

Dell™ Chassis Management  
Controller Firmware  
Version 2.10 User Guide



# Notes and Cautions



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



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

---

**Information in this document is subject to change without notice.**

© 2009 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 NT*, *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* and *SUSE* are registered trademarks of Novell Corporation 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 document 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.

**August 2009**

# Contents

1	Overview . . . . .	17
	<b>What's New For This Release . . . . .</b>	<b>17</b>
	<b>CMC Management Features . . . . .</b>	<b>18</b>
	<b>Security Features . . . . .</b>	<b>20</b>
	<b>Chassis Overview . . . . .</b>	<b>21</b>
	<b>Hardware Specifications . . . . .</b>	<b>21</b>
	TCP/IP Ports . . . . .	21
	<b>Supported Remote Access Connections . . . . .</b>	<b>23</b>
	<b>Supported Platforms . . . . .</b>	<b>23</b>
	<b>Supported Web Browsers . . . . .</b>	<b>24</b>
	<b>Supported Management Console Applications . . . . .</b>	<b>24</b>
	<b>WS-Management Support . . . . .</b>	<b>24</b>
	<b>Other Documents You May Need . . . . .</b>	<b>26</b>
2	Installing and Setting Up the CMC . . . . .	29
	<b>Before You Begin . . . . .</b>	<b>29</b>
	<b>Installing the CMC Hardware . . . . .</b>	<b>29</b>

<b>Installing Remote Access Software on a Management Station . . . . .</b>	<b>30</b>
Installing RACADM on a Linux Management Station . . . . .	30
Uninstalling RACADM From a Linux Management Station . . . . .	31
<b>Configuring a Web Browser . . . . .</b>	<b>31</b>
Proxy Server . . . . .	32
Microsoft® Phishing Filter . . . . .	33
Certificate Revocation List (CRL) Fetching . . . . .	33
Downloading Files From CMC With Internet Explorer . . . . .	33
Allow Animations in Internet Explorer . . . . .	34
<b>Setting Up Initial Access to the CMC . . . . .</b>	<b>34</b>
Basic CMC Network Connection . . . . .	35
Daisy-chain CMC Network Connection . . . . .	35
Configuring the CMC Network . . . . .	37
Configuring Networking Using the LCD Configuration Wizard . . . . .	38
<b>Accessing the CMC Through a Network . . . . .</b>	<b>44</b>
<b>Installing or Updating the CMC Firmware. . . . .</b>	<b>45</b>
Downloading the CMC Firmware . . . . .	45
Updating CMC Firmware Using the Web Interface. . . . .	46
Updating the CMC Firmware Using RACADM . . . . .	46
<b>Configuring CMC Properties . . . . .</b>	<b>47</b>
Configuring Power Budgeting . . . . .	47
Configuring CMC Network Settings . . . . .	47
Adding and Configuring Users . . . . .	47
Adding SNMP and E-mail Alerts . . . . .	48
Configuring Remote Syslog . . . . .	48

<b>Understanding the Redundant CMC Environment</b> . . . . .	<b>49</b>
About the Standby CMC . . . . .	49
Primary CMC Election Process. . . . .	50
Obtaining Health Status of Redundant CMC . . . . .	50
<b>3 Configuring CMC to Use Command Line Consoles</b> . . . . .	<b>51</b>
<b>Command Line Console Features on the CMC</b> . . . . .	<b>51</b>
<b>Using a Serial, Telnet, or SSH Console</b> . . . . .	<b>52</b>
<b>Using a Telnet Console With the CMC</b> . . . . .	<b>52</b>
<b>Using SSH With the CMC</b> . . . . .	<b>52</b>
Enabling SSH on the CMC . . . . .	53
Changing the SSH Port . . . . .	53
Enabling the Front Panel to iKVM Connection . . . . .	54
<b>Configuring Terminal Emulation Software</b> . . . . .	<b>54</b>
Configuring Linux Minicom . . . . .	55
<b>Connecting to Servers or I/O Modules With the Connect Command.</b> . . . . .	<b>56</b>
Configuring the managed server BIOS for serial console redirection. . . . .	58
Configuring Windows for serial console redirection. . . . .	59
Configuring Linux for Server Serial Console Redirection During Boot. . . . .	59
Configuring Linux for Server Serial Console Redirection After Boot . . . . .	61

