Keys	91
	Adding the Public Keys	92

Deleting the Public Keys	92
Logging in Using Public Key Authentication	92
Enabling a CMC User With Permissions	93
Disabling a CMC User	93
Configuring SNMP and E-mail Alerting	94
Configuring Multiple CMCs in Multiple Chassis	94
Creating a CMC Configuration File	95
Parsing Rules	97
Modifying the CMC IP Address.	99
Using RACADM to Configure Properties on iDRAC	100
Troubleshooting	101
5 Using the CMC Web Interface.	103
Accessing the CMC Web Interface	103
Logging In.	104
Logging Out.	105
Configuring Basic CMC Settings	105
Setting the Chassis Name	105
Setting the Date and Time on CMC.	106
Chassis Health Page.	106
Using Chassis Group.	107
Chassis Group Features	107
Setting up a Chassis Group.	108
Removing a Member from the Leader	109
Disbanding a Chassis Group	109

Disabling an Individual Member at the Member Chassis	110
Chassis Component Summary	110
Chassis Graphics	110
Chassis Health	112
Selected Component Information	113
Monitoring System Health Status	119
Viewing Chassis and Component Summaries	119
Viewing Power Budget Status	120
Viewing Server Model Name and Service Tag	120
Viewing the Health Status of All Servers	120
Editing Slot Names	124
Using Server's Host Name as the Slot Name	125
Setting the First Boot Device for Servers	125
Viewing the Health Status of an Individual Server	127
Viewing the Health Status of IOMs	132
Viewing the Health Status of the Fans	133
Viewing the iKVM Status	135
Viewing the Health Status of the PSUs.	137
Viewing Status of the Temperature Sensors	139
Viewing the LCD Status	140
Viewing World Wide Name/Media Access Control (WWN/MAC) IDs.	141
Fabric Configuration	141
WWN/MAC Addresses	142

Configuring CMC Network Properties	142
Setting Up Initial Access to CMC.	142
Configuring the Network LAN Settings.	143
Configuring CMC Network Security Settings	151
Configuring VLAN	153
Adding and Configuring CMC Users.	154
User Types	154
Adding and Managing Users	160
Configuring and Managing Microsoft Active Directory Certificates	163
Common Settings.	163
Standard Schema Settings	167
Extended Schema Settings.	167
Managing Active Directory Certificates	168
Kerberos Keytab	169
Configuring and Managing Generic Lightweight Directory Access Protocol Services	169
Selecting Your LDAP Servers	171
Managing LDAP Group Settings.	172
Managing LDAP Security Certificates	172
Securing CMC Communications Using SSL and Digital Certificates.	173
Secure Sockets Layer (SSL)	173
Certificate Signing Request (CSR)	174
Accessing the SSL Main Menu	174
Generating a New Certificate Signing Request	175

Uploading a Server Certificate	178
Uploading Webserver Key and Certificate	178
Viewing a Server Certificate	179
Managing Sessions	179
Configuring Services.	180
Configuring Power Budgeting	188
Managing Firmware Updates	189
Viewing the Current Firmware Versions	189
Updating Firmware	190
Recovering iDRAC Firmware Using CMC	195
Managing iDRAC.	196
iDRAC QuickDeploy.	196
iDRAC Network Settings	200
Launching Remote Console from CMC GUI	202
Launching iDRAC using Single Sign-On	203
FlexAddress	205
Viewing FlexAddress Status	205
Configuring FlexAddress	209
Chassis-Level Fabric and Slot FlexAddress Configuration	209
Server-Level Slot FlexAddress Configuration	210
Remote File Sharing	211
Frequently Asked Questions.	213
Troubleshooting CMC	215

6	Using FlexAddress	217
	Activating FlexAddress	218
	Verifying FlexAddress Activation.	220
	Deactivating FlexAddress	221
	Deactivating FlexAddress	222
	Configuring FlexAddress Using the CLI	222
	Additional FlexAddress Configuration for Linux.	223
	Viewing FlexAddress Status Using the CLI	223
	Configuring FlexAddress Using the GUI	224
	Wake-On-LAN with FlexAddress.	224
	Troubleshooting FlexAddress	224
	Command Messages	228
	FlexAddress DELL SOFTWARE LICENSE AGREEMENT	231
7	Using FlexAddress Plus	235
	Activating FlexAddress Plus	235
	FlexAddress vs FlexAddress Plus	236
	Scheme 1 and Scheme 2 MAC Address Allocation	237
8	Using the CMC Directory Service	241
	Using CMC with Microsoft Active Directory	241
	Active Directory Schema Extensions	241

Standard Schema Versus Extended Schema	241
Standard Schema Active Directory Overview.	242
Configuring Standard Schema Active Directory to Access CMC	244
Configuring CMC With Standard Schema Active Directory and Web Interface	244
Configuring CMC With Standard Schema Active Directory and RACADM	247
Extended Schema Overview.	248
Active Directory Schema Extensions.	248
Overview of the RAC Schema Extensions	249
Active Directory Object Overview	249
Configuring Extended Schema Active Directory to Access Your CMC	254
Extending the Active Directory Schema	254
Installing the Dell Extension to the Active Directory Users and Computers Snap-In	261
Adding CMC Users and Privileges to Active Directory.	262
Configuring CMC With Extended Schema Active Directory and the Web Interface	264
Configuring CMC With Extended Schema Active Directory and RACADM	267
Frequently Asked Questions	269
Configuring Single Sign-On	272
System Requirements.	272
Configuring Settings	273
Configuring Active Directory	273
Configuring CMC	274
Uploading the Kerberos Keytab File	274
Enabling Single Sign-On	275

Configuring the Browser For Single Sign-On Login	276
Logging into CMC Using Single Sign-On	277
Configuring Smart Card Two-Factor Authentication	278
System Requirements.	278
Configuring Settings	278
Configuring Active Directory	279
Configuring CMC	279
Uploading the Kerberos Keytab File	279
Enabling Smart Card Authentication	280
Configuring the Browser For Smart Card Login	280
Logging into CMC Using Smart Card	281
Troubleshooting the Smart Card Login	281
Using CMC with Generic LDAP	282
Configuring the Generic LDAP Directory to Access CMC	283
Configuring Generic LDAP Directory Service Using CMC Web-Based Interface	284
Selecting Your LDAP Servers.	286
Managing LDAP Group Settings	287
Managing LDAP Security Certificates	287
Configuring Generic LDAP Directory Service Using RACADM	288
Usage	288
Getting Help.	288
9 Power Management	289
Overview.	289
AC Redundancy Mode	289
Power Supply Redundancy Mode	291

No Redundancy Mode	292
Power Budgeting for Hardware Modules	293
Server Slot Power Priority Settings.	295
Dynamic Power Supply Engagement.	296
Redundancy Policies.	298
AC Redundancy	298
Power Supply Redundancy	298
No Redundancy	299
Power Conservation and Power Budget Changes	299
Power Supply and Redundancy Policy Changes in System Event Log.	306
Redundancy Status and Overall Power Health	308
Configuring and Managing Power.	308
Viewing the Health Status of the PSUs.	308
Viewing Power Consumption Status	311
Viewing Power Budget Status	315
Configuring Power Budget and Redundancy	320
Assigning Priority Levels to Servers	324
Setting the Power Budget	325
Server Power Reduction to Maintain Power Budget.	327
Executing Power Control Operations on the Chassis	327
Executing Power Control Operations on an IOM	329
Executing Power Control Operations on a Server	330
Troubleshooting.	332

10 Using the iKVM Module	333
Overview	333
iKVM User Interface	333
Security	333
Scanning	333
Server Identification	334
Video	334
Plug and Play	334
FLASH Upgradable	334
Physical Connection Interfaces	334
iKVM Connection Precedences	335
Tiering Through the ACI Connection	335
Using OSCAR	336
Navigation Basics	336
Configuring OSCAR	337
Managing Servers With iKVM	340
Peripherals Compatibility and Support	340
Viewing and Selecting Servers	340
Setting Console Security	344
Scanning Your System	348
Broadcasting to Servers	350
Managing iKVM From CMC	351
Enabling or Disabling the Front Panel	351
Enabling the Dell CMC Console Through iKVM	352
Viewing the iKVM Status and Properties	352
Updating the iKVM Firmware	354
Troubleshooting	355

11 I/O Fabric Management	361
Fabric Management	362
Invalid Configurations	363
Invalid Mezzanine Card (MC) Configuration	364
Invalid IOM-Mezzanine Card (MC) Configuration	364
Invalid IOM-IOM Configuration	364
Fresh Power-up Scenario	364
Monitoring IOM Health	365
Viewing the Health Status of an Individual IOM	368
Configuring Network Settings for an Individual IOM	370
Troubleshooting IOM Network Settings	373
12 Troubleshooting and Recovery	375
Overview	375
Chassis Monitoring Tools	375
Gathering Configuration information and Chassis Status and Logs	375
Usage	376
Supported Interfaces	376
CLI RACDUMP	376
Remote RACDUMP	377
Remote RACDUMP Usage	377
Telnet RACDUMP	378
Configuring LEDs to Identify Components on the Chassis	378
Configuring SNMP Alerts	379

Configuring E-mail Alerts	385
First Steps to Troubleshooting a Remote System	388
Monitoring Power and Executing Power	
Control Commands on the Chassis	389
Viewing Power Budget Status	389
Executing a Power Control Operation	389
Power Troubleshooting	389
Viewing Chassis Summaries	392
Viewing Chassis and Component	
Health Status.	397
Viewing the Event Logs	398
Viewing the Hardware Log	398
Viewing the CMC Log.	400
Using the Diagnostic Console	401
Resetting Components.	402
Troubleshooting Network Time Protocol	
(NTP) Errors	406
Interpreting LED Colors and Blinking Patterns	408
Troubleshooting a Non-responsive CMC	410
Observing the LEDs to Isolate	
the Problem.	411
Obtain Recovery Information From	
the DB-9 Serial Port	411
Recovering the Firmware Image	412
Troubleshooting Network Problems	413
Resetting Forgotten Administrator Password.	413

Troubleshooting Alerting	416
13 Diagnostics	417
Using the LCD Panel Interface	417
LCD Navigation	417
Main Menu	418
LCD Setup Menu	419
Language Setup Screen	419
Default Screen	419
Graphical Server Status Screen	420
Graphical Module Status Screen	421
Enclosure Menu Screen	421
Module Status Screen	422
Enclosure Status Screen	422
IP Summary Screen	422
Diagnostics	423
LCD Hardware Troubleshooting	423
Front Panel LCD Messages	426
LCD Error Messages	426
LCD Module and Server Status Information	433
Index	439

Overview

The Dell Chassis Management Controller (CMC) is a hot-pluggable systems management hardware and software solution designed to provide remote management capabilities and power control functions for Dell PowerEdge M1000e chassis systems.

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

The CMC, which has its own microprocessor and memory, is powered by the modular chassis into which it is plugged. To get started with the CMC, see "Installing and Setting Up the CMC" on page 29.

What's New For This Release

This release of CMC supports the following features:

- Multi-chassis management, which allows up to 8 other chassis to be visible from the lead chassis.
- Power Logging, which allows the user to collect power consumption measurements to a remote server.
- Save and restore configuration on a host.
- Improvement of SEL log.
- GPL/Open source compliant.
- Dell 8/4Gbps Fibre Channel Pass through IOM.
- Dell M8428-k IOM.
- Brocade BR1741M-k Dual Port Mezzanine Card.
- Server Performance Over Power Redundancy mode for power management.

CMC 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.
- Support for Microsoft Active Directory authentication — Centralizes CMC user IDs and passwords in Active Directory using the Standard Schema or an Extended Schema.
- 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 components — Enables you to update the firmware for CMC, servers, iKVM, and I/O module infrastructure devices.
- 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.
- Password-level security management — Prevents unauthorized access to a remote system.
- Role-based authority — Provides assignable permissions for different systems management tasks.
- 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. For more information, see "Using FlexAddress" on page 217.
- Graphical display of chassis component status and health.
- Support for single and multi-slot servers.
- Update multiple iDRAC management consoles firmware at once.
- 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 *reset* 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:

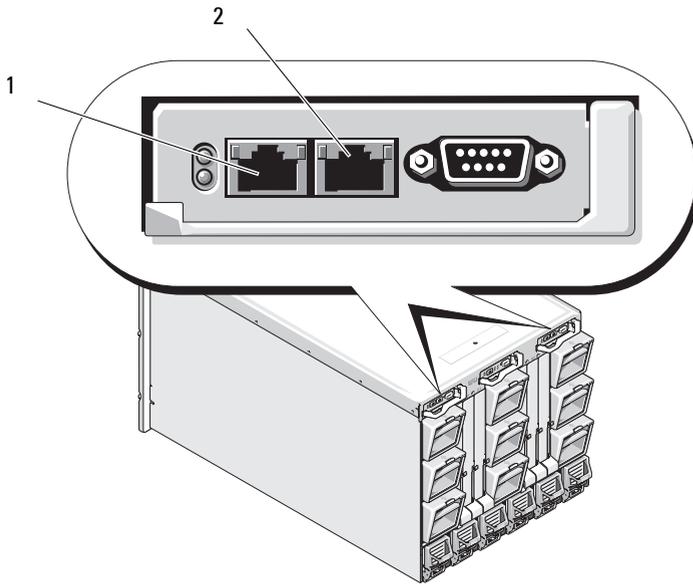
- User authentication through Active Directory (optional), or hardware-stored user IDs and passwords
 - Role-based authority, which enables an administrator to configure specific privileges for each user
 - User ID and password configuration through the Web interface
 - Web interface supports 128-bit 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

Figure 1-1 shows the facing edge of a CMC (inset) and the locations of the CMC slots in the chassis.

Figure 1-1. Dell M1000e Chassis and CMC



1 GB Port

2 STK Port

Hardware Specifications

TCP/IP Ports

You must provide port information when opening firewalls for remote access to a CMC.

Table 1-1. CMC Server Listening Ports

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

* Configurable port

Table 1-2. 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

Table 1-3. Supported Remote Access Connections

Connection	Features
CMC Network Interface ports	<ul style="list-style-type: none">• Two 10/100 GB ports; one for management and the other for chassis to chassis cable consolation• 10Mbps/100Mbps/1Gbps Ethernet through CMC GbE port• DHCP support• SNMP traps and e-mail event notification• GB port: Dedicated network interface for the CMC Web interface• STK: Uplink port for chassis to chassis management network cable consolation• 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	<ul style="list-style-type: none">• 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 to the serial console of a server, or I/O module, using the <code>connect</code> (or <code>racadm connect</code>) command
Other connections	<ul style="list-style-type: none">• 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 on the Dell Support website at support.dell.com/manuals.

Supported Web Browsers

The following Web Browsers are supported for CMC 3.1:

- Microsoft Internet Explorer 8.0 for Windows 7, Windows Vista, Windows XP, and Windows Server 2003 family.
- Microsoft Internet Explorer 7.0 for Windows 7, Windows Vista, Windows XP, and Windows Server 2003 family.
- Mozilla Firefox 1.5 (32-bit) – limited functionality.

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

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.

WS-Management Support

Web Services for Management (WS-MAN) is a Simple Object Access Protocol (SOAP)-based protocol used for systems management. WS-MAN provides a interoperable protocol for devices to share and exchange data across networks. CMC uses WS-MAN to convey Distributed Management Task Force (DMTF) Common Information Model (CIM)-based management information. CIM information defines the semantics and information types that can be manipulated in a managed system. The Dell-embedded server platform management interfaces are organized into profiles, where each profile defines the specific interfaces for a particular

management domain or area of functionality. Additionally, Dell has defined a number of model and profile extensions that provide interfaces for additional capabilities.

Access to WS-Management requires logging in using local user privileges with basic authentication over Secured Socket Layer (SSL) protocol at port 443. For information on setting user accounts, see the Session Management database property section in the *Command Line Reference Guide for iDRAC6 and CMC*.

The data available through WS-Management is a subset of data provided by the CMC instrumentation interface mapped to the following DMTF profiles version 1.0.0:

- Allocation Capabilities Profile
- Base Metrics Profile
- Base Server Profile
- Computer System Profile
- Modular System Profile
- Physical Asset Profile
- Dell Power Allocation Profile
- Dell Power Supply Profile
- Dell Power Topology Profile
- Power State Management Profile
- Profile Registration Profile
- Record Log Profile
- Resource Allocation Profile
- Role Based Authorization Profile
- Sensors Profile
- Service Processor Profile
- Simple Identity Management Profile
- Dell Active Directory Client Profile
- Boot Control Profile
- Dell Simple NIC Profile

The CMC WS-MAN implementation uses SSL on port 443 for transport security, and supports basic authentication. For information on setting user accounts, see the `cfgSessionManagement` database property section in the *Command Line Reference Guide for iDRAC6 and CMC*. 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**, <<http://support.microsoft.com/kb/968929>>.

There are additional implementation guides, white papers, profile, and code samples available in the Dell Tech Center at www.delltechcenter.com. For more information, see:

- DTMF Web site: www.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

Other Documents You May Need

In addition to this guide, you can access the following guides available on the Dell Support website 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 6 (iDRAC6) Enterprise for Blade Servers User 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.

Installing and Setting Up the CMC

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

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

For more information about installing and setting up redundant CMC environments see "Understanding the Redundant CMC Environment" on page 53."

Before You Begin

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

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

Installing the CMC Hardware

The 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. For more information about a standby CMC, see "Understanding the Redundant CMC Environment" on page 53.

Checklist for Integration of a Chassis

The following steps enable you to setup the chassis accurately:

- 1 Your CMC and the management station where you use your browser must be on the same network, which is called the management network. Cable the CMC Ethernet port labelled **GB** to management network.



NOTE: Do not place a cable in the CMC Ethernet port labelled **STK**. For more information to cable the STK port, see "Understanding the Redundant CMC Environment" on page 53.

- 2 For rack chassis, 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 provided at the side of the chassis or, power on the chassis from the CMC GUI after completing step 7.



NOTE: Do not power on the servers.

- 6 Using the LCD panel on the front of the system, provide the 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 GUI 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 GUI.
- 10 Connect to each iDRAC through the web browser and provide final configuration of iDRAC. Default username 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 CMC to your management network. If a chassis has just one CMC, make one connection on the management network. If the chassis has a redundant CMC, make two connections to the 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

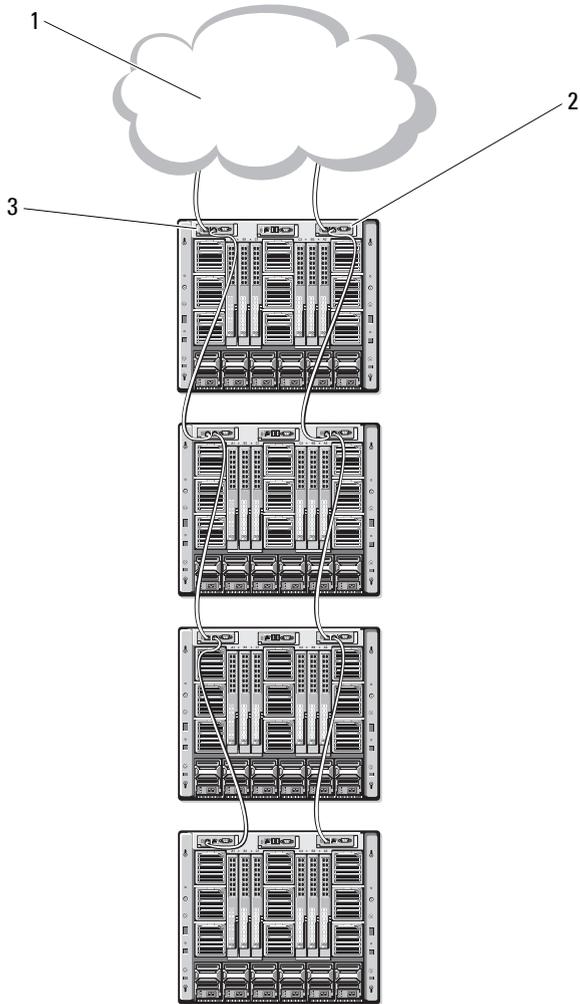
If you have multiple chassis in a rack, you can reduce the number of connections to the management network by daisy-chaining up to four chassis together. If each of the four chassis contains a redundant CMC, by daisy-chaining you can reduce the number of management network connections required from eight 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 the 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 the CMCs in the active CMC slot and the second CMC slot.

Figure 2-1 illustrates the arrangement of cables for four daisy-chained chassis, each with active and standby CMCs.

Figure 2-1. Daisy-chained CMC Network Connection



- 1 management network
- 3 active CMC

2 standby CMC

Figure 2-2, Figure 2-3, and Figure 2-4 show examples of incorrect cabling of the CMC.

Figure 2-2. Incorrect Cabling for CMC Network Connection - 2 CMCs

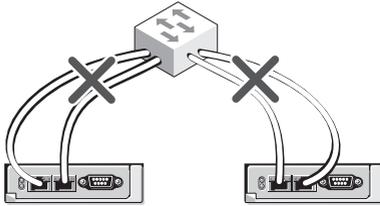


Figure 2-3. Incorrect Cabling for CMC Network Connection - Single CMC

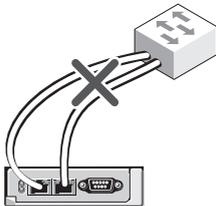
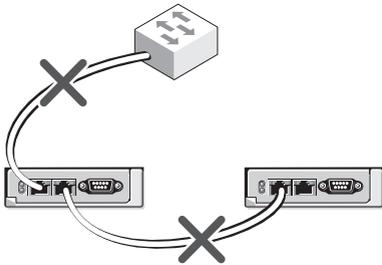


Figure 2-4. Incorrect Cabling for CMC Network Connection - 2 CMCs



Follow these steps 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: Never 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.

To get started with the CMC, see "Installing Remote Access Software on a Management Station" on page 35.

Installing Remote Access Software on a Management Station

You can access the 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 the Dell Support website at support.dell.com.

Installing RACADM on a Linux Management Station

- 1 Log on 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 "Using the RACADM Command Line Interface" on page 69.

 **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>
```

For more information on remote `racadm`, see "Accessing RACADM Remotely" on page 74 and the subsequent sections.

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 a Web Browser

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

Your 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:** Ensure that security measures on the management network, such as firewalls and proxy servers, do not prevent your Web browser from accessing the 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.

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

Follow these steps 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 the 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.
- 4 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.

Follow these steps to disable CRL fetching:

- 1 Start Internet Explorer.
- 2 Click **Tools**→ **Internet Options**, and then click **Advanced**.
- 3 Scroll to the Security section and uncheck **Check for publisher's certificate revocation**.
- 4 Click **OK**.

Downloading Files From CMC With Internet Explorer

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

Follow these steps 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 check **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.

Follow these steps 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 the CMC

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



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

For information on how to configure the CMC network settings, see "Configuring the CMC Network" on page 40. This initial configuration assigns the TCP/IP networking parameters that enable access to the CMC.

The 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.

The CMC is connected to the management network. All external access to the CMC and iDRACs is accomplished through the 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.

 **NOTE:** 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. The CMC and individual iDRAC network interfaces can be configured to use a VLAN with the `racadm setniccfg` command. For more information, see the *Dell Chassis Management Controller Administrator Reference Guide*.

If you have one chassis, connect the 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.

For more information on daisy-chained connection, see "Daisy-chain CMC Network Connection" on page 31."

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

Configuring the CMC Network

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

You can perform the initial network configuration of the CMC before or after the CMC has an IP address. If you configure the 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
- The CMC Web interface

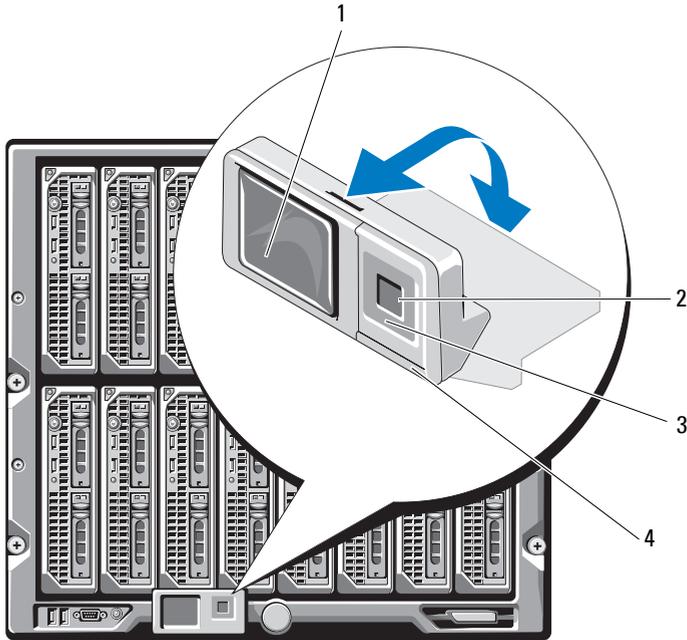
Configuring Networking Using the LCD Configuration Wizard



NOTE: The option to configure the CMC using the LCD Configuration Wizard is available only until the 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 is located on the bottom left corner on the front of the chassis. Figure 2-5 illustrates the LCD panel.

Figure 2-5. LCD Display



- | | | | |
|---|--------------------|---|----------------------------|
| 1 | LCD screen | 2 | selection ("check") button |
| 3 | scroll buttons (4) | 4 | status indicator LED |

The LCD screen displays menus, icons, pictures, and messages. 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.

Navigating in the LCD Screen

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 Configuration Wizard, 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.

For more information about using the LCD panel, see the LCD panel section in the *Command Line Reference Guide for iDRAC6 and CMC*.

Using the LCD Configuration Wizard

- 1** If you have not already done so, 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 displays.

- 2** Select your language using the arrow buttons, and then press the center button to select the **Accept/Yes** and press the center button again.
- 3** The **Enclosure** screen displays with the following question: **Configure Enclosure?**
 - a** Press the center button to continue to the **CMC Network Settings** screen. See step 4.
 - b** To exit the **Configure Enclosure** menu, select the **NO** icon and press the center button. See step 9.

- 4 Press the center button to continue to the **CMC Network Settings** screen.
- 5 Select your network speed (10Mbps, 100Mbps, Auto (1 Gbps)) using the down arrow button.



NOTE: 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 your network configuration does not match any of these values, Dell recommends that you 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.

- 6 Select the duplex mode (half or full) that matches your 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.



NOTE: 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.

- 7 Select the Internet Protocol (IPv4, IPv6, or both) that you want to use for the CMC.

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

- 8 Select the mode in which you want the CMC to obtain the NIC IP addresses:

Dynamic Host Configuration Protocol (DHCP) The CMC retrieves IP configuration (IP address, mask, and gateway) automatically from a DHCP server on your network. The CMC is assigned a unique IP address allotted over your network. If you have selected the DHCP option, press the center button. The **Configure iDRAC?** screen appears; go to step 10.

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:

- a 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.
- b Set the subnet mask, and then press the center button.
- c 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. Review 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.
- d 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.

- 9 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.

10 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.

11 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:

- a** 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.
- b** Set the subnet mask, and then press the center button.
- c** Set the gateway, and then press the center button.

a Select whether to **Enable** or **Disable** the IPMI LAN channel. Press the center button to continue.

b 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.

- 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.

- 12 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.
- 13 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.

The 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.

Accessing the CMC Through a Network

After you have configured the CMC network settings, you can remotely access the CMC using any of the following interfaces:

- Web interface
- Telnet console
- SSH
- Remote RACADM



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

Table 2-1. CMC Interfaces

Interface	Description
Web interface	<p>Provides remote access to the 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.</p> <p>For a list of supported Web browsers, see the Supported Browsers section in the <i>Dell System Software Support Matrix</i> on the Dell Support website at support.dell.com/manuals.</p>
Remote RACADM command line interface	<p>Provides remote access to the CMC from a management station using a command line interface (CLI). Remote RACADM uses the <code>racadm -r</code> option with the CMC's IP address to execute commands on the CMC.</p> <p>For more information on remote racadm, see "Accessing RACADM Remotely" on page 74 and subsequent sections.</p>
Telnet	<p>Provides command line access to the CMC through the network. The RACADM command line interface and the <code>connect</code> command, which is used to connect to the serial console of a server or IO module, are available from the CMC command line.</p> <p>NOTE: Telnet is an insecure protocol that transmits all data—including passwords—in plain text. When transmitting sensitive information, use the SSH interface.</p>
SSH	<p>Provides the same capabilities as Telnet using an encrypted transport layer for greater security.</p>



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

You can access the CMC and iDRAC Web interfaces through the CMC Network Interface using a supported Web browser; you can also launch them from the Dell Server Administrator or Dell OpenManage IT Assistant.

For a list of supported Web browsers, see the Supported Browsers section in the *Dell Systems Software Support Matrix* on the Dell Support website at support.dell.com/manuals. To access the CMC using a supported Web browser, see "Accessing the CMC Web Interface" on page 103. For information on Dell OpenManage IT Assistant, see "Installing Remote Access Software on a Management Station" on page 35.

To access the 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 your *Dell Server Administrator User's Guide*.

To access the CMC command line using Telnet or SSH, see "Configuring CMC to Use Command Line Consoles" on page 55.

For information about using RACADM, see "Using the RACADM Command Line Interface" on page 69.

For information about using the **connect**, or **racadm connect**, command to connect to servers and IO modules, see "Connecting to Servers or I/O Modules With the Connect Command" on page 61.

Installing or Updating the CMC Firmware

Downloading the CMC Firmware

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

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

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

-  **NOTE:** During updates of CMC firmware, it is normal for some or all of the fan units in the chassis to spin at 100%.
-  **NOTE:** The firmware update, by default, retains the current CMC settings. During the update process, you have the option to reset the CMC configuration settings back to the factory default settings.
-  **NOTE:** If you have redundant CMCs installed in the chassis, it is important to update both to the same firmware version. If the CMCs have different firmware and a failover occurs, unexpected results may occur.

You can use the RACADM `getsysinfo` command (see the `getsysinfo` command section in the *Command Line Reference Guide for iDRAC6 and CMC*) or the **Chassis Summary** page (see "Viewing the Current Firmware Versions" on page 189) to view the current firmware versions for the CMCs installed in your chassis.

If you have a standby CMC, it is recommended that you update both CMCs at the same time with a single operation. When the standby CMC has been updated, swap the CMCs' roles so that the newly updated CMC becomes the active CMC and the CMC with the older firmware becomes the standby. (See the `cmchangeover` command section in the *Command Line Reference Guide for iDRAC6 and CMC* for help in 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 `cmchangeover` 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 `cmchangeover` command.

Updating CMC Firmware Using the Web Interface

For instructions on using the Web interface to update CMC firmware, see "Updating the CMC Firmware" on page 190.

Updating the CMC Firmware Using RACADM

For instructions on using the RACADM `fwupdate` subcommand to update CMC firmware, see the `fwupdate` command section in the *Command Line Reference Guide for iDRAC6 and CMC*.

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.

For more information about using the Web interface, see "Accessing the CMC Web Interface" on page 103. For more information about using RACADM, see "Using the RACADM Command Line Interface" on page 69.



CAUTION: Using more than one CMC configuration tool at the same time may generate unexpected results.

Configuring Power Budgeting

The 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.

For more information about CMC power management, see "Power Management" on page 289.

For instructions on configuring power budgeting and other power settings using the Web interface, see "Configuring Power Budgeting" on page 188.

Configuring CMC Network Settings



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

You can configure the CMC network settings using one of the following tools:

- RACADM — For more information, see "Configuring Multiple CMCs in Multiple Chassis" on page 94.



NOTE: If you are deploying the CMC in a Linux environment, see "Installing RACADM on a Linux Management Station" on page 35.

- Web interface — For more information, see "Configuring CMC Network Properties" on page 142.

Adding and Configuring Users

You can add and configure CMC users using either RACADM or the CMC Web interface. You can also utilize Microsoft Active Directory to manage users.

For instructions on adding and configuring public key users for the CMC using RACADM, see "Using RACADM to Configure Public Key Authentication over SSH" on page 89. For instructions on adding and configuring users using the Web interface, see "Adding and Configuring CMC Users" on page 154.

For instructions on using Active Directory with your CMC, see "Using the CMC Directory Service" on page 241.

Adding SNMP and E-mail Alerts

You can configure the CMC to generate SNMP or e-mail alerts when certain chassis events occur. For more information, see "Configuring SNMP Alerts" on page 379 and "Configuring E-mail Alerts" on page 385.

Configuring Remote Syslog

The *remote syslog* feature is activated and configured through either the CMC GUI or the `racadm` command. Configuration options include the syslog server name (or IP address) and the UDP port that CMC uses when forwarding the log entries. You can specify up to 3 distinct syslog server destinations in the configuration. Remote syslog is an additional log target for the 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.

To configure CMC services:

- 1 Log in to the CMC Web interface.
- 2 Click the **Network** tab.
- 3 Click the **Services** subtab. The **Services** page appears.

For more information on configuring the remote syslog, see Table 5-56.

Understanding the Redundant CMC Environment

You can install a standby CMC that takes over if your active CMC fails. Your redundant CMC may be pre-installed or can be added at a later date. It is important that the 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 *Command Line Reference Guide for iDRAC6 and CMC*.)
- Run the RACADM **racreset** command on the active CMC. (See the **racreset** command section in the *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 on the Chassis" on page 327.)
- 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.

About the 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 the CMC firmware on your standby CMC, follow the instructions in "Installing or Updating the CMC Firmware" on page 49.

Active CMC Election Process

There is no difference between the two CMC slots; that is, slot does not dictate precedence. Instead, the CMC that is installed or booted first assumes the role of the active CMC. If AC power is applied with two CMCs installed, the 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 and Component Summaries" on page 119.

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 your system so you can perform systems management actions through the console. For information on using the RACADM commands in CMC through the command line console, see "Using the RACADM Command Line Interface" on page 69.

Command Line Console Features on the CMC

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.

Using a Serial, Telnet, or SSH Console

When you connect to the CMC command line, you can enter these commands:

Table 3-1. CMC Command Line Commands

Command	Description
racadm	RACADM commands begin with the keyword racadm and are followed by a subcommand, such as getconfig , serveraction , or getsensorinfo . See "Using the RACADM Command Line Interface" on page 69 for details on using RACADM.
connect	Connects to the serial console of a server or I/O module. See "Connecting to Servers or I/O Modules With the Connect Command" on page 61 for help using the connect command. NOTE: The racadm connect command can also be used.
exit, logout, and quit	These commands all perform the same action: they end the current session and return to a login prompt.

Using a Telnet Console With the CMC

Up to four Telnet client systems and four SSH clients may connect at any given 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 the 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 login procedure, 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 should 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 any given time. The session timeout is controlled by the `cfgSsnMgtSshIdleTimeout` property (see the database property chapter of the *Command Line Reference Guide for iDRAC6 and CMC* or from the **Services Management** page in the Web interface (see "Configuring Services" on page 180.)

CMC also supports the 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 "Using RACADM to Configure Public Key Authentication over SSH" on page 89.

Enabling SSH on the CMC

SSH is enabled by default. If SSH is disabled, then you can enable it using any other supported interface.

For instructions on enabling SSH connections on the CMC using RACADM, see the `config` command section and the `cfgSerial` database property section in the *Command Line Reference Guide for iDRAC6 and CMC*. For instructions on enabling SSH connections on the CMC using the Web interface, see "Configuring Services" on page 180.

Changing the SSH Port

To change the SSH port, run the following command:

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

For more information about `cfgSerialSshEnable` and `cfgRacTuneSshPort` properties, see the database property chapter of the *Command Line Reference Guide for iDRAC6 and CMC*.

The CMC SSH implementation supports multiple cryptography schemes, as shown in Table 3-2.

Table 3-2. Cryptography Schemes

Scheme Type	Scheme
Asymmetric Cryptography	Diffie-Hellman DSA/DSS 512–1024 (random) bits per NIST specification
Symmetric Cryptography	<ul style="list-style-type: none"> • AES256-CBC • RIJNDAEL256-CBC • AES192-CBC • RIJNDAEL192-CBC • AES128-CBC • RIJNDAEL128-CBC • BLOWFISH-128-CBC • 3DES-192-CBC • ARCFOUR-128
Message Integrity	<ul style="list-style-type: none"> • HMAC-SHA1-160 • HMAC-SHA1-96 • HMAC-MD5-128 • HMAC-MD5-96
Authentication	Password

Enabling the Front Panel to iKVM Connection

For information and instructions on using the iKVM front panel ports, see "Enabling or Disabling the Front Panel" on page 351.

Configuring Terminal Emulation Software

Your 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. Use the information in "Required Minicom Settings" on page 60 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 13.
- 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 **Save setup as config_name** and press <Enter>.
- 11 Select **Exit From Minicom** and press <Enter>.
- 12 At the command shell prompt, type `minicom <Minicom config file name>`.
- 13 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

Use Table 3-3 to configure any version of Minicom.

Table 3-3. 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 With the 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 in several ways:

- Using the CMC command line and the **connect**, or **racadm connect** command. For more information about **connect**, see the **racadm connect** command in the *Command Line Reference Guide for iDRAC6 and CMC*.
- Using the iDRAC Web interface serial console redirection feature.
- Using the iDRAC Serial Over LAN (SOL) functionality.

While 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, as well as 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 will display 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.

IOMs are labeled A1, A2, B1, B2, C1, and C2. (See Figure 11-1 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 Table 3-4.

Table 3-4. Mapping I/O Modules to Switches

I/O Module Label	Switch
A1	switch-a1
A2	switch-a2
B1	switch-b1
B2	switch-b2
C1	switch-c1
C2	switch-c2

 **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-n**, where *-n* is the slot number of the server; 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.

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" on page 340), or establish a Remote Console session from the iDRAC web GUI (see the *iDRAC 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 COM1Use 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.
- 7 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/sda1
#         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

10:0:wait:/etc/rc.d/rc 0
11:1:wait:/etc/rc.d/rc 1
12:2:wait:/etc/rc.d/rc 2
13:3:wait:/etc/rc.d/rc 3
14:4:wait:/etc/rc.d/rc 4
15:5:wait:/etc/rc.d/rc 5
16:6: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
```

Using the RACADM Command Line Interface

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. The CMC does not have support for scripting, so you cannot run the scripts directly on the CMC. For more information about configuring multiple CMCs, see "Configuring Multiple CMCs in Multiple Chassis" on page 94.

Using a Serial, Telnet, or SSH Console

You can log in to the CMC through a serial or Telnet/SSH connection, or through Dell CMC console on iKVM. To configure the CMC for serial or remote access, see "Configuring CMC to Use Command Line Consoles" on page 55. Commonly used subcommand options are listed in Table 4-2. A complete list of RACADM subcommands is listed in the RACADM Subcommands chapter of the *Command Line Reference Guide for iDRAC6 and CMC*.

Logging in to the CMC

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

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

Starting a Text Console

You can log in to the CMC using Telnet or SSH through a network, serial port, or a Dell CMC console through the iKVM. Open a Telnet or SSH session, connect and log in to the CMC.

For information about connecting to the CMC through iKVM, see "Using the iKVM Module" on page 333.

Using RACADM

RACADM subcommands can be run remotely from the serial, Telnet, or SSH console command prompt or through a normal command prompt.

Use RACADM subcommands to configure CMC properties and perform remote management tasks. To display a list of RACADM subcommands, type:

```
racadm help
```

When run without options or subcommands, RACADM displays syntax information and instructions on how to access subcommands and help.

To list syntax and command-line options for individual subcommands, type:

```
racadm help <subcommand>
```

RACADM Subcommands

Table 4-1 provides a brief list of common subcommands used in RACADM. For a complete list of RACADM subcommands, including syntax and valid entries, see the RACADM Subcommands chapter in the *Command Line Reference Guide for iDRAC6 and CMC*.

 **NOTE:** The **connect** command is available as both—RACADM command and built-in CMC command. The **exit**, **quit**, and **logout** commands are built-in CMC commands, not RACADM commands. None of these commands can be used with remote RACADM. For information about using these commands, see "Connecting to Servers or I/O Modules With the Connect Command" on page 61.

Table 4-1. RACADM Subcommands

Command	Description
help	Lists CMC subcommand descriptions.
help <subcommand>	Lists usage summary for the specified subcommand.
?	Lists CMC subcommand descriptions.
? <subcommand>	Lists usage summary for the specified subcommand.
arp	Displays the contents of the ARP table. ARP table entries may not be added or deleted.
chassisaction	Executes power-up, power-down, reset, and power-cycle on the chassis, switch, and KVM.
closessn	Closes a session.
clrraclog	Clears the CMC log and creates a single entry indicating the user and time that the log was cleared.
clrsel	Clears the System Event Log entries.
cmchangeover	Changes the state of the CMC from active to standby, or vice versa, in redundant CMC environments.
config	Configures the CMC.
connect	Connects to the serial console of a server or I/O module. See "Connecting to Servers or I/O Modules With the Connect Command" on page 61 for help using the connect subcommand.
deploy	Deploys a server by specifying required properties.

Table 4-1. RACADM Subcommands (continued)

Command	Description
feature	Displays active features and feature deactivation.
featurecard	Displays feature card status information.
fwupdate	Performs system component firmware updates, and displays firmware update status.
getassettag	Displays the asset tag for the chassis.
getchassisname	Displays the name of the chassis.
getconfig	Displays the current CMC configuration properties.
getdcinfo	Displays general I/O module and daughter card misconfiguration information.
getflexaddr	Displays the FlexAddress enabled/disabled status on a per slot/fabric basis. If used with the <code>-i</code> option, the command displays the WWN and MAC address for a particular slot.
getioinfo	Displays general I/O module information.
getkvminfo	Displays information about the iKVM.
getled	Displays the LED settings on a module.
getmacaddress	Displays a server's MAC address.
getmodinfo	Displays module configuration and status information.
getniccfg	Displays the current IP configuration for the controller.
getpbinfo	Displays power budget status information.
getpminfo	Displays power management status information.
getraclog	Displays the CMC log.
getractime	Displays the CMC time.
getredundancymode	Displays the redundancy mode of the CMC.
getsel	Displays the system event log (hardware log).
getsensorinfo	Displays information about system sensors.
getslotname	Displays the name of a slot in the chassis.
getssninfo	Displays information about active sessions.
getsvctag	Displays service tags.

Table 4-1. RACADM Subcommands (continued)

Command	Description
getsysinfo	Displays general CMC and system information.
gettracelog	Displays the CMCTrace log. If used with the <code>-i</code> option, the command displays the number of entries in the CMC trace log.
getversion	Displays the current software version, model information, and whether or not the device can be updated.
ifconfig	Displays the current CMC IP configuration.
krbkeytabupload	Uploads a Kerberos Keytab to the CMC.
netstat	Displays the routing table and the current connections.
ping	Verifies that the destination IPv4 address is reachable from the CMC with the current routing-table contents.
ping6	Verifies that the destination IPv6 address is reachable from the CMC with the current routing-table contents.
racdump	Displays the comprehensive chassis status and configuration state information, as well as historic event logs. Used for post deployment configuration verification and during debugging sessions.
racreset	Resets the CMC.
racresetcfg	Resets the CMC to the default configuration.
remoteimage	Connects, disconnects, or deploys a media file on a remote server
serveraction	Performs power management operations on the managed system.
setassettag	Sets the asset tag for the chassis.
setchassisname	Sets the name of the chassis.
setflexaddr	Enables/disables FlexAddress on a particular slot/fabric, when the FlexAddress feature is activated on the chassis
setled	Sets the LED settings on a module.
setniccfg	Sets the IP configuration for the controller.
setractime	Sets the CMC time.