4	Using the RACADM Command Line Interface . . . . .	65
	<b>Using a Serial, Telnet, or SSH Console . . . . .</b>	<b>65</b>
	Logging in to the CMC . . . . .	66
	Starting a Text Console . . . . .	66
	<b>Using RACADM. . . . .</b>	<b>66</b>
	RACADM Subcommands . . . . .	67
	Accessing RACADM Remotely . . . . .	71
	Enabling and Disabling the RACADM Remote Capability. . . . .	72
	Using RACADM Remotely. . . . .	72
	RACADM Error Messages . . . . .	73
	<b>Using RACADM to Configure the CMC. . . . .</b>	<b>74</b>
	<b>Configuring CMC IPv4 Network Properties . . . . .</b>	<b>74</b>
	Setting Up Initial Access to the CMC. . . . .	74
	Viewing Current Network Settings . . . . .	75
	Configuring the Network LAN Settings. . . . .	76
	Configuring the Network Security Settings . . . . .	80
	<b>Using RACADM to Configure Users . . . . .</b>	<b>80</b>
	Before You Begin . . . . .	80
	Adding a CMC User. . . . .	81
	<b>Using RACADM to Configure Public Key Authentication over SSH. . . . .</b>	<b>83</b>
	Before You Begin . . . . .	83
	Generating Public Keys for Windows. . . . .	84
	Generating Public Keys for Linux . . . . .	84
	Viewing the Public Keys . . . . .	85
	Adding the Public Keys . . . . .	85
	Deleting the Public Keys . . . . .	85

Logging in Using Public Key Authentication . . . . .	86
Enabling a CMC User With Permissions . . . . .	86
Disabling a CMC User . . . . .	87
<b>Configuring SNMP and E-mail Alerting . . . . .</b>	<b>87</b>
<b>Configuring Multiple CMCs in Multiple Chassis . . . . .</b>	<b>87</b>
Creating a CMC Configuration File . . . . .	89
Parsing Rules . . . . .	90
Modifying the CMC IP Address. . . . .	92
<b>Using RACADM to Configure Properties on iDRAC . . . . .</b>	<b>93</b>
<b>Troubleshooting . . . . .</b>	<b>95</b>
<b>5 Using the CMC Web Interface. . . . .</b>	<b>97</b>
<b>Accessing the CMC Web Interface . . . . .</b>	<b>97</b>
Logging In. . . . .	98
Logging Out. . . . .	99
<b>Configuring Basic CMC Settings . . . . .</b>	<b>99</b>
Setting the Chassis Name . . . . .	99
Setting the Date and Time on the CMC. . . . .	100
<b>Monitoring System Health Status . . . . .</b>	<b>100</b>
Viewing Chassis and Component Summaries. . . . .	100
Viewing Chassis Graphics and Component Health Status . . . . .	101
Viewing Power Budget Status . . . . .	101
Viewing Server Model Name and Service Tag . . . . .	102
Viewing the Health Status of All Servers. . . . .	102

Editing Slot Names . . . . .	104
Setting the First Boot Device for Servers . . . . .	106
Viewing the Health Status of an Individual Server . . . . .	107
Viewing the Health Status of IOMs . . . . .	113
Viewing the Health Status of the Fans . . . . .	114
Viewing the iKVM Status . . . . .	116
Viewing the Health Status of the PSUs . . . . .	117
Viewing Status of the Temperature Sensors . . . . .	119
<b>Viewing World Wide Name/Media Access Control (WWN/MAC) IDs . . . . .</b>	<b>121</b>
Fabric Configuration . . . . .	121
WWN/MAC Addresses . . . . .	121
<b>Configuring CMC Network Properties. . . . .</b>	<b>122</b>
Setting Up Initial Access to the CMC. . . . .	122
Configuring the Network LAN Settings. . . . .	122
Configuring CMC Network Security Settings . . . . .	129
<b>Configuring VLAN . . . . .</b>	<b>131</b>
<b>Adding and Configuring CMC Users . . . . .</b>	<b>132</b>
User Types . . . . .	132
Adding and Managing Users . . . . .	138