Table 4-1. RACADM Subcommands (continued)

Command	Description
setslotname	Sets the name of a slot in the chassis.
setsysinfo	Sets the name and location of the chassis.
sshpkauth	Uploads up to 6 different SSH public keys, deletes existing keys, and views the keys already in the CMC.
sslcertdownload	Downloads a certificate authority-signed certificate.
sslcertupload	Uploads a certificate authority-signed certificate or server certificate to the CMC.
sslcertview	Views a certificate authority-signed certificate or server certificate in the CMC.
sslcsrgen	Generates and downloads the SSL CSR.
sslresetcfg	Regenerates the self-signed certificate used by the CMC Web GUI.
testemail	Forces the CMC to send an e-mail over the CMC NIC.
testfeature	Allow you to verify a specific feature's configuration parameters. For example, it supports testing the Active Directory configuration using simple authentication (user name and password) or Active Directory configuration using Kerberos authentication (Single Sign-on or Smart Card Login).
testtrap	Forces the CMC to send an SNMP over the CMC Network Interface.
traceroute	Prints the route the IPv4 packets take to a network node.
traceroute6	Prints the route the IPv6 packets take to a network node.

Accessing RACADM Remotely

Table 4-2. Remote RACADM Subcommand Options

Option	Description
-r <racIpAddr>	Specifies the controller's remote IP address.
-r <racIpAddr>:<port>	Use <port number> if the CMC port number is not the default port (443)

Table 4-2. Remote RACADM Subcommand Options (*continued*)

Option	Description
-i	Instructs RACADM to interactively query the user for user name and password.
-u <usrName>	Specifies the user name that is used to authenticate the command transaction. If the -u option is used, the -p option must be used, and the -i option (interactive) is not allowed.
-p <password>	Specifies the password used to authenticate the command transaction. If the -p option is used, the -i option is not allowed.

To access RACADM remotely, type the following commands:

```
racadm -r <CMC IP address> -u <username> -p <password>  
<subcommand> <subcommand options>
```

```
racadm -i -r <CMC IP address> <subcommand> <subcommand  
options>
```



NOTE: The **-i** option instructs RACADM to interactively prompt for user name and password. Without the **-i** option, you must provide the user name and password in the command using the **-u** and **-p** options.

For example:

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

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

```
racadm -r <CMC IP address>:<port> -u <username> -p  
<password> <subcommand> <subcommand options>  
racadm -i -r <CMC IP address>:<port> <subcommand>  
<subcommand options>
```

Enabling and Disabling the RACADM Remote Capability

 **NOTE:** Dell recommends that you run these commands at the chassis.

The RACADM remote capability on the CMC is enabled by default. In the following commands, `-g` specifies the configuration group the object belongs to, and `-o` specifies the configuration object to configure.

To disable the RACADM remote capability, type:

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

To re-enable RACADM remote capability, type:

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

Using RACADM Remotely

 **NOTE:** Configure the IP address on your CMC before using the RACADM remote capability. For more information about setting up your CMC, see "Installing and Setting Up the CMC" on page 29.

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

Before you try to access RACADM remotely, confirm that you have permissions to do so. To display your user privileges, type:

```
racadm getconfig -g cfguseradmin -i n
```

where *n* is your user ID (1–16).

If you do not know your user ID, try different values for *n*.

 **NOTE:** The RACADM remote capability is supported only on management stations through a supported browser. For more information, see the Supported Browsers section in the *Dell Systems Software Support Matrix* on the Dell Support website at support.dell.com/manuals.

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

```
racadm getconfig -f <file name> -r <IP address>
```

or

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

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
```

RACADM Error Messages

For information about RACADM CLI error messages, see "Troubleshooting" on page 101.

Using RACADM to Configure the CMC

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

The CMC Web interface is the quickest way to configure the CMC (see "Using the CMC Web Interface" on page 103). However, if you prefer CLI or script configuration or need to configure multiple CMCs, use Remote RACADM, which is installed with the CMC agents on the management station.

Configuring CMC Network Properties

Before you can 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.

Setting Up Initial Access to the CMC

This section explains how to perform the initial CMC network configuration using RACADM commands. All of the configuration described in this section can be performed using the front panel LCD. See "Configuring Networking Using the LCD Configuration Wizard" on page 41.

 **CAUTION:** Changing settings on the CMC Network Settings screen may disconnect your current network connection.

For more information about network subcommands, see the RACADM Subcommands and Property Database Group and Object Definitions chapters of the *Command Line Reference Guide for iDRAC6 and CMC*.

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

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

Viewing Current IPv4 Network Settings

To view a summary of NIC, DHCP, network speed, and duplex settings, type:

```
racadm getniccfg
```

or

```
racadm getconfig -g cfgCurrentLanNetworking
```

Viewing Current IPv6 Network Settings

To view a summary of the network settings, type:

```
racadm getconfig -g cfgIpv6LanNetworking
```

To view IPv4 and IPv6 addressing information for the chassis type:

```
racadm getsysinfo
```

By default, the CMC requests and obtains a CMC IP address from the Dynamic Host Configuration Protocol (DHCP) server automatically.

You can disable this feature and specify static CMC IP address, gateway, and subnet mask.

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>
```

Viewing Current Network Settings

To view a summary of NIC, DHCP, network speed, and duplex settings, type:

```
racadm getniccfg
```

or

```
racadm getconfig -g cfgCurrentLanNetworking
```

To view IP address and DHCP, MAC address, and DNS information for the chassis, type:

```
racadm getsysinfo
```

Configuring the Network LAN Settings

-  **NOTE:** To perform the following steps, you must have **Chassis Configuration Administrator** privilege.
-  **NOTE:** The LAN settings, such as community string and SMTP server IP address, affect both the CMC and the external settings of the chassis.
-  **NOTE:** 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.
-  **NOTE:** 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.

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 the CMC" on page 78.

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 DHCP 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 up the CMC VLAN (IPv4 and IPv6)

- 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
```

Removing the CMC VLAN

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
```

Setting up a Server VLAN

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 id> 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
```

Removing a Server VLAN

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 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.

Setting the SMTP Server IP Address (IPv4 and IPv6)

You can enable the CMC to send e-mail alerts using Simple Mail Transfer Protocol (SMTP) to a specified IP address. To enable this feature, type:

```
racadm config -g cfgRemoteHosts -o  
cfgRhostsSmtpServerIpAddr <SMTP IP address>
```

where <SMTP IP address> is the IP address of the network SMTP server.



NOTE: 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 the Network Security Settings (IPv4 Only)



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

Enabling IP Range Checking (IPv4 Only)

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`

Using RACADM to Configure Users

Before You Begin

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 you ran the RACADM `racresetcfg` command, the only current user is `root` with the password `calvin`. The `racresetcfg` subcommand resets the CMC back to the original defaults.



CAUTION: Use caution when using the `racresetcfg` command, because it 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>
```

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

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

If the `cfgUserAdminUserName` object has no value, that index number, which is indicated by the `cfgUserAdminIndex` object, is available for use. If a name appears after the "=", that index is taken by that user name.



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

Adding a CMC User

To add a new user to the CMC configuration, you can use a few basic commands. Perform the following procedures:

- 1 Set the user name.
- 2 Set the password.
- 3 Set user privileges. For information about user privileges, see Table 5-40, and Table 5-41 in the database property chapter of the *Command Line Reference Guide for iDRAC6 and CMC*.
- 4 Enable the user.

Example

The following example describes how to add a new user named "John" with a "123456" password and LOGIN privilege to the CMC.



NOTE: See Table 3-1 in the database property chapter of the *Command Line Reference Guide for iDRAC6 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, type the following command:

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

Using RACADM to Configure Public Key Authentication over SSH

Before You Begin

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.

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

- 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 *Command Line Reference Guide for iDRAC6 and CMC*.

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.

Follow the instructions. 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 not have access to the public keys entered using the `sshpkauth` command.

Viewing the Public Keys

To view public keys that you have added to the CMC, type:

```
racadm sshpkauth -i svcacct -k all -v
```

To view just 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 the Public Keys

To add a public key to the CMC using the file upload (-f) option, type:

```
racadm sshpkauth -i svcacct -k 1 -p 0xffff -f <public key file>
```



NOTE: You can only use the file upload option with remote RACADM. For more information, see "Accessing RACADM Remotely" on page 74 and subsequent sections.

For public key privileges, see Table 3-1 in the Database Property chapter of *Dell Chassis Management Controller Administrator Reference Guide*.

To add a public key using the text upload option, type:

```
racadm sshpkauth -i svcacct -k 1 -p 0xffff -t "<public key text>"
```

Deleting the 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
```

Logging in Using Public Key Authentication

After the public keys are uploaded, you should be able to log into the CMC over SSH without having to enter a password. You also have the option of sending a single RACADM command as a command line argument to the SSH application. The command line options behave like remote RACADM since the session ends after the command is completed. For example:

Logging in:

```
ssh service@<domain>
```

Or

```
ssh service@<IP_address>
```

where <IP_address> is the IP address of the CMC.

Sending racadm commands:

```
ssh service@<domain> racadm getversion
```

```
ssh service@<domain> racadm getsel
```

When you log in using the service account, if a passphrase was set up when creating the public/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 ssh-agent. For setting up and using either of these applications, see the documentation provided from that application.

Enabling a CMC User With Permissions

To enable a user with specific administrative permissions (role-based authority), first locate an available user index by performing the steps in "Before You Begin" on page 87. Next, type the following command lines with the new user name and password.

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



NOTE: See Table 3-1 in the Database Property chapter of the *Dell Chassis Management Controller Administrator Reference Guide* 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.

Disabling a CMC User

Using RACADM, you can only disable CMC users manually and on an individual basis. You cannot delete users by using a configuration file.

The following example illustrates the command syntax that can be used to delete a CMC user:

```
racadm config -g cfgUserAdmin -i 2  
cfgUserAdminPrivilege 0x0
```

Configuring SNMP and E-mail Alerting

You can configure the CMC to send SNMP event traps and/or e-mail alerts when certain events occur on the chassis. For more information and instructions, see "Configuring SNMP Alerts" on page 379 and "Configuring E-mail Alerts" on page 385.

You can specify the trap destinations as appropriately-formatted numeric addresses (IPv6 or IPv4), or Fully-qualified domain names (FQDNs). Choose a format that is consistent with your networking technology/infrastructure.

 **NOTE:** The **Test TRAP** functionality does not detect improper choices based on current network configuration. For example, using an IPv6 destination in an IPv4-only environment.

Configuring Multiple CMCs in Multiple Chassis

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.

 **NOTE:** 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. For more information see "Accessing RACADM Remotely" on page 74.

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.

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 *Command Line Reference Guide for iDRAC6 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. See the database property chapter of the *Command Line Reference Guide for iDRAC6 and CMC* for a complete list of objects and groups.



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.

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 *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>
```

If you type `racadm getconfig -f <myexample>.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.

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.

Using RACADM to Configure Properties on iDRAC

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

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



NOTE: For more information on the property default values and ranges, see the *Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers User Guide*.

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
# cfgSsnMgtSSTimeout=N/A
# cfgSsnMgtTelnetMaxSessions=N/A
# cfgSsnMgtTelnetActiveSessions=N/A
# cfgSsnMgtTelnetTimeout=N/A
```

Troubleshooting

Table 4-3 lists common problems related to remote RACADM.

Table 4-3. Using Serial/ RACADM Commands: Frequently Asked Questions

Question	Answer
After performing a CMC reset (using the RACADM <code>racreset</code> subcommand), I enter a command and the following message is displayed: <code>racadm <subcommand></code> <code>Transport: ERROR:</code> <code>(RC=-1)</code> What does this message mean?	You must wait until the CMC completes the reset before issuing another command.
When I use the RACADM subcommands, I get errors that I do not understand.	You may encounter one or more of the following errors when using RACADM: <ul style="list-style-type: none">• Local error messages — Problems such as syntax, typographical errors, and incorrect names. Example: <code>ERROR: <message></code> Use the RACADM <code>help</code> 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 <code>racadm gettracelog</code> for debugging information.

Table 4-3. Using Serial/ RACADM Commands: Frequently Asked Questions (continued)

Question	Answer
While I was using remote RACADM, the prompt changed to a ">" and I cannot get the "\$" prompt to return.	If you type a non-matched double quotation mark (") or a non-matched single quotation (') in the command, the CLI changes to the ">" prompt and queue all commands. To return to the "\$" prompt, type <Ctrl>-d.
I tried using the following commands and received an error saying "Not Found": \$ logout \$ quit	The logout and quit commands are not supported in the CMC CLI interface.

Using the CMC Web Interface

CMC provides a Web interface that enables you to configure CMC properties and users, perform remote management tasks, and troubleshoot a remote (managed) system for problems. For everyday chassis management, use the CMC Web interface. This chapter provides information about how to perform common chassis management tasks using the CMC Web interface.

You can also perform all configuration tasks using local RACADM commands or command line consoles (serial console, Telnet, or SSH). For more information about using local RACADM, see "Using the RACADM Command Line Interface" on page 69. For information on using command line consoles, see "Configuring CMC to Use Command Line Consoles" on page 55.



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

Accessing the CMC Web Interface

To access the CMC Web interface over IPv4:

- 1 Open a supported Web browser window.

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

- 2 Type the following URL in the Address field, and then press <Enter>:

```
https://<CMC IP address>
```

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

```
https://<CMC IP address>:<port number>
```

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

The CMC Login page appears.

To access the CMC Web interface over IPv6:

- 1 Open a supported Web browser window.

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

- 2 Type the following URL in the **Address** field, and then press <Enter>:

`https://[<CMC IP address>]`

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

Specifying the HTTPS port number in the URL is optional if you are still using the default value (443). Otherwise, you must specify the port number. The syntax for the IPv6 CMC URL with the port number specified is:

`https://[<CMC IP address>]:<port number>`

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

The CMC **Login** page appears.

Logging In

 **NOTE:** To log in to CMC, you must have a CMC account with **Log In to CMC** privilege.

 **NOTE:** The default CMC user name is **root**, and the password is **calvin**. The root account is the default administrative account that ships with CMC. For added security, it is strongly recommended that you change the default password of the root account during initial setup.

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

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

You can log in as either a CMC user or as a Directory user.

To log in:

- 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.
- 2 In the **Password** field, type your CMC user password or Active Directory 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. See *Configuring Services* for more details.
- 4 Click **OK** or press `<Enter>`.

Logging Out

When you are logged in to the Web interface, you can log out at any time by clicking **Logout** in the upper right corner of any page.

 **NOTE:** Be careful to apply (save) any settings or information you enter on a page. If you log out or navigate away from that page without applying your changes, the changes are lost.

Configuring Basic CMC Settings

Setting the Chassis Name

You can set the name used 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.

To set the chassis name:

- 1 Log in to the CMC Web interface. The **Chassis Health** page displays.
- 2 Click the **Setup** tab. The **General Chassis Settings** page displays.
- 3 Type the new name in the **Chassis Name** field, and then click **Apply**.

Setting the 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.

- 1 Log in to the CMC Web interface. The **Chassis Health** page displays.
- 2 Click the **Setup** tab. The **General Chassis Settings** page displays.
- 3 Click the **Date/Time** subtab. The **Date/Time** page displays.
- 4 To synchronize the date and time with a Network Time Protocol (NTP) server, check **Enable NTP** and specify up to three NTP servers.
- 5 To set the date and time manually, uncheck **Enable NTP** and edit the **Date** and **Time** fields, select the **Time Zone** from the drop-down menu, and then click **Apply**.

To set the date and time using the command line interface, see the `config` command and `cfgRemoteHosts` database property group sections in the *Command Line Reference Guide for iDRAC6 and CMC*.

Chassis Health Page

When you log in to CMC, the **Chassis Health** page (**Chassis Overview**→**Properties**→**Health**) is displayed. The most frequently needed information and actions are available on this page. If your chassis is configured as a Group Lead, the **Group Health** page is displayed after login. For additional information, see "Using Chassis Group" on page 107.

The **Chassis Health** page displays a live graphical view of the chassis and its components, as well as the details of the components. Depending on the selected component, various actions or links to other pages are available. In addition, the latest events in the CMC Hardware Log are also displayed.

All information on the **Chassis Health** page is dynamically updated. This page contains two major sections: **Chassis Component Summary** at the top followed by the **Recent CMC Hardware Log Events** listing.

The **Chassis Component Summary** section (also entitled "Chassis Health" when the overall chassis information is shown) displays the graphics and their associated information. You can hide this entire section by clicking the **Close** icon.

The left half of the **Chassis Component Summary** section displays the graphics and Chassis **Quick Links**. The right half of this section displays information, links, and actions related to the selected component. Click the graphical representation of a component to select the component. The graphic is cast in blue after selection.

The **Recent CMC Hardware Log Events** list displays the latest 10 events from this log. The content of this section is dynamically updated and presented with the latest event at the top of the list. For more information on CMC Hardware Log entries, see "Viewing the Event Logs" on page 398.

Using 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.

Chassis Group Features

The Chassis Group GUI 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 the **Details** button.

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 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.

Setting up a Chassis Group

The Chassis Group is set up with the GUI:

- 1 Log in with 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 GUI 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.

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 Select the **Apply** button.
- 8 Repeat step 4 through step 7 to add a maximum of eight members.
The new members' Chassis Names appear in the dialog box labeled **Members**.

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 from the dialog box. 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. See the sub-section “Disabling an Individual Member at the Member Chassis” for the procedure.

Disbanding a Chassis Group

It is also possible to completely disband a group from the lead chassis. To do this:

- 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. See the sub-section “Disabling an Individual Member at the Member Chassis” for the procedure.

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. A member can be removed from a group at the member chassis by:

- 1 Login with chassis administrator privileges to the member chassis.
- 2 Click **Setup**→ **Group Administration**.
- 3 Select **None**, and then click **Apply**.

Chassis Component Summary

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. The server icon is used in Table 5-1 as an example. 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 5-1. 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.

Table 5-1. Server Icon States

Icon	Description
	No server is present.

The Chassis Quick Links are displayed below the Chassis Graphics.

Table 5-2. Chassis Quick Links

Field	Description
Configure Users	Navigate to Chassis Overview→ User Authentication→ Local Users
Network Configuration	Navigate to Chassis Overview→ Network→ Network
Power Configuration	Navigate to Chassis Overview→ Power→ Configuration
Firmware Update	Navigate to Chassis Overview→ Update→ Firmware Update

Chassis Health

When the page first displays, the right side of the page contains the chassis level information and alerts. All active critical and non-critical alerts are displayed.

When a component is clicked, the chassis level information is replaced with a display of information for the selected component. To return to the chassis level information, click **Return to Chassis Health** in the upper right corner.

Table 5-3. Chassis Page Information

Field	Description
Model	Displays the model of the Chassis LCD panel.
Firmware	Displays the firmware version of the active CMC.
Service Tag	Displays the service tag of the chassis. The service tag is a unique identifier that the manufacturer provides for support and maintenance.
Asset Tag	Displays the asset tag for the chassis.
Input Power	Amount of power that the chassis consumes presently.
Power Cap	User-assigned maximum Input Power to be consumed. As the chassis reaches this limit, servers begin to throttle to prevent a further rise in the required Input Power.
Power Policy	User-assigned preference for coordinating multiple Power Supply Units.
Health	Displays the overall health of the chassis power subsystem.

Selected Component Information

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

- **Health and Performance and Properties**
The Active Critical and Non-Critical events as shown by the hardware logs are displayed here, if there are any. Performance data which vary with time are also shown here.
- **Properties**
Component properties which do not vary with time or change only infrequently are displayed here.
- **Quick Links**
The Quick Links section provides a convenient means of navigation 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.

Table 5-4. Health and Performance Information - Servers

Item	Description
Power State	On/Off state of the server. See Table 5-23 for details on the various types of power states.
Health	Displays the text equivalent of the health icon.
Power Consumption	Amount of power that the server consumes at present.
Power Allocated	Amount of power budgeted for the server.
Temperature	Temperature read from the server temperature sensor.

Table 5-5. Server Properties

Item	Description
Name	User-assigned slot name.
Model	Server model, for example "PowerEdge M600" or "PowerEdge M605".
Service Tag	The service tag of the server. The service tag is a unique identifier that the manufacturer provides for support and maintenance. If the server is absent, this field is empty.
OS	Operating system on the server.
Host Name	Name of the server as established by the operating system.
iDRAC	Version of iDRAC firmware on the server.
BIOS	Server BIOS version.
CPLD	Version number of Complex Programmable Logic Device (CPLD) of the server.

Table 5-6. Quick Links - Servers

Item	Description
Server Status	Navigate to Server Overview → <selected server>→ Properties → Status
Launch Remote Console	Invokes a Keyboard-Video-Mouse (KVM) session on the server if the server supports this operation.
Launch iDRAC GUI	Invokes an iDRAC management console for the server.
Power On Server	Apply power to a server that is in the "Off" state.
Power Off Server	Remove power from a server that is in the "On" state.
Remote File Share	Navigate to Server Overview → Setup → Remote File Share
Deploy iDRAC Network	Navigate to Server Overview → Setup → iDRAC (Deploy iDRAC)

Table 5-7. IOM Health and Performance

Item	Description
Power State	Displays the power status of the I/O module: On, Off, or Unknown (Absent).
Role	Displays the I/O Module stacking membership while linking I/O modules together. Member indicates that the module is part of a stack set. Master indicates that the module is a primary access point.

Table 5-8. IOM Properties

Item	Description
Model	Displays the I/O module product name.
Service Tag	Displays the service tag of the I/O module. The service tag is a unique identifier provided by Dell for support and maintenance.

Table 5-9. Quick Links - I/O Modules

Item	Description
IOM Status	Navigate to I/O Modules → <Selected IOM>→ Properties → Status
Launch IOM GUI	If the <i>Launch IOM GUI</i> link is present for a particular I/O module, clicking it launches the IOM management console for that I/O module in a new browser window or tab.

Table 5-10. Active CMC Health and Performance

Item	Description
Redundancy Mode	Displays failover readiness of the standby CMC. If CMC firmware does not match, or CMC is not cabled properly to the management network, redundancy appears as not available
MAC Address	Displays the MAC address for the CMC Network Interface Card (NIC). The MAC address is a unique identifier for the CMC over the network.
IPv4	Displays the current IPv4 address for the CMC Network Interface.
IPv6	Displays the first IPv6 address for the CMC Network Interface.

Table 5-11. CMC Properties

Item	Description
Firmware	Displays the firmware version of the active CMC.
Standby Firmware	Displays the firmware version installed on the standby CMC. If you have not installed a second CMC, this field is displayed NA.
Last Updated	Displays when the firmware was last updated. If no updates have occurred, this field is displayed as NA.
Hardware	Displays the hardware version of the active CMC.

Table 5-12. Quick Links - CMC

Item	Description
CMC Status	Navigate to Chassis Controller → Properties → Status
Networking	Navigate to Chassis Overview → Network → Network
Firmware Update	Navigate to Chassis Overview → Update → Firmware Update

Table 5-13. iKVM Health and Performance

Item	Description
OSCAR Console	Displays whether the rear panel VGA connector is enabled (Yes or No) for access to CMC.

Table 5-14. iKVM Properties

Item	Description
Name	Displays the name of the iKVM.
Part Number	Displays the part number for the iKVM. The part number is a unique identifier provided by the vendor. Part number naming conventions differ from vendor to vendor.
Firmware	Displays the firmware version of the iKVM.
Hardware	Displays the hardware version of the iKVM.

Table 5-15. Quick Links - iKVM

Item	Description
iKVM Status	Navigate to iKVM → Properties → Status
Firmware Update	Navigate to Chassis Overview → Update → Firmware Update

Table 5-16. Fan Health and Performance

Item	Description
Speed	Displays the speed of the fan in revolutions per minute (RPM).

Table 5-17. Fan Properties

Item	Description
Lower Critical Threshold	Speed below which the fan is considered to have failed.
Upper Critical Threshold	Speed above which the fan is considered to have failed.

Table 5-18. Quick Links - Fan

Item	Description
Fan Status	Navigate to Fans → Properties → Status

Table 5-19. PSU Health and Performance

Item	Description
Power Status	Displays the power state of the power supplies (one of the following): Initializing, Online, Standby, In Diagnostics, Failed, Updating, Offline, or Unknown.

Table 5-20. PSU Properties

Item	Description
Capacity	Displays the capacity of the power supply (in Watts).

Table 5-21. Quick Links - PSU

Item	Description
Power Supply Status	Navigate to Power Supplies → Properties → Status
Power Consumption	Navigate to Chassis Overview → Power → Power Consumption
System Budget	Navigate to Chassis Overview → Power → Budget Status

Table 5-22. LCD Health and Performance

Item	Description
LCD Health	Displays the presence and health of the LCD panel.
Chassis Health	Displays the text description of Chassis Health.

There are no Quick Links for the LCD.

Monitoring System Health Status

Viewing Chassis and Component Summaries

CMC displays a graphical representation of the chassis on the **Chassis Health** page that provides a visual overview of installed component status. The **Chassis Health** page is dynamically updated, and the component subgraphic overlays and text hints are automatically changed to reflect the current state.

Figure 5-1. Example of Chassis Graphics in the Web Interface



The **Chassis Health** page provides an overall health status for the chassis, active and standby CMCs, server modules, IO Modules (IOMs), fans, iKVM, power supplies (PSUs), and LCD assembly. More detailed information for each component is displayed by clicking on that component. For instructions on viewing chassis and components summaries, see "Viewing Chassis Summaries" on page 392.

Viewing Power Budget Status

The **Power Budget Status** page displays the power budget status for the chassis, servers, and chassis power supply units (PSUs).

For instructions on viewing power budget status, see "Viewing Power Consumption Status" on page 311. For more information about CMC power management, see "Power Management" on page 289.

Viewing Server Model Name and Service Tag

The Model Name and Service Tag of each server can be obtained instantly using the following steps:

- 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.
- 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 the Health Status of All Servers

You can view the health status for all servers from the **Chassis Graphics** section on the **Chassis Health** page or the **Servers Status** page.

The Chassis Graphics provides a graphical overview of all servers installed in the chassis.

To view health status for all servers using Chassis Graphics:

- 1 Log in to the CMC Web interface.

The **Chassis Health** page is displayed. The left section of **Chassis Graphics** depicts the front view of the chassis and contains the health status of all servers. Server health status is indicated by the overlay of the server subgraphic:

- No overlay - server is present, powered on and communicating with CMC; there is no indication of an adverse condition.
- Amber caution sign - indicates that only warning alerts have been issued and that corrective action must be taken.
- Red X - indicates at least one failure condition is present. This means that CMC can still communicate with the component and the health status reported is critical.
- Grayed out - indicates that the component is present and not powered on. It is not communicating with CMC and there is no indication of an adverse condition.

The **Servers Status** page provides overviews of the servers in the chassis. To view health status for all servers using the Servers Status page:

- 1 Log in to the CMC Web interface.
- 2 Select **Server Overview** in the system tree. The **Servers Status** page appears.

Table 5-23. All Servers Status Information

Item	Description
Slot	Displays the location of the server. The slot number is a sequential number that identifies the server by its location within the chassis.
Name	Displays the name of the server, which by default is identified by its slot name (SLOT-01 to SLOT-16). NOTE: You can change the default server name. For instructions, see "Editing Slot Names" on page 124.
Model	Displays the server's model name. If this field is blank, the server is not present. If this field displays Extension of # (where the value of # is 1-8), the number # is the main slot of a multi-slot server.

Table 5-23. All Servers Status Information (continued)

Item	Description
Health	 OK Displays that the server is present and communicating with CMC. In the event of a communication failure between CMC and the server, CMC cannot obtain or display health status for the server.
	 Informational Displays information about the server when no change in health status (OK, Warning, Critical) has occurred.
	 Warning Displays that only warning alerts have been issued, and <i>corrective action must be taken</i> . If corrective actions are not taken, then critical failures that can affect the integrity of the server may occur.
	 Critical Displays that at least one Failure alert has been issued. Critical status represents a system failure on the server, and <i>corrective action must be taken immediately</i> .
	No Value When the server is absent from the slot, health information is not provided.
Launch Remote Console	<p>Click to launch a Keyboard-Video-Mouse (KVM) session on the server in a new browser window or tab. This icon is only displayed for a server where all of the following conditions are met:</p> <ul style="list-style-type: none"> • Server is PowerEdge M610, M610X, M710, M710HD, or M910. • The chassis power is on. • The LAN interface on the server is enabled. • The iDRAC version is 2.20 or later. <p>This feature functions correctly only if the following conditions are met:</p> <ul style="list-style-type: none"> • 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).

Table 5-23. All Servers Status Information (continued)

Item	Description
Launch iDRAC GUI	<p data-bbox="303 280 978 363">Left click the button to launch the iDRAC management console for a server in a new browser window or tab. This icon is only displayed for a server where all of the following conditions are met:</p> <ul data-bbox="311 379 751 483" style="list-style-type: none"><li data-bbox="311 379 535 403">• The server is present.<li data-bbox="311 419 563 443">• The chassis power is on.<li data-bbox="311 459 751 483">• The LAN interface on the server is enabled. <p data-bbox="303 499 945 555">This feature functions correctly only if the following condition is met:</p> <ul data-bbox="311 571 829 627" style="list-style-type: none"><li data-bbox="311 571 829 627">• The browser on host system allows pop-up windows (pop-up blocking is disabled). <p data-bbox="303 643 978 751">NOTE: If the server is removed from the chassis, the IP address of iDRAC is changed, or the network connection on iDRAC experiences any problems, then clicking the Launch iDRAC GUI icon may display an error page on the iDRAC LAN interface.</p>
Power State	<p data-bbox="303 770 692 794">Displays the power status of the server:</p> <ul data-bbox="311 810 958 1058" style="list-style-type: none"><li data-bbox="311 810 958 834">• N/A - CMC has not yet determined the power state of the server.<li data-bbox="311 850 792 874">• Off - Either the server is off or the chassis is off.<li data-bbox="311 890 675 914">• On - Both chassis and server are on.<li data-bbox="311 930 958 986">• Powering On - Temporary state between Off and On. When the action completes successfully, the Power State is On.<li data-bbox="311 1002 958 1058">• Powering Off - Temporary state between On and Off. When the action completes successfully, the Power State is Off.
Service Tag	<p data-bbox="303 1074 947 1161">Displays the service tag for the server. The service tag is a unique identifier provided by the manufacturer for support and maintenance. If the server is absent, this field is empty.</p>

For information on how to launch the iDRAC management console and single sign-on policies, see "Launching iDRAC using Single Sign-On" on page 203.

Editing Slot Names

The **Slot Names** page allows you to update slot names in the chassis. 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.



NOTE: 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.



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



NOTE: 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:

- 1 Log in to the CMC Web interface.
- 2 Select **Server Overview** in the **Chassis** menu in the system tree.
- 3 Click **Setup** → **Slot Names**. The **Slot Names** page displays.
- 4 Type the updated or new name for a slot in the **Slot Name** field. Repeat this action for each slot you want to rename.
- 5 Click **Apply**.
- 6 To restore the default slot name (SLOT-01 to SLOT-16, based on the server's slot position) to the server, press **Restore Default Value**.

Using Server's Host Name as the Slot Name

The **Slot Names** page allows to 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. See the *Dell OpenManage Server Administrator User's Guide* for more details on the OMSA agent.

To use server's host name as slot name:

- 1 Log in to the CMC Web interface.
- 2 Select **Server Overview** in the **Chassis** menu from the system tree.
- 3 Click **Setup** → **Slot Names**. The **Slot Names** page displays.
- 4 Select the **Use Host Name for the Slot Name** check box.
- 5 Click **Apply**.

Setting the First Boot Device for Servers

The **First Boot Device** page allows you to 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 you can also set a one-time boot device so that you can boot a special image to perform tasks such as running diagnostics or reinstalling an operating system.

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

Table 5-24. 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 the M610/M710/M805/M905 systems only.
Floppy	Boot from a floppy disk in the local floppy disk drive.

 **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 some or all servers in the chassis:

- 1 Log in to the CMC Web interface.
- 2 Click **Server Overview** in the system tree and then click **Setup**→ **First Boot Device**. A list of servers is displayed as one per row.
- 3 Select the boot device you want to use for each server from the list box.
- 4 If you want the server to boot from the selected device every time it boots, clear the **Boot Once** check box for the server.
If you want the server to boot from the selected device only on the next boot cycle, select the **Boot Once** check box for the server.
- 5 Click **Apply**.

Viewing the Health Status of an Individual Server

The health status for an individual server can be viewed in two ways: from the **Chassis Graphics** section on the **Chassis Health** page or the **Server Status** page.

The **Chassis Health** page provides a graphical overview of an individual server installed in the chassis.

To view health status for individual servers using Chassis Graphics:

- 1 Log in to the CMC Web interface.

The **Chassis Health** page is displayed. The top section of **Chassis Graphics** depicts the front view of the chassis and contains the health status for individual servers. Server health status is indicated by the overlay of the server subgraphic:

- No overlay - indicates that the server is present, powered on and communicating with the CMC; there is no indication of an adverse condition.
- Amber caution sign - indicates that only warning alerts have been issued and that corrective action must be taken.
- Red X - indicates at least one failure condition is present. This means that CMC can still communicate with the component and that the health status is reported as critical.
- Grayed out - indicates that the component is present and not powered on. It is not communicating with CMC and there is no indication of an adverse condition.

- 2 Move the cursor to hover over an individual server subgraphic.

A corresponding text hint or screen tip is displayed. The text hint provides additional information on that server.

- 3 Click the server subgraphic to select that server's information and display Quick Links on the right of the chassis graphics.

The **Server Status** page (separate from the *Servers Status* page) provides an overview of the server and a launch point to the Web interface for the Integrated Dell Remote Access Controller (iDRAC), which is the firmware used to manage the server.

 **NOTE:** To use the iDRAC user 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 Firmware User's Guide*.

To view the health status of an individual server:

- 1 Log in to the CMC Web interface.
- 2 Expand **Server Overview** in the system tree. All of the servers (1–16) appear in the expanded **Servers** list.
- 3 Click the server (slot) you want to view. The **Server Status** page displays.

You can also view the server status page by clicking the status link in the server **Quick Links** on the right side of the page.

Table 5-25. Individual Server Status - Properties

Item	Description
Slot	Displays the slot occupied by the server on the chassis. Slot numbers are sequential IDs, from 1 through 16 (there are 16 slots available on the chassis), that help identify the location of the server in the chassis.
Slot Name	Displays the name of the slot where the server resides.
Present	Displays whether the server is present in the slot (Yes or No). When the server is absent, the health, power state, and service tag information of the server is unknown (not displayed).

Table 5-25. Individual Server Status - Properties (continued)

Item	Description
Health	 OK Displays that the server is present and communicating with CMC. In the event of a communication failure between CMC and the server, CMC cannot obtain or display health status for the server.
	 Informational Displays information about the server when no change in health status (OK, Warning, Critical) has occurred.
	 Warning Displays that only warning alerts have been issued, and <i>corrective action must be taken</i> . If corrective actions are not taken, then critical failures that can affect the integrity of the server may occur.
	 Critical Displays that at least one Failure alert has been issued. Critical status represents a system failure on the server, and <i>corrective action must be taken immediately</i> .
	No Value When the server is absent from the slot, health information is not provided.
Server Model	Displays the model of the server in the chassis. Examples: PowerEdge M600 , PowerEdge M605 .
Service Tag	Displays the service tag for the server. The service tag a unique identifier provided by the manufacturer for support and maintenance. If the server is absent, this field is empty.
iDRAC Firmware	Displays the iDRAC version currently installed on the server.
CPLD Version	Displays the version number of Complex Programmable Logic Device (CPLD) of the server.
BIOS version	Displays the BIOS version on the server.
Operating System	Displays the operating system on the server.

Table 5-26. Individual Server Status - iDRAC System Event Log

Item	Description
Severity	 OK Indicates a normal event that does not require corrective actions.
	 Informational Indicates an informational entry on an event in which the Severity status has not changed.
	 Unknown Indicates an unknown/uncategorized event.
	 Warning Indicates a non-critical event for which corrective actions must be taken soon to avoid system failures.
	 Critical Indicates a critical event requiring immediate corrective actions to avoid system failures.
Date/Time	Displays the exact date and time the event occurred (for example, Wed May 02 16:26:55 2007).
Description	Provides a brief description of the event.

Table 5-27. Individual Server Status - iDRAC Network Settings

Item	Description
LAN Enabled	Indicates if the LAN channel is Enabled (Yes) or disabled (No).

Table 5-28. Individual Server Status - IPv4 iDRAC Network Settings

Item	Description
Enabled	Indicates if the IPv4 protocol is used on the LAN (Yes). If the server does not support IPv6, the IPv4 protocol is always enabled and this setting is not displayed.
DHCP Enabled	Indicates whether Dynamic Host Configuration Protocol (DHCP) is enabled (Yes) or disabled (No). If this option is enabled (Yes), the server retrieves IP configuration (IP address, subnet mask, and gateway) automatically from a DHCP server on your network. The server always has a unique IP Address allotted over your network.
IPMI over LAN Enabled	Indicates if the IPMI LAN channel is Enabled (Yes) or disabled (No).
IP Address	Specifies the IP address for the iDRAC network interface.
Subnet Mask	Specifies the subnet mask for the iDRAC network interface.
Gateway	Specifies the gateway for the iDRAC network interface.

Table 5-29. Individual Server Status - IPv6 iDRAC Network Settings

Item	Description
Enabled	Indicates if the IPv6 protocol is used on the LAN (Yes).
Autoconfiguration Enabled	Indicates if Autoconfiguration for IPv6 is enabled (Yes). If Autoconfiguration is enabled, the server retrieves IPv6 configuration (IPv6 address, Prefix Length, and IPv6 Gateway) automatically from an IPv6 router on your network. The server always has a unique IPv6 address over your network, and may be given up to 16 IPv6 addresses.
Link Local Address	IPv6 address assigned to CMC based upon the MAC address of CMC.
Gateway	Displays the IPv6 gateway for the iDRAC network interface.
IPv6 Address	Displays an IPv6 address for the iDRAC network interface. There may be up to 16 of these addresses. The prefix length, if nonzero, is given after a forward slash ("/").

Table 5-30. Individual Server Status - WWN/MAC Address

Item	Description
Slot	Displays the slot(s) occupied by the server on the chassis.
Location	Displays the location occupied by the Input/Output modules. The six locations are identified by a combination of the group name (A, B, or C) and slot number (1 or 2). Location names are: A1, A2, B1, B2, C1, or C2.
Fabric	Displays the type of the I/O fabric.
Server-Assigned	Displays the server-assigned WWN/MAC addresses embedded in the controller's hardware. WWN/MAC addresses showing N/A indicate that an interface for the specified fabric is not installed.
Chassis-Assigned	Displays the chassis-assigned WWN/MAC addresses used for the particular slot. WWN/MAC addresses showing N/A indicate that the FlexAddress feature is not installed. NOTE: A green check mark in the Server-Assigned and Chassis-Assigned columns indicates the type of active addresses. NOTE: When FlexAddress is enabled, slots without servers installed display the Chassis-Assigned MAC/WWN assignment for the embedded Ethernet controllers (Fabric A). The Chassis-Assigned addresses for fabrics B and C display N/A, unless these fabrics are in use on servers in populated slots; it is assumed that the same fabric types are deployed in the unpopulated slots.

For information on how to launch the iDRAC management console and single sign-on policies, see "Launching iDRAC using Single Sign-On" on page 203.

Viewing the Health Status of IOMs

The health status for the IOMs can be viewed in two ways: from the **Chassis Component Summary** section on the **Chassis Health** page or the **I/O Modules Status** page. The **Chassis Health** page provides a graphical overview of the IOMs installed in the chassis.

To view health status of the IOMs using Chassis Graphics:

- 1 Log in to the CMC Web interface.

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:

- No overlay - IOM is present, powered on and communicating with CMC; there is no indication of an adverse condition.
- Amber caution sign - indicates that only warning alerts have been issued and that corrective action must be taken.
- Red X - indicates at least one failure condition is present. This means that CMC can still communicate with the component and that the health status reported is critical.
- Grayed Out - indicates that the IOM is present and not powered on. It is not communicating with CMC and there is no indication of an adverse condition.

- 2 Use the cursor to hover over an individual IOM subgraphic.

A text hint or screen tip is displayed. The text hint provides additional information on that IOM.

- 3 Clicking the IOM subgraphic selects that IOM's information and **Quick Links** for display to the right of the chassis graphics.

The **I/O Modules Status** page provides overviews of all IOMs associated with the chassis. For instructions on viewing IOM health through the Web interface or RACADM, see "Monitoring IOM Health" on page 365.

Viewing the Health Status of the Fans



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.

The health status of the fans can be viewed in two ways: from the **Chassis Component Summary** section on the **Chassis Health** page or the **Fans Status** page. The **Chassis Health** page provides a graphical overview of all fans installed in the chassis.

To view health status for all fans using **Chassis Graphics**:

- 1 Log in to the CMC Web interface.

The **Chassis Health** page is displayed. The lower section of **Chassis Graphics** depicts the rear view of the chassis and contains the health status of all fans. Fan health status is indicated by the overlay of the fan subgraphic:

- No overlay - the fan is present and running; there is no indication of an adverse condition.
- Amber caution sign - indicates that only warning alerts have been issued and that corrective action must be taken.
- Red X - indicates at least one failure condition is present. This means that the health status is reported as critical.
- Grayed Out - indicates that the fan is present and not powered on. There is no indication of an adverse condition.

- 2 Use the cursor to hover over the an individual fan subgraphic.

A text hint or a screen tip is displayed. The text hint provides additional information on that fan.

- 3 Clicking the fan subgraphic selects that fan's information and **Quick Links** for display to the right of the chassis graphics.

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.

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.

To view the health status of the fan units:

- 1 Log in to the CMC Web interface.
- 2 Select **Fans** in the system tree. The **Fans Status** page displays.

You can also view the **Fan Status** page by clicking the status link in the fan information **Quick Links** on the right side of the page.

Table 5-31. Fans Health Status Information

Item	Description	
Name	Displays the fan name in the format FAN-<i>n</i> , where <i>n</i> is the fan number.	
Present	Indicates whether the fan unit is present (Yes or No).	
Health	 OK	Indicates that the fan unit is present and communicating with CMC. In the event of a communication failure between CMC and the fan unit, CMC cannot obtain or display health status for the fan unit.
	 Critical	Indicates that at least one Failure alert has been issued. Critical status represents a system failure on the fan unit, and corrective action must be taken immediately to prevent overheating and system shutdown.
	 Unknown	Displayed when the chassis is first powered on. In the event of a communication failure between CMC and the fan unit, CMC cannot obtain or display health status for the fan unit.
Speed	Indicates the speed of the fan in RPM.	

Viewing the iKVM Status

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

The health status of the iKVM associated with the chassis can be viewed on the **Chassis Health** page.

To view health status for the iKVM using **Chassis Graphics**:

1 Log in to the CMC Web interface.

The **Chassis Health** page is displayed. The lower section of **Chassis Graphics** depicts 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:

- No overlay - iKVM is present, powered on and communicating with CMC; there is no indication of an adverse condition.
- Amber caution sign - indicates that only warning alerts have been issued and that corrective action must be taken.
- Red X - indicates at least one failure condition is present. This means that CMC can still communicate with the iKVM and that the health status reported is critical.
- Grayed Out - indicates that the iKVM is present and not powered on. It is not communicating with CMC and there is no indication of an adverse condition.

2 Use the cursor to hover over the iKVM subgraphic.

A text hint or a screen tip is displayed. The text hint provides additional information on that iKVM.

3 Clicking the iKVM subgraphic selects the iKVM's information and **Quick Links** for display to the right of the chassis graphics.

You can also view the **iKVM Status** page by clicking the status link in the iKVM **Quick Links** on the right side of the chassis graphics.

For additional instructions on viewing iKVM status and setting properties for the iKVM, see:

- "Viewing the iKVM Status and Properties" on page 352
- "Enabling or Disabling the Front Panel" on page 351
- "Enabling the Dell CMC Console Through iKVM" on page 352
- "Updating the iKVM Firmware" on page 354

For more information about iKVM, see "Using the iKVM Module" on page 333.

Viewing the Health Status of the PSUs

The health status of the PSUs associated with the chassis can be viewed in two ways: from the **Chassis Component Summary** section on the **Chassis Health** page or the **Power Supply Status** page. The **Chassis Health** page provides a graphical overview of all PSUs installed in the chassis.

To view health status for all PSUs using **Chassis Graphics**:

- 1 Log in to the CMC Web interface.

The **Chassis Health** page is displayed. The lower section of **Chassis Graphics** depicts 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:

- No overlay - PSU is present, powered on and communicating with CMC; there is no indication of an adverse condition.
 - Amber caution sign - indicates that only warning alerts have been issued and that corrective action must be taken.
 - Red X - indicates at least one failure condition is present. This means that CMC can still communicate with the PSU and that the health status is reported as critical.
 - Grayed Out - indicates that the PSU is present and not powered on. It is not communicating with CMC and there is no indication of an adverse condition.
- 2 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.
 - 3 Clicking on the PSU subgraphic selects that PSU's information and **Quick Links** for display to the right of the chassis graphics.

The **Power Supply Status** page displays the status and readings of the PSUs associated with the chassis. For more information about CMC power management, see "Power Management" on page 289.

To view the health status of the PSUs:

- 1 Log in to the CMC Web interface.
- 2 Select **Power Supplies** in the system tree. The **Power Supply Status** page displays.

You can also view the **PSU Status** page by clicking the status link in the PSU Quick Links on the right side of the chassis graphics.

Table 5-32. Power Supply Health Status Information

Item	Description	
Name	Displays the name of the PSU: <i>PS-n</i> , where <i>n</i> is the power supply number.	
Present	Indicates whether the power supply is present (Yes or No).	
Health	 OK	Indicates that the PSU is present and communicating with CMC. Indicates that the health of the PSU is OK. In the event of a communication failure between CMC and the fan unit, CMC cannot obtain or display health status for the PSU.
	 Critical	Indicates that the PSU has a failure and the health is critical. Corrective action must be taken immediately. Failure to do so may cause the component to shutdown due to power loss.
	 Unknown	Displayed with the chassis is first powered on. In the event of a communication failure between CMC and the PSU, CMC cannot obtain or display health status for the PSU.
Power Status	Indicates the power state of the PSU: Online , Off , or Slot Empty .	
Capacity	Displays the power capacity in watts.	

Table 5-33. System Power Status

Item	Description
Overall Power Health	Displays the health status (OK , Non-Critical , Critical , Non-Recoverable , Other , Unknown) of the power management for the entire chassis.
System Power Status	Displays the power status (On , Off , Powering On , Powering Off) of the chassis.

Table 5-33. System Power Status (continued)

Item	Description
Redundancy	Displays the power supply redundancy status. Values include: No: Power Supplies are not redundant. Yes: Full Redundancy in effect.

Viewing Status of the Temperature Sensors

The **Temperature Sensors Status** page displays the status and readings of the temperature probes on the entire chassis (chassis and servers).



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.

To view the health status of the temperature probes:

- 1 Log in to the CMC Web interface.
- 2 Select **Temperature Sensors** in the system tree. The **Temperature Sensors Status** page displays.

Table 5-34. Temperature Sensors Health Status Information

Item	Description
ID	Displays the location of the temperature probe.
Name	Displays the name of each temperature probe for the chassis and servers.
Present	Indicates whether the module is present (Yes) or absent (No) in the chassis.
Health	 OK Indicates that the module is present and communicating with CMC. In the event of a communication failure between CMC and the server, CMC cannot obtain or display the health status for the server.

Table 5-34. Temperature Sensors Health Status Information (continued)

Item	Description
 Warning	Indicates that only warning alerts have been issued, and corrective action must be taken. If corrective actions are not taken, then critical or severe failures that can affect the integrity of the module may occur.
 Severe	Indicates that one failure alert has been issued. Severe status represents a system failure on the module and corrective action must be taken immediately.
 Unknown	Indicates that communication with the module has not been established. This is usually because the chassis is off or the chassis has not completed initialization.
Reading	Displays the current temperature in degrees Centigrade and Fahrenheit.
Threshold Maximum	Displays the highest temperature, in degrees Centigrade and Fahrenheit, at which a Failure alert is issued.

Viewing the LCD Status

You can view the health status of the LCD using the chassis graphics associated with the chassis on the **Chassis Health** page.

To view the health status for the LCD:

- 1 Log in to the CMC Web interface.

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:

- No overlay - LCD is present, powered on, and communicating with CMC. There is no adverse condition.
- Amber caution sign - warning alerts have been issued and corrective action must be taken.
- Red X - at least one failure condition is present. The health status is critical.

- Grayed Out - the LCD is present and not powered on. It is not communicating with CMC and there is no adverse condition.
- 2 Move the cursor over the LCD subgraphic. The corresponding text hint or screen tip, which provides additional information on the LCD is displayed.
 - 3 Click the LCD subgraphic to select the LCD's information and display it to the right side of the chassis graphics.

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: See "Using FlexAddress" on page 217 for more information on the FlexAddress feature.

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 Chassis-Assigned addresses are checked, those addresses are used even if one server is replaced with another server.

Configuring CMC Network Properties



NOTE: Network configuration changes can result in the loss of connectivity on current network login.

Setting Up Initial Access to CMC

Before you can begin configuring 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 CMC.



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

- 1 Log in to the Web interface.
- 2 Select **Chassis Overview** in the system tree.

- 3 Click the **Network** tab. The **Network Configuration** page appears.
- 4 Enable or disable DHCP for CMC by selecting or clearing the **Use DHCP (For CMC Network Interface IP Address)** check box.
- 5 If you disabled DHCP, type the IP address, gateway, and subnet mask.
- 6 Click **Apply Changes** at the bottom of the page.

Configuring the Network LAN Settings



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



NOTE: The settings on the **Network Configuration** page, such as community string and SMTP server IP address, affect both CMC and the external settings of the chassis.



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

To configure the Network LAN settings:

- 1 Log in to the Web interface.
- 2 Click the **Network** tab.
- 3 Configure the CMC network settings described in Table 5-35 through Table 5-37.
- 4 Click **Apply Changes**.

To configure IP range and IP blocking settings, click the **Advanced Settings** button (see "Configuring CMC Network Security Settings" on page 151.)

To refresh the contents of the **Network Configuration** page, click **Refresh**.

To print the contents of the **Network Configuration** page, click **Print**.

Table 5-35. Network Settings

Setting	Description
CMC MAC Address	Displays the chassis' MAC address, which is a unique identifier for the chassis over the computer network.
Enable CMC Network Interface	<p>Enables the Network Interface of CMC.</p> <p>Default: Enabled. If this option is checked:</p> <ul style="list-style-type: none">• CMC communicates with and is accessible over the computer network.• The Web interface, CLI (remote RACADM), WSMAN, Telnet, and SSH associated with CMC are available. <p>If this option is not checked:</p> <ul style="list-style-type: none">• The CMC Network Interface cannot communicate over the network.• Communication to the chassis through CMC is not available.• The Web interface, CLI (remote RACADM), WSMAN, Telnet, and SSH associated with the CMC are not available.• The server iDRAC Web interface, local CLI, I/O modules, and iKVM are still accessible.• Network addresses for the iDRAC6 and CMC can be obtained, in this case, from the chassis' LCD. <p>NOTE: Access to the other network-accessible components in the chassis is not affected when the network on the chassis is disabled (or lost).</p>
Register CMC on DNS	<p>This property registers the CMC name on the DNS Server.</p> <p>Default: Unchecked (disabled) by default</p> <p>NOTE: Some DNS Servers only register names of 31 characters or fewer. Make sure the designated name is within the DNS required limit.</p>

Table 5-35. Network Settings (continued)

Setting	Description
DNS CMC Name	Displays the CMC name only when Register CMC on DNS is selected. The default CMC name is <i>CMC_service_tag</i> , where <i>service tag</i> is the service tag of the chassis, for example: CMC-00002. The maximum number of characters is 63. The first character must be a letter (a-z, A-Z), followed by an alphanumeric (a-z, A-Z, 0-9) or a hyphen (-) characters.
Use DHCP for DNS Domain Name	Uses the default DNS domain name. This check box is active only when Use DHCP (For CMC Network Interface IP Address) is selected. Default: Enabled
DNS Domain Name	The default DNS Domain Name is a blank character. This field can be edited only when the Use DHCP for DNS Domain Name check box is selected.
Auto Negotiation (1 Gb)	Determines whether CMC automatically sets the duplex mode and network speed by communicating with the nearest router or switch (On) or allows you to set the duplex mode and network speed manually (Off). Default: On If Auto Negotiation is On , CMC automatically communicates with the nearest router or switch and operates at 1 Gb speed. If Auto Negotiation is Off , you must set the duplex mode and network speed manually.

Table 5-35. Network Settings (continued)

Setting	Description
Network Speed	<p>Set the network speed to 100 Mbps or 10 Mbps to match your network environment.</p> <p>NOTE: 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 your network configuration does not match any of these values, it is recommended that you use Auto Negotiation or refer to your network equipment manufacturer.</p> <p>NOTE: To use 1000 Mb or 1 Gb speeds, select Auto Negotiation.</p>
Duplex Mode	<p>Set the duplex mode to full or half to match your network environment.</p> <p>Implications: 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.</p> <p>NOTE: The network speed and duplex mode settings are not available if Auto Negotiation is set to On.</p>
MTU	<p>Sets the size of the Maximum Transmission Unit (MTU), or the largest packet that can be passed through the interface.</p> <p>Configuration range: 576 – 1500.</p> <p>Default: 1500.</p> <p>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.</p>

Table 5-36. IPv4 Settings

Setting	Description
Enable IPv4	Allow CMC to use the IPv4 protocol to communicate on the network. Clearing this box does not prevent IPv6 networking from occurring. Default: Checked (enabled)
DHCP Enable	<p>Enables CMC to request and obtain an IP address from the IPv4 Dynamic Host Configuration Protocol (DHCP) server automatically. Default: Checked (enabled)</p> <p>If this option is checked, CMC retrieves IPv4 configuration (IP Address, subnet mask, and gateway) automatically from a DHCP server on your network. CMC always has a unique IP Address allotted over your network.</p> <p>NOTE: When this feature is enabled, the Static IP Address, Static Subnet Mask, and Static Gateway property fields (located immediately following this option on the Network Configuration page) are disabled, and any previously entered values for these properties are ignored.</p> <p>If this option is not checked, you must manually type the Static IP Address, Static Subnet Mask, and Static Gateway in the text fields immediately following this option in the Network Configuration page.</p>
Static IP Address	Specifies the IPv4 address for the CMC Network Interface.
Static Subnet Mask	Specifies the static IPv4 subnet mask for the CMC Network Interface.

Table 5-36. IPv4 Settings (continued)

Setting	Description
Static Gateway	<p>Specifies the IPv4 gateway for the CMC Network Interface.</p> <p>NOTE: The Static IP Address, Static Subnet Mask, and Static Gateway fields are active only if DHCP Enable (the property field preceding these fields) is disabled (unchecked). In that case, you must manually type the Static IP Address, Static Subnet Mask, and Static Gateway for CMC to use over the network.</p> <p>NOTE: The Static IP Address, Static Subnet Mask, and Static Gateway fields apply only to the chassis device. They do not affect the other network-accessible components in the chassis solution, such as the server network, local access, I/O modules, and iKVM.</p>
Use DHCP to Obtain DNS Server Addresses	<p>Obtains the primary and secondary DNS server addresses from the DHCP server instead of the static settings.</p> <p>Default: Checked (enabled) by default</p> <p>NOTE: If Use DHCP (For CMC Network Interface IP Address) is enabled, then enable the Use DHCP to Obtain DNS Server Addresses property.</p> <p>If this option is checked, CMC retrieves its DNS IP address automatically from a DHCP server on your network.</p> <p>NOTE: When this property is enabled, the Static Preferred DNS Server and Static Alternate DNS Server property fields (located immediately following this option on the Network Configuration page) are inactivated, and any previously entered values for these properties are ignored.</p> <p>If this option is not selected, CMC retrieves the DNS IP address from the Static Preferred DNS Server and Static Alternate DNS Server. The addresses of these servers are specified in the text fields immediately following this option on the Network Configuration page.</p>

Table 5-36. IPv4 Settings (continued)

Setting	Description
Static Preferred DNS Server	Specifies the static IP address for the preferred DNS Server. The Static Preferred DNS Server is implemented only when Use DHCP to Obtain DNS Server Addresses is disabled.
Static Alternate DNS Server	Specifies the static IP address for the alternate DNS Server. The Static Alternate DNS Server is implemented only when Use DHCP to obtain DNS Server addresses is disabled. If you do not have an alternate DNS Server, type an IP address of 0.0.0.0.

Table 5-37. IPv6 Settings

Setting	Description
Enable IPv6	Allows CMC to use the IPv6 protocol to communicate on the network. Unchecking this box does not prevent IPv4 networking from occurring. Default: Checked (enabled)
AutoConfiguration Enable	<p>Allows CMC to use the IPv6 protocol to obtain IPv6 related address and gateway settings from an IPv6 router configured to provide this information. CMC then has a unique IPv6 address on your network. Default: Checked (enabled)</p> <p>NOTE: When this feature is enabled, the Static IPv6 Address, Static Prefix Length, and Static Gateway property fields (located immediately following this option on the Network Configuration page) are disabled, and any previously entered values for these properties are ignored.</p> <p>If this option is not checked, you must manually type the Static IPv6 Address, Static Prefix Length, and Static Gateway in the text fields located immediately following this option on the Network Configuration page.</p>
Static IPv6 Address	Specifies the IPv6 address for the CMC Network Interface when Autoconfiguration is not enabled.
Static Prefix Length	Specifies the IPv6 prefix length for the CMC Network Interface when Autoconfiguration is not enabled.
Static Gateway	<p>Specifies the static IPv6 gateway for the CMC Network Interface when Autoconfiguration is not enabled.</p> <p>NOTE: The Static IPv6 Address, Static Prefix Length, and Static Gateway fields are active only if AutoConfiguration Enable (the property field preceding these fields) is disabled (unchecked). In that case, you must manually type the Static IPv6 Address, Static Prefix Length, and Static Gateway for CMC to use over the IPv6 network.</p> <p>NOTE: The Static IPv6 Address, Static Prefix Length, and Static Gateway fields apply only to the chassis device. They do not affect the other network-accessible components in the chassis solution, such as the server network, local access, I/O modules, and iKVM.</p>

Table 5-37. IPv6 Settings (continued)

Setting	Description
Static Preferred DNS Server	Specifies the static IPv6 Address for the preferred DNS Server. The entry for Static Preferred DNS Server is considered only when Use DHCP to Obtain DNS Server Addresses is disabled or unchecked. There is an entry for this Server in both IPv4 and IPv6 configuration areas.
Static Alternate DNS Server	Specifies the static IPv6 Address for the alternate DNS Server. If you do not have an alternate DNS server, type an IPv6 Address of "::". The entry for Static Alternate DNS Server is considered only when Use DHCP to Obtain DNS Server Addresses is disabled or unchecked. There is an entry for this server in both IPv4 and IPv6 configuration areas.

Configuring CMC Network Security Settings



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

- 1 Log in to the Web interface.
- 2 Click the **Network** tab.
The **Network Configuration** page displays.
- 3 Click the **Advanced Settings** button.
The **Network Security** page displays.
- 4 Configure the CMC network security settings.

Table 5-38 describes the settings on the **Network Security** page.



NOTE: The IP Range and IP Blocking settings are applicable to IPv4 only.

Table 5-38. Network Security Page Settings

Settings	Description
IP Range Enabled	Enables the IP Range checking feature, which defines a specific range of IP addresses that can access CMC.
IP Range Address	Determines the base IP address for range checking.

Table 5-38. Network Security Page Settings (continued)

Settings	Description
IP Range Mask	<p>Defines a specific range of IP addresses that can access the CMC, a process called IP range checking.</p> <p>IP range checking allows access to CMC only from clients or management stations whose IP addresses are within the user-specified range. All other logins are denied.</p> <p>For example:</p> <p>IP range mask: 255.255.255.0 (11111111.11111111.11111111.00000000)</p> <p>IP range address: 192.168.0.255 (11000000.10101000.00000000.11111111)</p> <p>The resulting IP address range is any address that contains 192.168.0, that is, any address from 192.168.0.0 through 192.168.0.255.</p>
IP Blocking Enabled	<p>Enables the IP address blocking feature, which limits the number of failed login attempts from a specific IP address for a pre-selected time span.</p>
• IP Blocking Fail Count	<p>Sets the number of login failures attempted from an IP address before the login attempts are rejected from that address.</p>
• IP Blocking Fail Window	<p>Determines the time span in seconds within which IP Blocking Fail Count failures must occur to trigger the IP Block Penalty Time.</p>
• IP Blocking Penalty Time	<p>The time span in seconds within which login attempts from an IP address with excessive failures are rejected.</p> <p>NOTE: The IP Blocking Fail Count, IP Blocking Fail Window, and IP Blocking Penalty Time fields are active only if the IP Blocking Enabled check box (the property field preceding these fields) is checked (enabled). In that case, you must manually type IP Blocking Fail Count, IP Blocking Fail Window, and IP Blocking Penalty Time properties.</p>

5 Click **Apply** to save your settings.

To refresh the contents of the **Network Security** page, click **Refresh**.

To print the contents of the **Network Security** page, click **Print**.

Configuring VLAN

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.

- 1 Log in to the Web interface.
- 2 Click the **Network** tab→ **VLAN** subtab.

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

- 3 Configure the CMC/iDRAC VLAN settings.

Table 5-39 describes the **settings** on the **Network Security** page.

Table 5-39. VLAN Tag Settings

Setting	Description
Slot	Displays the slot occupied by the server in the chassis. Slots are sequential IDs, from 1 to 16 (for the 16 available slots in the chassis), that help identify the location of the server in the chassis.
Name	Displays the name of the server in each slot.
Enable	Enables VLAN if the check box is selected. VLAN is disabled by default.
Priority	Indicates the frame priority level, which can be used to prioritize different types of traffic (voice, video, and data). Valid priorities are 0 to 7; where 0 (default) is the lowest and 7 is the highest.
ID	Displays the VLAN ID (identification). Valid VLAN IDs are: 1 to 4000 and 4021 to 4094. The default VLAN ID is 1.

- 4 Click **Apply** to save the settings.

You can also access this page from the **Chassis Overview**→ **Servers**→ **Setup** tab→ **VLAN** subtab.

Adding and Configuring CMC Users

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

User Types

There are two types of users: CMC users and iDRAC users. CMC users are also known as "chassis users." Since iDRAC resides on the server, iDRAC users are also known as "server users."

CMC users can be local users or directory service users. iDRAC users can also be local users 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 5-40. 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.

Table 5-40. User Types (continued)

Privilege	Description
Chassis Configuration Administrator	<p>User can add or change data that:</p> <ul style="list-style-type: none">• 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• 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. <p>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.</p>
User Configuration Administrator	<p>User can:</p> <ul style="list-style-type: none">• Add a new user• Delete an existing 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	<p>User can clear the hardware log and CMC log.</p>
Chassis Control Administrator (Power Commands)	<p>CMC users with the Chassis Power Administrator privilege can perform all power-related operations:</p> <ul style="list-style-type: none">• Control chassis power operations, including power on, power off, and power cycle.

Table 5-40. User Types (continued)

Privilege	Description
Server Administrator	<p data-bbox="305 280 958 335">This a blanket privilege granting a CMC user all rights to perform any operation on any servers present in the chassis.</p> <p data-bbox="305 352 958 520">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.</p> <p data-bbox="305 537 958 624">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:</p> <ul data-bbox="305 641 958 772" style="list-style-type: none"><li data-bbox="305 641 723 667">• The same user name exists on the server<li data-bbox="305 679 958 734">• The same user name must have the exact same password on the server<li data-bbox="305 746 897 772">• The user must have the privilege to execute the command <p data-bbox="305 790 958 957">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.</p> <hr data-bbox="305 970 969 973"/> <p data-bbox="305 979 941 1120">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. Based on the privileges responding from the server, CMC firmware decides if the user has the right to perform the action.</p> <p data-bbox="305 1137 927 1246">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.</p>

Table 5-40. User Types (continued)

Privilege	Description
Server Administrator (continued)	Server Configuration Administrator: <ul style="list-style-type: none">• Set IP address• Set gateway• Set subnet mask• Set first boot device Configure Users: <ul style="list-style-type: none">• Set iDRAC root password• iDRAC reset Server Control Administrator: <ul style="list-style-type: none">• 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.
Super User	User has root access to CMC and has User Configuration Administrator and Login to CMC User privileges. Only users with Super User privileges can grant new or existing users Debug Command Administrator and Super User privileges.

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 pre-defined set, the CMC Group automatically changes to Custom.

Table 5-41. CMC Group Privileges

User Group	Privileges Granted
Administrator	<ul style="list-style-type: none">• CMC Login User• Chassis Configuration Administrator• User Configuration Administrator• Clear Logs Administrator• Server Administrator• Test Alert User• Debug Command Administrator• Fabric A Administrator• Fabric B Administrator• Fabric C Administrator
Power User	<ul style="list-style-type: none">• 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

Table 5-41. CMC Group Privileges (continued)

User Group	Privileges Granted
Custom	Select any combination of the following permissions: <ul style="list-style-type: none"> • CMC Login User • Chassis Configuration Administrator • User Configuration Administrator • Clear Logs Administrator • Chassis Control Administrator (Power Commands) • Super User • Server Administrator • Test Alert User • Debug Command Administrator • Fabric A Administrator • Fabric B Administrator • Fabric C Administrator
None	No assigned permissions.

Table 5-42. Comparison of Privileges Between CMC Administrators, Power Users, and Guest Users

Privilege Set	Administrator Permissions	Power User Permissions	Guest User Permissions
CMC Login User	✓	✓	✓
Chassis Configuration Administrator	✓	✗	✗
User Configuration Administrator	✓	✗	✗
Clear Logs Administrator	✓	✓	✗
Chassis Control Administrator (Power Commands)	✓	✓	✗

Table 5-42. Comparison of Privileges Between CMC Administrators, Power Users, and Guest Users (continued)

Privilege Set	Administrator Permissions	Power User Permissions	Guest User Permissions
Super User	✓	✗	✗
Server Administrator	✓	✓	✗
Test Alert User	✓	✓	✗
Debug Command Administrator	✓	✗	✗
Fabric A Administrator	✓	✓	✗
Fabric B Administrator	✓	✓	✗
Fabric C Administrator	✓	✓	✗

Adding and Managing Users

From the **Users** and **User Configuration** pages in the Web interface, you can view information about CMC users, add a new user, and change settings for an existing user.

You can configure up to 16 local users. If additional users are required and your company uses Microsoft Active Directory or generic Lightweight Directory Access Protocol (LDAP) services, you can configure it to provide access to CMC. Active Directory configuration allows you to add and control CMC user privileges to your existing users in your Active Directory software, in addition to the 16 local users. For more information, see "Using the CMC Directory Service" on page 241. For more information about LDAP, see the "Using CMC with the Lightweight Directory Access Protocol Services" section.

Users can be logged in through Web interface, Telnet serial, SSH, and iKVM sessions. A maximum of 22 active sessions (Web interface, Telnet serial, SSH, and iKVM, in any combination) can be divided among users.

 **NOTE:** 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, click **User ID 1** to open the **User Configuration** page. Help for that page is available through the Help link at the top right corner of the page.

To add and configure CMC users:

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

- 1 Log in to the Web interface.
- 2 Click the **User Authentication** tab. The **Local Users** page appears, listing each user's user ID, user name, CMC privilege, and login state, including those of the root user. User IDs available for configuration have no user information displayed.
- 3 Click an available user ID number. The **User Configuration** page displays. To refresh the contents of the **Users** page, click **Refresh**. To print the contents of the **Users** page, click **Print**.
- 4 Select general settings for the user.

Table 5-43. General User Settings for Configuring a New or Existing CMC Username and Password

Property	Description
User ID	(Read only) Identifies a user by one of 16 preset, sequential numbers used for CLI scripting purposes. The User ID identifies the particular user when configuring the user through the CLI tool (RACADM). You cannot edit the User ID. If you are editing information for user root, this field is static. You cannot edit the user name for root.
Enable User	Enables or disables the user's access to CMC.

Table 5-43. General User Settings for Configuring a New or Existing CMC Username and Password (continued)

Property	Description
User Name	<p>Sets or displays the unique CMC user name associated with the user. The user name can contain up to 16 characters. CMC user names cannot include forward slash (/) or period (.) characters.</p> <p>NOTE: If you change the user name, the new name does not appear in the user interface until your next login. Any user logging in after you apply the new user name can see the change immediately.</p>
Change Password	<p>Allows an existing user's password to be changed. Set the new password in the New Password field.</p> <p>The Change Password check box cannot be selected if you are configuring a new user. You can select it only when changing an existing user setting.</p>
Password	<p>Sets a new password for an existing user. To change the password, you must also select the Change Password check box. The password can contain up to 20 characters, which display as dots as you type.</p>
Confirm Password	<p>Verifies the password you entered in the New Password field.</p> <p>NOTE: The New Password and Confirm New Password fields are editable only when you are (1) configuring a new user; or (2) editing the settings for an existing user, and the Change Password check box is selected.</p>

- 5 Assign the user to a CMC user group. Table 5-40 describes CMC user privileges.

When you select a user privilege setting from the CMC Group drop-down menu, the enabled privileges (shown as checked boxes in the list) display according to the pre-defined settings for that group.

You can customize the privileges settings for the user by checking or un-checking boxes. After you have selected a CMC Group or made Custom user privilege selections, click **Apply Changes** to keep the settings.

- 6 Click **Apply Changes**.

To refresh the contents of the **User Configuration** page, click **Refresh**.

To print the contents of the **User Configuration** page, click **Print**.

Configuring and Managing Microsoft Active Directory Certificates



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



NOTE: For more information about Active Directory configuration and how to configure Active Directory with Standard Schema or Extended Schema, see "Using the CMC Directory Service" on page 241.

You can use the Microsoft Active Directory service to configure your software to provide access to CMC. Active Directory service allows you to add and control the CMC user privileges of your existing users.

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

- 1 Log in to the Web interface.
- 2 Click the **User Authentication** tab, and then click the **Directory Services** subtab. Select the radio button for Microsoft Active Directory Standard Schema or Extended Schema. The Active Directory tables appear.

Common Settings