<b>Configuring and Managing Microsoft Active Directory Certificates</b> . . . . .	<b>141</b>
Configuring Active Directory (Standard Schema and Extended Schema) . . . . .	142
Uploading an Active Directory Certificate Authority-Signed Certificate . . . . .	146
Viewing an Active Directory Certificate Authority-Signed Certificate . . . . .	146
<b>Securing CMC Communications Using SSL and Digital Certificates</b> . . . . .	<b>147</b>
Secure Sockets Layer (SSL) . . . . .	147
Certificate Signing Request (CSR) . . . . .	148
Accessing the SSL Main Menu . . . . .	149
Generating a New Certificate Signing Request . . . . .	149
Uploading a Server Certificate . . . . .	152
Viewing a Server Certificate . . . . .	153
<b>Managing Sessions</b> . . . . .	<b>153</b>
<b>Configuring Services</b> . . . . .	<b>154</b>
<b>Configuring Power Budgeting</b> . . . . .	<b>162</b>
<b>Managing Firmware Updates</b> . . . . .	<b>163</b>
Viewing the Current Firmware Versions . . . . .	163
Updating Firmware . . . . .	164
Recovering iDRAC Firmware Using the CMC . . . . .	169
<b>Managing iDRAC</b> . . . . .	<b>170</b>
iDRAC QuickDeploy . . . . .	170
iDRAC Network Settings . . . . .	174
Launching iDRAC using Single Sign-On . . . . .	176

<b>FlexAddress</b> . . . . .	<b>178</b>
Viewing FlexAddress Status . . . . .	178
Configuring FlexAddress . . . . .	182
Chassis-Level Fabric and Slot FlexAddress Configuration . . . . .	182
Server-Level Slot FlexAddress Configuration . . . . .	183
<b>Remote File Sharing</b> . . . . .	<b>184</b>
<b>Frequently Asked Questions</b> . . . . .	<b>186</b>
<b>Troubleshooting the CMC</b> . . . . .	<b>188</b>
<b>6 Using FlexAddress</b> . . . . .	<b>189</b>
<b>Activating FlexAddress</b> . . . . .	<b>190</b>
Verifying FlexAddress Activation . . . . .	191
<b>Deactivating FlexAddress</b> . . . . .	<b>193</b>
Deactivating FlexAddress . . . . .	193
<b>Configuring FlexAddress Using the CLI</b> . . . . .	<b>194</b>
Additional FlexAddress Configuration for Linux . . . . .	195
<b>Viewing FlexAddress Status Using the CLI</b> . . . . .	<b>195</b>
<b>Configuring FlexAddress Using the GUI</b> . . . . .	<b>196</b>
<b>Wake-On-LAN with FlexAddress</b> . . . . .	<b>196</b>
<b>Troubleshooting FlexAddress</b> . . . . .	<b>196</b>
<b>Command Messages</b> . . . . .	<b>200</b>
<b>FlexAddress DELL SOFTWARE     LICENSE AGREEMENT</b> . . . . .	<b>202</b>

7	Using the CMC With Microsoft Active Directory . . . . .	207
	<b>Active Directory Schema Extensions . . . . .</b>	<b>207</b>
	Extended Schema Versus Standard Schema. . . . .	207
	<b>Extended Schema Overview. . . . .</b>	<b>208</b>
	Active Directory Schema Extensions . . . . .	208
	Overview of the RAC Schema Extensions . . . . .	209
	Active Directory Object Overview . . . . .	209
	Configuring Extended Schema Active Directory to Access Your CMC . . . . .	213
	Extending the Active Directory Schema . . . . .	213
	Installing the Dell Extension to the Active Directory Users and Computers Snap-In. . . . .	219
	Adding CMC Users and Privileges to Active Directory . . . . .	220
	Configuring the CMC With Extended Schema Active Directory and the Web Interface . . . . .	223
	Configuring the CMC With Extended Schema Active Directory and RACADM . . . . .	226
	<b>Standard Schema Active Directory Overview . . . . .</b>	<b>228</b>
	Configuring Standard Schema Active Directory to Access Your CMC . . . . .	230
	Configuring the CMC With Standard Schema Active Directory and Web Interface . . . . .	230
	Configuring the CMC With Standard Schema Active Directory and RACADM . . . . .	233
	<b>Frequently Asked Questions. . . . .</b>	<b>234</b>
	<b>Configuring Single Sign-On . . . . .</b>	<b>236</b>
	<b>System Requirements . . . . .</b>	<b>237</b>