This section allows you to configure and view common Active Directory settings for CMC.

Table 5-44. Common Settings

Field	Description
Enable Active Directory	Enables Active Directory Login on CMC. You must install SSL certificates for the Active Directory servers signed by the same certificate authority and upload it to CMC.

Table 5-44. Common Settings (continued)

Field	Description
Enable Smart Card Login	<p>Enables Active Directory inter-operation based on the Kerberos Authentication supported by a Dell-supplied, auto-installed browser plug-in and Smart Card usage. To enable Smart Card, select the check box. To disable Smart Card, clear the check box. If you enable Smart Card, you must also configure your Microsoft Windows Client Workstation to correctly operate with Smart Card Reader functionality. This involves installing the correct drivers for the Smart Card Reader being used and also, the correct drivers for the actual Smart Card used. These Smart Card drivers vary by vendor. The Smart Card must be properly programmed with the necessary credentials using the Smart Card Enrollment Services provided by the appropriate Active Directory Server.</p> <p>NOTE: Smart Card Login and Single Sign-On selections are mutually exclusive. You can select only one at a time.</p>
Enable Single Sign-On	<p>Enables CMC to utilize Active Directory. To enable Single Sign-On, select the check box. To disable Single Sign-On, clear the check box. If you enable Single Sign-On, you must also set the Active Directory properties and select the schema you want to use.</p> <p>NOTE: Smart Card Login and Single Sign-On selections are mutually exclusive. You can select only one at a time.</p>

Table 5-44. Common Settings (continued)

Field	Description
Enable SSL Certificate Validation	<p>Enables SSL certificate validation for CMC's Active Directory SSL connection. To disable the SSL certificate validation, clear the check box.</p> <p>Warning: Disabling this feature may expose the authentication to a man-in-the-middle attack.</p> <p>The browser operation requires that CMC be accessed through a HTTP URL which contains a fully qualified domain address for CMC, that is http://cmc-6g2wxfl.dom.net. A plain IP address for CMC does not result in proper Single Sign-On operation. To support fully qualified domain addresses, it is necessary to register CMC with the Domain Name Service of the Active Directory Server.</p> <p>If a Single Sign-On browser authentication is unsuccessful, the usual Local or Active Directory username/password browser authentication method is automatically presented. Similarly, a Logout action after a successful Single Sign-On presents the username/password method. Single Sign-On usage is intended for convenience and is not meant to be restrictive.</p> <p>NOTE: Smart Card based browser authentication is only supported for Microsoft Windows Clients and Internet Explorer browsers.</p> <p>The Dell supplied, auto-loaded, browser plug-in (ActiveX control) is dependent on the Microsoft Windows Client operating system having the following runtime component pre-installed - Microsoft Visual C++ 2005 Redistributable Package (x86). The following link may help locate the component: http://www.microsoft.com/downloads/details.aspx?FamilyID=32BC1BEE-A3F9-4C13-9C99-220B62A191EE&displaylang=en. The Windows Client needs 'elevated privileges' to successfully install the ActiveX Control. Similarly, the browser configuration needs the capability to accept installation of 'unsigned' ActiveX Controls.</p>

Table 5-44. Common Settings (continued)

Field	Description
	Enabling Smart Card enforces a Smart Card Only policy for browser authentication. All other methods of browser authentication such as Local or Active Directory username/password authentication are restricted. If the Smart Card Only usage enforcement policy is to be adopted, it is important that the Smart Card operation be fully validated before all other access methods to CMC are disabled. Otherwise, it is possible to inadvertently lock all access to CMC.
Root Domain Name	Specifies the domain name used by Active Directory. The root domain name is the fully qualified root domain name for the forest. NOTE: The root domain name must be a valid domain name using the x.y naming convention, where x is a 1-256 character ASCII string with no blank spaces between characters, and y is a valid domain type such as com, edu, gov, int, mil, net, or org.
AD Timeout	Sets the time in seconds after which an idle Active Directory session is automatically closed. Valid values: 15-300 seconds Default: 90 seconds
Specify AD Server to search (optional)	Enables (when checked) directed call on the domain controller and global catalog. If you enable this option, you must also specify the domain controller and global catalog locations in the following settings. NOTE: The name on the Active Directory CA Certificate does not be matched against the specified Active Directory server or the Global Catalog server.
Domain Controller	Specifies the server where your Active Directory service is installed. This option is valid only if Specify AD Server to search (Optional) is enabled.
Global Catalog	Specifies the location of the global catalog on the Active Directory domain controller. The global catalog provides a resource for searching an Active Directory forest. This option is valid only if Specify AD Server to search (Optional) is enabled.

Standard Schema Settings

Displayed when Microsoft Active Directory (Standard Schema) is selected, this section presents the role groups with associated names, domains, and privileges for any role groups that have already been configured.

To change the settings for a role group, click the role group button in the Role Groups list.



NOTE: If you click a role group link prior to applying any new settings you have made, you lose those settings. To avoid losing any new settings, click **Apply** before clicking a role group button.

The Configure Role Group page displays:

- Group Name – The name that identifies the role group in the Active Directory associated with the CMC card.
- Group Domain – The domain where the group is located.
- Group Privilege – The privilege level for the group.

Click **Apply** to save the settings.

Click **Go back to Configuration Page** to return to the **Directory Services** page.

To refresh the contents of the **Directory Services** page, click **Refresh**.

To print the contents of the **Directory Services** page, click **Print**.

Extended Schema Settings

Displayed when Microsoft Active Directory (Extended Schema) is selected, this section presents the following properties:

- CMC Device Name - Displays the name of the RAC Device Object you created for CMC. The CMC Device Name uniquely identifies the CMC card in Active Directory. The CMC Device Name must be the same as the common name of the new RAC Device Object you created in your domain controller. The CMC Name must be a 1-256 character ASCII string with no blank spaces between characters. For more information about RAC Device Objects, see your CMC User's Guide.

- CMC Domain Name - Displays the DNS name (string) of the domain where the Active Directory RAC Device Object resides. The CMC domain name must be a valid domain name consisting of *x.y*, where *x* is a 1-256 character ASCII string with no blank spaces between characters, and *y* is a valid domain type such as com, edu, gov, int, mil, net, or org.

Managing Active Directory Certificates

This sections displays the properties for the Active Directory certificate that was recently uploaded to the CMC. If you uploaded a certificate, use this information to verify that the certificate is valid and has not expired.

 **NOTE:** By default, CMC does not have a certificate authority-issued server certificate for Active Directory. You must upload a current, certificate authority-signed server certificate.

The following properties for the certificate are displayed:

- Serial Number - The certificate's serial number.
- Subject Information - The certificate's subject (name of the person or company certified).
- Issuer Information - The certificate's issuer (name of the Certificate Authority).
- Valid From - The starting date of the certificate.
- Valid To - The expiry date of the certificate.

Use the following controls to upload and download this certificate:

- Upload - Initiates the upload process for the certificate. This certificate, which you obtain from Active Directory, grants access to CMC.
- Download - Initiates the download process. You are prompted for the location to save the file. When you select this option and click **Next**, a **File Download** dialog box appears. Use this dialog box to specify a location on your management station or shared network for the server certificate.

 **NOTE:** By default, CMC does not have a certificate authority-issued server certificate for Active Directory. You must upload a current, certificate authority-signed server certificate.

Kerberos Keytab

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.

 **NOTE:** CMC does not have a Kerberos Keytab for Active Directory. You must upload a currently generated Kerberos Keytab. See "Configuring Single Sign-On" on page 272 for detailed information.

The following actions are allowed:

- Browse - Opens a **Browse** dialog box, from which you select the server certificate you want to upload.
- Upload - Initiates the upload process for the certificate using the file path you specify.

Configuring and Managing Generic Lightweight Directory Access Protocol Services

You can use the Generic Lightweight Directory Access Protocol (LDAP) Service to configure your software to provide access to CMC. LDAP allows you to add and control the CMC user privileges of your existing users.

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

To view and configure LDAP:

- 1 Log in to the Web interface.
- 2 Click the **User Authentication** tab, and then click the **Directory Services** subtab. The **Directory Services** page appears.
- 3 Click the radio button associated with Generic LDAP.
- 4 Configure the options shown and click **Apply**.

The following configuration options are available.

Table 5-45. Common Settings

Setting	Description
Generic LDAP Enabled	Enables the generic LDAP service on CMC.
Use Distinguished Name to Search Group Membership	Specifies the distinguished name (DN) of LDAP groups whose members are allowed access to the device.
Enable SSL Certificate Validation	If checked, CMC uses the CA certificate to validate the LDAP server certificate during SSL handshake.
Bind DN	Specifies the distinguished name of a user used to bind to the server when searching for the login user's DN. If not provided an anonymous bind is used.
Password	A bind password to use in conjunction with the bind DN. NOTE: The bind password is sensitive data, and must be properly protected.
Base DN to Search	The DN of the branch of the directory where all searches must start from.
Attribute of User Login	Specifies the attribute to search for. If not configured, the default is to use uid. It is recommended to be unique within the chosen base DN, otherwise a search filter must be configured to ensure the uniqueness of the login user. If the user DN cannot be uniquely identified by searching the combination of attribute and search filter, login fails with an error.
Attribute of Group Membership	Specifies the LDAP attribute that is used to check for group membership. This must be an attribute of the group class. If not specified, the member and unique member attributes are used.
Search Filter	Specifies a valid LDAP search filter. This is used if the user attribute cannot uniquely identify the login user within the chosen base DN. If not provided, defaults to (objectClass=*), which searches for all objects in the tree. The maximum length of this property is 1024 characters.

Table 5-45. Common Settings (continued)

Setting	Description
Network Timeout (seconds)	Sets the time in seconds after which an idle LDAP session is automatically closed.
Search Timeout (seconds)	Sets the time in seconds after which a search is automatically closed.

Selecting Your LDAP Servers

You can configure the server to use with Generic LDAP in two ways. Static Servers allows the administrator to place a FQDN or IP address within the field. Alternatively, a list of LDAP servers can be retrieved by looking up their SRV record within the DNS. The following are the properties in the LDAP Servers section:

- Use Static LDAP Servers - Selecting this option causes the LDAP service to use the specified servers with the port number provided (see details below).
 **NOTE:** You must select Static or DNS.
- LDAP Server Address - Specify the FQDN or IP of the LDAP server. To specify multiple, redundant LDAP servers that serve the same domain, provide the list of all servers separated by comma. CMC tries to connect to each server in turn, until it makes a successful connection.
- LDAP Server Port - Port of LDAP over SSL, default to 636 if not configured. Non-SSL port is not supported in CMC version 3.0 as the password cannot be transported without SSL.
- Use DNS to find LDAP Servers - Selecting this option causes LDAP to use the search domain and the service name through DNS. You must select Static or 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.

Managing LDAP Group Settings

The table in the Group Settings section lists role groups, displaying associated names, domains, and privileges for any role groups that are already configured.

- To configure a new role group, click a role group name that does not have a name, domain, and privilege listed.
- To change the settings for an existing role group, click the role group name.

When you click a role group name, the **Configure Role Group** page appears. Help for that page is available through the **Help** link at the top right corner of the page.

Managing LDAP Security Certificates

This sections displays the properties for the LDAP certificate recently uploaded to CMC. If you uploaded a certificate, use this information to verify that the certificate is valid and has not expired.



NOTE: By default, CMC does not have a certificate authority-issued server certificate for Active Directory. You must upload a current, certificate authority-signed server certificate.

The following properties for the certificate are displayed:

- Serial Number - The certificate's serial number.
- Subject Information - The certificate's subject (name of the person or company certified).
- Issuer Information - The certificate's issuer (name of the Certificate Authority).
- Valid From - The starting date of the certificate.
- Valid To - The expiry date of the certificate.

Use the following controls to upload and download this certificate:

- Upload - Initiates the upload process for the certificate. This certificate, which you obtain from your LDAP server, grants access to CMC.
- Download - Initiates the download process. You are prompted for the location to save the file. When you select this option and click **Next**, a **File Download** dialog box appears. Use this dialog box to specify a location on your management station or shared network for the server certificate.

Securing CMC Communications Using SSL and Digital Certificates

This subsection provides information about the following data security features that are incorporated in your CMC:

- Secure Sockets Layer (SSL)
- Certificate Signing Request (CSR)
- Accessing the SSL Main Menu
- Generating a new CSR
- Uploading a Server Certificate
- Viewing a Server Certificate

Secure Sockets Layer (SSL)

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.

Accessing the SSL Main Menu



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.

- 1 Log in to the Web interface.
- 2 Click the **Network** tab, and then click the **SSL** subtab. The **SSL Main Menu** page appears.

Use the **SSL Main Menu** page options to generate a CSR to send to a certificate authority. The CSR information is stored on the CMC firmware.

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.

Table 5-46. SSL Main Menu Options

Field	Description
Generate a New Certificate Signing Request (CSR)	Select this option and click Next to open the Generate Certificate Signing Request (CSR) page, where you can generate a CSR request for a secure Web certificate to submit to a certificate authority. NOTE: Each new CSR overwrites any previous CSR on CMC. For a certificate authority to accept your CSR, the CSR in CMC must match the certificate returned from the certificate authority.
Upload Server Certificate Based on Generated CSR	Select this option and click Next to display the Certificate Upload page, where you can upload an existing certificate that your company holds title to and uses to control access to CMC. NOTE: Only X509, Base 64-encoded certificates are accepted by CMC. DER-encoded certificates are not accepted. Uploading a new certificate replaces the default certificate you received with your CMC.
Upload Webserver key and Certificate	Select this option and click Next to open the Webserver Key and Certificate Upload page, where you can upload an existing Web server key and server certificate that your company holds title to and uses to control access to CMC. NOTE: Only X.509, Base64 encoded certificates are accepted by CMC. Binary DER-encoded certificates are not accepted. Uploading a new certificate replaces the default certificate you received with your CMC.
View Server Certificate	Select the option and click the Next button to open the View Server Certificate page where you can view the current server certificate.

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.

When a CSR is generated from the **Generate Certificate Signing Request (CSR)** page, 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.

To generate a CSR:

- 1 From the **SSL Main Menu** page, select **Generate a New Certificate Signing Request (CSR)**, and then click **Next**. The **Generate Certificate Signing Request (CSR)** page displays.
- 2 Type a value for each CSR attribute value.
- 3 Click **Generate**. A **File Download** dialog box appears.
- 4 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.

Table 5-47. Generate Certificate Signing Request (CSR) Page Options

Field	Description
Common Name	<p>The exact name being certified (usually the Web server's domain name, for example, www.xyzcompany.com/).</p> <p>Valid: Alphanumeric characters (A–Z, a–z, 0–9); hyphens, underscores, and periods.</p> <p>Not valid: Non-alphanumeric characters not noted above (such as, but not limited to, @ # \$ % & *); characters used primarily in non-English languages, such as ß, å, é, ü.</p>
Organization Name	<p>The name associated with your organization (example: XYZ Corporation).</p> <p>Valid: Alphanumeric characters (A–Z, a–z, 0–9); hyphens, underscores, periods, and spaces.</p> <p>Not valid: Non-alphanumeric characters not noted above (such as, but not limited to, @ # \$ % & *).</p>
Organization Unit	<p>The name associated with an organizational unit, such as a department (example: Enterprise Group).</p> <p>Valid: Alphanumeric characters (A–Z, a–z, 0–9); hyphens, underscores, periods, and spaces.</p> <p>Not valid: Non-alphanumeric characters not noted above (such as, but not limited to, @ # \$ % & *).</p>
Locality	<p>The city or other location of your organization (examples: Atlanta, Hong Kong).</p> <p>Valid: Alphanumeric characters (A–Z, a–z, 0–9) and spaces.</p> <p>Not Valid: Non-alphanumeric characters not noted above (such as, but not limited to, @ # \$ % & *).</p>
State	<p>The state, province, or territory where the entity that is applying for a certification is located (examples: Texas, New South Wales, Andhra Pradesh).</p> <p>NOTE: Do not use abbreviations.</p> <p>Valid: Alphanumeric characters (upper- and lower-case letters; 0–9); and spaces.</p> <p>Not valid: Non-alphanumeric characters not noted above (such as, but not limited to, @ # \$ % & *).</p>

Table 5-47. Generate Certificate Signing Request (CSR) Page Options (continued)

Field	Description
Country	The country where the organization applying for certification is located.
Email	Your organization's e-mail address. You may type any e-mail address you want to have associated with the CSR. The e-mail address must be valid, containing the at (@) sign (example: name@xyzcompany.com). NOTE: This e-mail address is an optional field.

Uploading a Server Certificate

- 1 From the **SSL Main Menu** page, select **Upload Server Certificate Based on Generated CSR**, and then click **Next**. The **Certificate Upload** page displays.
- 2 Type the file path in the text field, or click **Browse** to select the file.
- 3 Click **Apply**. If the certificate is invalid, an error message displays.



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.

To refresh the contents of the **Certificate Upload** page, click **Refresh**.

To print the contents of the **Certificate Upload** page, click **Print**.

Uploading Webserver Key and Certificate

- 1 Select **Upload Webserver Key and Certificate** option, and then click **Next**.
- 2 Enter **Private Key File** using the browse menu.
- 3 Enter **Certificate File** using the browse menu.
- 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.



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

 **NOTE:** 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.

Viewing a Server Certificate

From the **SSL Main Menu** page, select **View Server Certificate**, and then click **Next**. The **View Server Certificate** page displays.

Table 5-48 describes the fields and associated descriptions listed in the **Certificate** window.

Table 5-48. Certificate Information

Field	Description
Serial	Certificate serial number.
Subject	Certificate attributes entered by the subject.
Issuer	Certificate attributes returned by the issuer.
notBefore	Issue date of the certificate.
notAfter	Expiration date of the certificate.

To refresh the contents of the **View Server Certificate** page, click **Refresh**.

To print the contents of the **View Server Certificate** page, click **Print**.

Managing Sessions

The **Sessions** page displays all current instances of connections to the chassis and allows you to terminate any active session.

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

To manage or terminate a session:

- 1 Log in to CMC through the Web.
- 2 Click the **Network** tab then click the **Sessions** subtab.
- 3 On the **Sessions** page, locate the session you want to terminate and click the appropriate button.

Table 5-49. Sessions Properties

Property	Description
Session ID	Displays the sequentially generated ID number for each instance of a login.
Username	Displays the user's login name (local user or Active Directory user). Examples of Active Directory user names are <i>name@domain.com</i> , <i>domain.com/name</i> , <i>domain.com\name</i> .
IP Address	Displays the user's IP address.
Session Type	Describes the session type: Telnet, serial, SSH, Remote RACADM, SMASH CLP, WSMAN, or a GUI session.
Terminate	Allows you to terminate any of the sessions listed, except for your own. To terminate the associated session, click the button. This column is displayed only if you have Chassis Configuration Administrator privileges.

Configuring Services

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 CLI tool for communicating to CMC.

 **NOTE:** The remote (RACADM) CLI tool and the Web interface use the Web server. In the event that the Web Server is not active, the remote RACADM and the Web interface are not operable.

 **NOTE:** In an event of a Web server reset, 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: the network configuration or network security properties are changed through the CMC Web user interface or RACADM; the 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.

To configure CMC services:

- 1 Log in to the CMC Web interface.
- 2 Click the **Network** tab.
- 3 Click the **Services** subtab. The **Services** page appears.
- 4 Configure the following services as required:
 - CMC serial console (Table 5-50)
 - Web server (Table 5-51)
 - SSH (Table 5-52)
 - Telnet (Table 5-53)
 - Remote RACADM (Table 5-54)
 - SNMP (Table 5-55)
 - Remote Syslog (Table 5-56)
- 5 Click **Apply**, and then update all default time outs and maximum time out limits

Table 5-50. CMC Serial Console Settings

Setting	Description
Enabled	Enables Telnet console interface on CMC. Default: Unchecked (disabled)
Redirect Enabled	Enables the serial/text console redirection to the server through your serial/Telnet/SSH client from CMC. The CMC connects to iDRAC that internally connects to the server COM2 port. Configuration options: Checked (enabled), unchecked (disabled) Default: Checked (enabled)

Table 5-50. CMC Serial Console Settings (continued)

Setting	Description
Idle Timeout	<p>Displays the number of seconds before an idle serial session is automatically disconnected. A change to the Timeout setting takes effect at the next login; it does not affect the current session.</p> <p>Timeout Range: 0 or 60 to 10800 seconds. To disable the Timeout feature, enter 0.</p> <p>Default: 1800 seconds</p>
Baud Rate	<p>Displays the data speed on the external serial port on the CMC.</p> <p>Configuration options: 9600, 19200, 28800, 38400, 57600, and 115200 bps.</p> <p>Default: 115200 bps</p>
Authentication Disabled	<p>Enables CMC Serial Console login authentication.</p> <p>Default: Unchecked (disabled)</p>
Escape Key	<p>Allows you to specify the Escape key combination that terminates serial/text console redirection when using the connect or racadm connect command.</p> <p>Default: ^\ (Hold <Ctrl> and type a backslash (\) character)</p> <p> NOTE: The caret character ^ represents the <Ctrl> key.</p> <p>Configuration options:</p> <ul style="list-style-type: none">• Decimal value (example: 95)• Hexadecimal value (example: 0x12)• Octal value (example: 007)• ASCII value (example: ^a) <p>ASCII values may be represented using the following Escape key codes:</p> <ul style="list-style-type: none">• Esc followed by any alphabetic character (a-z, A-Z)• Esc followed by the following special characters: [] \ ^ _• Maximum Allowed Length: 4

Table 5-50. CMC Serial Console Settings (continued)

Setting	Description
History Size Buffer	Displays the maximum size of the serial history buffer, which holds the last characters written to the Serial Console. Default: 8192 characters
Login Command	Specifies the serial command that is automatically executed when a user logs into the CMC Serial Console interface. Example: connect server-1 Default: [Null]

Table 5-51. Web Server Settings

Setting	Description
Enabled	Enables Web Server services (access through remote RACADM and the Web interface) for CMC. Default: Checked (enabled)
Max Sessions	Displays the maximum number of simultaneous Web user interface sessions allowed for the chassis. A change to the Max Sessions property takes effect at the next login; it does not affect current Active Sessions (including your own). The remote RACADM is not affected by the Max Sessions property for the Web Server. Allowed range: 1–4 Default: 4 NOTE: If you change the Max Sessions property to a value less than the current number of Active Sessions and then log out, you cannot log back in until the other sessions have been terminated or expired.

Table 5-51. Web Server Settings (continued)

Setting	Description
Idle Timeout	<p>Displays the number of seconds before an idle Web user interface session is automatically disconnected. A change to the Timeout setting takes effect at the next login; it does not affect the current session.</p> <p>Timeout range: 60 to 10800 seconds.</p> <p>Default: 1800 seconds</p>
HTTP Port Number	<p>Displays the default port used by CMC that listens for a server connection.</p> <p>NOTE: When you provide the HTTP address on the browser, the Web server automatically redirects and uses HTTPS.</p> <p>If the default HTTP port number (80) has been changed, you must include the port number in the address in the browser address field, as shown:</p> <p style="padding-left: 40px;"><code>http://<IP address>:<port number></code></p> <p>where <i>IP address</i> is the IP address for the chassis, and <i>port number</i> is the HTTP port number other than the default of 80.</p> <p>Configuration range: 10–65535</p> <p>Default: 80</p>
HTTPS Port Number	<p>Displays the default port used by CMC that listens for a secured server connection.</p> <p>If the default HTTPS port number (443) has been changed, you must include the port number in the address in the browser address field, as shown:</p> <p style="padding-left: 40px;"><code>https://<IP address>:<port number></code></p> <p>where <i><IP address></i> is the IP address for the chassis, and <i><port number></i> is the HTTPS port number other than the default of 443.</p> <p>Configuration range: 10–65535</p> <p>Default: 443</p>

Table 5-52. SSH Settings

Setting	Description
Enabled	Enables the SSH on CMC. Default: Checked (enabled)
Max Sessions	The maximum number of simultaneous SSH sessions allowed for the chassis. A change to this property takes effect at the next login; it does not affect current Active Sessions (including your own). Configurable range: 1–4 Default: 4 NOTE: If you change the Max Sessions property to a value less than the current number of Active Sessions and then log out, you cannot log in again till the other sessions have been terminated or expired.
Idle Timeout	Displays the number of seconds before an idle SSH session is automatically disconnected. A change to the Timeout setting takes effect at the next login; it does not affect the current session. Timeout Range: 0 or 60–10800 seconds. To disable the Timeout feature, enter 0. Default: 1800 seconds
Port Number	Port used by CMC that listens for a server connection. Configuration range: 10–65535 Default: 22

Table 5-53. Telnet Settings

Setting	Description
Enabled	Enables Telnet console interface on CMC. Default: Unchecked (disabled)
Max Sessions	Displays the maximum number of simultaneous Telnet sessions allowed for the chassis. A change to this property takes effect at the next login; it does not affect current Active Sessions (including your own). Allowed range: 1–4 Default: 4 NOTE: If you change the Max Sessions property to a value less than the current number of Active Sessions and then log out, you cannot log in again until the other sessions have been terminated or expired.
Idle Timeout	Displays the number of seconds before an idle Telnet session is automatically disconnected. A change to the Timeout setting takes effect at the next login; it does not affect the current session. Timeout Range: 0 or 60–10800 seconds. To disable the Timeout feature, enter 0. Default: 1800 seconds
Port Number	Displays the port used by CMC that listens for a server connection. Default: 23

Table 5-54. Remote RACADM Settings

Setting	Description
Enabled	Enables the remote RACADM utility access to CMC. Default: Checked (enabled)
Max Sessions	Displays the maximum number of simultaneous RACADM sessions allowed for the chassis. A change to this property takes effect at the next login; it does not affect current Active Sessions (including your own). Allowed range: 1–4 Default: 4 NOTE: If you change the Max Sessions property to a value less than the current number of Active Sessions and then log out, you cannot log in again until the other sessions have been terminated or expired.
Idle Timeout	Displays the number of seconds before an idle racadm session is automatically disconnected. A change to the Idle Timeout setting takes effect at the next login; it does not affect the current session. To disable the Idle Timeout feature, enter 0. Timeout Range: 0, or 10 to 1920 seconds. To disable the Timeout feature, enter 0. Default: 30 seconds

Table 5-55. SNMP Configuration

Setting	Description
Enabled	Enables SNMP on CMC. Valid Values: Checked (enabled), unchecked (disabled) Default: unchecked (disabled)
Community Name	Displays the community string used to get data from CMC's SNMP daemon.

Table 5-56. Remote Syslog Configuration

Setting	Description
Enabled	Enables the transmission and remote capture of CMC log and Hardware log entries to the specified server(s). Valid values: Checked (enabled), unchecked (disabled) Default: unchecked (disabled)
Syslog Server 1	The first of three possible servers to host a copy of the CMC and hardware log entries. Specified as a Host Name, an IPv6 address, or an IPv4 address.
Syslog Server 2	The second of three possible servers to host a copy of the CMC and hardware log entries. Specified as a Host Name, an IPv6 address, or an IPv4 address.
Syslog Server 3	The third of three possible servers to host a copy of the CMC and hardware log entries. Specified as a Host Name, an IPv6 address, or an IPv4 address.
Syslog Port Number	Specifies the port number on the remote server for receiving a copy of CMC and hardware log entries. The same port number is used for all three servers. A valid syslog port number is in the 10-65535 range. Default: 514

Configuring Power Budgeting

CMC allows you to budget and manage power to the chassis. The power management service optimizes power consumption and re-allocates power to different modules based on the demand.

For instructions on configuring power through CMC, see "Configuring and Managing Power" on page 308.

For more information on CMC's power management service, see "Power Management" on page 289.

Managing Firmware Updates

This section describes how to use the Web interface to update firmware. The following Chassis components can be updated using the GUI or RACADM commands:

- CMC — active and standby
- iKVM
- iDRAC
- IOM infrastructure devices

When you update firmware, there is a recommended process to follow that can prevent a loss of service if the update fails. See "Installing or Updating the CMC Firmware" on page 49 for guidelines to follow before you use the instructions in this section.

Viewing the Current Firmware Versions

The Update page displays the current version of all the updatable components in the chassis. These may include the iKVM firmware, active CMC firmware, (if applicable) the standby CMC firmware, the iDRAC firmware, and the IOM infrastructure device firmware. For more information see "Updating the IOM Infrastructure Device Firmware" on page 193.

To open an update page for selected devices:

- 1 Click on the device name or select the **Select/Deselect All** check box.
- 2 Click **Apply Update**.

An update page for the selected devices displays.

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. See "Recovering iDRAC Firmware Using CMC" on page 195 for the steps to recover iDRAC firmware using CMC.

To view the chassis components that can be updated:

- 1 Log in to the Web interface. For more information, see "Accessing the CMC Web Interface" on page 103.
- 2 Click **Chassis Overview** in the system tree.
- 3 Click the **Update** tab. The **Firmware Update** page appears.

To view the updatable server components:

- 1 Log in to the Web interface. For more information, see "Accessing the CMC Web Interface" on page 103.
- 2 Click **Server Overview** in the system tree.
- 3 Click the **Update** tab. The **Server Component Update** appears.

Updating Firmware



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



NOTE: The firmware update retains the current CMC and iKVM settings.



NOTE: 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" on page 180.

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. The basic steps involved in updating device firmware are:

- Select the devices to update
- Click the **Apply** button below the grouping
- Click **Browse** to select the firmware image
- Click **Begin Firmware Update** to start the update process. A message that states **Transferring file image** is displayed, followed by a status progress page.



NOTE: Be sure you have the latest firmware version. You can download the latest firmware image file from the Dell Support website at support.dell.com.

Updating the CMC Firmware



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



NOTE: 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.

 **NOTE:** To avoid disconnecting other users during a reset, notify authorized users who might 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. Help for that page is available through the **Help** link at the top right corner of the page.

 **NOTE:** When transferring files to and from CMC, the file transfer icon spins during the transfer. If your icon is not animated, make sure that your browser is configured to allow animations. See "Allow Animations in Internet Explorer" on page 39 for instructions.

 **NOTE:** If you experience problems downloading files from CMC using Internet Explorer, enable the **Do not save encrypted pages to disk** option. See "Downloading Files From CMC With Internet Explorer" on page 39 for instructions.

To update the CMC firmware:

1 On the **Firmware Update** page, select CMC or CMCs to update by selecting the **Update Targets** check box for CMC(s). Both CMCs can be updated at the same time.

2 Click the **Apply CMC Update** button below the CMC component list.

 **NOTE:** The default CMC firmware image name is **firmimg.cmc**. CMC firmware should be updated first, before updating IOM infrastructure device firmware.

3 In the **Firmware Image** field, enter the path to the firmware image file on your management station or shared network, or click **Browse** to navigate to the file location.

4 Click **Begin Firmware Update**. 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 can vary greatly based on connection speed. When the internal update process begins, the page automatically refreshes and the Firmware update timer displays.

Additional instructions to follow:

- Do not use the **Refresh** button 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.

- Update status displays in the **Update State** field; this field is automatically updated during the file transfer process.



NOTE: The update may take several minutes for CMC.

- 5 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. See your Web browser's online help for instructions on how to clear the browser cache.

Updating the iKVM Firmware



NOTE: The iKVM resets and becomes temporarily unavailable after the firmware has been uploaded successfully.

- 1 Log back in to CMC Web interface.
- 2 Select **Chassis Overview** in the system tree.
- 3 Click the **Update** tab. The **Firmware Update** page appears.
- 4 Select the iKVM to update by selecting the **Update Targets** check box for that iKVM.
- 5 Click the **Apply iKVM Update** button below the iKVM component list.
- 6 In the **Firmware Image** field, enter the path to the firmware image file on your management station or shared network, or click **Browse** to navigate to the file location.



NOTE: The default iKVM firmware image name is **ikvm.bin**; however, the iKVM firmware image name can be changed by the user to avoid confusion with previous images.

- 7 Click **Begin Firmware Update**.
- 8 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 can vary greatly based on connection speed. When the internal update process begins, the page automatically refreshes and the Firmware update timer displays. Additional instructions to follow:

- Do not use the **Refresh** button 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.
- Update status displays in the **Update State** field; this field is automatically updated during the file transfer process.



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

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

Updating the 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 GUI only if the current revision on the component and the component image on CMC do not match.

- 1 Log back in to CMC Web interface.
- 2 Select **Chassis Overview** in the system tree.
- 3 Click the **Update** tab. The **Firmware Update** page appears.
- 4 Select the IOM device to update by selecting the **Update Targets** check box for that IOM device.
- 5 Click the **Apply IOM Update** button below the IOM component list.



NOTE: The **Firmware Image** field does not display for an IOM infrastructure device (IOMINF) target because the required image resides on CMC. CMC firmware should be updated first, before updating IOMINF firmware.

IOMINF updates are allowed by CMC 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 be listed as updatable devices.

- 6 Click **Begin Firmware Update**. 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 can vary greatly

based on connection speed. When the internal update process begins, the page automatically refreshes and the Firmware update timer displays. Additional instructions to follow:

- Do not use the **Refresh** button or navigate to another page during the file transfer.
- Update status displays in the **Update State** field; this field is automatically updated during the file transfer process.



NOTE: No file transfer timer is displayed when updating IOMINF firmware. The update process may cause a brief loss of connectivity to the IOM device since the device performs a restart when the update is complete. When the update is complete, the new firmware is displayed and the updated system is no longer present on the **Firmware Update** page.

Updating the Server iDRAC Firmware



NOTE: The iDRAC (on a Server) resets and become temporarily unavailable after firmware updates have been uploaded successfully.



NOTE: The iDRAC firmware must be at version 1.4 or greater for servers with iDRAC, or 2.0 or greater for servers with iDRAC6 Enterprise.

- 1 Log back in to the CMC Web interface.
- 2 Select **Chassis Overview** in the system tree.
- 3 Click the **Update** tab. The **Firmware Update** page appears.
- 4 Select the iDRAC or iDRACs to update by selecting the **Update Targets** check box those devices.
- 5 Click the **Apply iDRAC Update** button below the iDRAC component list.
- 6 In the **Firmware Image** field, enter the path to the firmware image file on your management station or shared network, or click **Browse** to navigate to the file location.
- 7 Click **Begin Firmware Update**. 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 can vary greatly based on connection speed. When the internal update process begins, the page automatically refreshes and the firmware update timer displays. Additional instructions to follow:
 - Do not use the **Refresh** button 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.
- Update status displays in the **Update State** field; this field is automatically updated during the file transfer process.



NOTE: The update may take several minutes for CMC or Server.

Recovering iDRAC Firmware Using CMC

iDRAC firmware is typically updated using iDRAC facilities such as the iDRAC Web interface, the SM-CLP command line interface, or operating system specific update packages downloaded from support.dell.com. See the *iDRAC Firmware User's Guide* for instructions for updating the iDRAC firmware.

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.

Follow these steps to update the iDRAC firmware.

- 1 Download the latest iDRAC firmware to your management computer from support.dell.com.
- 2 Log in to the Web interface (see "Accessing the CMC Web Interface" on page 103).
- 3 Click **Chassis Overview** in the system tree.
- 4 Click the **Update** tab. The **Firmware Update** page appears.
- 5 Select the iDRAC or iDRACs of the same model to update by selecting the **Update Targets** check box those devices.
- 6 Click the **Apply iDRAC Update** button below the iDRAC component list.
- 7 Click **Browse**, browse to the iDRAC firmware image you downloaded, and click **Open**.



NOTE: The default iDRAC firmware image name is **firmimg.imc**. CMC firmware should be updated first, before updating IOM infrastructure device firmware.

- 8 Click **Begin Firmware Update**. Additional instructions to follow:
 - Do not use the **Refresh** button 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.
- Update status displays in the **Update State** field; this field is automatically updated during the file transfer process.



NOTE: It can take up to ten minutes to update the iDRAC firmware.

Managing iDRAC

CMC provides the **Deploy iDRAC** page to allow the user to configure installed and newly inserted server's iDRAC network configuration settings. A user can configure one or more installed iDRAC devices from this page. The user can also configure the default iDRAC network configuration settings and root password for servers that are installed later; these default settings are the **iDRAC QuickDeploy** settings.

For more information on the behaviour of iDRAC, see the *iDRAC User's Guides* on the Dell Support website at support.dell.com/manuals.

iDRAC QuickDeploy

The **iDRAC QuickDeploy** section of the **Deploy iDRAC** page contains network configuration settings that are applied to newly inserted servers. You may use these settings to automatically populate the **iDRAC Network Settings** table that is below the **QuickDeploy** section. Once **QuickDeploy** is enabled, the **QuickDeploy** settings are applied to servers when that server is installed. See step 8 in "Configuring Networking Using the LCD Configuration Wizard" on page 41 for more information on the iDRAC **QuickDeploy** settings.

Follow these steps to enable and set the **iDRAC QuickDeploy** settings:

- 1 Log in to the CMC Web interface.
- 2 Select **Server Overview** in the system tree.
- 3 Click the **Setup** tab. The **Deploy iDRAC** page appears.
- 4 Set the **QuickDeploy** settings accordingly.

Table 5-57. QuickDeploy Settings

Setting	Description
QuickDeploy Enabled	Enables/disables the QuickDeploy feature that automatically applies the iDRAC settings configured on this page to newly inserted servers; the auto configuration <i>must</i> 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. Default: Unchecked (disabled)
Set iDRAC Root Password on Server Insertion	Specifies whether a server's iDRAC root password should be changed to the value provided in the iDRAC Root Password text box when the server is inserted.
iDRAC Root Password	When Set iDRAC Root Password on Server Insertion and QuickDeploy Enabled are checked, this 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/disables the iDRAC LAN channel. Default: Unchecked (disabled)
Enable iDRAC IPv4	Enables/disables IPv4 on iDRAC. Default setting is enabled.
Enable iDRAC IPMI over LAN	Enables/disables the IPMI over LAN channel for each iDRAC present in the chassis. Default: Unchecked (disabled)
Enable iDRAC DHCP	Enables/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 can not be modified since DHCP is used to automatically assign these settings for each iDRAC. Default: Unchecked (disabled)

Table 5-57. QuickDeploy Settings (continued)

Setting	Description
Starting iDRAC IPv4 Address (Slot 1)	<p>Specifies the static IP address of the iDRAC of 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.</p> <p>NOTE: The subnet mask and the gateway are not incremented like the IP address.</p> <p>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 either the Save QuickDeploy Settings or Auto-Populate Using QuickDeploy Settings buttons are pressed.</p>
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 stateless address auto configuration. Default setting is enabled.
iDRAC IPv6 Gateway	Specifies the default IPv6 gateway to be assigned to the iDRACs. Default setting is "::".
iDRAC IPv6 Prefix Length	Specifies the prefix length to be assigned for the IPv6 addresses on the iDRAC. Default setting is 64.

- 5 To save the selections click the **Save QuickDeploy Settings** button. If you made changes to the iDRAC network setting, click the **Apply iDRAC Network Settings** button to deploy the settings to the iDRAC.

- 6 To update the table to the last saved QuickDeploy settings, and restore the iDRAC Network settings to the current values for each installed server, click **Refresh**.



NOTE: Clicking the **Refresh** button deletes all iDRAC QuickDeploy and iDRAC Network configuration settings that have not been saved.

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 checked, 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. Pressing the **Refresh** button too soon may display only partially correct data for one or more iDRAC servers.

iDRAC Network Settings

The **iDRAC Network Settings** section of the **Deploy iDRAC** page contains a table listing all installed server's iDRAC IPv4 and IPv6 network configuration settings. 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. Changing a field and clicking **Apply iDRAC Network Settings** saves the changed field to the iDRAC. Follow these steps to enable and set the **iDRAC Network Settings**:

- 1 Log in to the CMC Web interface.
- 2 Select **Server Overview** in the system tree.
- 3 Click the **Setup** tab.
The **Deploy iDRAC** page appears.
- 4 Select the check box for **QuickDeploy Enabled** to enable the QuickDeploy settings.
- 5 Set the remaining **iDRAC Network Settings** accordingly.

Table 5-58. iDRAC Network Settings

Setting	Description
Slot	Displays the slot occupied by the server in the chassis. Slot numbers are sequential IDs, from 1 to 16 (there are 16 slots available on the chassis), that help identify the location of the server in the chassis. NOTE: When there are fewer than 16 servers occupying slots, only those slots populated by servers are displayed.
Name	Displays the server name of the server in each slot. By default, the slots are named SLOT-01 to SLOT-16 . NOTE: The slot name cannot be blank or NULL.
Enable LAN	Enables (checked) or disables (unchecked) the LAN channel. NOTE: When LAN is not selected (disabled), all other network configuration settings, (IPMI over LAN, DHCP, IP Address Subnet Mask and Gateway) are not used. These fields are not accessible.

Table 5-58. iDRAC Network Settings (continued)

Setting	Description
Change Root Password	Enables (when checked) the ability to change the password of the iDRAC root user. The iDRAC Root Password and Confirm iDRAC Root Password fields must be provided for this operation to be successful.
DHCP	If selected DHCP is used to acquire the iDRAC IP address, subnet mask and default gateway, otherwise the values defined in the iDRAC network configuration fields are used. LAN must be enabled to set this field
IPMI over LAN	Enables (checked) or disables (unchecked) the IPMI LAN channel. LAN must be enabled to set this field.
IP Address	The static IPv4 or IPv6 address assigned to the iDRAC located in this slot.
Subnet Mask	Specifies the subnet mask assigned to the iDRAC installed in this slot.
Gateway	Specifies the default gateway assigned to the iDRAC which is installed in this slot.
Enable IPv4	Enables the iDRAC in the slot to use the IPv4 protocol on the network. You must select the Enable LAN option for this option to be active. Default setting is enabled.
Enable IPv6	Enables the iDRAC in the slot to use the IPv6 protocol on the network. You must select the Enable LAN option and clear the Autoconfiguration option for this option to be active. Default setting is disabled. NOTE: This option is available only if the server is IPv6 capable.
Autoconfiguration	Enables the iDRAC to obtain IPv6 settings (Address and prefix length) from a DHCPv6 server and also enables stateless address auto configuration. NOTE: This option is available only if the server is IPv6 capable.
Prefix Length	Specifies the length, in bits, of the IPv6 subnet to which this iDRAC belongs.

- 6 To deploy the setting to iDRAC, click **Apply iDRAC Network Settings** button. If you made changes to the **QuickDeploy** settings, they are also saved.
- 7 To restore the iDRAC Network settings to the current values for each installed server, and update the **QuickDeploy** table to the last saved **QuickDeploy** settings click **Refresh**.

 **NOTE:** Clicking **Refresh** button deletes all iDRAC QuickDeploy and iDRAC Network configuration settings that have not been 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. Press the **Refresh** button 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. Pressing the **Refresh** button too soon may display only partially correct data for a one or more iDRAC servers.

Launching Remote Console from CMC GUI

This feature allows you to launch a Keyboard-Video-Mouse (KVM) session directly on the server.

To launch a server remote console from the CMC GUI Homepage:

- 1 Click on the specified server in the chassis graphic.
- 2 On **Quicklinks**, click the **Launch Remote Console** link.

To launch a server remote console from the **Servers Status** page:

- 1 On System tree, select **Server Overview**.
- 2 Click **Launch Remote Console** in the table for the specified server.

To launch a server Remote Console for an individual:

- 1 Expand **Server Overview** in the system tree. All servers (1–16) appear in the expanded servers list.
- 2 In the system tree, click the server you want to view. The **Server Status** page appears.
- 3 Click **Launch Remote Console**.

The remote console feature is supported only when all of the following conditions are met:

- The chassis power is on.
- Server is PowerEdge M610, M610X, M710, M710HD, or M910.
- 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).



NOTE: Remote Console can also be launched from the iDRAC GUI. See iDRAC GUI for more details.

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.

To launch the iDRAC management console from the **Servers** page:

- 1 Log in to the CMC Web interface.
- 2 Select **Server Overview** in the system tree. The **Servers Status** page appears.
- 3 Click the **Launch iDRAC GUI** button for the server you want to manage.

To launch the iDRAC management console for an individual server:

- 1 Log in to the CMC Web interface.
- 2 Expand **Server Overview** in the system tree. All of the servers (1–16) appear in the expanded **Servers** list.
- 3 Click the server you want to view. The **Server Status** page displays.
- 4 Click the **Launch iDRAC GUI** button.

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

- 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** button 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.



NOTE: If the server is removed from the chassis, the iDRAC IP address is changed, or the iDRAC network connection experiences a problem, then clicking the Launch iDRAC GUI icon may display an error page.

FlexAddress

This section describes the FlexAddress Web interface screens. 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:** You must purchase and install the FlexAddress upgrade to have access to the configuration screens. If the upgrade has not been 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.

Viewing FlexAddress Status

You can use the Web interface to view FlexAddress status information. You can view status information for the entire chassis or for an individual server. The information displayed includes:

- Fabric configuration.
- FlexAddress active/not active.
- Slot number and name.
- Chassis-assigned and server-assigned addresses.
- Addresses in use.

 **NOTE:** You can also view FlexAddress status using the command line interface. For more command information, see "Using FlexAddress" on page 217.

Viewing Chassis FlexAddress Status

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 whether FlexAddress is active for the chassis:

- 1 Log in to the Web interface (see "Accessing the CMC Web Interface" on page 103).
- 2 Click **Chassis Overview** in the system tree.
- 3 Click the **Setup** tab. The **General Setup** page appears. The FlexAddress entry has a value of **Active** or **Not Active**; a value of active means that the feature is installed on the chassis. A value of not active means that the feature is not installed and not in use on the chassis.

To display a FlexAddress status overview for each server module:

- 1 Log in to the Web interface ("Accessing the CMC Web Interface" on page 103).
- 2 Click **Server Overview**→**Properties**→**WWN/MAC**.
- 3 The **FlexAddress Summary** page is displayed. This page allows you to view the WWN configuration and MAC addresses for all slots in the chassis.

The status page presents the following information:

Fabric Configuration	<p>Fabric A, Fabric B, and Fabric C display the type of the Input/Output fabric installed.</p> <p>iDRAC displays the server management MAC address.</p> <p>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.</p>
WWN/MAC Addresses	<p>Displays FlexAddress configuration for each slot in the chassis. Information displayed includes:</p> <ul style="list-style-type: none">• iDRAC management controller is not a fabric but its FlexAddress is treated like one.• Slot number and location• FlexAddress active/not active status• Fabric type• Server-assigned and chassis-assigned WWN/MAC addresses in use <p>A green check mark indicates the active address type, either server-assigned or chassis-assigned.</p>

- 4 For additional information, click **Help**.

Viewing Server FlexAddress Status

FlexAddress status information can also be displayed for each individual server. The server level information displays a FlexAddress status overview for that server.

To view FlexAddress server information:

- 1 Log in to the Web interface (see "Accessing the CMC Web Interface" on page 103).
- 2 Expand **Server Overview** in the system tree. All of the servers (1–16) appear in the expanded **Servers** list.
- 3 Click the server you want to view.
The **Server Status** page displays.
- 4 Click the **Setup** tab, and the **FlexAddress** subtab. The **Deploy FlexAddress** page is displayed. This page allows you to view the WWN configuration and MAC addresses for the selected server.

The status page presents the following information:

Table 5-59. Status Page Information

FlexAddress Enabled	Displays whether the FlexAddress feature is active or not active for the particular slot.
Current State	Displays the current FlexAddress configuration: <ul style="list-style-type: none">• Chassis-Assigned - selected slot address is chassis assigned using the FlexAddress. The slot-based WWN/MAC addresses remain the same even if a new server is installed.• Server-Assigned - server uses the server-assigned address or the default address embedded into the controller hardware.
Power State	Displays the current power status of the servers; values are: On , Powering On , Powering Off , Off , and N/A (if a server is not present).

Table 5-59. Status Page Information

Health		OK	Indicates that FlexAddress is present and providing status to CMC. In the event of a communication failure between CMC and FlexAddress, CMC cannot obtain or display health status for FlexAddress.
		Informational	Displays information about FlexAddress when no change in health status (OK, Warning, Critical) has occurred.
		Warning	Indicates that only warning alerts have been issued, and corrective action must be taken . If corrective actions are not taken, then critical failures that can affect the integrity of the server could occur.
		Critical	Indicates that at least one Failure alert has been issued. Critical status represents a system failure on the server, and corrective action must be taken immediately .
		No Value	When FlexAddress is absent, health information is not provided.
iDRAC firmware	Displays the iDRAC version currently installed on the server.		
BIOS Version	Displays the current BIOS version of the server module.		
Slot	Slot number of the server associated with the fabric location.		
Location	Displays the location of the Input/Output (I/O) module in the chassis by group number (A, B, or C) and slot number (1 or 2). Slot names: A1, A2, B1, B2, C1, or C2.		
Fabric	Displays the type of fabric.		
Server-Assigned	Displays the server-assigned WWN/MAC addresses that are embedded in the controller's hardware.		
Chassis-Assigned	Displays the chassis-assigned WWN/MAC addresses that are used for the particular slot.		

5 For additional information, click **Help**.

Configuring FlexAddress

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. See support.dell.com/manuals for this document.

The server must be off before you begin configuration. You can enable or disable FlexAddress on a per fabric basis. Additionally, you can enable/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: You can also configure FlexAddress using the command line interface. For more command information, see "Using FlexAddress" on page 217.

Chassis-Level Fabric and Slot FlexAddress Configuration

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.

Perform the following steps to enable or disable fabrics and slots to use the FlexAddress feature:

- 1 Log on to the Web interface (see "Accessing the CMC Web Interface" on page 103).
- 2 Click **Server Overview** in the system tree.
- 3 Click the **Setup** tab → **FlexAddress** subtab. The **Deploy FlexAddress** page is displayed.
- 4 The **Select Fabrics for Chassis-Assigned WWN/MACs** displays a check box for **Fabric A**, **Fabric B**, **Fabric C**, and **iDRAC**.
- 5 Click the check box for each fabric you want to enable FlexAddress on. To disable a fabric, click the check box to clear the selection.

 **NOTE:** If no fabrics are selected, FlexAddress is not be enabled for the selected slots.

The **Select Slots for Chassis-Assigned WWN/MACs** page displays an **Enabled** check box for each slot in the chassis (1 - 16).

- 6 Click the **Enabled** check box for each slot you want to enable FlexAddress on. If you want to select all slots, use the **Select/Deselect All** check box. To disable a slot, click the **Enabled** check box to clear the selection.

 **NOTE:** If a server is present in the slot, it needs to be powered off before the FlexAddress feature can be enabled on that slot.

 **NOTE:** If no slots are selected, FlexAddress is not be enabled for the selected fabrics.

- 7 Click **Apply** to save the changes.
For additional information, click **Help**.

Server-Level Slot FlexAddress Configuration

At the server level, you can enable or disable the FlexAddress feature for individual slots.

To enable or disable an individual slot to use the FlexAddress feature:

- 1 Log in to the Web interface (see "Accessing the CMC Web Interface" on page 103).
- 2 Expand **Server Overview** in the system tree. All of the servers (1–16) appear in the expanded **Servers** list.
- 3 Click the server you want to view. The **Server Status** page displays.
- 4 Click the **Setup** tab, and the **FlexAddress** subtab. The **FlexAddress Status** page is displayed.
- 5 Use the pull down menu for **FlexAddress Enabled** to make your selection; select **Yes** to enable FlexAddress or select **No** to disable FlexAddress.
- 6 Click **Apply** to save the changes. For additional information, click **Help**.

Remote File Sharing

The Remote Virtual Media File Share option 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.

- 1 Log in to the Web interface (see "Accessing the CMC Web Interface" on page 103).
- 2 Click **Server Overview** in the system tree.
- 3 Click the **Setup** tab, and the **Remote File Sharing** subtab. The **Deploy Remote File Share** page is displayed.
- 4 Set the Remote File Sharing settings.

Table 5-60. Remote File Sharing Settings

Setting	Description
Image File Path	<p>Image File Path is only needed for connect and deploy operations. It does not apply to disconnect operations. The path name of the network drive is mounted to the server through a Windows SMB or Linux/Unix NFS protocol.</p> <p>For example, to connect to CIFS:</p> <pre>//<IP to connect for CIFS file system>/<file path>/<image name></pre> <p>To connect to NFS:</p> <pre>//<IP to connect for NFS file system>:/<file path>/<image name></pre> <p>File names that end with .img are connected as virtual floppies. File names that end with .iso are connected as virtual CD/DVDs. The maximum number of characters is 511.</p>
User Name	<p>User Name is only needed for connect and deploy operations. It does not apply to disconnect operations. The maximum number of characters you can specify in this field is 40.</p>
Password	<p>Password is only needed for connect and deploy operations. It does not apply to disconnect operations. The maximum number of characters you can specify in this field is 40.</p>

Table 5-60. Remote File Sharing Settings (continued)

Setting	Description
Slot	Identifies the location of the slot. Slot numbers are sequential from 1 to 16 (for the 16 available slots in the chassis).
Name	Displays the name of the slot. Slots are named depending on their position in the chassis.
Model	Displays the model name of the server.
Power State	Displays the power status of the server: N/A – CMC has not yet determined the power state of the server. Off – Either the server is off or the chassis is off. On – Both the chassis and the server are on. Powering On – Temporary state between Off and On. On success, the Power State is On. Powering Off – Temporary state between On and Off. On success, the Power State is Off.
Connect Status	Displays the remote file share connection status.
Select/Deselect All	Select this option before initiating a remote file share operation. Remote file share operations are: Connect, Disconnect, and Deploy.

5 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.

Frequently Asked Questions

Table 5-61 lists the frequently asked questions while managing or recovering a remote system.

Table 5-61. Managing and Recovering a Remote System

Question	Answer
<p>When accessing the CMC Web interface, I get a security warning stating the host name of the SSL certificate does not match the host name of CMC.</p>	<p>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).</p> <p>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.</p> <p>To ensure that the CSR matches the registered DNS CMC name:</p> <ol style="list-style-type: none">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 check box.4 Enter the CMC name In the DNS CMC Name field.5 Click Apply Changes. <p>For more information about generating CSRs and issuing certificates, see "Securing CMC Communications Using SSL and Digital Certificates" on page 173.</p>

Table 5-61. Managing and Recovering a Remote System (continued)

Question	Answer
Why are the remote RACADM and Web-based services unavailable after a property change?	<p>It may take a minute for the remote RACADM services and the Web interface to become available after the CMC Web server resets.</p> <p>The CMC Web server is reset after the following occurrences:</p> <ul style="list-style-type: none">• When changing the network configuration or network security properties using the CMC Web user interface• When the <code>cfgRacTuneHttpsPort</code> property is changed (including when a <code>config -f <config file></code> changes it)• When <code>racresetcfg</code> is used or a chassis configuration backup is restored.• When CMC is reset• When a new SSL server certificate is uploaded
Why doesn't my DNS server register my CMC?	Some DNS servers only register names of 31 characters or fewer.
When accessing the CMC Web interface, I get a security warning stating the SSL certificate was issued by a certificate authority that is not trusted.	<p>CMC includes a default CMC server certificate to ensure network security for the Web interface and remote RACADM features. This certificate is <i>not</i> 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 issuing certificates, see "Securing CMC Communications Using SSL and Digital Certificates" on page 173.</p>

Table 5-61. Managing and Recovering a Remote System (continued)

Question	Answer
<p>The following message is displayed for unknown reasons:</p> <pre>Remote Access: SNMP Authentication Failure</pre> <p>Why does this happen?</p>	<p>As part of discovery, IT Assistant attempts to verify the device's get and set community names. In IT Assistant, you have the get community name = public and the set community name = private. By default, the community name for the 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.</p> <p>You can change the CMC community name using RACADM.</p> <p>To see the CMC community name, use the following command:</p> <pre>racadm getconfig -g cfgOobSnmp</pre> <p>To set the CMC community name, use the following command:</p> <pre>racadm config -g cfgOobSnmp -o cfgOobSnmpAgentCommunity <community name></pre> <p>To prevent SNMP authentication traps from being generated, you must input community names that are accepted by the agent. Since CMC only allows one community name, you must input the same get and set community name for IT Assistant discovery setup.</p>

Troubleshooting CMC

The CMC Web interface provides tools for identifying, diagnosing, and fixing problems with your chassis. For more information about troubleshooting, see "Troubleshooting and Recovery."

Using 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 would change and Ethernet network management tools and SAN resources would need to be reconfigured to be aware of the new server module.

FlexAddress allows CMC to assign WWN/MAC IDs to a particular slot and *override* the factory IDs. If the server module is replaced, the slot-based 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.

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 file `pwwn_mac.xml`. 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:

$$\langle \text{mac_start} \rangle + 0\text{xCF} (208 - 1) = \text{mac_end}$$

where 208 is the `mac_count` and the formula is

$$\langle \text{mac_start} \rangle + \langle \text{mac_count} \rangle - 1 = \langle \text{mac_end} \rangle$$

For example: $(\text{starting_mac})00188BFFDCFA + 0\text{xCF} = (\text{ending_mac})00188BFFDCC9$.



NOTE: Lock the SD card prior to inserting in the USB "Memory Card Reader" to prevent accidentally modifying any of the contents. You *must unlock* the SD card before inserting into CMC.

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, which are listed in the table below, 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
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 ensure 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 by using the steps in the next section, "Verifying FlexAddress Activation" on page 220.

Verifying FlexAddress Activation

To ensure proper activation of FlexAddress, RACADM commands can be used to verify the SD feature card and FlexAddress activation.

Use the following RACADM command to verify the SD feature card and its status:

```
racadm featurecard -s
```

Table 6-1. 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 <code>racadm racreset</code> 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 further information on the RACADM commands, see the **feature** and **featurecard** command sections of the *Command Line Reference Guide for iDRAC6 and CMC*.

Deactivating FlexAddress

The FlexAddress 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.



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.

Deactivating FlexAddress

Use the following RACADM command to deactivate the FlexAddress feature and restore the SD card:

```
racadm feature -d -c flexaddress
```

The command returns the following status message upon successful deactivation:

```
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 *Command Line Reference Guide for iDRAC6 and CMC*.

Configuring FlexAddress Using the CLI



NOTE: You must enable both—the slot and fabric—for the chassis-assigned MAC address to be pushed to the iDRAC.



NOTE: You can also view FlexAddress status using the graphical user interface. For more information, see "FlexAddress" on page 205.

You can use the command line interface to enable or disable FlexAddress on a per fabric basis. Additionally, you can enable/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 only 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. For this feature to work, the fabric must be enabled and the server must be powered off.

Enabled slots are 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.

Use the following RACADM command to enable or disable fabrics:

```
racadm setflexaddr [-f <fabricName> <state>]
```

```
<fabricName> = A, B, C, or iDRAC
```

<state> = 0 or 1

Where 0 is disable and 1 is enable.

Use the following RACADM command to enable or disable slots:

```
racadm setflexaddr [-i <slot#> <state>]
```

<slot#> = 1 to 16

<state> = 0 or 1

Where 0 is disable and 1 is enable.

For additional information on the command, see the **setflexaddr** command section of the *Command Line Reference Guide for iDRAC6 and CMC*.

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 YAST (Yet another Setup Tool) on your Linux system to configure your 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/changed hardware on the system. Kudzu presents you with The Hardware Discovery Menu; it detects the MAC address change as hardware was removed and new hardware added.

Viewing FlexAddress Status Using the CLI

You can use the command line interface to view FlexAddress status information. You can view status information for the entire chassis or for a particular slot. The information displayed includes:

- Fabric configuration
- FlexAddress enabled/disabled
- Slot number and name
- Chassis-assigned and server-assigned addresses
- Addresses in use

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#>]
```

<slot#> = 1 to 16

See "Configuring FlexAddress Using the CLI" on page 222 for additional details on FlexAddress configuration. For additional information on the command, see the `getflexaddr` command section of the *Command Line Reference Guide for iDRAC6 and CMC*.

Configuring FlexAddress Using the GUI

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.

Troubleshooting FlexAddress

This section contains troubleshooting information for FlexAddress.

- 1 What happens if a feature card is removed?
Nothing happens. Feature cards can be removed and stored or may be left in place.
- 2 What happens if a feature card that was used in one chassis is removed and put into another chassis?

The Web interface displays an error that states:

```
This feature card was activated with a different
chassis. It must be removed before accessing the
FlexAddress feature.
```

```
Current Chassis Service Tag = XXXXXXXXX
```

```
Feature Card Chassis Service Tag = YYYYYYYY
```

An entry is added to the CMC log that states:

```
cmc <date timestamp> : feature
'FlexAddress@XXXXXXXX' not activated; chassis ID=
'YYYYYYY'
```

- 3** 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` returns a message of:

```
No feature card inserted
```

```
ERROR: can't open file
```

- 4** 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 an error that states:

```
This feature card was activated with a
different chassis. It must be removed before
accessing the FlexAddress feature.
```

```
Current Chassis Service Tag = XXXXXXXXX
```

```
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.

5 Do I get an error if I have two feature cards installed in my redundant CMC system?

The feature card in the active CMC is active and installed in the chassis. The second card is ignored by CMC.

6 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
```

7 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.
```

8 What happens to my 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.

- 9 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.
- 10 What happens if you are replacing a CMC unit with one that has firmware prior to 1.10 in a chassis with redundant CMCs?

In a chassis with redundant CMCs, if you are replacing a CMC unit 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 be removed.

- a Ensure the active CMC firmware is always version 1.10 or later.
- b Remove the standby CMC and insert the new CMC in its place.
- c From the Active CMC, upgrade the standby CMC firmware to 1.10 or later.



NOTE: If you do not update the standby CMC firmware to 1.10 or later and a failover occurs, the FlexAddress feature is not configured and you need to reactivate and reconfigure the feature.

- 11 The SD card was not in the chassis when I executed the deactivation command on the FlexAddress. How do I recover my SD card now?

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.

- 12** I have the SD card properly installed and all the firmware/software updates installed. I see that FlexAddress is active, but I can't see anything on the server deployment screen to deploy it? What is wrong?

This is a browser caching issue; shut down the browser and relaunch.

- 13** What happens to FlexAddress if I need to reset my chassis configuration using the RACADM command, `racresetcfg`?

The FlexAddress feature is still be activated and ready to use. All fabrics and slots is selected as default.



NOTE: It is highly recommended that you power down your chassis before issuing the RACADM command `racresetcfg`.

Command Messages

The following table lists the RACADM commands and output for common FlexAddress situations.

Table 6-2. FlexAddress Commands and Output

Situation	Command	Output
SD card in the active CMC module is bound to another service tag.	<code>\$racadm featurecard -s</code>	The feature card inserted is valid and contains the following feature(s) FlexAddress: The feature card is bound to another chassis, svctag = J310TF1 SD card SN =0188BFFE03A

Table 6-2. FlexAddress Commands and Output (continued)

Situation	Command	Output
SD card in the active CMC module that is bound to the same service tag.	<code>\$racadm featurecard -s</code>	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.	<code>\$racadm featurecard -s</code>	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)	<code>\$racadm setflexaddr [-f <fabricName> <slotState>] OR</code> <code>\$racadm setflexaddr [-i <slot#> <slotState>]</code>	ERROR: Flexaddress feature is not active on the chassis
Guest user attempts to set FlexAddress on slots/fabrics	<code>\$racadm setflexaddr [-f <fabricName> <slotState>]</code> <code>\$racadm setflexaddr [-i <slot#> <slotState>]</code>	ERROR: Insufficient user privileges to perform operation

Table 6-2. FlexAddress Commands and Output (continued)

Situation	Command	Output
Deactivating FlexAddress feature with chassis powered ON	<code>\$racadm feature -d -c flexaddress</code>	ERROR: Unable to deactivate the feature because the chassis is powered ON
Guest user tries to deactivate the feature on the chassis	<code>\$racadm feature -d -c flexaddress</code>	ERROR: Insufficient user privileges to perform operation
Changing the slot/fabric FlexAddress settings while the server modules are powered ON	<code>\$racadm setflexaddr -i 1 1</code>	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 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 SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY 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.

Using 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 WWN/MAC (World Wide Name/Media Access Control) addresses to Fibre Channel and Ethernet devices. Chassis assigned WWN/MAC addresses are globally unique and specific to a server slot.

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. Please 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.

Table 7-1. Updates Required for Flexaddress Plus

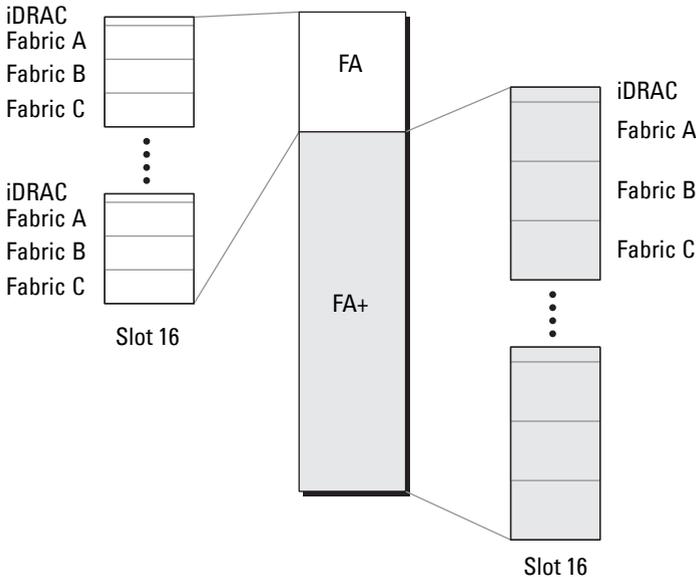
Component	Minimum required version
Server Module BIOS	PowerEdge M710hd
iDRAC	Version 3.0 or later
CMC	Version 3.0 or later

FlexAddress vs FlexAddress Plus

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 table below 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 7-1. FlexAddress (FA) vs FlexPlusAddress (FA+) Features



Scheme 1 and Scheme 2 MAC Address Allocation

For backward compatibility with FA, the addresses in FA+ are divided into two groups: the first group has 208 addresses and the second group has 2928 addresses. In the first group, 13 MACs are allocated to each of the 16 slots in the same way FA does. In the second group, 183 MACs are allocated for each slot.

The allocation of the 13 MAC addresses of the first group for each server is divided as: one for iDRAC and four for each fabric, A, B, and C. Within each fabric, A, B, and C, two addresses are allocated for port 1 and two addresses are allocated for port 2. The result is:

- 1 MAC for iDRAC management
- 4 MACs for fabric A (two MACs for port 1, two MACs for port 2)
- 4 MACs for fabric B (two MACs for port 1, two MACs for port 2)
- 4 MACs for fabric C (two MACs for port 1, two MACs for port 2)

For references, this MAC address allocation is called scheme 1.

The allocation of the 183 MAC address for the second group of each server is also divided as: three for iDRAC, 60 for each fabric, A, B and C. Within each fabric, 30 addresses are allocated for port 1 and 30 addresses are allocated for port 2. The result is:

- 3 MACs for iDRAC management
- 60 MACs for fabric A (30 MACs for port 1, 30 MACs for port 2)
- 60 MACs for fabric B (30 MACs for port 1, 30 MACs for port 2)
- 60 MACs for fabric C (30 MACs for port 1, 30 MACs for port 2)

For references, this MAC address allocation is called scheme 2.

The common way of MAC addresses allocation is to allocate MAC addresses per fabric from scheme 1 initially. If a fabric requires more addresses than scheme 1 can provide, additional two MACs per fabric is allocated from scheme 2.

When a chassis is activated only with FA and it has a server with a network configuration that requires more addresses than scheme 1 can provide, the additional addresses are not available. The status is displayed as `Not Installed`.

If a chassis currently has FA activated, FA does not need to be deactivated in order to add FA+.

In this case, the MAC address allocations are applied as follows:

- The MAC addresses of scheme 1 are allocated from FA of the feature card 1.0. There is no change in the previous WWN/MAC configuration.
- The additional MAC addresses of scheme 2 are allocated from the scheme 2 addresses of FA+.

MAC Address Allocation Example

Assume that, the starting address of MACs in FA is 00:FA:AE:58:59:2B, the starting address of the MACs in scheme 2 of FA+ is 00:FB:AE:58:59:FB. The server is in slot 1, the network configuration for the server is:

- 1 MAC for iDRAC
- 8 MACs for fabric A
- 4 MACs for fabric B
- 4 MACs for fabric C

Since fabric A needs four more MAC addresses than scheme 1 can provide, the first 4 MACs are allocated from FA based on scheme 1 with two MACs for port 1, and two MACs for port 2. The additional four MACs are allocated from FA+ based on scheme 2, with two MACs for port 1 and two MACs for port 2. The MAC addresses allocation for iDRAC for fabric B and C are from FA based on scheme 1.

The starting address of fabric A port 1 from FA+ is 00:23:AE:58:59:FE, because the first 3 MACs are reserved for iDRAC. Thus the chassis-assigned MAC addresses for the server are:

iDRAC	00:FA:AE:58:59:2B (from FA)
<hr/>	
Fabric A port 1:	00:FA:AE:58:59:2C (from FA)
	00:FA:AE:58:59:2D (from FA)
	00:FB:AE:58:59:FE (from FA+)
	00:FB:AE:58:59:FF (from FA+)

Fabric A port 2:	00:FA:AE:58:59:2E (from FA)
	00:FA:AE:58:59:2F (from FA)
	00:FB:AE:58:5A:00 (from FA+)
	00:FB:AE:58:5A:01 (from FA+)
<hr/>	
Fabric B port 1:	00:FA:AE:58:59:30 (from FA)
	00:FA:AE:58:59:31 (from FA)
<hr/>	
Fabric B port 2:	00:FA:AE:58:59:32 (from FA)
	00:FA:AE:58:59:33 (from FA)
<hr/>	
Fabric C port 1:	00:FA:AE:58:59:34 (from FA)
	00:FA:AE:58:59:35 (from FA)
<hr/>	
Fabric C port 2:	00:FA:AE:58:59:36 (from FA)
	00:FA:AE:58:59:37 (from FA)

When a chassis with no previous FA—either it has never been activated or it was activated and then deactivated—and it has a server with the network configuration that requires more addresses than scheme 1 can provide, the scheme 1 allocation acquires addresses from scheme 1 of FA and scheme 2 allocation acquires addresses from scheme 2 of FA+.

Using the same example, the chassis-assigned MAC addresses of the same server in this scenarios are as follows:

iDRAC	00:FB:AE:58:59:2B (FA)
<hr/>	
Fabric A port 1:	00:FB:AE:58:59:2C (FA)
	00:FB:AE:58:59:2D (FA)
	00:FB:AE:58:59:FE (FA+)
	00:FB:AE:58:59:FF (FA+)
<hr/>	
Fabric A port 2:	00:FB:AE:58:59:2E (FA)
	00:FB:AE:58:59:2F (FA)
	00:FB:AE:58:5A:00 (FA+)
	00:FB:AE:58:5A:01 (FA+)
<hr/>	
Fabric B port 1:	00:FB:AE:58:59:30 (FA)
	00:FB:AE:58:59:31 (FA)

Fabric B port 2:	00:FB:AE:58:59:32 (FA)
	00:FB:AE:58:59:33 (FA)
<hr/>	
Fabric C port 1:	00:FB:AE:58:59:34 (FA)
	00:FB:AE:58:59:35 (FA)
<hr/>	
Fabric C port 2:	00:FB:AE:58:59:36 (FA)
	00:FB:AE:58:59:37 (FA)

Using the CMC Directory Service

A directory service maintains a common database of all information needed for controlling network users, computers, printers, and so on. If your company uses the Microsoft Active Directory service software or the LDAP Directory Service software, you can configure CMC to use directory based user authentication.

Using CMC with Microsoft Active Directory



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 is supported only on Windows 2008.

Active Directory Schema Extensions

You can use Active Directory to define user access on CMC through two methods:

- The standard schema solution that uses only the standard Active Directory group objects.
- The extended schema solution that uses Active Directory objects defined by Dell.

Standard Schema Versus Extended Schema

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

With the standard schema solution:

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

With the extended schema solution:

- All of the access control objects are maintained in Active Directory.
- Configuring user access on different CMCs with different privilege levels allows maximum flexibility.

Standard Schema Active Directory Overview

Using standard schema for Active Directory integration requires configuration on both Active Directory and CMC.

On the Active Directory side, a standard group object is used as a role group. A user who has CMC access is a member of the role group.

In order 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. Unlike the extended schema solution, the role and the privilege level is defined on each CMC card, not in the Active Directory. Up to five role groups can be configured and defined in each CMC. Table 5-41 shows the privileges level of the role groups and Table 8-1 shows the default role group settings.

Figure 8-1. Configuration of CMC with Active Directory and Standard Schema

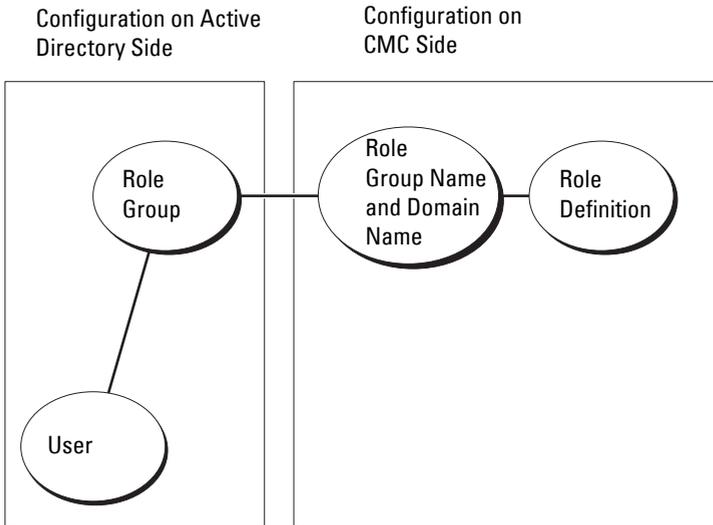


Table 8-1. Default Role Group Privileges

Role Group	Default Privilege Level	Permissions Granted	Bit Mask
1	None	<ul style="list-style-type: none">• CMC Login User• Chassis Configuration Administrator• User Configuration Administrator• Clear Logs Administrator• Chassis Control Administrator (Power Commands)• Super User• Server Administrator• Test Alert User• Debug Command User• Fabric A Administrator• Fabric B Administrator• Fabric C Administrator	0x00000fff
2	None	<ul style="list-style-type: 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	0x000000f9
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 "User Types" on page 154.

There are two ways to enable Standard Schema Active Directory:

- With the CMC Web interface. See "Configuring CMC With Standard Schema Active Directory and Web Interface" on page 244.
- With the RACADM CLI tool. See "Configuring CMC With Standard Schema Active Directory and RACADM" on page 247.

Configuring Standard Schema Active Directory to Access CMC

Perform the following steps to configure the Active Directory before an Active Directory user can access CMC:

- 1 On an Active Directory server (domain controller), open the Active Directory Users and Computers Snap-in.
- 2 Create a group or select an existing group. The name of the group and the name of this domain must be configured on CMC using the Web interface or RACADM.

For more information, see "Configuring CMC With Standard Schema Active Directory and Web Interface" on page 244 or "Configuring CMC With Standard Schema Active Directory and RACADM" on page 247.

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

Configuring CMC With Standard Schema Active Directory and Web Interface

- 1 Log in to the CMC Web interface.
- 2 Select **Chassis** in the system tree.
- 3 Click **User Authentication**→**Directory Services**.The **Directory Services** page is displayed.
- 4 Select the radio button next to **Microsoft Active Directory (Standard Schema)**. The **Active Directory Configuration and Management** page appears.

- 5 In the **Common Settings** section:
 - a Select the **Enable Active Directory** check box.
 - b Type the **Root Domain Name**.
 **NOTE:** The **Root domain name** must be a valid domain name using the *x.y* naming convention, where *x* is a 1–256 character ASCII string with no spaces between characters, and *y* is a valid domain type such as com, edu, gov, int, mil, net, or org.
 - c Type the **Timeout** in seconds. Timeout range is 15–300 seconds. Default timeout period is 90 seconds.
- 6 If you want the directed call to search the domain controller and global catalog, select the **Search AD Server to search (Optional)** check box, and do the following:
 - a In the **Domain Controller** text field, type the server where your Active Directory service is installed.
 - b In the **Global Catalog** text field, type the location of the global catalog on the Active Directory domain controller. The global catalog provides a resource for searching an Active Directory forest.
- 7 Click **Apply** to save your settings.
 **NOTE:** You must apply your settings before continuing to the next step. If you do not apply the settings, you will lose the settings you entered after you navigate to the next page.
- 8 In the **Standard Schema Settings** section, click a **Role Group**. The **Configure Role Group** page appears.
- 9 Type the **Group Name**. The group name identifies the role group in the Active Directory associated with the CMC card.
- 10 Type the **Group Domain**. The **Group Domain** is the fully qualified root domain name for the forest.
- 11 In the **Role Group Privileges** page, select privileges for the group.
If you modify any of the privileges, the existing **Role Group Privilege** (Administrator, Power User, or Guest User) changes to either the Custom group or the appropriate Role Group Privilege. See Table 5-41.
- 12 Click **Apply** to save the Role Group settings.
- 13 Click **Go Back To Configuration** page.

- 14 Upload your domain forest Root certificate authority-signed certificate into CMC. In the **Certificate Management** section, type the file path of the certificate or browse to the certificate file. Click the **Upload** button to transfer 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.

- 15 Click **Apply**. The CMC Web server automatically restarts after you click **Apply**.
- 16 Log out and then log in to CMC to complete the CMC Active Directory feature configuration.
- 17 Select **Chassis** in the system tree.
- 18 Click the **Network** tab.
- 19 Click the **Network** subtab. The **Network Configuration** page appears.
- 20 If **Use DHCP (for CMC Network Interface IP Address)** is selected under **Network Settings**, 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 your primary and alternate DNS server IP addresses.

- 21 Click **Apply Changes**.
The CMC Standard Schema Active Directory feature configuration is complete.

Configuring CMC With Standard Schema Active Directory and RACADM

To configure the CMC Active Directory Feature with Standard Schema using the RACADM CLI, use the following commands:

- 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 Table 3-1 in the database property chapter of the *Dell Chassis Management Controller Administrator Reference Guide*.

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 Overview

There are two ways to enable Extended Schema in Active Directory:

- Using the CMC Web interface. For instructions, see "Configuring CMC With Extended Schema Active Directory and the Web Interface" on page 264.
- Using the RACADM CLI tool. For instructions, see "Configuring CMC With Extended Schema Active Directory and RACADM" on page 267.

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. 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 to address your company's environment-specific needs. Dell has extended the schema to include the necessary changes to support remote management Authentication and Authorization.

Each Attribute or Class that is added to an existing Active Directory Schema must be defined with a unique ID. To maintain unique IDs across the industry, Microsoft maintains a database of Active Directory Object Identifiers (OIDs). To extend the schema in Microsoft's Active Directory, Dell established unique OIDs, unique name extensions, and uniquely linked attribute IDs for Dell-specific Attributes and Classes:

Dell extension: dell

Dell base OID: 1.2.840.113556.1.8000.1280

RAC LinkID range: 12070–2079

Overview of the RAC Schema Extensions

Dell provides a group of properties that you can configure. The Dell extended schema include Association, Device, and Privilege properties.

The Association property links together users or groups with a specific set of privileges to one or more RAC devices. This model provides an Administrator maximum flexibility over the different combinations of users, RAC privileges, and RAC devices on the network without adding too much complexity.

Active Directory Object Overview

When there are two CMCs on the network that you want to integrate with Active Directory for Authentication and Authorization, you must 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.

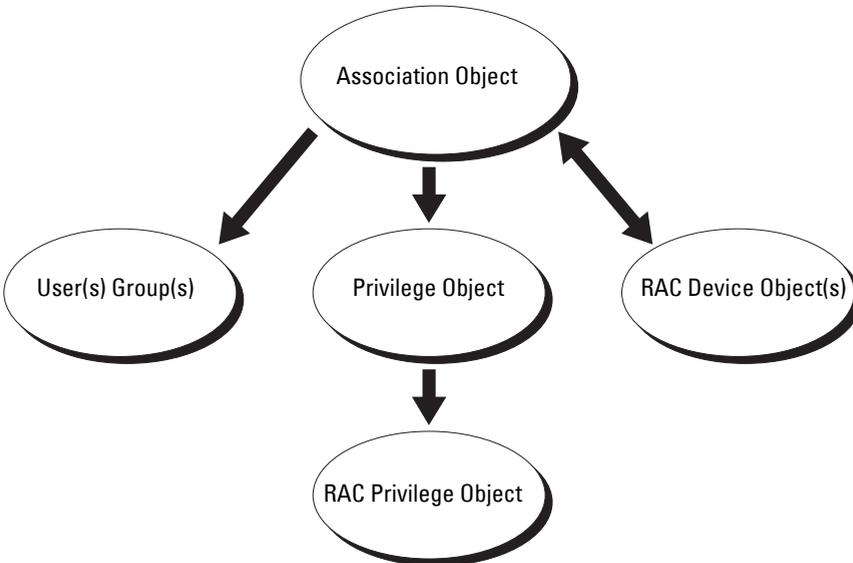
The RAC Device object is the link to the RAC firmware for querying Active Directory for authentication and authorization. When a RAC is added to the network, the Administrator must configure the RAC and its device object with its Active Directory name so users can perform authentication and authorization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

Figure 8-2 illustrates that the Association Object provides the connection that is needed for all of 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.

Figure 8-2. Typical Setup for Active Directory Objects

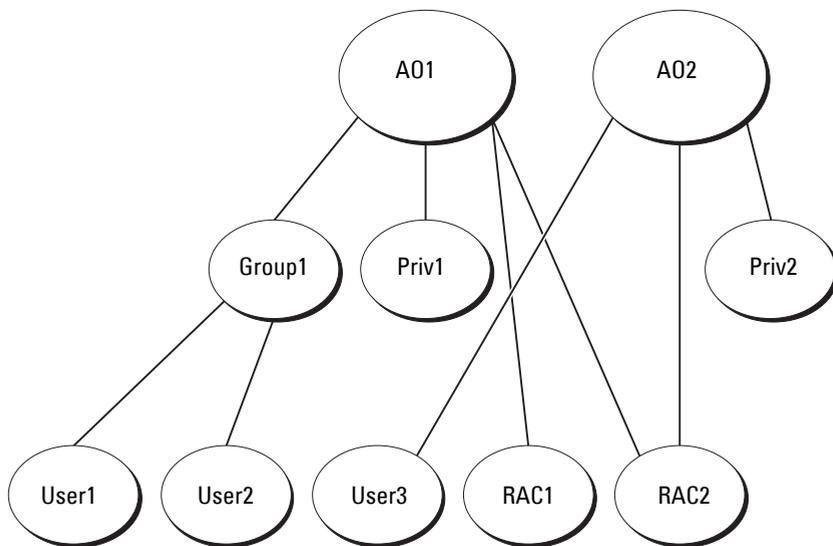


The Association Object allows for as many or as few users and/or groups as well as RAC Device Objects. However, the Association Object only includes one Privilege Object per Association Object. The Association Object connects the "Users" who have "Privileges" on the RACs (CMCs).

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. Figure 8-3 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.

Figure 8-3. Setting Up Active Directory Objects in a Single Domain



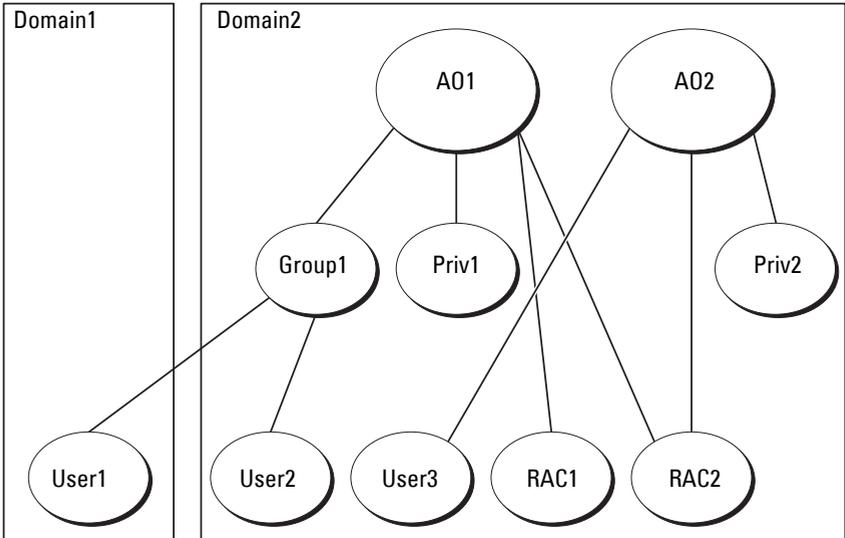
To configure the objects for the single domain scenario:

- 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.

For detailed instruction, see "Adding CMC Users and Privileges to Active Directory" on page 262.

Figure 8-4 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.

Figure 8-4. Setting Up Active Directory Objects in Multiple Domains



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.

Figure 8-4 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 Access Your CMC

Before using Active Directory to access your CMC, configure the Active Directory software and CMC:

- 1 Extend the Active Directory schema (see "Extending the Active Directory Schema" on page 254).
- 2 Extend the Active Directory Users and Computers Snap-In (see "Installing the Dell Extension to the Active Directory Users and Computers Snap-In" on page 261).
- 3 Add CMC users and their privileges to Active Directory (see "Adding CMC Users and Privileges to Active Directory" on page 262).
- 4 Enable SSL on each of your domain controllers.
- 5 Configure the CMC Active Directory properties using either the CMC Web interface or the RACADM (see "Configuring CMC With Extended Schema Active Directory and the Web Interface" on page 264 or "Configuring CMC With Extended Schema Active Directory and RACADM" on page 267).

Extending the Active Directory Schema

Extending your Active Directory schema adds a Dell organizational unit, schema classes and attributes, and example privileges and association objects to the Active Directory schema. Before you extend the schema, ensure that you have Schema Admin privilege 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 be added to the schema.

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

- <DVDdrive>:\SYSMGMT\ManagementStation\support\OActiveDirectory_Tools\<installation type>\LDIF Files
- <DVDdrive>:\SYSMGMT\ManagementStation\support\OActiveDirectory_Tools\<installation type>\Schema Extender

To use the LDIF files, see the instructions in the readme included in the **LDIF_Files** directory. For instructions on using the Dell Schema Extender to extend the Active Directory Schema, see "Using the Dell Schema Extender" on page 255.

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

Using the Dell Schema Extender

 **CAUTION:** The Dell Schema Extender uses the **SchemaExtenderOem.ini** file. To ensure that the Dell Schema Extender utility functions properly, do not modify the name of this file.

- 1 In the Welcome screen, click Next.
- 2 Read and understand the warning and click Next.
- 3 Select **Use Current Log In Credentials** or enter a user name and password with schema administrator rights.

- 4 Click **Next** to run the Dell Schema Extender.
- 5 Click **Finish**.

The schema is extended. To verify the schema extension, use the Microsoft Management Console (MMC) and the Active Directory Schema Snap-In to verify that the following exist:

- Classes — see Table 8-2 through Table 8-7
- Attributes — see Table 8-8

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

Table 8-2. Class Definitions for Classes Added to the Active Directory Schema

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

Table 8-3. dellRacDevice Class

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

Table 8-4. dellAssociationObject Class

OID	1.2.840.113556.1.8000.1280.1.1.1.2
Description	Represents the Dell Association Object. The Association Object provides the connection between the users and the devices.
Class Type	Structural Class
SuperClasses	Group
Attributes	dellProductMembers dellPrivilegeMember

Table 8-5. dellRAC4Privileges Class

OID	1.2.840.113556.1.8000.1280.1.1.1.3
Description	Defines Authorization Rights (privileges) for the CMC device.
Class Type	Auxiliary Class
SuperClasses	None
Attributes	dellIsLoginUser dellIsCardConfigAdmin dellIsUserConfigAdmin dellIsLogClearAdmin dellIsServerResetUser dellIsTestAlertUser dellIsDebugCommandAdmin dellPermissionMask1 dellPermissionMask2

Table 8-6. dellPrivileges Class

OID	1.2.840.113556.1.8000.1280.1.1.1.4
Description	Container Class for the Dell Privileges (Authorization Rights).
Class Type	Structural Class
SuperClasses	User
Attributes	dellRAC4Privileges

Table 8-7. dellProduct Class

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

Table 8-8. 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.	
OID: 1.2.840.113556.1.8000.1280.1.1.2.1	FALSE
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	FALSE
Distinguished Name: (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	

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

Assigned OID/Syntax Object Identifier	Single Valued
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	TRUE
Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
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	TRUE
Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
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	TRUE
Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
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	TRUE
Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
Attribute: dellIsLogClearAdmin	
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	TRUE
Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
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	TRUE
Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	

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

Assigned OID/Syntax Object Identifier	Single Valued
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	TRUE
Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
Attribute: dellIsDebugCommandAdmin	
Description: TRUE if the user has Debug Command Admin rights on the device.	
OID: 1.2.840.113556.1.8000.1280.1.1.2.11	TRUE
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	TRUE
Case Ignore String(LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	
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	TRUE
Case Ignore String(LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	
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	FALSE
Distinguished Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	
Attribute: dellPermissionsMask1	

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

Assigned OID/Syntax Object Identifier	Single Valued
OID: 1.2.840.113556.1.8000.1280.1.6.2.1 Integer (LDAPATYPE_INTEGER)	
Attribute: dellPermissionsMask2	
OID: 1.2.840.113556.1.8000.1280.1.6.2.2 Integer (LDAPATYPE_INTEGER)	

Installing the Dell Extension to the Active Directory Users and Computers Snap-In

When you extend the schema in Active Directory, you must also extend the Active Directory Users and Computers Snap-In so the administrator can manage RAC (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 **Dell Extension to the Active Directory User's and Computers Snap-In** option during the installation procedure. See the *Dell OpenManage Server Administrator Installation Guide* and *Dell OpenManage Management Station Software Installation Guide* for additional instructions about installing systems management software.

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

Installing the Administrator Pack

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

Opening the Active Directory Users and Computers Snap-In

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

- 1 If you are logged into the domain controller, click **Start Admin Tools** → **Active Directory Users and Computers**.

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

The Microsoft Management Console (MMC) appears.

- 2 In the **Console 1** window, click **File** (or **Console** on systems running Windows 2000).
- 3 Click **Add/Remove Snap-in**.
- 4 Select the **Active Directory Users and Computers Snap-In** and click **Add**.
- 5 Click **Close** and click **OK**.

Adding 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, Association, and Privilege objects. To add each object type:

- 1 Create a RAC device Object.
- 2 Create a Privilege Object.
- 3 Create an Association Object.
- 4 Add objects to an Association Object.

Creating a RAC Device Object

- 1 In the MMC **Console Root** window, right-click a container.
- 2 Select **New→ Dell RAC Object**.
The **New Object** window appears.
- 3 Type a name for the new object. The name must be identical to CMC Name that you type in step 8a of "Configuring CMC With Extended Schema Active Directory and the Web Interface" on page 264.
- 4 Select **RAC Device Object**.
- 5 Click **OK**.

Creating a Privilege Object



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

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

- 3 Type a name for the new object.
- 4 Select **Privilege Object**.
- 5 Click **OK**.
- 6 Right-click the privilege object that you created, and select **Properties**.
- 7 Click the **RAC Privileges** tab and select the privileges that you want the user to have. For more information about CMC user privileges, see "User Types" on page 154.

Creating an Association Object

The Association Object is derived from a Group and must contain a Group Type. The Association Scope specifies the Security Group Type for the Association Object. When you create an Association Object, choose the Association Scope that applies to the type of objects you intend to add.

For example, if you select **Universal**, the association objects are only available when the Active Directory Domain is functioning in Native Mode or above.

- 1 In the **Console Root** (MMC) window, right-click a container.
- 2 Select **New**→ **Dell RAC Object**.
This opens the **New Object** window.
- 3 Type a name for the new object.
- 4 Select **Association Object**.
- 5 Select the scope for the **Association Object**.
- 6 Click **OK**.

Adding Objects to an Association Object

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

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

Adding Users or User Groups

- 1 Right-click the **Association Object** and select **Properties**.

- 2 Select the **Users** tab and click **Add**.
- 3 Type the user or User Group name and click **OK**.

Click the **Privilege Object** tab to add the privilege object to the association that defines the user's or user group's privileges when authenticating to a RAC device. Only one privilege object can be added to an Association Object.

Adding Privileges

- 1 Select the **Privileges Object** tab and click **Add**.
- 2 Type the Privilege Object name and click **OK**.

Click the **Products** tab to add one or more RAC devices to the association. The associated devices specify the RAC devices connected to the network that are available for the defined users or user groups. Multiple RAC devices can be added to an Association Object.

Adding RAC Devices or RAC Device Groups

To add RAC devices or RAC device groups:

- 1 Select the **Products** tab and click **Add**.
- 2 Type the RAC device or RAC device group name and click **OK**.
- 3 In the **Properties** window, click **Apply** and click **OK**.

Configuring CMC With Extended Schema Active Directory and the Web Interface

- 1 Log in to the CMC Web interface.
- 2 Select **Chassis** in the system tree.
- 3 Click **User Authentication**→ **Directory Services**.
The **Directory Services** page is displayed.
- 4 Select **Microsoft Active Directory (Extended Schema)**.
- 5 In the **Common Settings** section:
 - a Verify that the **Enable Active Directory** check box is checked.
 - b Type the **Root Domain Name**.

 **NOTE:** The **Root domain name** must be a valid domain name using the *x.y* naming convention, where *x* is a 1–256 character ASCII string with no spaces between characters, and *y* is a valid domain type such as com, edu, gov, int, mil, net, or org.

c Type the **Timeout** time in seconds. **Configuration range:** 15–300 seconds. **Default:** 90 seconds

6 **Optional:** If you want the directed call to search the domain controller and global catalog, select the **Search AD Server to search (Optional)** check box, then:

a In the **Domain Controller** text field, type the server where your Active Directory service is installed.

b In the **Global Catalog** text field, type the location of the global catalog on the Active Directory domain controller. The global catalog provides a resource for searching an Active Directory forest.

 **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.

7 In the **Extended Schema Settings** section:

a Type the **CMC Device Name**. The **CMC Name** uniquely identifies the CMC card in Active Directory. The **CMC Name** must be the same as the common name of the new CMC object you created in your Domain Controller. The **CMC Name** must be a 1–256 character ASCII string with no spaces between characters.

b Type the **CMC Domain Name** (example: `cmc.com`). The **CMC Domain Name** is the DNS name (string) of the domain where the Active Directory CMC object resides. The name must be a valid domain name consisting of *x.y*, where *x* is a 1–256 character ASCII string with no spaces between characters, and *y* is a valid domain type such as com, edu, gov, int, mil, net, or org.

8 Click **Apply** to save your settings.

 **NOTE:** You must apply your settings before continuing to the next step, in which you navigate to another page. If you do not apply the settings, you lose the settings you entered when you navigate to the next page.

- 9 In the **Manage Certificates** section, type the file path of the certificate in the text field, or click **Browse** to select the certificate file. Click the **Upload** button to transfer 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.

SSL certificate validation is required by default. There is a new setting in the `cfgActiveDirectory` RACADM group and within the GUI to disable the certificate check.

 **CAUTION: Disabling this certificate is risky.**

To turn on SSL certificate validation (default):

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

To turn off SSL certificate validation:

```
racadm config -g cfgActiveDirectory -o  
cfgADCertValidationEnable 0
```

The SSL certificates for the domain controller must be signed by the root certificate authority. The root certificate authority-signed certificate must be available on the management station accessing CMC.

- 10 Click **Apply**. The CMC Web server automatically restarts after you click **Apply**.
- 11 Log back in to the CMC Web interface.
- 12 Select **Chassis** in the system tree, click the **Network** tab, then click the **Network** subtab. The **Network Configuration** page is displayed.
- 13 If **Use DHCP (for CMC Network Interface IP Address)** is enabled (checked), 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., or

- 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.

14 Click Apply Changes.

The CMC Extended Schema Active Directory feature configuration is complete.

Configuring CMC With Extended Schema Active Directory and RACADM

Using the following commands to configure the CMC Active Directory Feature with Extended Schema using the RACADM CLI tool instead of the Web interface.

- 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 "Accessing RACADM Remotely" on page 74.

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.

Frequently Asked Questions

Table 8-9. Using CMC With Active Directory: Frequently Asked Questions

Question	Answer
Can I log into CMC using Active Directory 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 forces you to create these two objects in the same domain. Other objects can be in different domains.
Are there any restrictions on Domain Controller SSL configuration?	Yes. All SSL certificates for Active Directory servers in the forest must be signed by the same root certificate authority-signed certificate, because CMC only allows you to upload one trusted certificate authority-signed SSL certificate.

Table 8-9. Using CMC With Active Directory: Frequently Asked Questions (continued)

Question	Answer
I created and uploaded a new RAC certificate and now the Web interface does not launch.	<p data-bbox="493 280 960 392">If you use Microsoft Certificate Services to generate the RAC certificate, you may have inadvertently chose User Certificate instead of Web Certificate when creating the certificate.</p> <p data-bbox="493 408 960 520">To recover, generate a CSR, and then create a new Web certificate from Microsoft Certificate Services and upload it using the following RACADM commands:</p> <pre data-bbox="493 536 960 663">racadm sslcsrgen [-g] [-f {filename}] racadm sslcertupload -t 1 -f {web_sslcert}</pre>

Table 8-9. Using CMC With Active Directory: Frequently Asked Questions (continued)

Question	Answer
What can I do if I cannot log into CMC using Active Directory authentication? How do I troubleshoot the issue?	<p>1 Ensure that you use the correct user domain name during a login and not the NetBIOS name.</p> <p>2 If you have a local CMC user account, log into CMC using your local credentials.</p> <p>After you are logged in, perform the following steps:</p> <ul style="list-style-type: none">a Ensure that you have checked the Enable Active Directory check box on the CMC Active Directory configuration page.b Ensure that the DNS setting is correct on the CMC Networking configuration page.c Ensure that you have uploaded the Active Directory certificate from your Active Directory root certificate authority-signed certificate to CMC.d Check the Domain Controller SSL certificates to ensure that they have not expired.e Ensure that your CMC Name, Root Domain Name, and CMC Domain Name match your Active Directory environment configuration.f Ensure that the CMC password has a maximum of 127 characters. While CMC can support passwords of up to 256 characters, Active Directory only supports passwords that have a maximum length of 127 characters.

Configuring Single Sign-On

Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows 7, and Windows Server 2008 can use Kerberos, a network authentication protocol, 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.

Starting with CMC version 2.10, CMC can use Kerberos to support two additional types of login mechanisms—single sign-on and Smart Card login. 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.

 **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.

System Requirements

To use the Kerberos authentication, your network must include:

- DNS server
- Microsoft Active Directory Server

 **NOTE:** If you are using Active Directory on Windows 2003, ensure that you have the latest service packs and patches installed on the client system. If you are using Active Directory on Windows 2008, ensure 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 and 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

Configuring Settings

Prerequisites

- The Kerberos realm & Key Distribution Center (KDC) for Active Directory (AD) has been setup (ksetup).
- A robust NTP and DNS infrastructure to avoid issues with clock drift & reverse lookup.
- The CMC standard schema role group with authorized members.

Configuring Active Directory

On the CMC **Properties** dialog box under the **Accounts** options section, configure these settings:

- **Account is trusted for delegation** — Currently CMC does not use forwarded credentials that are created when this option is selected. You may or may not select this option depending upon other services requirements.
- **Account is sensitive and cannot be delegated** — You may or may not select this option depending upon other services requirements.
- **User Kerberos DES encryption types for the account** — Select this option.
- **Do not require Kerberos preauthentication** — Do not select this option.

Run the ktpass utility—part of Microsoft Windows—on the domain controller (Active Directory server) where you want to map CMC to a user account in Active Directory. For example,

```
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, @REALM_NAME must be uppercase. In addition, CMC supports the DES-CBC-MD5 type of cryptography for Kerberos authentication.

This procedure produces a keytab file that you must upload 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 at: technet2.microsoft.com/windowsserver/en/library/64042138-9a5a-4981-84e9-d576a8db0d051033.msp?mfr=true.

Configuring CMC

 **NOTE:** The configuration steps described in this section apply only to the CMC's Web access.

Configure CMC to use the Standard Schema role group(s) set up in Active Directory. For more information, see "Configuring Standard Schema Active Directory to Access CMC" on page 244.

Uploading the Kerberos 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.

To upload the keytab file:

- 1 Navigate to the **User Authentication** tab→ **Directory Services** subtab. Ensure that **Microsoft Active Directory Standard** or **Extended Schema** is selected. If not, select your preference and click **Apply**.
- 2 Click **Browse** on the **Kerberos Keytab Upload** section, navigate to the folder where the keytab file is saved and click **Upload**.
When the upload is complete, a message box is displayed indicating a successful or failed upload.

Enabling Single Sign-On

- 1 Click **Chassis Management Controller Network Security** tab→ **Active Directory**→ **Configure Active Directory**.
The **Active Directory Configuration and Management** page is displayed.
 - 2 On the **Active Directory Configuration and Management** page, select:
 - **Single Sign-On** — this option enables you to log in to CMC using the cached credentials obtained when you log in to the Active Directory.
-  **NOTE:** All command line out-of-band interfaces including secure shell (SSH), Telnet, Serial, and remote RACADM remain unchanged for this option.
- 3 Scroll to the bottom of the page and click **Apply**.

You can test the Active Directory using Kerberos authentication by using the CLI command test feature:

```
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 repeat the command. For more information, see *Command Line Reference Guide for iDRAC6 and CMC* on support.dell.com/manuals.