<b>Configuring Settings</b> . . . . .	<b>238</b>
Prerequisites . . . . .	238
Configuring Active Directory . . . . .	238
Configuring the CMC . . . . .	239
Uploading the Kerberos Keytab File . . . . .	239
Enabling Single Sign-On . . . . .	240
Configuring the Browser For Single Sign-On Login . . . . .	240
Logging into the CMC Using Single Sign-On . . . . .	241
<b>Configuring Smart Card Two-Factor Authentication</b> . . . . .	<b>242</b>
System Requirements. . . . .	242
Configuring Settings . . . . .	242
Configuring Active Directory . . . . .	243
Configuring the CMC . . . . .	243
Uploading the Kerberos Keytab File . . . . .	243
Enabling Smart Card Authentication . . . . .	244
Configuring the Browser For Smart Card Login . . . . .	244
Logging into the CMC Using Smart Card . . . . .	244
Logging in Using Smart Card . . . . .	245
Troubleshooting the Smart Card Login . . . . .	245
<b>8 Power Management.</b> . . . . .	<b>247</b>
<b>Overview</b> . . . . .	<b>247</b>
AC Redundancy Mode . . . . .	247
Power Supply Redundancy Mode . . . . .	250
No Redundancy Mode . . . . .	251
Power Budgeting for Hardware Modules . . . . .	252
Server Slot Power Priority Settings. . . . .	255
Dynamic Power Supply Engagement. . . . .	256

<b>Redundancy Policies</b> . . . . .	<b>258</b>
AC Redundancy. . . . .	258
Power Supply Redundancy. . . . .	258
No Redundancy. . . . .	259
Power Conservation and Power Budget Changes . . . . .	259
Power Supply and Redundancy Policy Changes in System Event Log . . . . .	262
Redundancy Status and Overall Power Health . . . . .	263
<b>Configuring and Managing Power</b> . . . . .	<b>263</b>
Viewing the Health Status of the PSUs. . . . .	263
Viewing Power Consumption Status . . . . .	266
Viewing Power Budget Status . . . . .	270
Configuring Power Budget and Redundancy . . . . .	275
Assigning Priority Levels to Servers . . . . .	279
Setting the Power Budget . . . . .	280
Server Power Reduction to Maintain Power Budget . . . . .	282
Executing Power Control Operations on the Chassis . . . . .	282
Executing Power Control Operations on an IOM. . . . .	284
Executing Power Control Operations on a Server . . . . .	284
Troubleshooting. . . . .	286
<b>9 Using the iKVM Module</b> . . . . .	<b>287</b>
<b>Overview</b> . . . . .	<b>287</b>
iKVM User Interface . . . . .	287
Security . . . . .	287
Scanning . . . . .	287

Server Identification . . . . .	288
Video . . . . .	288
Plug and Play . . . . .	288
FLASH Upgradable . . . . .	288
<b>Physical Connection Interfaces . . . . .</b>	<b>288</b>
iKVM Connection Precedences . . . . .	289
Tiering Through the ACI Connection . . . . .	289
<b>Using OSCAR . . . . .</b>	<b>290</b>
Navigation Basics. . . . .	290
Configuring OSCAR . . . . .	291
<b>Managing Servers With iKVM . . . . .</b>	<b>294</b>
Peripherals Compatibility and Support . . . . .	294
Viewing and Selecting Servers . . . . .	295
Setting Console Security . . . . .	298
Scanning Your System . . . . .	302
Broadcasting to Servers . . . . .	304
<b>Managing iKVM From the CMC . . . . .</b>	<b>305</b>
Enabling or Disabling the Front Panel . . . . .	305
Enabling the Dell CMC Console Through iKVM. . . . .	306
Viewing the iKVM Status and Properties. . . . .	306
Updating the iKVM Firmware . . . . .	308
<b>Troubleshooting . . . . .</b>	<b>310</b>