Configuring the Browser For Single Sign-On Login

Single Sign-on 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

- 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/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**.

Logging into CMC Using Single Sign-On

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

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

For example, `cmc-6G2WXF1.cmcad.lab`

where `cmc-6G2WXF1` is the cmc-name

`cmcad.lab` is the domain-name.

 **NOTE:** If you changed the default HTTPS port number (port 80), access the CMC Web page 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.

The CMC Single Sign-On page is displayed.

- 3 Click Login.

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 than Internet Explorer, the login fails and the browser only displays a blank page.

Configuring Smart Card Two-Factor Authentication

Traditional authentication schemes use user name and password to authenticate users. Two-factor-authentication, on the other hand, 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, a network authentication protocol, uses this two-factor authentication mechanism allowing systems to prove their authenticity. Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008 use Kerberos as their preferred authentication method. Starting with CMC version 2.10, CMC can use Kerberos to support Smart Card login.



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.

System Requirements

The "System Requirements" on page 272 for Smart Card are the same as Single Sign-On.

Configuring Settings

The "Prerequisites" on page 273 for Smart Card are the same as Single Sign-On.

Configuring Active Directory

- 1 Set up Kerberos realm & Key Distribution Center (KDC) for Active Directory, if not already configured (ksetup).



NOTE: Ensure a robust NTP and DNS infrastructure to avoid issues with clock drift & reverse lookup.

- 2 Create Active Directory users for each CMC, configured to use Kerberos DES encryption but not pre-authentication.
- 3 Register the CMC users to the Key Distribution Center with Ktpass (this also outputs a key to upload to CMC).

Configuring CMC



NOTE: The configuration steps described in this section apply only to the CMC's Web access.

Configure CMC to use the Standard Schema role group(s) set up in Active Directory. For more information, see "Configuring Standard Schema Active Directory to Access CMC" on page 244.

Uploading the Kerberos 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.

To upload the keytab file:

- 1 Navigate to the **User Authentication** tab→ **Directory Services** subtab. Ensure that **Microsoft Active Directory Standard** or **Extended Schema** is selected. If not, select your preference and click **Apply**.
- 2 Click **Browse** in the **Kerberos Keytab Upload** section, navigate to the folder where the keytab file is saved and click **Upload**.

When the upload is complete, a message box is displayed indicating a successful or failed upload.

Enabling Smart Card Authentication

- 1 Navigate to the **User Authentication** tab→ **Directory Services** subtab. Ensure that **Microsoft Active Directory Standard** or **Extended Schema** is selected.
 - 2 In the **Common Settings Section**, select:
 - **Smart Card** — this option requires that you insert a Smart Card into reader and enter the PIN number.
-  **NOTE:** All command line out-of-band interfaces including secure shell (SSH), Telnet, Serial, and remote RACADM remain unchanged for this option.
- 3 Scroll to the bottom of the page and click **Apply**.

You can test the Active Directory using Kerberos authentication by using the CLI command `testfeature`.

Type:

```
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 repeat the command. For more information, see the RACADM command `testfeature` documentation.

Configuring the 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.

Logging into CMC Using Smart Card



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

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

For example, `cmc-6G2WXF1.cmcad.lab`

where `cmc-6G2WXF1` is the cmc-name

`cmcad.lab` is the domain-name.



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.

The CMC Single Sign-On page is displayed prompting you to insert the Smart Card.

- 3 Insert the Smart Card into the reader and click OK.
The PIN pop-up dialog box is displayed.
- 4 Optionally, select a session timeout. This is the amount of time you stay logged in with no activity. The default value is defined as the Web Service Idle Timeout. See Configuring Services for more details.
- 5 Enter the PIN and click OK.

Troubleshooting the Smart Card Login

The following tips help you to debug an inaccessible Smart Card:

ActiveX plug-in is unable to detect the Smart Card reader

Ensure that the Smart Card is supported on the Microsoft Windows operating system. Windows supports a limited number of Smart Card cryptographic service providers (CSPs).

Tip: As a general check to see if the Smart Card CSPs are present on a particular client, insert the Smart Card in the reader at the Windows login

(Ctrl-Alt-Del) screen and check to see if Windows detects the Smart Card and displays the PIN dialog-box.

Incorrect Smart Card PIN

Check to see if the Smart Card has been locked out due to too many attempts with an incorrect PIN. In such cases, the issuer of the Smart Card in the organization is able to help you get a new Smart Card.

Unable to Log into CMC as an Active Directory User

If you cannot log into CMC as an Active Directory user, try logging into CMC without enabling the Smart Card logon. You also have the option of disabling the Smart Card Logon through the local RACADM using the following commands:

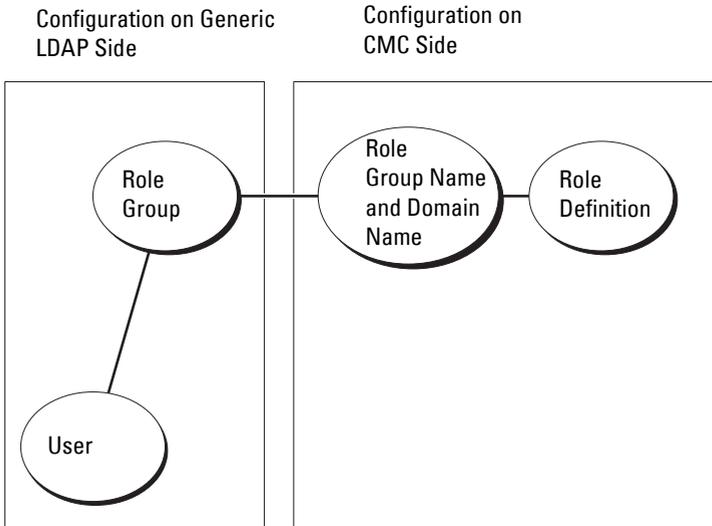
```
racadm config -g cfgActiveDirectory -o cfgADSCLEnable 0
racadm config -g cfgActiveDirectory -o cfgADSSOEnable 0
```

Using CMC with Generic LDAP

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. Table 5-41 shows the privileges level of the role groups and Table 8-1 shows the default role group settings.

Figure 8-5. Configuration of CMC with Generic LDAP



Configuring the Generic LDAP Directory to Access CMC

The CMC's Generic LDAP implementation uses two phases in granting access to a user. Phase 1 begins with user authentication, followed by phase 2 for user authorization.

Authentication and Authorization of the LDAP Users

Some directory servers require a bind before any searches can be performed against a specific LDAP server. The steps for authentication are:

- 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 then the user is considered authenticated. The next phase is authorization. CMC stores a maximum of 5 groups and their corresponding privileges. A user has the option to be added to multiple groups within the directory service. If the user is a member of multiple groups, then the user obtains the privileges of all their groups.

The authorization steps are:

- 1 Search through each configured group for the user's DN within the **member** or **uniqueMember** attributes. This field can be configured by the administrator.
- 2 For every group the user is a member of, add their privileges together.

Configuring Generic LDAP Directory Service Using CMC Web-Based Interface

You can use the Generic Lightweight Directory Access Protocol (LDAP) Service to configure your software to provide access to CMC. LDAP allows you to add and control the CMC user privileges of your existing users.



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

For more information about LDAP configuration configuring Generic LDAP, see "Using CMC with Generic LDAP" on page 282.

To view and configure LDAP, follow these steps:

- 1 Log in to the Web interface.
- 2 Click the **User Authentication** tab, and then click the **Directory Services** subtab. The **Directory Services** page appears.
- 3 Click the radio button associated with Generic LDAP.
- 4 Configure the options shown and click **Apply**.

The following configuration options are available.

Table 8-10. Common Settings

Setting	Description
Generic LDAP Enabled	Enables the generic LDAP service on CMC.
Use Distinguished Name to Search Group Membership	Specifies the distinguished name (DN) of LDAP groups whose members are allowed access to the device.
Enable SSL Certificate Validation	If checked, CMC uses the CA certificate to validate the LDAP server certificate during SSL handshake.
Bind DN	Specifies the distinguished name of a user used to bind to the server when searching for the login user's DN. If not provided an anonymous bind is used.
Password	A bind password to use in conjunction with the bind DN. NOTE: The bind password is sensitive data, and must be properly protected.
Base DN to Search	The DN of the branch of the directory where all searches must start from.
Attribute of User Login	Specifies the attribute to search for. If not configured, the default is to use uid. It is recommended to be unique within the chosen base DN, otherwise a search filter must be configured to ensure the uniqueness of the login user. If the user DN cannot be uniquely identified by searching the combination of attribute and search filter, login fails with an error.
Attribute of Group Membership	Specifies the LDAP attribute that is used to check for group membership. This must be an attribute of the group class. If not specified, the member and unique member attributes are used.
Search Filter	Specifies a valid LDAP search filter. This is used if the user attribute cannot uniquely identify the login user within the chosen base DN. If not provided, defaults to (objectClass=*), which searches for all objects in the tree. The maximum length of this property is 1024 characters.

Table 8-10. Common Settings (continued)

Setting	Description
Network Timeout (seconds)	Sets the time in seconds after which an idle LDAP session is automatically closed.
Search Timeout (seconds)	Sets the time in seconds after which a search is automatically closed.

Selecting Your LDAP Servers

You can configure the server to use with Generic LDAP in two ways. Static Servers allows the administrator to place a FQDN or IP address within the field. Alternatively, a list of LDAP servers can be retrieved by looking up their SRV record within the DNS.

The following are the properties in the LDAP Servers section:

- Use Static LDAP Servers — Selecting this option causes the LDAP service to use the specified servers with the port number provided (see details below).

 **NOTE:** You must select Static or DNS.

- LDAP Server Address — Specify the FQDN or IP of the LDAP server. To specify multiple, redundant LDAP servers that serve the same domain, provide the list of all servers separated by comma. CMC tries to connect to each server in turn, until it makes a successful connection.
- LDAP Server Port — Port of LDAP over SSL, default to 636 if not configured. Non-SSL port is not supported in CMC version 3.0 as the password cannot be transported without SSL.
- Use DNS to find LDAP Servers — Selecting this option causes LDAP to use the search domain and the service name through DNS. You must select Static or 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.

Managing LDAP Group Settings

The table in the Group Settings section lists role groups, displaying associated names, domains, and privileges for any role groups that are already configured.

- To configure a new role group, click a role group name that does not have a name, domain, and privilege listed.
- To change the settings for an existing role group, click the role group name.

When you click a role group name, the **Configure Role Group** page appears. Help for that page is available through the **Help** link at the top right corner of the page.

Managing LDAP Security Certificates

This sections displays the properties for the LDAP certificate recently uploaded to CMC. If you uploaded a certificate, use this information to verify that the certificate is valid and has not expired.



NOTE: By default, CMC does not have a certificate authority-issued server certificate for Active Directory. You must upload a current, certificate authority-signed server certificate.

The following properties for the certificate are displayed:

- Serial Number - The certificate's serial number.
- Subject Information - The certificate's subject (name of the person or company certified).
- Issuer Information - The certificate's issuer (name of the Certificate Authority).
- Valid From - The starting date of the certificate.
- Valid To - The expiry date of the certificate.

Use the following controls to upload and download this certificate:

- Upload - Initiates the upload process for the certificate. This certificate, which you obtain from your LDAP server, grants access to CMC.
- Download - Initiates the download process. You are prompted for the location to save the file. When you select this option and click **Next**, a **File Download** dialog box appears. Use this dialog box to specify a location on your management station or shared network for the server certificate.

Configuring Generic LDAP Directory Service Using RACADM

 **NOTE:** This feature supports both IPv4 and IPv6.

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.

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`.

Usage

To login to CMC using an LDAP user, use the username at the login prompt and the user's password at the password prompt. If a LDAP user cannot be logged in for any reason, CMC falls back and attempts to use a local login with the same username and password. This allows a login if network connectivity is broken or the LDAP server is not reachable.

Getting Help

CMC's `tracelog` contains some information on why a user may fail to login. To triage LDAP login failures, it is recommended to use the `racadm testfeature -f LDAP` command with the debugging turned on.

Power Management

Overview

The Dell PowerEdge M1000e server enclosure is the most power-efficient modular server enclosure in the market. It is designed to include highly-efficient power supplies and fans, has an optimized layout so that air flows 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 PowerEdge M1000e modular enclosure takes in AC power and distributes the load across all active internal power supply units (PSUs). The system can deliver up to 11637 Watts of AC power that is allocated to server modules and the associated enclosure infrastructure.



NOTE: Actual power delivery is based on configuration and workload.

The Power Management features of the M1000e help administrators configure the enclosure to reduce power consumption and to tailor power management to their unique requirements and environments.

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.

AC Redundancy Mode

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.

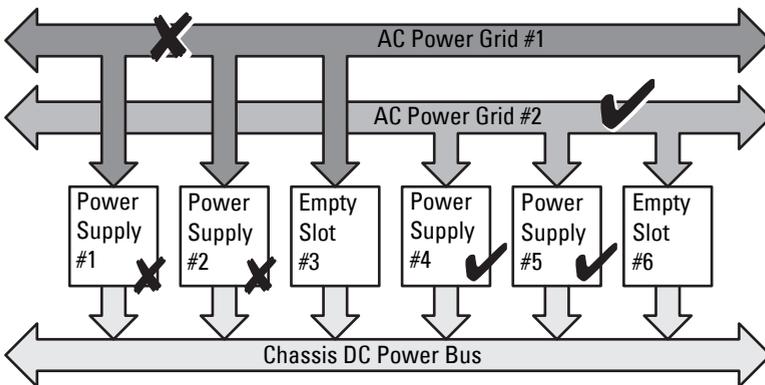
NOTE: AC redundancy is only met when the load requirements do not exceed the capacity of the weakest power grid.

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.

If for some reason CMC is unable to maintain AC redundancy then E-mail and/or SNMP alerts are sent to administrators if the Redundancy Lost event is configured for alerting.

Figure 9-1. Figure 8-2. 2 PSUs per grid and a power failure on grid 1



NOTE: 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 Mode

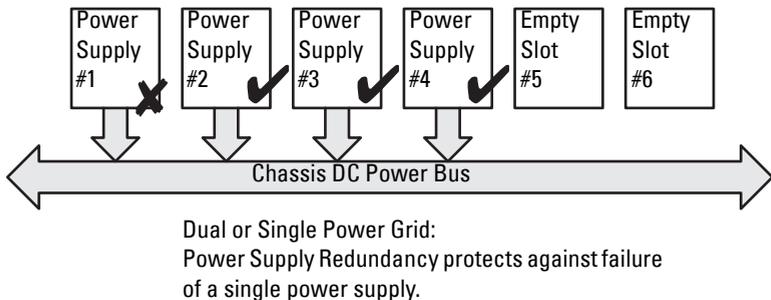
The power supply redundancy mode is useful when redundant power grids are not available, but you may want to be protected against a single PSU failure bringing down your servers in a modular enclosure. The highest capacity PSU is kept in online reserve for this purpose. This forms a Power Supply redundancy pool.

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 9-2. Power Supply Redundancy: Totally 4 PSUs with a failure of one PSU.



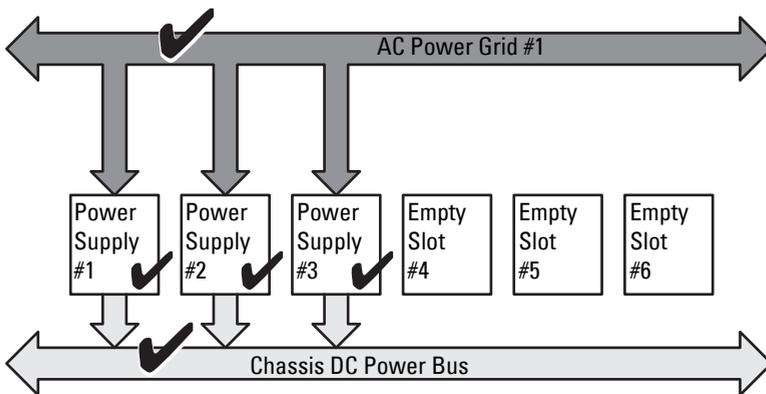
No Redundancy Mode

The **no redundancy mode** is the factory default setting for 3 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**.

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 9-3. No Redundancy with three PSUs in the chassis



Single Power Grid:
No protection against grid or power supply failure

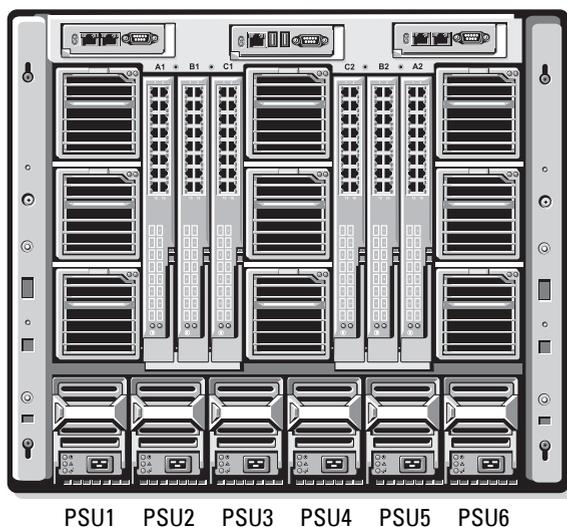
A PSU failure brings other PSUs out of Standby mode, as needed, to support the chassis power allocations. If you have 4 PSUs, and require only three, then in the event that one fails, the fourth PSU is brought online. A chassis can have all 6 PSUs online.

When you enable DPSE, the extra PSUs may be placed in Standby mode to increase efficiency and save power. For more information, see "Dynamic Power Supply Engagement" on page 296.

Power Budgeting for Hardware Modules

Figure 9-4 illustrates a chassis that contains a six-PSU configuration. The PSUs are numbers 1-6, starting on the left-side of the enclosure.

Figure 9-4. 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 *iDRAC 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 below 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** below 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 11637 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.

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 which servers 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 would be powered on first. These higher priority servers would then get their maximum power allocation, while lower priority servers may 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. So 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.

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 2 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 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.

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

The default redundancy configuration for a chassis depends on how many PSUs it contains, as shown in Table 9-1.

Table 9-1. 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 Conservation and Power Budget Changes

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 of the servers in the chassis by giving each server a number from 1 through 9. The default priority level for all servers is 1. The lower the number, the higher the priority level.

For instructions on assigning server priority levels, see "Using RACADM" on page 323.

You can assign server priority using the GUI:

- 1 Click **Servers** in the system tree.
- 2 Click **Power**→**Priority**.

Power Conservation and Max Conservation Mode

CMC performs maximum power conservation when:

- The user selects maximum conservation mode using the Web interface or RACADM.
- An automated command line script, issued by a UPS device, selects 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 user or an automated command line script clears the maximum conservation mode.

Using the Web Interface

You can select or clear the Max Power Conservation mode using the GUI:

- 1** Click **Chassis Overview** in the system tree.
- 2** Click **Power**→ **Configuration**.
- 3** Select the **Max Power Conservation Mode** box to enable maximum power conservation and click **Apply**.
- 4** Clear the **Max Power Conservation Mode** box to restore normal operation and click **Apply**.

Using RACADM

Open a serial/Telnet/SSH console to CMC and log in.

- 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
```

110V PSUs Operation

Some PSUs support operation with 110V AC input. This input can exceed what is allowed 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.

Using the Web Interface

Verify that the 110 V circuit is rated for the current expected, and then perform the following steps:

- 1** Click **Chassis Overview** in the system tree.
- 2** Click **Power**→ **Configuration**.
- 3** Select **Allow 110 VAC Operation** and click **Apply**.

Using RACADM

Verify that your 110 V circuit is rated for the expected current, and then perform the following steps:

- 1** Open a serial/Telnet/SSH text console to CMC and log in.
- 2** Enable 110 VAC PSUs:

```
racadm config -g cfgChassisPower -o  
cfgChassisAllow110VACOperation 1
```

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 supplies in the chassis do not provide sufficient power, both for redundancy, as well as full performance, then in order to preserve redundancy, some servers may not be:

- Granted sufficient power for full performance.
- Powered on.

Using the Web Interface

To enable Server Performance Over Power Redundancy, perform the following steps:

- 1** Click **Chassis Overview** in the system tree.
- 2** Click **Power**→ **Configuration**.
- 3** Select **Server Performance Over Power Redundancy** and click **Apply**.

To disable Server Performance Over Power Redundancy, perform the following steps:

- 1 Click **Chassis Overview** in the system tree.
- 2 Click **Power**→ **Configuration**.
- 3 Clear **Server Performance Over Power Redundancy** and click **Apply**.

Using RACADM

To enable Server Performance Over Power Redundancy, perform the following steps:

- 1 Open a serial/Telnet/SSH text console to CMC and log in.
- 2 Enable Server Performance Over Power Redundancy:

```
racadm config -g cfgChassisPower -o  
cfgChassisPerformanceOverRedundancy 1
```

To disable Server Performance Over Power Redundancy, perform the following steps:

- 1 Open a serial/Telnet/SSH text console to CMC and log in.
- 2 Disable Server Performance Over Power Redundancy:

```
racadm config -g cfgChassisPower -o  
cfgChassisPerformanceOverRedundancy 0
```

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.

Using the Web Interface

You can enable power remote logging using the GUI. To do so, log in to the GUI, and do the following:

- 1 Click **Chassis Overview** in the system tree.
- 2 Click **Power**→ **Configuration**.

- 3 Select **Power Remote Logging**, to enable you to log power events to a remote host.
- 4 Specify the required logging interval (1–1440 minutes).
- 5 Click **Apply**, to save changes.

Using RACADM

Open a serial, Telnet or SSH text console to CMC, log in, and configure power remote logging as shown:

- 1 To enable the power remote logging feature, enter the following command:

```
racadm config -g cfgRemoteHosts -o  
cfgRhostsSyslogPowerLoggingEnabled 1
```

- 2 To specify the desired logging interval, enter the following command:

```
racadm config -g cfgRemoteHosts -o  
cfgRhostsSyslogPowerLoggingInterval n
```

where n is 1-1440 minutes.

- 3 To determine if the power remote logging feature is enabled, enter the following command:

```
racadm getconfig -g cfgRemoteHosts -o  
cfgRhostsSyslogPowerLoggingEnabled
```

- 4 To determine the power remote logging interval, enter the following command:

```
racadm getconfig -g cfgRemoteHosts -o  
cfgRhostsSyslogPowerLoggingInterval
```



NOTE: 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. See the remote syslog configuration instructions for more details.

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.



NOTE: To set the redundancy policy, see "Configuring Power Budget and Redundancy" on page 320.

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.

Table 9-2 describes the actions taken by CMC when a new server is powered on in the scenario described above.

Table 9-2. 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: <ul style="list-style-type: none"> • 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.

Table 9-3 describes the firmware response to a PSU power down or removal as it applies to various PSU redundancy configurations.

Table 9-3. 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.

Table 9-3. Chassis Impact from PSU Failure or Removal (continued)

PSU Configuration	Dynamic PSU Engagement	Firmware Response
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.

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 "Redundancy Policies" on page 298.

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. Table 9-4 lists the SEL entries that are related to power supply changes.

Table 9-4. 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. Table 9-5 lists the SEL entries that are related to power redundancy policy changes.

Table 9-5. SEL Events for Power Redundancy Status Changes

Power Policy Event	System Event Log (SEL) Entry
Redundancy lost	redundancy lost was asserted
Redundancy regained	redundancy lost was de-asserted

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.

Configuring and Managing Power

You can use the Web-based and RACADM interfaces to manage and configure power controls on CMC. Specifically, you can:

- View power allocations, consumption, and status for the chassis, servers, and PSUs.
- Configure System Input Power Cap and Redundancy Policy for the chassis.
- Execute power control operations (power-on, power-off, system reset, power-cycle) for the chassis.

Viewing the Health Status of the PSUs

The **Power Supply Status** page displays the status and readings of the PSUs associated with the chassis.

Using the Web Interface

The PSU health status can be viewed in two ways: from the **Chassis Graphics** section on the **Chassis Status** page or the **Power Supply Status** page. The **Chassis Graphics** page provides a graphical overview of all PSUs installed in the chassis.

To view health status for all PSUs using **Chassis Graphics**:

- 1 Log in to the CMC Web interface.
- 2 The **Chassis Status** page is displayed. The lower section of **Chassis Graphics** depicts the rear view of the chassis and contains the health status of all PSUs. PSU health status is indicated by the color of the PSU subgraphic:
 - Green — PSU is present, powered on and communicating with CMC; there is no indication of an adverse condition.
 - Amber — Indicates a PSU failure. See the CMC log for details on the failure condition.
 - Gray — Occurs during PSU initialization and when the PSU is set to standby, during Chassis power up, or PSU insertion. PSU is present and not powered on. There is no indication of an adverse condition.
- 3 Use the cursor to hover over the an individual PSU subgraphic and a corresponding text hint or screen tip is displayed. The text hint provides additional information on that PSU.
- 4 The PSU subgraphic is hyperlinked to the corresponding CMC GUI page to provide immediate navigation to the **Power Supply Status** page for all PSUs.

To view the health status of the PSUs using **Power Supply Status**:

- 1 Log in to the CMC Web interface.
- 2 Select **Power Supplies** in the system tree. The **Power Supply Status** page displays.

Table 9-6 and Table 9-7 provide descriptions of the information provided on the Power Supply Status page.

Table 9-6. Power Supplies

Item	Description
Name	Displays the name of the power supply unit: PS-[n], where [n] is the power supply number.
Present	Indicates whether the PSU is Present or Absent .

Table 9-6. Power Supplies (continued)

Item	Description
Health	 OK Indicates that the PSU is present and communicating with CMC. In the event of a communication failure between CMC and the power supply, CMC cannot obtain or display health status for the PSU.
	 Warning Indicates that only Warning alerts have been issued, and corrective action must be taken. If corrective actions are not taken, it could lead to critical or severe power failures that can affect the integrity of the chassis.
	 Severe Indicates that at least one Failure alert has been issued for the power supply. Severe status indicates a power failure on the chassis, and corrective action must be taken immediately.
Power Status	Displays the power state of the power supplies (one of the following): Initializing, Online, Stand By, In Diagnostics, Failed, Offline, Unknown, or Absent.
Capacity	Displays the power supply's capacity in watts.

Table 9-7. System Power Status

Item	Description
Overall Power Health	Displays the health status (OK, Non-Critical, Critical, Non-Recoverable, Other, Unknown) of the power management for the entire chassis.
System Power Status	Displays the power status (On, Off, Powering On, Powering Off) of the chassis.
Redundancy	Displays the power supply redundancy status. Values include: No: Power Supplies are not redundant. Yes: Full Redundancy in effect.

Using RACADM

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

```
racadm getpminfo
```

For more information about `getpminfo`, including output details, see the *Command Line Reference Guide for iDRAC6 and CMC* on the Dell Support website at support.dell.com/manuals.

Viewing Power Consumption Status

CMC provides the actual input power consumption for the entire system on the **Power Consumption Status** page.

Using the Web Interface



NOTE: To perform power management actions, you must have **Chassis Control Administrator** privilege.

- 1 Log in to the CMC Web interface.
- 2 Select **Chassis Overview** in the system tree.
- 3 Click **Power**→ **Power Consumption**. The **Power Consumption** page displays.

Table 9-8 through Table 9-11 describe the information displayed on the **Power Consumption** page.



NOTE: You can also view the power redundancy status under **Power Supplies** in the **System** tree→ **Status** tab.

Using RACADM

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

```
racadm getpminfo
```

Table 9-8. Real-Time Power Statistics

Item	Description
System Input Power	Displays the current cumulative power consumption of all modules in the chassis measured from the input side of the PSUs. The value for system input power is indicated in both watts and BTU/h units.
Peak System Power	Displays the maximum system level input power consumption since the value was last cleared. This property allows you to track the maximum power consumption by the system (chassis and modules) recorded over a period of time. Click the Reset Peak/Min Power Statistics button below the table to clear this value. The value for peak system power is indicated in both watts and BTU/h units.
Peak System Power Start Time	Displays the date and time recorded when the peak system power consumption value was last cleared. The timestamp is displayed in the format hh:mm:ss MM/DD/YYYY , where hh is hours (0-24), mm is minutes (00-60), ss is seconds (00-60), MM is the month (1-12), DD is the day (1-31), and YYYY is the year. This value is reset with the Reset Peak/Min Power Statistics button and also when CMC resets or fails over.
Peak System Power Timestamp	Displays the date and time recorded when the peak system power consumption value occurred over the time period being recorded. The timestamp is displayed in the format hh:mm:ss MM/DD/YYYY , where hh is hours (0-24), mm is minutes (00-60), ss is seconds (00-60), MM is the month (1-12), DD is the day, 1-31, and YYYY is the year.
Minimum System Power	Displays the minimum system level AC power consumption value (in watts) over the time since the user last cleared this value. This property allows you to track the minimum power consumption by the system (chassis and modules) recorded over a period of time. Click the Reset Peak/Min Power Statistics button below the table to clear this value. The value for minimum system power is displayed in both watts and BTU/h units. This value is reset with the Reset Peak/Min Power Statistics button and also when CMC resets or fails over.

Table 9-8. Real-Time Power Statistics (continued)

Item	Description
Minimum System Power Start Time	Displays the date and time recorded when the minimum system power consumption value was last cleared. The timestamp is displayed in the format hh:mm:ss MM/DD/YYYY , where hh is hours (0-24), mm is minutes (00-60), ss is seconds (00-60), MM is the month (1-12), DD is the day (1-31), and YYYY is the year. This value is reset with the Reset Peak/Min Power Statistics button and also when CMC resets or fails over.
Minimum System Power Timestamp	Displays the date and time recorded when the minimum system power consumption occurred over the time period being recorded. The format of the timestamp is the same as described for Peak System Power Timestamp .
System Idle Power	Displays the estimated power consumption of the chassis when it is in idle state. The idle state is defined as the state of the chassis while it's ON and all modules are consuming power while in the idle state. <i>This is an estimated value and not a measured value.</i> It is computed as the cumulative power allocated to chassis infrastructure components (I/O modules, fans, iKVM, iDRAC controllers and front panel LCD) and the minimum power requirement of all servers that have been allocated power and that are in the powered-on state. The value for system idle power is displayed in both watts and BTU/h units.
System Potential Power	Displays the estimated power consumption of the chassis when it is operating at maximum power. The maximum power consumption is defined as the state of the chassis while it is ON and all modules are consuming maximum power. <i>This is an estimated value derived from historical aggregate power consumption of the system configuration and not a measured value.</i> It is computed as the cumulative power allocated to chassis infrastructure components (I/O modules, fans, iKVM, iDRAC controllers and the front panel LCD) and the maximum power requirement of all servers that have been allocated power and are in the powered-on state. The value for system potential power is displayed in both watts and BTU/h units.
System Input Current Reading	Displays the total input current draw of the chassis based on the sum of the input current draw of each of the individual PSU modules in the chassis. The value for system input current reading is displayed in Amps.

Table 9-9. Real-Time Energy Statistics Status

Item	Description
System Energy Consumption	Displays the current cumulative energy consumption for all modules in the chassis measured from the input side of the power supplies. The value is displayed in KWh and it is a cumulative value.
System Energy Consumption Start Time	Displays the date and time recorded when the system energy consumption value was last cleared, and the new measurement cycle began. The timestamp is displayed in the format hh:mm:ss MM/DD/YYYY , where hh is hours (0-24), mm is minutes (00-60), ss is seconds (00-60), MM is the month (1-12), DD is the day (1-31), and YYYY is the year. This value is reset with the Reset Energy Statistics button, but persists through a CMC reset or fail over operation.
System Energy Consumption Timestamp	Displays the date and time when the system energy consumption was calculated for display. The timestamp is displayed in the format hh:mm:ss MM/DD/YYYY , where hh is hours (0-24), mm is minutes (00-60), ss is seconds (00-60), MM is the month (1-12), DD is the day (1-31), and YYYY is the year.

Table 9-10. System Power Status

Item	Description
Overall Power Health	Indicates the health status of the chassis' power subsystem.: <ul style="list-style-type: none"> • Green Check Icon for OK • Yellow Exclamation Icon for Non-Critical • Red X Icon for Critical
System Power Status	Displays the power status (On , Off , Powering On , Powering Off) of the chassis.
Redundancy	Displays the redundancy status. Valid values are: No — PSUs are not redundant Yes — full redundancy in effect

Table 9-11. Server Modules

Item	Description
Slot	Displays the location of the server module. The Slot is a sequential number (1–16) that identifies the server module by its location within the chassis.
Name	Displays the server name. The server name can be redefined by the user.
Present	Displays whether the server is present in the slot (Yes or No). If this field displays Extension of # (where the # is 1-8), then number that follows it is the main slot of a multi-slot server.
Actual (AC)	Real-time measurement of the actual power consumption of the server. The measurement is displayed in watts AC.
Cumulative Power Start Time	Real-time measurement of the cumulative power that the server has consumed since the time displayed in the Start Time field. The measurement is presented in KiloWatt Hour (kWh) units.
Peak Consumption Time Stamp	Displays the peak power that the server consumed at one time. The time when the peak power consumption occurred is recorded in the Time Stamp field. The measurement is displayed in watts.

Viewing Power Budget Status

CMC provides power status overviews of the power subsystem on the **Power Budget Status** page.

Using the Web Interface



NOTE: To perform power management actions, you must have **Chassis Control Administrator** privilege.

- 1 Log in to the CMC Web interface.
- 2 Select **Chassis Overview** in the system tree.
- 3 Click **Power**→ **Budget Status**.

The **Power Budget Status** page displays.

Table 9-12 through Table 9-15 describe the information displayed on the **Power Budget Status** page.

See "Configuring Power Budget and Redundancy" on page 320 for information about configuring the settings for this information.

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 *Command Line Reference Guide for iDRAC6 and CMC*.

Table 9-12. System Power Policy Configuration

Item	Description
System Input Power Cap	<p>Displays the user configured maximum power consumption limit for the entire system (chassis, CMC, servers, I/O modules, power supply units, iKVM, and fans). CMC enforces this limit via reduced server power allocations, or by powering off lower priority server modules. The value for system input power cap is displayed in watts, BTU/h and percent units.</p> <p>If the chassis power consumption exceeds the System Input Power Cap, then the performance of lower priority servers is reduced until total power consumption falls below the cap.</p> <p>In cases where the servers are set to the same priority, then the selection of the server for power reduction, or power-off action, is based on the server slot number order. For example, the server in slot 1 is selected first and the server in slot 16 is selected last.</p>

Table 9-12. System Power Policy Configuration (continued)

Item	Description
Redundancy Policy	<p data-bbox="330 271 991 335">Displays the current redundancy configuration: AC Redundancy, Power Supply Redundancy, and No Redundancy.</p> <p data-bbox="330 343 991 526">AC Redundancy — Power input is load-balanced across all PSUs. Half of them should be cabled to one AC grid and the other half should be cabled to another grid. When the system is running optimally in AC Redundancy mode, power is load-balanced across all active supplies. In case of a grid failure, the PSUs on the functioning AC grid take over without interruption.</p> <p data-bbox="330 534 991 646">Power Supply Redundancy — The capacity of the highest-rated PSU in the chassis is held in reserve, ensuring that a failure of any one PSU does not cause the server modules or chassis to power down.</p> <p data-bbox="330 654 991 774">Power Supply Redundancy may not use all six PSUs; it uses sufficient PSUs to assure that on the failure of any one the remaining can continue to supply power to the chassis. The other PSUs may be placed in Standby mode if DPSE is enabled.</p> <p data-bbox="330 782 991 901">No Redundancy — The power from all active PSUs are sufficient to power the entire chassis, including the chassis, servers, I/O modules, iKVM, and CMC. The remaining PSUs may be placed in standby mode if DPSE is enabled.</p> <p data-bbox="330 909 991 1037"> CAUTION: The No Redundancy mode uses only the minimum required number of PSUs at a time, with no backup. Failure of one of the PSUs in use could cause the server modules to lose power and data.</p>
Dynamic Power Supply Engagement	<p data-bbox="330 1050 991 1241">Displays whether Dynamic Power Supply Engagement is enabled or disabled. Enabling this feature allows CMC to put under-utilized PSUs into standby mode based on the redundancy policy that is set and the power requirements of the system. Putting under-utilized PSUs into standby mode increases the utilization, and efficiency, of the online PSUs, saving power.</p>

Table 9-13. Power Budgeting

Item	Description
System Input Max Power Capacity	Maximum input power that the available power supplies can supply to the system (in watts).
Input Redundancy Reserve	<p>Displays the amount of redundant power (in watts) in reserve that can be utilized in the event of an AC grid or power supply unit (PSU) failure.</p> <p>When the chassis is configured to operate in AC Redundancy mode, the Input Redundancy Reserve is the amount of reserve power that can be utilized in the event of an AC grid failure.</p> <p>When the chassis is configured to operate in Power Supply Redundancy mode, the Input Redundancy Reserve is the amount of reserve power that can be utilized in the event of a PSU failure.</p>
Input Power Allocated to Servers	Displays (in watts) the cumulative input power that CMC allocates to servers based on their configuration.
Input Power Allocated to Chassis Infrastructure	Displays (in watts) the cumulative input power that CMC allocates to the chassis infrastructure (Fans, IO modules, iKVM, CMC, Standby CMC and iDRAC on servers).
Total Input Power Available for Allocation	Displays the total chassis power, in watts, still available for allocation.
Standby Input Power Capacity	<p>Displays the amount of standby input power (in watts) that is available in the event of a Power Supply fault or Power Supply removal from the system. This field may show readings when the system has multiple power supplies and the Dynamic Power Supply Engagement is enabled.</p> <p>NOTE: It is possible to see a PSU in standby mode but not contribute to the Standby Input Power Capacity value. In this case, the watts from this PSU are contributing to the Total Input Power Available for Allocation value.</p>

Table 9-14. Server Modules

Item	Description
Slot	Displays the location of the server module. The Slot is a sequential number (1–16) that identifies the server module by its location within the chassis.
Name	Displays the server name. The server name is defined by the user.
Type	Displays the type of the server.
Priority	<p>Displays the priority level allotted to the server slot in the chassis for power budgeting. CMC uses this value in its calculations when power must be reduced or reallocated based on user-defined power limits or power supply or power grid failures.</p> <p>Priority levels: 1 (highest) through 9 (lowest)</p> <p>Default: 1</p> <p>NOTE: Server slot priority level is associated with the server slot—not with the server inserted into the slot. If you move a server to a different slot in the chassis or to a different chassis, the priority previously associated with new slot determines the priority of the relocated server.</p>
Power State	<p>Displays the power status of the server:</p> <ul style="list-style-type: none">• N/A: CMC has not determined the power state of the server.• Off: Either the server or chassis is off.• On: Both chassis and server are on.• Powering On: Temporary state between Off and On. When the powering on cycle completes, the Power State changes to On.• Powering Off: Temporary state between On and Off. When the powering off cycle completes, the Power State changes to Off.
Budget Allocation - Actual	<p>Displays the power budget allocation for the server module.</p> <ul style="list-style-type: none">• Actual: Current power budget allocation for each server.

Table 9-15. Chassis Power Supplies

Item	Description
Name	Displays the name of the PSU in the format PS- <i>n</i> , where <i>n</i> , is the PSU number.
Power State	Displays the power state of the PSU — Initializing, Online, Stand By, In Diagnostics, Failed, Unknown, or Absent (missing).
Input Volts	Displays the present input voltage of the power supply.
Input Current	Displays the present input current of the power supply.
Output Rated Power	Displays the maximum output power rating of the power supply.

Configuring Power Budget and Redundancy

CMC’s power management service optimizes power consumption for the entire chassis (the chassis, servers, IOMs, iKVM, CMC, and PSUs) and re-allocates power to different modules based on the demand.

Using the Web Interface

 **NOTE:** To perform power management actions, you must have **Chassis Control Administrator** privilege.

- 1 Log in to the CMC Web interface.
- 2 Select **Chassis Overview** in the system tree.
- 3 Click **Power**→ **Configuration**.
The **Budget/Redundancy Configuration** page displays.
- 4 Set any or all of the properties described in Table 9-16 according to your needs.
- 5 Click **Apply** to save your changes.

To refresh the content on the **Budget/Redundancy Configuration** page, click **Refresh**. To print the contents, click **Print**.

Table 9-16. Configurable Power Budget/Redundancy Properties

Item	Description
System Input Power Cap	<p data-bbox="380 295 1006 502">System Input Power Cap is the maximum AC power that the system is allowed to allocate to servers and chassis infrastructure. It can be configured by the user to any value that exceeds the minimum power needed for servers that are powered on and the chassis infrastructure; configuring a value that falls below the minimum power needed for servers and the chassis infrastructure fails.</p> <p data-bbox="380 510 1006 662">The power allocated to Servers and Chassis Infrastructure can be found in the User Interface on the Chassis Overview → Power → Power Budget status page under Power Budgeting section or by using the CLI RACADM utility command (<code>racadm getpbinfo</code>).</p> <p data-bbox="380 670 1006 790">Users can power off one or more server(s) to lower the current power allocation, and re-attempt setting a lower value for System Input Power Cap (if desired) or simply configure the cap prior to powering on the servers.</p> <p data-bbox="380 798 1006 917">To change this setting, it is possible to enter a value in any of the units. The interface ensures that the unit field that was last changed will be the value that is submitted when those changes are applied.</p> <p data-bbox="380 925 1006 989">NOTE: See the Datacenter Capacity Planner (DCCP) tool at www.dell.com/calc for capacity planning.</p> <p data-bbox="380 997 1006 1206">NOTE: When value changes are specified in watts, the submitted value exactly reflects what is actually applied. However, when the changes are submitted in either of the BTU/h or percent units, the submitted value may not exactly reflect what is actually applied. This is because these units are converted to watts and then applied; and the conversion is susceptible to some rounding error.</p>

Table 9-16. Configurable Power Budget/Redundancy Properties (continued)

Item	Description
Redundancy Policy	<p>This option allows you to select one the following options:</p> <ul style="list-style-type: none"> • No Redundancy: Power from the power supplies is used to power the entire chassis, including the chassis, servers, I/O modules, iKVM, and CMC. No power supplies must be kept in reserve. <p>NOTE: The No Redundancy mode uses only the minimum required number of power supplies at a time. If the minimum number of PSUs are installed, then there is no backup available. Failure of one of the three power supplies being used could cause the servers to lose power and/or data. If more than the minimum required number of PSUs are present, then the additional PSUs may be placed in Standby mode for improving power efficiency if DPSE is enabled.</p> <ul style="list-style-type: none"> • Power Supply Redundancy: The capacity of the highest-rated power supply in the chassis is kept in reserve, ensuring that a failure of any one power supply does not cause the server modules or chassis to power down (hot spare). <p>Power Supply Redundancy mode may not utilize all installed power supplies. Any additional power supplies, if present, may be placed in Standby mode for improving power efficiency, when DPSE is enabled. Power Supply Redundancy mode prevents server modules from powering up if the power consumption of the chassis exceeds the rated power. Failure of two power supplies may cause some or all server modules in the chassis to power down. Server module performance is not degraded in this mode.</p> <ul style="list-style-type: none"> • AC Redundancy: This mode divides half the PSUs into two power grids (for example, PSUs 1-3 make up power grid 1 and PSUs 4-6 make up power grid 2). Failure of a PSU or loss of AC power to one grid reports the redundancy status as lost.
Server Performance Over Power Redundancy	<p>This option favors server performance and server powerup, over maintaining power redundancy. For more information about this feature, see "Server Performance Over Power Redundancy" on page 301.</p>

Table 9-16. Configurable Power Budget/Redundancy Properties (continued)

Item	Description
Enable Dynamic Power Supply Engagement	<p>On selection, enables dynamic power management. In Dynamic Engagement mode, the power supplies are turned ON (online) or OFF (standby) based on power consumption, optimizing the energy consumption of the entire chassis.</p> <p>For example, your power budget is 5000 watts, your redundancy policy is set to AC redundancy mode, and you have six power supply units. CMC determines that four of the power supply units can manage the AC redundancy while the other two remain in standby mode. If an additional 2000W of power is needed for newly installed servers or power efficiency of the existing system configuration is required to be improved, then the two standby power supply units are engaged.</p>
Disable Chassis Power Button	<p>On selection, disables the chassis power button. If the check box is selected and you attempt to change the power state of the chassis by pressing the chassis power button, the action is ignored.</p>
Allow 110 VAC Operation	<p>On selection, permits normal operation if any power supply units are connected to 110V AC input. For more information see "110V PSUs Operation" on page 300.</p>
Max Conservation Mode	<p>On selection, immediately enters the maximum power conservation mode. For more information see "Power Conservation and Max Conservation Mode" on page 299.</p>

Using RACADM

To enable and set the redundancy policy:



NOTE: To perform power management actions, you must have **Chassis Control Administrator** privilege.

- 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:

```
racadm config -g cfgChassisPower -o  
cfgChassisRedundancyPolicy 1
```

sets the redundancy policy to 1.

- 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:

```
racadm config -g cfgChassisPower -o  
cfgChassisDynamicPSUEngagementEnable 0
```

disables dynamic PSU engagement.

For information about RACADM commands for chassis power, see the `config`, `getconfig`, `getpbinfo`, and `cfgChassisPower` sections in the *Command Line Reference Guide for iDRAC6 and CMC*.

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 reconfigure the priority for the new slot location.



NOTE: To perform power management actions, you must have **Chassis Configuration Administrator** privilege.

Using the Web Interface

- 1 Log in to the CMC Web interface.
- 2 Select **Servers Overview** in the system tree. The **Servers Status** page appears.
- 3 Click **Power**→ **Server Priority**.
The **Server Priority** page appears, listing all of the servers in your chassis.
- 4 Select a priority level (1–9, with 1 holding the highest priority) for one, multiple, or all servers. The default value is 1. You can assign the same priority level to multiple servers.
- 5 Click **Apply** to save your changes.

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, the following command:

```
racadm config -g cfgServerInfo -o cfgServerPriority -i  
5 1
```

sets the priority level to 1 for the server in slot 5.

Setting the Power Budget



NOTE: To perform power management actions, you must have **Chassis Control Administrator** privilege.

Using the Web Interface

- 1 Log in to the CMC Web interface.
- 2 Click **Chassis Overview** in the system tree. The **Chassis Health** page appears.
- 3 Click the **Power** tab.
The **Power Consumption Status** page appears.

- 4 Click the **Configuration** subtab.

The **Budget/Redundancy Configuration** page appears.

- 5 Type a budget value of up to 11637 watts in the **System Input Power Cap** text field.

 **NOTE:** 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 this value, CMC displays a failure message.

 **NOTE:** When value changes are specified in watts, the submitted value will exactly reflect what is actually applied. However, when the changes are submitted in either of the BTU/h or percent units, the submitted value may not exactly reflect what is actually applied. This is because these units are converted to watts and then applied; and the conversion is susceptible to some rounding error.

- 6 Click **Apply** to save your changes.

Using RACADM

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

```
racadm config -g cfgChassisPower -o  
cfgChassisPowerCap <value>
```

where <value> is a number between 2715–11637 representing the maximum power limit in watts. The default is 11637.

For example, the following command:

```
racadm config -g cfgChassisPower -o  
cfgChassisPowerCap 5400
```

sets the maximum power budget to 5400 watts.

 **NOTE:** The power budget is limited to 11637 Watts. If you attempt to set an AC power budget value that exceeds the power capacity of your chassis, CMC displays a failure message.

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, 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** (see "Setting the Power Budget" on page 325.)
- A power failure occurs in a non-redundant configuration.

For information about assigning priority levels to servers, see "Executing Power Control Operations on the Chassis" on page 327.

Executing Power Control Operations on the Chassis



NOTE: To perform power management actions, you must have **Chassis Control Administrator** privilege.



NOTE: Power control operations affect the entire chassis. For power control operations on an IOM, see "Executing Power Control Operations on an IOM" on page 329. For power control operations on servers, see "Executing Power Control Operations on a Server" on page 330.

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).

Using the Web Interface

- 1 Log in to the CMC Web interface.
- 2 Select **Chassis Overview** in the system tree.
- 3 Click the **Power** tab.
The **Power Consumption Status** page displays.
- 4 Click the **Control** subtab.
The **Chassis Power Control** page displays.

5 Click the corresponding radio buttons to select one of the following **Power Control Operations**:

- **Power On System** — Turns on the chassis power (the equivalent of pressing the power button when the chassis power is **OFF**). This option is disabled if the chassis is already powered **ON**.



NOTE: This action powers on the chassis and other subsystems (iDRAC on the servers, IOMs, and iKVM). Servers do not power on.

- **Power Off System** — Turns off the chassis power. This option is disabled if the chassis is already powered **OFF**.



NOTE: This action powers off the chassis (chassis, servers, IOMs, iKVM, and power supplies). CMCs remain powered on, but in virtual standby state; a power supply unit and fans provide cooling for CMCs in this state. The power supply also provides power to the fans that run at low speed.

- **Power Cycle System (cold boot)** — Powers off and then reboots the system (cold boot). This option is disabled if the chassis is already powered **OFF**.



NOTE: This action powers off and then reboots the entire chassis (chassis, servers which are configured to always power on, IOMs, iKVM, and power supplies).

- **Reset CMC** — Resets CMC without powering off (warm reboot). (This option is disabled if CMC is already powered off).



NOTE: This action only resets CMC. No other components are affected.

- **Non-Graceful Shutdown** — This action forces a non-graceful power off of the entire chassis (chassis, servers, IOMs, iKVM, and power supplies). This does not attempt to cleanly shutdown the operating system of the servers prior to powering off.

6 Click **Apply**. A dialog box appears requesting confirmation.

7 Click **OK** to perform the power management action (for example, cause the system to reset).

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 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 Control Administrator** privilege.

Using the Web Interface

- 1 Log in to the CMC Web interface.
- 2 Select **I/O Modules Overview**.
The **I/O Modules Status** page displays.
- 3 Click the **Power** tab.
The **Power Control** page displays.
- 4 Select the operation you want to execute (**reset** or **power cycle**) from the drop-down menu beside the IOM in the list.
- 5 Click **Apply**.
A dialog box appears requesting confirmation.
- 6 Click **OK** to perform the power management action (for example, cause the IOM to power cycle).

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**.

Executing Power Control Operations on a Server



NOTE: To perform power management actions, you must have **Chassis Control Administrator** privilege.

CMC enables you to remotely perform several power management actions, for example, an orderly shutdown, on an individual server in the chassis.

Using the Web Interface

- 1 Log in to the CMC Web interface.
- 2 Expand **Server Overview** in the system tree, and then select the server on which you want to execute a power control operation. The **Server Status** page displays.
- 3 Click the **Power** tab.
The **Server Power Management** page displays.
- 4 **Power Status** displays the power status of the server (one of the following):
 - **N/A** - CMC has not yet determined the power state of the server.
 - **Off** - Either the server is off or the chassis is off.
 - **On** - Both chassis and server are on.
 - **Powering On** - Temporary state between Off and On. When the action completes successfully, the **Power State** is **On**.
 - **Powering Off** - Temporary state between On and Off. When the action completes successfully, the **Power State** is **Off**.
- 5 Select one of the following **Power Control Operations** by clicking its radio button:
 - **Power On Server** — Turns on the server power (equivalent to pressing the power button when the server power is off). This option is disabled if the server is already powered on.
 - **Power Off Server** — Turns off the server power (equivalent to pressing the power button when the server power is on).
 - **Graceful Shutdown** — Powers off and then reboots the server.

- **Reset Server (warm boot)** — Reboots the server without powering off. This option is disabled if the server is powered off.
 - **Power Cycle Server (cold boot)** — Powers off and then reboots the server. This option is disabled if the server is powered off.
- 6 Click **Apply**. A dialog box appears requesting confirmation.
 - 7 Click **OK** to perform the power management action (for example, cause the server to reset).



NOTE: All of the power control operations can be performed on multiple servers from the **Servers** → **Power** → **Control** page.

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>* indicates the operation you want to execute: `powerup`, `powerdown`, `powercycle`, `graceshutdown`, or `hardreset`.

110V Operation

Some models of power supplies (PSUs) are capable of operating both from 220V mains as well as 110V mains. 110V power may have limited capacity; hence when any 110V connection is detected, the chassis does not grant any additional server power requests until the user acknowledges 110V operation by changing that power configuration property. The user must verify that the 110V circuit in use can deliver the power required for the chassis configuration before the acknowledgement. After acknowledgement, the chassis grants all future appropriate server power requests and uses all available power supply capacity.

The user can reset the 110V acknowledgement at any time from the GUI or RACADM after initial installation. Power supply entries are logged to the SEL log when 110V power supplies are detected and when 110V supplies are removed. Entries are also logged to the SEL log when acknowledged and unacknowledged by the user.

The overall power health is at least in Non-Critical state when the chassis is operating in 110V mode and the user has not acknowledged the 110V operation. The "Warning" icon is displayed on the GUI 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.

Troubleshooting

For power supply and power-related issue troubleshooting, see "Troubleshooting and Recovery" on page 375.

Using the iKVM Module

Overview

The local access KVM module for your 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 your 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.

iKVM User Interface

The iKVM uses the On Screen Configuration and Reporting (OSCAR) graphical user interface, which is activated by a hot key. OSCAR allows you to select one of the servers or the Dell CMC command line you wish to access with the local keyboard, display, and mouse.

Only one iKVM session per chassis is allowed.

Security

The OSCAR user interface allows you to protect your system with a screen saver password. After a user-defined time, the screen saver mode engages, and access is prohibited until the appropriate password is entered to reactivate OSCAR.

Scanning

OSCAR 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 slots names for all 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 servers using OSCAR is overwritten.

CMC identifies a slot by assigning it a unique name. To change slot names using the CMC Web interface, see "Editing Slot Names." To change a slot name using RACADM, see the `setslotname` section in the *Command Line Reference Guide for iDRAC6 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

You can update the iKVM firmware using the CMC Web interface or RACADM `fwupdate` command. For more information, see "Managing iKVM From CMC" on page 351.

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, 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 to each type of connection so that when there are multiple connections, only one connection is available while others are disabled.

The order of precedence for iKVM connections is as follows:

- 1 Front panel
- 2 ACI
- 3 Rear Panel

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 the 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

* 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 an overview of the OSCAR interface.

Navigation Basics

Table 10-1. OSCAR Keyboard and Mouse Navigation

Key or Key Sequence	Result
<ul style="list-style-type: none">• <Print Screen>-<Print Screen>• <Shift>-<Shift>• <Alt>-<Alt>• <Ctrl>-<Ctrl>	Any of these key sequences can open OSCAR, depending on your 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 the OK button, then 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.

Table 10-1. OSCAR Keyboard and Mouse Navigation (continued)

Key or Key Sequence	Result
<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.
<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

Table 10-2. OSCAR Setup Menu Features

Feature	Purpose
Menu	Changes the server listing between numerically by slot or alphabetically by name.
Security	<ul style="list-style-type: none">• 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.

To access the **Setup** dialog box:

- 1 Press <Print Screen> to launch the OSCAR interface. The **Main** dialog box appears.
- 2 Click **Setup**. The **Setup** dialog box appears.

Changing the Display Behavior

Use the **Menu** dialog box to change the display order of servers and set a Screen Delay Time for OSCAR.

To access the **Menu** dialog box:

- 1 Press <Print Screen> to launch OSCAR. The **Main** dialog box appears.
- 2 Click **Setup** and then **Menu**. The **Menu** dialog box appears.

To choose the default display order of servers in the **Main** dialog box:

- 1 Select **Name** to display servers alphabetically by name.
or
Select **Slot** to display servers numerically by slot number.
- 2 Click **OK**.

To assign one or more key sequences for OSCAR activation:

- 1 Select a key sequence from the **Invoke OSCAR** menu.
- 2 Click **OK**.

The default key to invoke OSCAR is <Print Screen>.

To set a Screen Delay Time for the OSCAR:

- 1 Enter the number of seconds (0 through 9) to delay display of OSCAR after you press <Print Screen>. Entering <0> launches OSCAR with no delay.
- 2 Click **OK**.

Setting a time to delay display of OSCAR allows you to complete a soft switch. To perform a soft switch, see "Soft Switching" on page 342.

Controlling the Status Flag

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.

Table 10-3. OSCAR Status Flags

Flag	Description
	Flag type by name
	Flag indicating that the user has been disconnected from all systems
	Flag indicating that Broadcast mode is enabled

To access the **Flag** dialog box:

- 1 Press <Print Screen>. The **Main** dialog box appears.
- 2 Click **Setup** and then **Flag**. The **Flag** dialog box appears.

To specify how the status flag displays:

- 1 Select **Displayed** to show the flag all the time 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.

- 2 Select a flag color from the **Display Color** section. Options are black, red, blue, and purple.
- 3 In **Display Mode**, select **Opaque** for a solid color flag or **Transparent** to see the desktop through the flag.
- 4 To position the status flag on the desktop:
 - a Click **Set Position**. The **Set Position Flag** displays.
 - b Left-click on the title bar and drag it to the desired location on the desktop.
 - c Right-click to return to the **Flag** dialog box.

 **NOTE:** Changes made to the flag position are not saved until you click **OK** in the **Flag** dialog box.

- 5 Click **OK** to save settings.
To exit without saving 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 your servers. In addition, the iKVM includes a system input to establish a CMC command line console connection to CMC.

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

Use the OSCAR Main dialog box to view, configure, and manage servers through the iKVM. You can view your 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.

To access the **Main** dialog box:

Press <Print Screen> to launch the OSCAR interface. The **Main** dialog box appears.

or

If a password has been assigned, the **Password** dialog box appears. Type your password and click **OK**. The **Main** dialog box appears.

For more information about setting a password, see "Setting Console Security" on page 344.



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 and then clicking **OK**.

Viewing the Status of Your Servers

The status of the servers in your chassis is indicated in the right columns of the **Main** dialog box. The following table describe the status symbols.

Table 10-4. OSCAR Interface Status Symbols

Symbols	Description
	(Green dot.) Server is online.
	(Red X.) Server is offline or absent from chassis.
	(Yellow dot.) Server is not available.
	(Green A or B.) 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 servers. When you select a server, the iKVM reconfigures the keyboard and mouse to the proper settings for that server.

- To select servers:

Double-click the server name or the slot number.

or

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>.

or

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:

Press <Print Screen> to access OSCAR and then click **Disconnect**.

or

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 "Controlling the Status Flag" on page 338.

Soft Switching

Soft switching is switching between servers using a hotkey sequence. You can soft switch to a server by pressing <Print Screen> and then typing the first few characters of its name or number. If you previously set a **delay time** (the number of seconds before the **Main** dialog box is displayed after <Print Screen> is pressed) and you press the key sequences before that time has elapsed, the OSCAR interface does not display.

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**.

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 in step 3 (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 in step 3 (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. (For information about order of connection precedence, see "iKVM Connection Precedences.")

For information about enabling or disabling the front panel connection, see "Enabling or Disabling the 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 GUI console redirection feature both have access to the console and are able to type simultaneously.

To prevent this scenario, the remote user, before starting the iDRAC GUI console redirection, 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 work 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 the Status of Your Servers").

Setting Console Security

OSCAR enables you to configure security settings on your iKVM console. You can establish a screen saver mode that engages after your console remains unused for a specified delay time. Once engaged, your 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 your console with password protection, set or change your 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. See "Clearing a Lost or Forgotten Password."

Accessing the Security Dialog Box

- 1 Press <Print Screen>. The **Main** dialog box appears.
- 2 Click **Setup** and the **Security**. The **Security** dialog box appears.

Setting or Changing the Password

- 1 Single-click and press <Enter> or double-click in the **New** field.
- 2 Type the new password in the **New** field and then 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 then press <Enter>.
- 4 Click **OK** if you only want to change your password, and then close the dialog box.

Password-protecting Your Console

- 1 Set your password as described in the previous procedure.
- 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 your monitor is ENERGY STAR compliant, select **Energy**; otherwise select **Screen**.



NOTE: 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. When it concludes, you are returned to the **Security** dialog box.

Logging In

- 1 Press <Print Screen> to launch OSCAR. The **Password** dialog box appears.
- 2 Type your password and then click **OK**. The **Main** dialog box appears.

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 Your Console

- 1 From 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 Leaving the **New** field empty, press <Enter>.
- 4 Single-click and press <Enter>, or double-click in the **Repeat** field.
- 5 Leaving the **Repeat** field empty, press <Enter>.
- 6 Click **OK** if you only want to eliminate your password.

Enabling Screen Saver Mode With No Password Protection



NOTE: If your console is password protected, you must first remove password protection. Follow the steps in the previous procedure before following the steps below.

- 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 displays. Click **OK** to start the test.

The test takes 10 seconds. When it concludes, you are returned to the **Security** dialog box.

 **NOTE:** Enabling screen saver mode disconnects the user from a server; 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:

- 1 In the **Security** dialog box, clear the **Enable Screen Saver** box.
- 2 Click **OK**.

To immediately turn on the screen saver, press <Print Screen>, then press <Pause>.

Clearing a 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:

- 1 Log in to the CMC Web interface.
- 2 Select **iKVM** from the **Chassis** submenu.
- 3 Click the **Setup** tab. The **iKVM Configuration** page displays.
- 4 Click **Restore Default Values**.

You can then change the password from the default using **OSCAR**. See "Setting or Changing the 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 **racresetcfg** section in the *Command Line Reference Guide for iDRAC6 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 Click the radio button for the desired language, and then 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 appears.
- 2 Click **Commands** and then **Display Versions**. The **Version** dialog box appears.

The top half of the **Version** dialog box lists the subsystem versions in the appliance.

- 3 Click or press <Esc> to close the **Version** dialog box.

Scanning Your System

In scan mode, the iKVM automatically scans from slot to slot (server to server). You can scan up to 16 servers by specifying which servers you want to scan and the number of seconds that each server is displayed.

To add servers to the scan list:

- 1 Press <Print Screen>. The **Main** dialog box appears.
- 2 Click **Setup** and then **Scan**. The **Scan** dialog box appears, listing of all servers in the chassis.
- 3 Select the box next to the servers you wish to scan.
or
Double-click the server name or slot.
or
Press <Alt > and the number of the server you wish 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 the **Add/Remove** button, and then click **OK**.

To remove a server from the **Scan** list:

- 1 In the **Scan** dialog box, select the box next to the server to be removed.
or
Double-click the server name or slot.
or
Click the **Clear** button to remove all servers from the **Scan** list.
- 2 Click the **Add/Remove** button, and then click **OK**.

To start Scan mode:

- 1 Press <Print Screen>. The **Main** dialog box appears.
- 2 Click **Commands**. The **Command** dialog box appears.
- 3 Select the **Scan Enable** box.
- 4 Click **OK**. A message appears indicating that the mouse and keyboard have been reset.
- 5 Click to close the message box.

To cancel 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. Scanning stops at the currently selected server.

or

Press <Print Screen>. The **Main** dialog box appears; select a server in the list.

- 2 Click the **Commands** button. The **Commands** dialog box appears.
- 3 Clear the **Scan Enable** box.

Broadcasting to Servers

You can simultaneously control more than one server in the system to ensure that all selected servers receive identical input. You can choose to broadcast keystrokes and/or mouse movements independently.

 **NOTE:** You can broadcast up to 16 servers at a time.

To broadcast to servers:

- 1 Press <Print Screen>. The **Main** dialog box appears.
- 2 Click **Setup** and then **Broadcast**. The **Broadcast** dialog box appears.

 **NOTE:** 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.

 **NOTE:** 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. Because these conditions are extremely difficult to achieve, broadcasting mouse movements to multiple servers may have unpredictable results.

- 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. Click or press <Escape> to return to the **Main** dialog box.
- 5 Click **Commands**. The **Commands** dialog box appears.
- 6 Click the **Broadcast Enable** box to activate broadcasting. The **Broadcast Warning** dialog box appears.
- 7 Click **OK** to enable the broadcast.
To cancel and return to the **Commands** dialog box, click or press <Esc>.
- 8 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.

To turn broadcasting off:

From the **Commands** dialog box, clear the **Broadcast Enable** box.

Managing iKVM From CMC

Enabling or Disabling the Front Panel

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 the **config** command section in the *Command Line Reference Guide for iDRAC6 and CMC*.

To enable or disable access to the iKVM from the front panel using the Web interface:

- 1 Log in to the CMC Web interface.
- 2 Select iKVM in the system tree. The **iKVM Status** page displays.
- 3 Click the **Setup** tab. The **iKVM Configuration** page displays.
- 4 To enable, select the **Front Panel USB/Video Enabled** check box. To disable, clear the **Front Panel USB/Video Enabled** check box.
- 5 Click **Apply** to save the setting.

Enabling the Dell CMC Console Through iKVM

To enable the iKVM to access the Dell CMC console using RACADM, open a serial/Telnet/SSH text console to CMC, log in, and type:

```
racadm config -g cfgKVMInfo -o  
cfgKVMAccessToCMCEnable 1
```

To enable the Dell CMC console using the Web interface:

- 1 Log in to the CMC Web interface.
- 2 Select iKVM in the system tree. The **iKVM Status** page displays.
- 3 Click the **Setup** tab. The **iKVM Configuration** page displays.
- 4 Select the **Allow access to CMC CLI from iKVM** check box.
- 5 Click **Apply** to save the setting.

Viewing the iKVM Status and Properties

The local access KVM module for your Dell M1000e server chassis is called the Avocent Integrated KVM Switch Module, or iKVM. The health status of the iKVM associated with the chassis can be viewed on the **Chassis Properties Health** page under the **Chassis Graphics** section.

To view health status for the iKVM using **Chassis Graphics**:

- 1 Log in to the CMC Web interface.
- 2 The **Chassis Status** page is displayed. The right section of **Chassis Graphics** depicts the rear view of the chassis and contains the health status of the iKVM. iKVM health status is indicated by the color of the iKVM subgraphic:

- Green - iKVM is present, powered on and communicating with the CMC; there is no indication of an adverse condition.
 - Amber - iKVM is present, but may or may not be powered on, or may or may not be communicating with CMC; an adverse condition may exist.
 - Gray - iKVM is present and not powered on. It is not communicating with CMC and there is no indication of an adverse condition.
- 3** Use the cursor to hover over the iKVM subgraphic and a corresponding text hint or screen tip is displayed. The text hint provides additional information on that iKVM.
 - 4** The iKVM subgraphic is hyperlinked to the corresponding CMC GUI page to provide immediate navigation to the **iKVM Status** page.

For more information about iKVM, see "Using the iKVM Module."

To view the status of the iKVM using the **iKVM Status** page:

- 1** Log in to the CMC Web interface.
- 2** Select **iKVM** in the system tree. The **iKVM Status** page displays.

Table 10-5. iKVM Status Information

Item	Description
Presence	Displays whether the iKVM module is Present or Absent .
Power State	Displays the power status of the iKVM: On , Off , or N/A (Absent) .
Name	Displays the product name of the iKVM.
Manufacturer	Displays in the manufacturer of the iKVM.
Part Number	Displays the part number for the iKVM. The part number is a unique identifier provided by the vendor.
Firmware Version	Displays the firmware version of the iKVM.
Hardware Version	Displays the hardware version of the iKVM.
Front Panel Connected	Displays whether the monitor is connected to the front panel VGA connector (Yes or No). This information is provided to CMC so it can determine whether a local user has front-panel access to the chassis.

Table 10-5. iKVM Status Information (continued)

Item	Description
Rear Panel Connected	Indicates whether the monitor is connected to the rear panel VGA connector (Yes or No). This information is provided to CMC so it can determine whether a local user has rear-panel access to the chassis.
Tiering Port Connected	The iKVM supports seamless tiering with external KVM appliances from Dell and Avocent using built-in hardware. When the iKVM is tiered, the servers in the chassis can be accessed through the screen display of the external KVM switch from which the iKVM is tiered.
Front Panel USB/Video Enabled	Displays whether the front panel VGA connector is enabled (Yes or No).
Allow access to CMC from iKVM	Indicates whether the CMC command console through iKVM is enabled (Yes or No).

Updating the iKVM Firmware

You can update the iKVM firmware using the CMC Web interface or RACADM.

To update the iKVM firmware using the CMC Web interface:

- 1** Log in to the CMC Web interface.
- 2** Click **Chassis** in the system tree.
- 3** Click the **Update** tab. The **Updatable Components** page displays.
- 4** Click the iKVM name. The **Firmware Update** page appears.
- 5** In the **Firmware Image** field, enter the path to the firmware image file on your management station or shared network, or click **Browse** to navigate to the file location.



NOTE: The default iKVM firmware image name is **ikvm.bin**; however, the iKVM firmware image name can be changed by the user.

- 6** Click **Begin Firmware Update**. A dialog box prompts you to confirm the action.
- 7** 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 can vary greatly

based on connection speed. When the internal update process begins, the page automatically refreshes and the Firmware update timer displays. Additional instructions to follow:

- Do not use the **Refresh** button 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.
- Update status displays in the **Update State** field; this field is automatically updated during the file transfer process. Certain older browsers do not support these automatic updates. To manually refresh the **Update State** field, click **Refresh**.



NOTE: The update may take up to one minute for the iKVM.

When the update is complete, iKVM resets and the new firmware is updated and displayed on the **Updatable Components** page.

To update the iKVM firmware using RACADM, open a serial/Telnet/SSH text console to CMC, log in, and type:

```
racadm fwupdate -g -u -a <TFTP server IP address or FQDN> -d <filepath/filename> -m kvm
```

For example:

```
racadm fwupdate -gua 192.168.0.10 -d ikvm.bin -m kvm
```

For more information about the **fwupdate** subcommand, see the **fwupdate** command section in the *Command Line Reference Guide for iDRAC6 and CMC*.

Troubleshooting



NOTE: 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.

Table 10-6. Troubleshooting iKVM

Problem	Likely Cause and Solution
The message "User has been disabled by CMC control" appears on the monitor connected to the front panel.	<p>The front panel connection has been disabled by CMC.</p> <p>You can enable the front panel using either the CMC Web interface or RACADM.</p> <p>To enable the front panel using the Web interface:</p> <ol style="list-style-type: none">1 Log in to the CMC Web interface.2 Select iKVM in the system tree.3 Click the Setup tab.4 Select the Front Panel USB/Video Enabled check box.5 Click Apply to save the setting. <p>To enable the front panel using RACADM, open a serial/Telnet/SSH text console to CMC, log in, and type:</p> <pre>racadm config -g cfgKVMInfo -o cfgKVMAccessToCMCEnable 1</pre>
The rear panel access does not work.	<p>The front panel setting is enabled by CMC, and a monitor is currently connected to the front panel.</p> <p>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."</p>

Table 10-6. Troubleshooting iKVM (continued)

Problem	Likely Cause and Solution
The message "User has been disabled as another appliance is currently tiered" appears on the monitor connected to the rear panel.	<p>A network cable is connected to the iKVM ACI port connector and to a secondary KVM appliance.</p> <p>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.</p>
The iKVM's amber LED is blinking.	<p>There are three possible causes:</p> <p>There is problem with the iKVM, for which the iKVM requires reprogramming. To fix the problem, follow the instructions for updating iKVM firmware (see "Updating the iKVM Firmware").</p> <p>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.</p> <p>The iKVM firmware has detected a hardware error. For additional information, view the iKVM status.</p> <p>To view iKVM status using the Web interface:</p> <ol style="list-style-type: none">1 Log in to the CMC Web interface.2 Select iKVM in the system tree. <p>To view iKVM status using RACADM, open a serial/Telnet/SSH text console to CMC, log in, and type:</p> <pre>racadm getkvminfo</pre>

Table 10-6. Troubleshooting iKVM (continued)

Problem	Likely Cause and Solution
My 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: <ol style="list-style-type: none">1 Log in to the CMC Web interface.2 Select iKVM in the system tree.3 Click the Setup tab.4 Clear (un-check) the Front Panel USB/Video Enabled check box.5 Click Apply to save the setting. To disable the front panel using RACADM, open a serial/Telnet/SSH text console to CMC, log in, and type: <pre>racadm config -g cfgKVMInfo -o cfgKVMFrontPanelEnable 0</pre>

Table 10-6. Troubleshooting iKVM (continued)

Problem	Likely Cause and Solution
In the OSCAR menu, the Dell CMC connection is displaying a red X, and I cannot connect to CMC.	<p>There are two possible causes:</p> <p>The Dell CMC console has been disabled. In this case, you can enable it using either the CMC Web interface or RACADM.</p> <p>To enable the Dell CMC console using the Web interface:</p> <ol style="list-style-type: none">1 Log in to the CMC Web interface.2 Select iKVM in the system tree.3 Click the Setup tab.4 Select the Allow access to CMC CLI from iKVM check box.5 Click Apply to save the setting. <p>To enable the Dell CMC connection using RACADM, open a serial/Telnet/SSH text console to CMC, log in, and type:</p> <pre>racadm config -g cfgKVMInfo -o cfgKVMAccessToCMCEnable 1</pre> <p>CMC is unavailable because it is initializing, switching over to the standby CMC, or reprogramming. In this case, simply wait until CMC finishes initializing.</p>
The slot name for a server is displayed as "Initializing" in OSCAR, and I cannot select it.	<p>Either the server is initializing or the iDRAC on that server failed initialization.</p> <p>First, wait 60 seconds. If the server is still initializing, the slot name appears as soon as initialization is complete, and you can select the server.</p> <p>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 re-initialize.</p>

I/O Fabric Management

The chassis can hold up to six I/O modules (IOMs), each of which can be pass-through or switch modules.

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 3 discrete data paths by letter: A, B and C. These paths are described as “FABRICS” and support Ethernet, Fibre Channel or InfiniBand. These discrete fabric paths are split into 2 IO “Banks”, bank one and two. Each server IO adapter (Mezzanine Card or LOM) can have either 2 or 4 ports depending on capability. These ports are split out evenly to IOM banks one and two to allow for redundancy. When you deploy your Ethernet, iSCSI or FibreChannel networks, span their redundant links across banks one and two for maximum availability. We denote the discrete IOM with the fabric Identifier and the Bank number.

Example: “A1” denotes Fabric “A” in bank “1”. “C2” Denotes Fabric “C” in 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 (mezzanine card)** slot in each server module.
- For **Group C**, the IOM slots are permanently connected to the **second MC (mezzanine card)** in each server module.



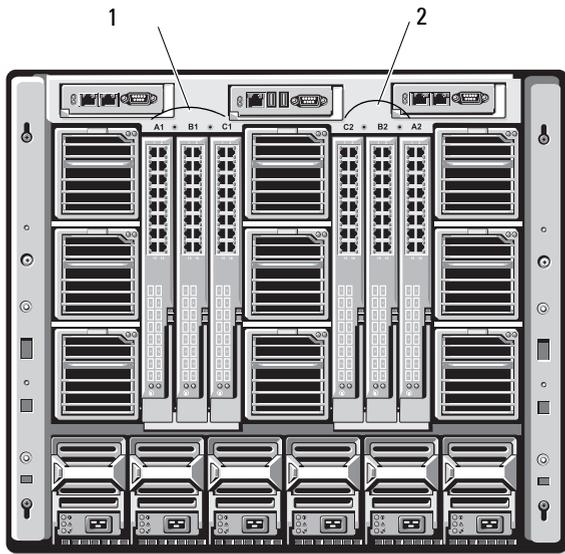
NOTE: In the CMC CLI, IOMs are referred to by the convention, switch-*n*. A1=switch-1, A2=switch-2, B1=switch-3, B2=switch-4, C1=switch-5, and C2=switch-6.

Fabric Management

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 could cause electric or functional problems to the chassis or its components. Fabric management prevents invalid configurations from powering on.

Figure 11-1 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 11-1. 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.



NOTE: 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 servers's fabric type is different from the existing IOM fabric
- 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
- Invalid IOM-IOM configuration, where a newly installed IOM has a different or incompatible fabric type from an IOM already installed in its group

Invalid Mezzanine Card (MC) Configuration

An invalid MC configuration occurs when a single server's LOM or MC is not supported by its corresponding IOM. In this case, all the other servers in the chassis can be running, but the server with the mismatched MC card does not be allowed to power on. The power button on the server flashes Amber to alert a fabric mismatch. For information about CMC and hardware logs, see "Viewing the Event Logs" on page 398.

Invalid IOM-Mezzanine Card (MC) Configuration

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. For information about CMC and hardware logs, see "Viewing the Event Logs" on page 398.

Invalid IOM-IOM Configuration

CMC holds the newly installed IOM in powered-off state, causes the IOM's error LED to blink, and creates entries in CMC and hardware logs about the mismatch. For information about CMC and hardware logs, see "Viewing the Event Logs" on page 398.

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, no verification of their fabric types is 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 as long as 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

The health status for the IOMs can be viewed in two ways: from the **Chassis Graphics** section on the **Chassis Status** page or the **I/O Modules Status** page. The **Chassis Graphics** page provides a graphical overview of the IOMs installed in the chassis.

To view health status of the IOMs using Chassis Graphics:

- 1 Log in to the CMC Web interface.
- 2 The **Chassis Status** page is displayed. The right 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 color of the IOM subgraphic:
 - Green - IOM is present, powered on and communicating with CMC; there is no indication of an adverse condition.
 - Amber - IOM is present, but may or may not be powered on, or may or may not be communicating with CMC; an adverse condition may exist.
 - Gray - IOM is present and not powered on. It is not communicating with CMC and there is no indication of an adverse condition.
- 3 Use the cursor to hover over an individual IOM subgraphic and a corresponding text hint or screen tip is displayed. The text hint provides additional information on that IOM.
- 4 The IOM subgraphic is hyperlinked to the corresponding CMC GUI page to provide immediate navigation to the **I/O Module Status** page associated with that IOM.

To view the health status of all IOMs using the **I/O Modules Status** page:

- 1 Log in to the CMC Web interface.
- 2 Select **I/O Modules** in the **Chassis** menu in the system tree.
- 3 Click the **Properties** tab.

4 Click the **Status** subtab. The **I/O Modules Status** page displays.

Table 11-1. I/O Modules Status Information

Item	Description	
Slot	Displays the location of the I/O module in the chassis by group number (A, B, or C) and Bank (1 or 2). IOM Enumeration: A1, A2, B1, B2, C1, or C2 .	
Present	Displays whether the IOM is present (Yes or No).	
Health	 OK	Indicates that the IOM is present and communicating with CMC. In the event of a communication failure between CMC and the server, CMC cannot obtain or display health status for the IOM.
	 Informational	Displays information about the IOM when no change in health status (OK, Warning, Severe) has occurred.
	 Warning	<p>Indicates that warning alerts have been issued, and corrective action must be taken. If corrective actions are not taken, it could lead to critical or severe failures that can affect the integrity of the IOM.</p> <p>Examples of conditions causing Warnings: IOM fabric mismatch with the server's mezzanine card fabric; invalid IOM configuration, where the newly installed IOM does not match the existing IOM on the same group.</p>
	 Severe	<p>Indicates that at least one Failure alert has been issued. Severe status represents a system failure on the IOM, and corrective action must be taken immediately.</p> <p>Examples of conditions causing Severe status: Failure in IOM detected; IOM was removed.</p>

NOTE: Any change in health is logged to both the hardware and CMC log. For more information, see "Viewing the Event Logs" on page 398.

Table 11-1. I/O Modules Status Information (continued)

Item	Description
Fabric	<p>Displays the type of fabric for the IOM: Gigabit Ethernet, 10GE XAUI, 10GE KR, 10GE XAUI KR, FC 4 Gbps, FC 8 Gbps, SAS 3 Gbps, SAS 6 Gbps, Infiniband SDR, Infiniband DDR, Infiniband QDR, PCIe Bypass Generation 1, PCIe Bypass Generation 2.</p> <p>NOTE: Knowing the fabric types of the IOMs in your chassis is critical in preventing IOM mismatches within the same group. For information about I/O fabric, see "I/O Fabric Management" on page 361.</p>
Name	Displays the IOM product name.
Launch IOM Management Console	<p>If the button is present for a particular I/O module, clicking it launches the IOM management console for that I/O module in a new browser window or tab.</p>  <p>NOTE: This option is only available for the managed switch I/O modules. It is not available for pass-through I/O modules or unmanaged Infiniband switches.</p> <p>NOTE: If an I/O Module is inaccessible because it is powered off, its LAN interface is disabled, or the module has not been assigned a valid IP address, the Launch IOM GUI option is not displayed for that I/O Module.</p> <p>NOTE: You are prompted to log in to I/O module management interface.</p> <p>NOTE: You can configure the I/O module IP address using CMC GUI, as described in "Configuring Network Settings for an Individual IOM" on page 370.</p>
Role	<p>When linking I/O modules together, the Role displays the I/O Module stacking membership. Member means the module is part of a stack set. Master indicates the module is a primary access point.</p>
Power Status	Displays the power status of the IOM: On , Off , or N/A (Absent) .
Service Tag	<p>Displays the service tag for the IOM. The service tag is a unique identifier provided by Dell for support and maintenance.</p> <p>Any change in health is logged to both the hardware and CMC log. For more information, see "Viewing the Event Logs" on page 398.</p> <p>NOTE: Pass-throughs do not have service tags. Only switches have service tags.</p>

Viewing the Health Status of an Individual IOM

The **I/O Module Status** page (separate from the *I/O Modules Status* page) provides an overview of an individual IOM.

To view the health status of an individual IOM:

- 1 Log in to the CMC Web interface.
- 2 Expand **I/O Modules** in the system tree. All of the IOMs (1–6) appear in the expanded **I/O Modules** list.
- 3 Click the IOM you want to view in the **I/O Modules** list in the system tree.
- 4 Click the **Status** subtab. The **I/O Modules Status** page displays.

Table 11-2. I/O Module Health Status Information

Item	Description
Location	Displays the location of the IOM in the chassis by group number (A, B, or C) and slot number (1 or 2). Slot names: A1, A2, B1, B2, C1, or C2.
Name	Displays name of the IOM.
Present	Displays whether the IOM is Present or Absent .
Health	 OK Indicates that the IOM is present and communicating with CMC. In the event of a communication failure between CMC and the server, CMC cannot obtain or display health status for the IOM.
	 Informational Displays information about the IOM when no change in health status (OK, Warning, Severe) has occurred. Examples of conditions causing Informational status: the IOM presence was detected; a user requested IOM power cycle.

Table 11-2. I/O Module Health Status Information (continued)

Item	Description
 Warning	<p>Indicates that warning alerts have been issued, and corrective action must be taken. If corrective actions are not taken, it could lead to critical or severe failures that can affect the integrity of the IOM.</p> <p>Examples of conditions causing Warnings: IOM fabric mismatch with the server's mezzanine card fabric; invalid IOM configuration, where the newly installed IOM does not match the existing IOM on the same group.</p>
 Severe	<p>Indicates that at least one Failure alert has been issued. Severe status represents a system failure on the IOM, and corrective action must be taken immediately.</p> <p>Examples of conditions causing Severe status: Failure in IOM detected; IOM was removed.</p>
<p>NOTE: Any change in health is logged to both the hardware and CMC log. For information on viewing logs, see "Viewing the Hardware Log" on page 398 and "Viewing the CMC Log" on page 400.</p>	
Power Status	Displays the power status of the IOM: On , Off , or N/A (Absent).
Service Tag	Displays the service tag for the IOM. The service tag is a unique identifier provided by Dell for support and maintenance.
Fabric	<p>Displays the type of fabric for the IOM: Gigabit Ethernet, 10GE XAUI, 10GE KR, 10GE XAUI KR, FC 4 Gbps, FC 8 Gbps, SAS 3 Gbps, SAS 6 Gbps, Infiniband SDR, Infiniband DDR, Infiniband QDR, PCIe Bypass Generation 1, PCIe Bypass Generation 2.</p> <p>NOTE: Knowing the fabric types of the IOMs in your chassis is critical in preventing IOM mismatches within the same group. For information about I/O fabric, see "I/O Fabric Management" on page 361.</p>

Table 11-2. I/O Module Health Status Information (continued)

Item	Description
MAC Address	Displays the MAC address for the IOM. The MAC address is a unique address assigned to a device by the hardware vendor as a means for identification. NOTE: Pass-throughs do not have MAC addresses. Only switches have MAC addresses.
Role	Displays the I/O module stacking membership when modules are linked together: <ul style="list-style-type: none"><li data-bbox="322 523 751 547">• Member - the module is part of a stack set<li data-bbox="322 563 785 587">• Master - the module is a primary access point.

Configuring Network Settings for an Individual IOM

The I/O Modules Setup page allows you to specify the network settings for the interface used to manage the IOM. For Ethernet switches, the out-of-band management port (IP address) is what is configured. The in-band management port (that is, VLAN1) is not configured using this interface.



NOTE: To change settings on the I/O Modules Configuration page, you must have Fabric A Administrator privileges to configure IOMs in Group A; Fabric B Administrator privileges to configure IOMs in Group B; or 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. Refer to the IOM documentation for the default in-band management IP address.



NOTE: Only those IOMs present in the chassis are displayed.



NOTE: Do not configure I/O module network settings for Ethernet pass-through and Infiniband switches.

To configure the network settings for an individual IOM:

- 1 Log in to the CMC Web interface.
- 2 Click **I/O Modules** in the system tree. Click the **Setup** subtab. The **Configure I/O Modules Network Settings** page displays.
- 3 To configure network settings for I/O modules, type/select values for the following properties, and then click **Apply**.



NOTE: Only IOMs that are powered on can be configured.



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.