10 I/O Fabric Management . . . . .	315
<b>Fabric Management</b> . . . . .	<b>316</b>
<b>Invalid Configurations</b> . . . . .	<b>317</b>
Invalid Mezzanine Card (MC) Configuration . . . . .	317
Invalid IOM-Mezzanine Card (MC) Configuration . . . . .	318
Invalid IOM-IOM Configuration. . . . .	318
<b>Fresh Power-up Scenario</b> . . . . .	<b>318</b>
<b>Monitoring IOM Health</b> . . . . .	<b>319</b>
Viewing the Health Status of an Individual IOM. . . . .	322
Configuring Network Settings for an Individual IOM. . . . .	324
Troubleshooting IOM Network Settings . . . . .	326
11 Troubleshooting and Recovery . . . . .	327
<b>Overview</b> . . . . .	<b>327</b>
<b>Chassis Monitoring Tools</b> . . . . .	<b>327</b>
Configuring LEDs to Identify Components on the Chassis . . . . .	327
Configuring SNMP Alerts. . . . .	328
Configuring E-mail Alerts. . . . .	334
<b>First Steps to Troubleshooting     a Remote System</b> . . . . .	<b>337</b>
<b>Monitoring Power and Executing     Power Control Commands on the Chassis</b> . . . . .	<b>337</b>
Viewing Power Budget Status . . . . .	337
Executing a Power Control Operation . . . . .	338

<b>Power Supply Troubleshooting</b> . . . . .	<b>338</b>
<b>Viewing Chassis Summaries</b> . . . . .	<b>341</b>
<b>Viewing Chassis and Component Health Status</b> . . . . .	<b>345</b>
<b>Viewing the Event Logs</b> . . . . .	<b>346</b>
Viewing the Hardware Log . . . . .	347
Viewing the CMC Log . . . . .	349
Firmware Update Error Codes . . . . .	350
<b>Using the Diagnostic Console</b> . . . . .	<b>352</b>
<b>Resetting Components</b> . . . . .	<b>353</b>
<b>Troubleshooting Network Time Protocol (NTP) Errors</b> . . . . .	<b>357</b>
<b>Interpreting LED Colors and Blinking Patterns</b> . . . . .	<b>359</b>
<b>Troubleshooting a Non-responsive CMC</b> . . . . .	<b>361</b>
Observing the LEDs to Isolate the Problem . . . . .	362
Obtain Recovery Information From the DB-9 Serial Port . . . . .	362
Recovering the Firmware Image . . . . .	363
<b>Troubleshooting Network Problems</b> . . . . .	<b>364</b>
<b>Disabling a Forgotten Password</b> . . . . .	<b>364</b>
<b>Troubleshooting Alerting</b> . . . . .	<b>366</b>
 Glossary . . . . .	 367
 Index . . . . .	 375



# 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."

## What's New For This Release

This release of CMC supports the following features:

- IPv6 — CMC now supports the IPv6 protocol.

The IPv6 Ready Logo Committee's mission is to define the test specifications for IPv6 conformance and interoperability testing, to provide access to self-test tools, and to deliver the IPv6 Ready Logo. CMC and iDRAC are Phase-2 IPv6 Ready Logo certified, and the Logo ID is 02-C-000378 (Dell PowerEdge M1000e). For information on the IPv6 Ready Logo Program, see [www.ipv6ready.org](http://www.ipv6ready.org).

- VLAN tagging — The CMC and the iDRACs now support the ability to assign their network traffic to a virtual LAN (VLAN).
- Single sign-on for active directory accounts — Single sign-on allows users authenticated using Microsoft® Active Directory® on their local systems to automatically apply those credentials to the CMC Web user interface.

- Two-Factor Authentication using Smart Card — Provides added security — a smart card plus a PIN to authenticate a user instead of just a password.
- Public Key Authentication (PKA) over SSH — Improves SSH scripting automation by removing the need to embed or prompt for user ID/password.
- Power management enhancements — Flexible power supply redundant modes: 1+1, 2+1, and 3+1. Additional fault-tolerant AC redundant modes: 1+1, 2+2, and 3+3.
- Additional error reporting options — The iDRAC system events log is displayed on the **Blade Status** page eliminating the need to log into the iDRAC to view them. Also, CMC events are now also posted to a remote syslog server.
- Remote Virtual Media File Share option — to map a file from a share drive on the network to one or more blades through the CMC, to deploy or update an operating system.
- Ability to read and clear SEL entries for servers from the CMC.

## 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, or Telnet or SSH connection
- Support for Microsoft<sup>®</sup> Active Directory<sup>®</sup> 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 - 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 to potential managed node issues through an e-mail message or SNMP trap
- Remote power management — Provides remote power management functions, such as shutdown and reset 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")
- 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

## 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)



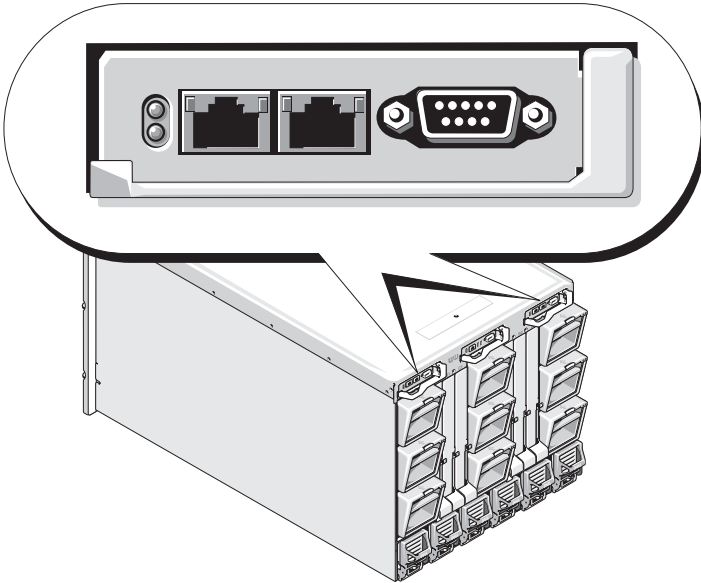
**NOTE:** Telnet does not support SSL encryption.

- Configurable IP ports (where 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 number of 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**



## Hardware Specifications

### TCP/IP Ports

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

Table 1-1 identifies the ports on which the CMC listens for server connections. Table 1-2 identifies the ports that the CMC uses as clients.

**Table 1-1. CMC Server Listening Ports**

<b>Port Number</b>	<b>Function</b>
22*	SSH
23*	Telnet
80*	HTTP
161	SNMP Agent
443*	HTTPS

\* Configurable port

**Table 1-2. CMC Client Port**

<b>Port Number</b>	<b>Function</b>
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 lists the connection features.

**Table 1-3. Supported Remote Access Connections**

Connection	Features
CMC NIC	<ul style="list-style-type: none"><li>• 10Mbps/100Mbps/1Gbps Ethernet via CMC GbE port</li><li>• DHCP support</li><li>• SNMP traps and e-mail event notification</li><li>• Dedicated network interface for the CMC Web interface</li><li>• Network interface for the iDRAC and I/O Modules (IOMs)</li><li>• Support for Telnet/SSH command console and RACADM CLI commands including system boot, reset, power-on, and shutdown commands</li></ul>
Serial port	<ul style="list-style-type: none"><li>• Support for serial console and RACADM CLI commands including system boot, reset, power-on, and shutdown commands</li><li>• Support for binary interchange for applications specifically designed to communicate with a binary protocol to a particular type of IOM</li><li>• 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</li></ul>
Other connections	<ul style="list-style-type: none"><li>• Access to the Dell CMC Console through the Avocent® Integrated KVM Switch Module (iKVM)</li></ul>

## 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 PowerEdge Compatibility Guide* located on the Dell Support website at [support.dell.com](http://support.dell.com).