Table 11-3. Configure I/O Module Network Settings

Item	Description
Slot	Displays the location of the IOM in the chassis by group number (A, B, or C) and slot number (1 or 2). Slot names: A1, A2, B1, B2, C1, or C2. (The Slot value cannot be changed.)
Name	Displays the IOM product name. (The IOM name cannot be changed.)
Power State	Displays the Power State of the IOM. (The Power State cannot be changed from this page.)

Table 11-3. Configure I/O Module Network Settings (continued)

Item	Description
DHCP Enabled	<p data-bbox="292 280 958 363">Enables the IOM on the chassis to request and obtain an IP address from the Dynamic Host Configuration Protocol (DHCP) server automatically.</p> <p data-bbox="292 379 575 403">Default: Checked (enabled).</p> <p data-bbox="292 419 896 502">If this option is checked, the IOM retrieves IP configuration (IP address, subnet mask, and gateway) automatically from a DHCP server on your network.</p> <p data-bbox="292 518 913 632">NOTE: When this feature is enabled, the IP Address, Gateway, and Subnet Mask property fields (located immediately adjacent following this option) are inactivated, and any previously entered values for these properties are ignored.</p> <p data-bbox="292 647 919 730">If this option is not checked, you must manually enter a valid IP address, gateway, and subnet mask in the corresponding text fields immediately following this option.</p>
IP Address	Specifies the IP address for the IOM network interface.
Subnet Mask	Specifies the subnet mask for the IOM network interface.
Gateway	Specifies the gateway for the IOM network interface.

Troubleshooting IOM Network Settings

The following list contains troubleshooting items for IOM network settings:

- CMC can read the IP address setting too quickly after a configuration change; it displays 0.0.0.0 after clicking **Apply**. You must hit the refresh button in order 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, refer to the *Dell PowerConnect M6220 Switch Important Information* document and the *Dell PowerConnect 6220 Series Port Aggregator White Paper*.

Troubleshooting and Recovery

Overview

This section explains how to perform tasks related to recovering and troubleshooting problems on the remote system using the CMC Web interface.

- Gathering Configuration information, error status and error logs.
- Managing power on a remote system.
- Viewing chassis information.
- Viewing the event logs.
- Using the Diagnostic Console.
- Reset Components.
- Troubleshooting Network Time Protocol (NTP) problems.
- Troubleshooting network problems.
- Troubleshooting alerting problems.
- Resetting forgotten administrator password.
- Error codes and logs.

Chassis Monitoring Tools

Gathering Configuration information and Chassis Status and Logs

The `racdump` subcommand provides a single command to get comprehensive chassis status, configuration state information, and the historic event logs.

Usage

```
racadm racdump
```

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 command can be run remotely from the serial, Telnet, or SSH console command prompt or through a normal command prompt.

To list syntax and command-line options for RACDUMP subcommands, type:

```
racadm help <racdump>
```

CLI RACDUMP

Racdump includes the following subsystems and aggregates the following RACADM commands:

Table 12-1. Subsystems and RACADM Commands

Subsystem	RACADM Command
General System/RAC information	getsysinfo
Session information	getssinfo
Sensor information	getsensorinfo
Switches information (IO Module)	getioinfo

Table 12-1. Subsystems and RACADM Commands

Subsystem	RACADM Command
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

Usage

```
racadm racdump
```

Remote RACDUMP

Remote RACADM is a client side utility, which can be executed from a management station through the out of band network interface. A remote capability option (-r) is provided that allows you to connect to the managed system and execute RACADM subcommands from a remote console or management station. To use the remote capability, you need a valid user name (-u option) and password (-p option), and CMC IP address.



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

- racadm getconfig -f <file name>
- racadm sslcertdownload -t <type> [-f <filename>]

Remote RACDUMP Usage

To use the RACDUMP subcommand remotely, type the following commands:

```
racadm -r <CMC IP address> -u <username> -p <password>
```

<subcommand> <subcommand options>

```
racadm -i -r <CMC IP address> <subcommand> <subcommand options>
```

 **NOTE:** The `-i` option instructs RACADM to interactively prompt for user name and password. Without the `-i` option, you must provide the user name and password in the command using the `-u` and `-p` options.

For example:

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

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

```
racadm -r <CMC IP address>:<port> -u <username> -p
<password> <subcommand> <subcommand options>
racadm -i -r <CMC IP address>:<port> <subcommand>
<subcommand options>
```

Telnet RACDUMP

SSH/Telnet RACDUMP is used to refer to the RACDUMP command usage from a SSH or Telnet prompt.

For more information on RACDUMP instruction see the section "Using the RACADM Command Line Interface" on page 69 and the "CMC Administrators Reference Guide."

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.

Using the Web Interface

To enable blinking for one, multiple, or all component LEDs:

- 1 Log in to the CMC Web interface.
- 2 Click **Chassis** in the system tree.
- 3 Click the **Troubleshooting** tab.
- 4 Click the **Identify** subtab. The **Identify** page displays, featuring a list of all components on the chassis.
- 5 To enable blinking for a component LED, check the box beside the device name and then click **Blink**.
- 6 To disable blinking for a component LED, check the box beside the device name and then click **UnBlink**.

Using RACADM

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

```
racadm settled -m <module> [-1 <ledState>]
```

where *<module>* specifies the module whose LED you want to configure.

Configuration options:

- *server-n* where *n*=1-16
- *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 SNMP Alerts

Simple network management protocol (SNMP) traps, or *event traps*, are similar to e-mail event alerts. They are used by a management station to receive unsolicited data from CMC.

You can configure CMC to generate event traps. Table 12-2 provides an overview of the events that trigger SNMP and e-mail alerts. For information on e-mail alerts, see "Configuring E-mail Alerts" on page 385.

 **NOTE:** Starting with CMC version 2.10, SNMP is now IPv6 enabled. You can include an IPv6 address or fully qualified domain name (FQDN) in the destination for an event alert.

Table 12-2. Chassis Events That Can Generate SNMP and Email Alerts

Event	Description
Fan Probe Failure	A fan is running too slow or not at all.
Battery Probe Warning	A battery has stopped functioning.
Temperature Probe Warning	The temperature is approaching excessively high or low limits.
Temperature Probe Failure	The temperature is either too high or too low for proper operation.
Redundancy Degraded	Redundancy for the fans and/or power supplies has been reduced.
Redundancy Lost	No redundancy remains for the fans and/or power supplies.
Power Supply Warning	The power supply is approaching a failure condition.
Power Supply Failure	The power supply has failed.
Power Supply Absent	An expected power supply is not present.
Hardware Log Failure	The hardware log is not functioning.
Hardware Log Warning	The hardware log is almost full.
Server Absent	An expected server is not present.
Server Failure	The server is not functioning.
KVM Absent	An expected KVM is not present.
KVM Failure	The KVM is not functioning.

Table 12-2. Chassis Events That Can Generate SNMP and Email Alerts (continued)

Event	Description
IOM Absent	An expected IOM is not present.
IOM Failure	The IOM is not functioning.
Firmware Version Mismatch	There is a firmware mismatch for the chassis or server firmware.
Chassis Power Threshold Error	Power consumption within the chassis reached the System Input Power Cap.
SDCARD Absent	There is no media in the CMC's Secure Digital (SD) card slot, and a configured CMC feature requires it.
SDCARD Error	An error occurred while accessing the media in the CMC's Secure Digital (SD) card slot.

You can add and configure SNMP alerts using the Web interface or RACADM.

Using the Web Interface



NOTE: To add or configure SNMP alerts, you must have **Chassis Configuration Administrator** privilege.



NOTE: 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, click User ID 1 to open the **User Configuration** page. Help for that page is available through the **Help** link at the top right corner of the page.

- 1 Log in to the CMC Web interface.
- 2 Select **Chassis** in the system tree.
- 3 Click the **Alerts** tab. The **Chassis Events** page appears.
- 4 Enable alerting:
 - a Select the check boxes of the events for which you want to enable alerting. To enable all events for alerting, select the **Select All** check box.
 - b Click **Apply** to save your settings.
- 5 Click the **Traps Settings** subtab. The **Chassis Event Alert Destinations** page displays.

- 6 Type a valid address in an empty **Destination** field.



NOTE: A valid address is an address that receives the trap alerts. 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

- 7 Type the **SNMP Community String** to which the destination management station belongs.



NOTE: The community string on the **Chassis Event Alert Destinations** page 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.

- 8 Click **Apply** to save your changes.

To test an event trap for an alert destination:

- 1 Log in to the CMC Web interface.
- 2 Select **Chassis** in the system tree.
- 3 Click the **Alerts** tab. The **Chassis Events** page displays.
- 4 Click the **Traps Settings** tab. The **Chassis Event Alert Destinations** page displays.
- 5 Click **Send** in the **Test Trap** column beside the destination.



NOTE: Specify trap destinations as appropriately-formatted numeric addresses (IPv6 or IPv4), or Fully-qualified domain names (FQDNs). Choose a format that is consistent with your networking technology/infrastructure. The **Test Trap** functionality is unable to detect improper choices based on current network configuration (e.g. use of an IPv6 destination in an IPv4-only environment).

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 may skip step 2 if you have already selected filter mask.

- 2 Enable alerting by typing:

```
racadm config -g cfgAlerting -o cfgAlertingEnable 1
```

- 3 Specify the events for which you want CMC to generate by typing:

```
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, etc.) 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 12-3. 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

Table 12-3. Event Traps Filter Masks (continued)

Event	Filter Mask Value
IOM Failure	0x200000
Firmware Version Mismatch	0x00400000
Chassis Power Threshold Error	0x01000000
SDCARD Absent	0x02000000
SDCARD Error	0x04000000
Chassis Group Error	0x8000000

4 Enable traps alerting by typing:

```
racadm config -g cfgTraps -o cfgTrapsEnable 1 -i <index>
```

where *<index>* is a value 1–4. The index number is used by CMC 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 by typing:

```
racadm config -g cfgTraps -o  
cfgTrapsAlertDestIPAddr <IP address> -i <index>
```

where *<IP address>* is a valid destination, and *<index>* is the index value you specified in step 4.

6 Specify the community name by typing:

```
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 you 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 you specify (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.

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 unsure of the index number, type:

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

Configuring E-mail Alerts

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.

Table 12-2 provides an overview of the events that trigger e-mail and SNMP alerts. For information on SNMP alerts, see "Configuring SNMP Alerts" on page 379.

You can add and configure e-mail alerts using the Web interface or RACADM.

Using the Web Interface

 **NOTE:** To add or configure e-mail alerts, you must have **Chassis Configuration Administrator** privilege.

- 1 Log in to the CMC Web interface.
- 2 Select **Chassis** in the system tree.
- 3 Click the **Alerts** tab. The **Chassis Events** page appears.
- 4 Enable alerting:
 - a Select the check boxes of the events for which you want to enable alerting. To enable all events for alerting, select the **Select All** check box.
 - b Click **Apply** to save your settings.

- 5 Click the **Email Alert Settings** subtab. The **Email Alert Destinations** page displays.
- 6 Specify the SMTP server IP address:
 - a Locate the **SMTP (Email) Server** field, and then type the SMTP hostname or IP address.
 **NOTE:** You must configure the SMTP e-mail server to accept relayed emails from the CMC's IP address, a feature which is normally turned off in most mail servers due to security concerns. For instructions as to how to accomplish this in a secure manner, refer to the documentation that came with your SMTP server.
 - b Enter the desired originator e-mail for the alert, or leave it blank to use the default e-mail originator. The default is `cmc@<IP_address>` where `<IP_address>` is the IP address of CMC. To enter a value, the syntax of the e-mail name is `<emailname>[@<domain>]`, and an e-mail domain can be optionally specified.
If `@<domain>` is not specified and there is an active CMC network domain, then the e-mail address of `<emailname>@<cmc_domain>` is used as the source e-mail. If `@<domain>` is not specified and CMC has no active network domain, then the IP address of CMC is used (for example, `<emailname>@<IP_address>`).
 - c Click **Apply** to save your changes.
- 7 Specify the e-mail address(es) that receive the alerts:
 - a Type a valid e-mail address in an empty **Destination Email Address** field.
 - b Enter an optional **Name**. This is the name of the entity receiving the e-mail. If a name is entered for an invalid e-mail address, it is ignored.
 - c Click **Apply** to save your settings.

To send a test e-mail to an e-mail alert destination:

- 1 Log in to the CMC Web interface.
- 2 Select **Chassis** in the system tree.
- 3 Click the **Alerts** tab. The **Chassis Events** page appears.
- 4 Click the **Email Alert Settings** subtab. The **Email Alert Destinations** page displays.
- 5 Click **Send** in the **Destination Email Address** column beside the destination.

Using RACADM

- 1 Open a serial/Telnet/SSH text console to CMC and log in.
- 2 Enable alerting by typing:

```
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 you want CMC to generate by typing:

```
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 12-3 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 on "Using RACADM" on page 382.

- 4 Enable e-mail alerting by typing:

```
racadm config -g cfgEmailAlert -o  
cfgEmailAlertEnable 1 -i <index>
```

where *<index>* is a value 1–4. The index number is used by CMC to distinguish up to four configurable destination e-mail addresses.

- 5 Specify a destination e-mail address to receive the e-mail alerts by typing:

```
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 party receiving the e-mail alert by typing:

```
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 you 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 by configuring the `cfgRhostsSmtpServerIpAddr` database property by typing:

```
racadm config -g cfgRemoteHosts -o
cfgRhostsSmtpServerIpAddr host.domain
```

where `host.domain` is a full-qualified domain name.

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: **racadm getconfig -g cfgEmailAlert -i <index>**. If the index is configured, values appear for the `cfgEmailAlertAddress` and `cfgEmailAlertEmailName` objects.

First Steps to Troubleshooting a Remote System

The following questions are commonly used to troubleshoot high-level problems in the managed system:

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

Monitoring Power and Executing Power Control Commands on the Chassis

You can use the Web interface or RACADM to:

- View the system's current power status.
- Perform an orderly shutdown through the operating system when rebooting, and power the system on or off.

For information about power management on CMC and configuring power budget, redundancy, and power control, see "Power Management" on page 289.

Viewing Power Budget Status

For instructions on viewing power budget status for the chassis, servers, and PSUs using either the Web interface or RACADM, see "Viewing Power Consumption Status" on page 311.

Executing a Power Control Operation

For instructions on powering on, powering off, resetting, or power-cycling the system using the CMC Web interface or RACADM, see "Executing Power Control Operations on the Chassis" on page 327, "Executing Power Control Operations on an IOM" on page 329, and "Executing Power Control Operations on a Server" on page 330.

Power Troubleshooting

Use the items below to assist in troubleshooting 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 max 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.

Viewing Chassis Summaries

CMC provides rollup overviews of the chassis, active and standby CMCs, iKVM, fans, temperature sensors, and I/O modules (IOMs).

Using the Web Interface

To view summaries of the chassis, CMCs, iKVM, and IOMs:

- 1 Log in to the CMC Web interface.
- 2 Select **Chassis** in the system tree.
- 3 Click the **Summary** tab. The **Chassis Summary** page displays.

Table 12-4, Table 12-5, Table 12-6, and Table 12-7 describe the information displayed on the **Chassis Summary** page.

Table 12-4. Chassis Summary

Item	Description
Name	Displays the name of the chassis. The name identifies the chassis on the network. For information on setting the name of the chassis, see "Editing Slot Names" on page 124.
Model	Displays the chassis model or manufacturer. For example, PowerEdge 2900.
Service Tag	Displays the service tag of the chassis. The service tag is a unique identifier provided by the manufacturer for support and maintenance.
Asset Tag	Displays the asset tag of the chassis.
Location	Displays the location of the chassis.
CMC Failover Ready	Displays (Yes , No) whether the standby CMC (if present) is capable of taking over in the event of a failover condition.
System Power Status	Displays the system power status.

Table 12-5. CMC Summary

Item	Description
Active CMC Information	
Name	Displays the name of CMC. For example, Active CMC or Standby CMC.
Description	Provides a brief description of the purpose of CMC.
Date/Time	Displays the date and time set on the active CMC.
Active CMC Location	Displays the slot location of the active CMC.
Redundancy Mode	Displays if the standby CMC is present in the chassis.
Primary Firmware Version	Displays the firmware version of the active CMC.
Firmware Last Updated	Displays when the firmware was last updated. If no updates have occurred, this property displays as N/A.
Hardware Version	Displays the hardware version of the active CMC.

Table 12-5. CMC Summary (continued)

Item	Description
MAC Address	Displays the MAC address for the CMC Network Interface. The MAC address is a unique identifier for CMC over the network.
IP Address	Displays the IP address of the CMC Network Interface.
Gateway	Displays the gateway of the CMC Network Interface.
Subnet Mask	Displays the subnet mask of the CMC Network Interface.
Use DHCP (for Network Interface IP Address)	Displays whether CMC is enabled to request and obtain automatically an IP address from the Dynamic Host Configuration Protocol (DHCP) server (Yes or No). The default setting for this property is No.
Primary DNS Server	Displays the primary DNS server name.
Alternate DNS Server	Displays the alternate DNS server name.
Use DHCP for DNS Domain Name	Displays use of DHCP to acquire the DNS Domain name (Yes, No).
DNS Domain Name	Displays the DNS Domain name.

Table 12-5. CMC Summary (continued)

Item	Description
Standby CMC Information	
Present	Displays (Yes , No) whether a second (standby) CMC is installed.
Standby Firmware Version	Displays the CMC firmware version installed on the standby CMC.

Table 12-6. iKVM Summary

Item	Description
Present	Displays whether the iKVM module is present (Yes or No).
Name	Displays the name of the iKVM. The name identifies the iKVM on the network.
Manufacturer	Displays the iKVM model or manufacturer.
Part Number	Displays the part number for the iKVM. The part number is a unique identifier provided by the vendor. Part number naming conventions differ from vendor to vendor.
Firmware Version	Displays the firmware version of the iKVM.
Hardware Version	Displays the hardware version of the iKVM.
Power Status	Displays the power status of the iKVM: On , Off , N/A (Absent).
Front Panel USB/Video Enabled	Displays whether the front panel VGA and USB connectors are enabled (Yes or No).
Allow Access to CMC CLI from iKVM	Displays that CLI access is enabled on the iKVM (Yes or No).

Table 12-7. IOM Summary

Item	Description
Location	Displays the slot occupied by the IOMs. Six slots are identified by group name (A, B, or C) and slot number (1 or 2). Slot names: A-1, A-2, B-1, B-2, C-1, or C-2.
Present	Displays whether the IOM is present (Yes or No).
Name	Displays the name of the IOM.
Fabric	Displays the type of fabric.
Power Status	Displays the power status of the IOM: On , Off , or N/A (Absent).
Service Tag	Displays the service tag of the IOM. The service tag a unique identifier provided by the manufacturer for support and maintenance.

Using RACADM

- 1 Open a serial/Telnet/SSH text console to CMC and log in.
- 2 To view chassis and CMC summaries, type:
`racadm getsysinfo`
- 3 To view the iKVM summary, type:
`racadm getkvminfo`
- 4 To view the IOM summary, type:
`racadm getioinfo`

Viewing Chassis and Component Health Status

Using the Web Interface

To view chassis and component health summaries:

- 1 Log in to the CMC Web interface.
- 2 Select **Chassis** in the system tree. The **Chassis Health** page displays.

The **Chassis Graphics** section provides a graphical view of the front and rear of the chassis. This graphical representation provides a visual overview of the components installed within the chassis and its corresponding status.

Each graphic displays a real-time representation of the installed components. The component state is indicated by the overlay of the component subgraphic.

- No overlay - the component is present, powered on and communicating with CMC; there is no indication of an adverse condition.
- Amber caution sign - indicates that only warning alerts have been issued and that corrective action must be taken.
- Red X - indicates at least one failure condition is present. This means that CMC can still communicate with the component and that the health status is reported as critical.
- Grayed Out - indicates that the component is present and not powered on. It is not communicating with CMC and there is no indication of an adverse condition.

All components display a corresponding text hint or screen tip when the mouse is placed over the component subgraphic. Component status is dynamically updated, and the component subgraphic colors and text hints are automatically changed to reflect the current state.

Clicking on the component subgraphic selects that component's information and **Quick Links** for display below the chassis graphics.

The CMC Hardware Log section provides the latest 10 entries of the CMC Hardware Log for reference (see [Viewing the Hardware Log](#)).

Using RACADM

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

```
racadm getmodinfo
```

Viewing the Event Logs

The **Hardware Log** and **CMC Log** pages display system-critical events that occur on the managed system.

Viewing the 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 SNMP Alerts" on page 379 and "Configuring E-mail Alerts" on page 385.

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
```

Using the Web Interface

You can view, save a text file version of, and clear the hardware log in the CMC Web interface.

Table 12-8 provides descriptions of the information provided on the **Hardware Log** page in the CMC Web interface.

To view the hardware log:

- 1 Log in to the CMC Web interface.
- 2 Click **Chassis** in the system tree.
- 3 Click the **Logs** tab.
- 4 Click the **Hardware Log** subtab. The **Hardware Log** page displays.

To save a copy of the hardware log to your managed station or network:

- 1 Click **Save Log**.

A dialog box opens.

- 2 Select a location for a text file of the log.



NOTE: Because 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.

Table 12-8. Hardware Log Information

Item	Description
Severity	 OK Indicates a normal event that does not require corrective actions.
	 Informational Indicates an informational entry on an event in which the Severity status has not changed.
	 Unknown Indicates a noncritical event for which corrective actions should be taken soon to avoid system failures.
	 Warning Indicates a critical event requiring immediate corrective actions to avoid system failures.
	 Severe Indicates a critical event that requires immediate corrective actions to avoid system failures.

Table 12-8. Hardware Log Information (continued)

Item	Description
Date/Time	Displays the exact date and time the event occurred (for example, Wed May 02 16:26:55 2007). If no date/time appears, then the event occurred at System Boot.
Description	Provides a brief description, generated by CMC, of the event (for example, Redundancy lost, Server inserted).

Using RACADM

- 1 Open a serial/Telnet/SSH text console to CMC and log in.
- 2 To view the hardware log, type:

```
racadm getsel
```


To clear the hardware log, type:

```
racadm clrsel
```

Viewing the CMC Log

CMC generates a log of chassis-related events.



NOTE: To clear the hardware log, you must have **Clear Logs Administrator** privilege.

Using the Web Interface

You can view, save a text file version of, and clear the CMC log in the CMC Web interface.

You can re-sort the log entries by Source, Date/Time, or Description by clicking the column heading. Subsequent clicks on the column headings reverse the sort.

Table 12-9 provides descriptions of the information provided on the **CMC Log** page in the CMC Web interface.

To view the CMC log:

- 1 Log in to the CMC Web interface.
- 2 Click **Chassis** in the system tree.
- 3 Click the **Logs** tab.

- 4 Click the **CMC Log** subtab. The **CMC Log** page displays.
- 5 To save a copy of the CMC log to your managed station or network, click **Save Log**.

A dialog box opens; select a location for a text file of the log.

Table 12-9. CMC Log Information

Command	Result
Source	Displays the interface (such as CMC) that caused the event.
Date/Time	Displays the exact date and time the event occurred (for example, Wed May 02 16:26:55 2007).
Description	Provides a short description of the action, such as a login or a logout, login failure, or clearing the logs. Descriptions are generated by CMC.

Using RACADM

- 1 Open a serial/Telnet/SSH text console to CMC and log in.
- 2 To view the hardware log, type:


```
racadm getraclog
```

 To clear the hardware log, type:


```
racadm clrraclog
```

Using the Diagnostic Console

The **Diagnostic Console** page enables an advanced user, or a user under the direction of technical support, to diagnose issues related to the chassis hardware using CLI commands.



NOTE: To modify these settings, you must have **Debug Command Administrator** privilege.

To access the **Diagnostic Console** page:

- 1 Log in to the CMC Web interface.
- 2 Click **Chassis** in the system tree.
- 3 Click the **Troubleshooting** tab.
- 4 Click the **Diagnostics** subtab. The **Diagnostic Console** page displays.

To execute a diagnostic CLI command, type the command into the **Enter RACADM Command** field, and then click **Submit** to execute the diagnostic command. A diagnostic results page appears.

To return to the **Diagnostic Console** page, click **Go Back to Diagnostic Console Page** or **Refresh**.

The Diagnostic Console supports the commands listed in Table 12-10 as well as the RACADM commands.

Table 12-10. Supported Diagnostic Commands

Command	Result
arp	Displays the contents of the address resolution protocol (ARP) table. ARP entries may not be added or deleted.
ifconfig	Displays the contents of the network interface table.
netstat	Prints the contents of the routing table.
ping <IP address>	Verifies that the destination <IP address> is reachable from CMC with the current routing-table contents. You must type a destination IP address in the field to the right of this option. An Internet control message protocol (ICMP) echo packet is sent to the destination IP address based on the current routing-table contents.
gettracelog	Displays the trace log (may take a few seconds to display the log). The gettracelog -i command returns the number of records in the trace log. NOTE: For more information about the gettracelog command, see the gettracelog command section in the <i>Command Line Reference Guide for iDRAC6 and CMC</i> .

Resetting Components

The **Reset Components** page allows users to reset the active CMC, or to virtually reseal 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 access the **Diagnostic Console** page:

- 1 Log in to the CMC Web interface.
- 2 Click **Chassis** in the system tree.
- 3 Click the **Troubleshooting** tab.
- 4 Click the **Reset Components** subtab. The **Reset Components** page displays. The **CMC Summary** section of the **Reset Components** page displays the following information:

Table 12-11. CMC Summary

Attribute	Description
Health	 OK CMC is present and communicating with its components.
	 Informational Displays information about CMC when no change in health status (OK, Warning, Severe) has occurred.
	 Warning Warning alerts have been issued, and corrective action must be taken . If corrective actions are not taken, critical or severe failures that can affect the integrity of CMC can occur.
	 Severe At least one failure alert has been issued. Severe status represents a CMC system failure, and corrective action must be taken immediately .
Date/Time	Displays the date and time for the CMC using the format <i>MM/DD/YYYY</i> , where <i>MM</i> is the month, <i>DD</i> is the date, and <i>YYYY</i> is the year.
Active CMC Location	Displays the location of the active CMC.
Redundancy Mode	Displays Redundant if a standby CMC is present in the chassis, and No Redundancy if no standby CMC is present in the chassis.

5 The **Virtual Reset Server** section of the **Reset Components** page displays the following information:

Table 12-12. Virtual Reset Server

Attribute	Description	
Slot	Displays the slot occupied by the server in the chassis. Slot names are sequential IDs, from 1 to 16, to help identify the location of the server in the chassis.	
Name	Displays the name of the server in each slot.	
Present	Displays whether the server is present in the slot (Yes or No).	
Health		OK The server is present and communicating with CMC. In the event of a communication failure between CMC and the server, the CMC cannot obtain or display health status for the server.
		Informational Displays information about the server when there is no change in health status (OK, Warning, Severe).
		Warning Warning alerts have been issued, and corrective action must be taken . If corrective actions are not taken, critical or severe failures that can affect the integrity of the server can occur.
		Severe At least one failure alert has been issued. Severe status represents a CMC system failure, and corrective action must be taken immediately .

Table 12-12. Virtual Reseat Server

Attribute	Description
iDRAC Status	<p>Displays the status of the server iDRAC embedded management controller:</p> <ul style="list-style-type: none">• N/A - Server is not present, or the chassis is not powered on.• Ready - iDRAC is ready and operating normally.• Corrupted - iDRAC firmware is corrupted. Use the iDRAC firmware update utility to repair the firmware.• Failed - Unable to communicate with iDRAC. Use the Virtual Reseat check box to clear the error. If this fails, manually remove and replace the server to clear the error.• FW Update - iDRAC firmware update in progress; allow the update to complete before attempting any action.• Initializing - iDRAC reset in progress; wait for the controller to complete powering-on before attempting any action.
Power State	<p>Displays the server power status:</p> <ul style="list-style-type: none">• N/A - CMC has not determined the power state of the server.• Off - The server or the chassis is off.• On - The chassis and server are on.• Powering On - Temporary state between Off and On. Once the powering on cycle completes, the Power State changes to On.• Powering Off - Temporary state between On and Off. Once the powering off cycle completes, the Power State changes to Off.
Virtual Reseat	Select the check box to virtually reseat that server.

- 6** To virtual reseat a server, click the check box of the servers to reseat, and then select **Apply Selections**. This operation causes the servers to behave as if they were removed and reinserted.
- 7** Select **Reset/Failover CMC** to cause the active CMC to reset. If a standby CMC is present and a chassis is fully redundant, a failover occurs causing the standby CMC to become active.

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 a number of reasons:

- There could be a problem with the NTP Server 1, NTP Server 2, and NTP Server 3 settings.
- An invalid host name or IP address may have been accidentally entered.
- There could be a network connectivity problem that prevents CMC from communicating with any of the configured NTP servers.
- There could be a DNS problem, preventing any of the NTP server host names from being resolved.

CMC provides tools to troubleshoot these problems, with the primary source of troubleshooting information being the CMC Trace Log. This log contains an error message for NTP related failures. If CMC is unable to synchronize with any of the remote NTP servers that have been configured, then it derives its timing from the local system clock.

If CMC is synchronized to the local system clock rather than a remote time server, 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 gettractime -n
```

If an ‘*’ is not displayed against one of the configured servers, something may not be set up properly. The output of the above command also contains detailed NTP statistics that may be useful in debugging why the server does not synchronize. If you attempt to configure an NTP server that is Windows based, it may help to increase the MaxDist parameter for ntpd. Before changing this parameter, read and understand all implications of doing so, especially since the default setting should 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, restart the ntpd by disabling NTP, waiting 5-10 seconds, then enabling NTP again.



NOTE: NTP may take an additional 3 minutes to try and 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 unable to synchronize with any of the configured NTP servers.

There may be other NTP related trace log entries to assist in your troubleshooting effort. If it is a NTP server IP address misconfiguration problem, you may see an 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 has been 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
```

See "Using the Diagnostic Console" on page 401 for information on how to enter the gettracelog command to review the trace log using the CMC GUI.

Interpreting LED Colors and Blinking Patterns

The LEDs on the chassis provide information by color and blinking/not blinking:

- 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 "Configuring LEDs to Identify Components on the Chassis" on page 378).

Table 12-13. 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

Table 12-13. LED Color and Blinking Patterns (continued)

Component	LED Color, Blinking Pattern	Meaning
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
	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

Table 12-13. LED Color and Blinking Patterns (continued)

Component	LED Color, Blinking Pattern	Meaning
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 a Non-responsive CMC



NOTE: It is not possible to log in to the standby CMC using a serial console.

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 by observing the LEDs on CMC, obtaining recovery information using the DB-9 serial port, or recovering the CMC firmware image.

Observing the LEDs to Isolate the Problem

Facing the front of CMC as it is installed in the chassis, you see two LEDs on the left side of the card.

Top LED — The top green LED indicates power. If it is NOT on:

- 1 Verify that you have AC present to at least one power supply.
- 2 Verify that the CMC card is seated properly. You can release/pull on 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 could 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, you can recover CMC by uploading the CMC firmware image.



NOTE: A normal CMC boot/reset takes over a minute to fully boot into its OS 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 the DB-9 Serial Port

If the bottom LED is amber, recovery information should be 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 returned to Dell.
- If the prompt indicates **Bad FW Images**, then follow the steps in "Recovering the Firmware Image" on page 412 to fix the problem.

Recovering the Firmware Image

CMC enters recover mode when a normal CMC OS 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, **firming.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 alerting and networking. You can access the trace log using the CMC Web interface (see "Using the Diagnostic Console") or RACADM (see "Using the RACADM Command Line Interface" and the `gettracelog` command section in the *Command Line Reference Guide for iDRAC6 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 Forgotten 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 Figure 12-1. 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: Ensure 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 Figure 12-1.

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 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.

 **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. See Figure 12-1 to locate the password jumper on the CMC board.

Figure 12-1. Password Reset Jumper Location

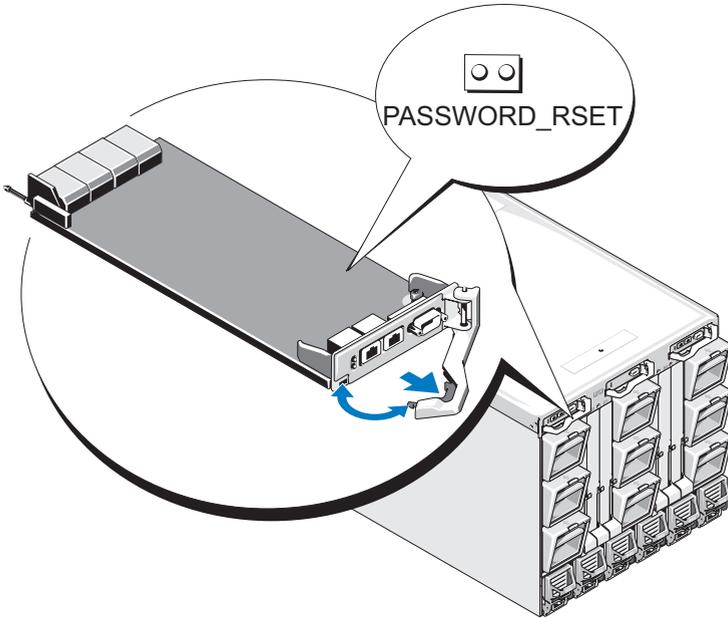


Table 12-14. CMC Password Jumper Settings

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:** Ensure 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 simply wait for it to finish rebooting. If you have redundant CMCs in your chassis, then initiate a changeover to make the jumpered CMC module active. On the GUI interface:
 - a Navigate to the **Chassis** page, click the **Power** tab→ **Control** subtab.
 - b Select the **Reset CMC (warm boot)** button.
 - c 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 any needed management actions, including creating a new administrator password in place of the forgotten one.
- 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.

Troubleshooting Alerting

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.

You can configure SNMP alerts using the Web interface. For information, see "Configuring SNMP Alerts."

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 down 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 for server errors, use the iDRAC Web interface or command line interface to clear the server's System Event Log (SEL) to remove the server errors from the LCD.

Using the LCD Panel Interface

You can use the LCD panel to perform configuration and diagnostics, and to obtain status information about the chassis and its contents.

LCD Navigation

Use the buttons to the right of the LCD screen to operate the LCD panel. 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.

The center button activates the selected item.

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 Table 13-1 are used in navigating between LCD screens:

Table 13-1. 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.
or		NOTE: The amber background indicates that the opposite view has errors.
		Component Identify. Blinks the blue LED on a component. NOTE: There is a blinking blue rectangle around this icon when Component Identify is enabled.

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.
- 1** Use the up and down arrow buttons to highlight an item.
 - 2** 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.
- 1 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.
 - 2 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:

- 1 Highlight the rotate icon.
- 2 Press the center button.

To view the status screen for a server:

- 1 Use the arrow buttons to highlight the desired server.
- 2 Press the center button. The **Server Status** screen displays.

To return to the Main Menu:

- 1 Use the arrow buttons to highlight the **Back** icon.
- 2 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:

- 1 Highlight the rotate icon.
- 2 Press the center button.

To view the status screen for a module:

- 1 Use the up, down, left, and right arrow buttons to highlight the desired module.
- 2 Press the center button. The **Module Status** screen displays.

To return to the **Main Menu**:

- 1 Use the arrow buttons to highlight the **Back** icon.
- 2 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**
- 1 Use the navigation buttons to highlight the desired item. (Highlight the **Back** icon to return to the **Main Menu**.)
 - 2 Press the center button. The selected screen displays.

Module Status Screen

The **Module Status** screen displays information and error messages about a module. See "LCD Module and Server Status Information" on page 433 and "LCD Error Messages" on page 426 for messages that can appear on this screen.

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. See "LCD Error Messages" on page 426 for messages that can appear on this screen.

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** a blinking icon with an amber background displays next to the menu item—Server or Enclosure—that leads to the faulty server or module.

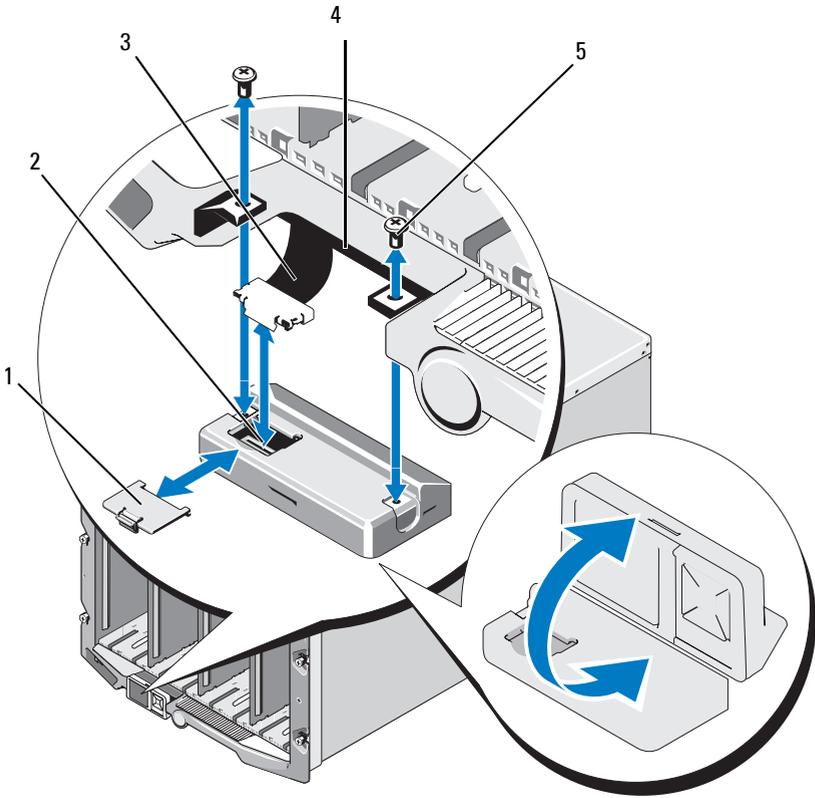
By following the blinking amber icons down through the LCD menu system, you can display the status screen and error messages for the item that has the problem.

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 13-1. Removing and Installing the LCD Module



- | | | | |
|---|--------------|---|------------|
| 1 | cable cover | 2 | LCD module |
| 3 | ribbon cable | 4 | hinges (2) |
| 5 | screws (2) | | |

Table 13-2. LCD Hardware Trouble Shooting 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. LED and LCD is off.	Defective LCD screen. The LCD cable is not connected properly or is faulty; or the LCD module is faulty.	Replace the LCD module. Review the hardware log using the GUI or RACADM commands. Look for a message that states: <ul style="list-style-type: none"> • 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 format is as follows:

<Severity> <Sensor Name>: <Sensor Type> sensor for <Entity>, <Description of event>

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 13-3. 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 13-4. 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 can not 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 13-5. 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 13-6. 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 13-7. 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 13-8. 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 13-9. 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.

Table 13-9. Server Status Screen (continued)

Severity	Message	Cause
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.
Critical	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.

Table 13-9. Server Status Screen (continued)

Severity	Message	Cause
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.

Table 13-9. Server Status Screen (continued)

Severity	Message	Cause
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.

Table 13-9. Server Status Screen (continued)

Severity	Message	Cause
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 13-10. CMC Status

Item	Description
Example: CMC1, CMC2	Name/Location.
No Errors	If no error occurs then "No Errors" is displayed, else lists error messages.

Table 13-10. CMC Status (continued)

Item	Description
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 13-11. 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 13-12. 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 13-13. 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 13-14. 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 13-15. 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 13-16. 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.

Table 13-16. Server Status (continued)

Item	Description
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 13-16 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 finished booting. For more information on this feature, see "*Command Line Reference Guide for iDRAC6 and CMC*"

Index

A

ACI, 335

Activating FlexAddress Plus, 235

Active Directory, 241

adding CMC users, 262

configuring access to the
CMC, 254

configuring and managing
certificates, 163

extending schemas, 254

objects, 249

schema extensions, 248

using with standard schema, 242

adding

SNMP alerts, 379

alerts

troubleshooting, 416

Analog Console Interface, 333

C

Certificate Signing Request
(CSR)

about, 174

generating a new certificate, 175

certificates

Active Directory, 163

SSL and digital, 173

uploading a server certificate, 178

viewing a server certificate, 179

CMC

configuring, 264

creating a configuration file, 95

downloading firmware, 49

feature sets, 20

installing, 29

log, 400

redundant environment, 53

setting up, 29

CMC VLAN, 84

command line console

features, 55

configuration file

creating, 95

configuring

CMC from the LCD panel, 49

CMC remote RACADM, 48

power budgeting, 49

remote RACADM, 48

SNMP alerts, 379

Configuring and Managing

Generic Lightweight

Directory Access Protocol

Services, 169

connect command

CMC command line

connection, 61

E

Enabling or Disabling DCHP, 82

F

fabric management, 361

feature sets of CMC, 20

featurecard, 220

firmware

- downloading, 49

- managing, 189

- updating, CMC, 190

- updating, iKVM, 192

- updating, IOM infrastructure device, 193

- updating, Server iDRAC, 194

FlexAddress, 217

- activating, 218

- activation verification, 220

- configuring using CLI, 222

- deactivating, 221

- license agreement, 231

- Linux configuration, 223

- troubleshooting, 224

- viewing status using CLI, 223

- Wake-On-LAN, 224

frequently asked questions

- managing and recovering a remote system, 213

- using the CMC with Active Directory, 269

H

hardware log, 398

hardware specifications, 23

I

I/O fabric, 361

iDRAC

- recovering firmware, 195

iKVM, 333

installing CMC, 29

L

LDC panel

- configuring CMC from, 49

logs

- CMC, 400

- hardware, 398

M

managed system

- accessing through the local serial port, 56

management station

- configuring terminal emulation, 59

Microsoft Active Directory, 241

N

Network LAN Settings, 80

network properties
 configuring manually, 78
 configuring using racadm, 78

O

OSCAR, 333

P

parsing rules, 97
password
 disabling, 413
 reset jumper location, 415
power budgeting
 configuring, 49
power conservation, 299
proxy server, 37

R

RAC

 see Remote Access
 Connection, 24

RACADM

 uninstalling from Linux
 management station, 36

racadm utility

 configuring network
 properties, 78

 parsing rules, 97

Red Hat Enterprise Linux
 configuring for serial console
 redirection, 63

redundant environment, 53

remote access connection
 (RAC), 24

remote RACADM
 configuring, 48

S

Secure Sockets Layer (SSL)
 about, 173

security
 using SSL and digital
 certificates, 173

serial console
 using, 56

server certificate
 uploading, 178
 viewing, 179

services
 configuring, 180

setting up CMC, 29

Single Sign-On, 272

slot names
 editing, 124
 naming rules, 124

snap-in
 installing the Dell extension, 261

- SNMP alerts
 - adding and configuring, 379
- specifications
 - hardware, 23
- standard schema
 - using with Active Directory, 242

T

- telnet console
 - using, 56

U

- Using FlexAddress Plus, 236

V

- Viewing Current IPv4 Network Settings, 79
- Viewing Current IPv6 Network Settings, 79

W

- web browser
 - configuring, 36
 - supported browsers, 25
- web interface
 - accessing, 103
 - configuring email alerts, 385
- WS-Management, 25