## Supported Web Browsers

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](http://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, refer to the IT Assistant documentation set available on the Dell Support Web site at [support.dell.com](http://support.dell.com).

## 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; the CIM information defines the semantics and information types that can be manipulated in a managed system. The Dell-embedded server platform management interfaces are organized into profiles, where each profile defines the specific interfaces for a particular management domain or area of functionality. Additionally, Dell has defined a number of model and profile extensions that provide interfaces for additional capabilities.

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 `cfgSessionManagement` database property section in the *Dell Chassis Management Controller Firmware Administrator Reference Guide*.



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 *Dell Chassis Management Controller Firmware Administrator Reference Guide*. Web services interfaces can be utilized by leveraging client infrastructure, such as Windows<sup>®</sup> WinRM and Powershell CLI, open source utilities like WSMANCLI, and application programming environments like Microsoft<sup>®</sup> .NET<sup>®</sup>.

There are additional implementation guides, white papers, profile, and code samples available in the Dell Tech Center at [www.delltechcenter.com](http://www.delltechcenter.com).

For more information, also see:

- DTMF Web site: [www.dmtf.org/standards/profiles/](http://www.dmtf.org/standards/profiles/)
- WS-MAN release notes or Read Me file.
- [www.wbemsolutions.com/ws\\_management.html](http://www.wbemsolutions.com/ws_management.html)
- DMTF WS-Management Specifications:  
[www.dmtf.org/standards/wbem/wsman](http://www.dmtf.org/standards/wbem/wsman)

## Other Documents You May Need

In addition to this User's Guide, the following documents provide additional information about the setup and operation of the CMC. All of these documents may be accessed at [support.dell.com](http://support.dell.com):

- 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 are also available to provide more information about the system in which your 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](http://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.
- Updates are sometimes included with the system to describe changes to the system, software, and/or documentation.



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

- Release notes or readme files may be included to provide last-minute updates to the system or documentation or advanced technical reference material intended for experienced users or technicians.
- 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*.



# 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

Additionally, you can find information about installing and setting up redundant CMC environments at "Understanding the Redundant CMC Environment."

## Before You Begin

Prior to setting up your CMC environment, download the latest version of the CMC firmware from the Dell Support website at [support.dell.com](http://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

Because the CMC is preinstalled on your chassis, no installation is required. To get started with the CMC that is installed on your system, see "Installing Remote Access Software on a Management Station."

You can install a second CMC to run as a standby to the primary CMC. For more information about a standby CMC, see "Understanding the Redundant CMC Environment."

# 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.

If you want to use remote RACADM from your management station, you will need to install it using the *Dell Systems Management Tools and Documentation DVD*. Your system includes the *Dell Systems Management Tools and Documentation DVD*. 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 you need 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](http://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 If necessary, mount the DVD to a location of your choice using 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 manually mount the DVD-ROM and then run the executables.

- 4 Navigate to the `SYSMGMT/ManagementStation/linux/rac` directory. To install the RAC software, enter the following command:

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

- 5 For help with the RACADM command, type `racadm help` after issuing the previous commands. For more information about RACADM, see "Using the RACADM Command Line Interface."



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

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

## Uninstalling RACADM From a Linux Management Station

- 1 Log on as root to the system where you want to uninstall the management station features.
- 2 Use the `rpm query` command to determine which version of the DRAC Tools is installed. Use the `rpm -qa | grep mgmtst-racadm` command.
- 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](http://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.

You must ensure that security measures on the management network, such as firewalls and proxy servers, do not prevent your Web browser from accessing the CMC.

Also, be aware that 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, there are Internet Explorer settings that can interfere with connectivity even when you are using a command line interface to access the management network.

## **Proxy Server**

If you have a proxy server for browsing and it 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 when 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**, then click **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 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** and then in the **No Proxy for** field, add 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, you may experience delays of several seconds when accessing the CMC, whether 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 Check 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 is using 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**, 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. For information on how to configure the CMC network settings, see "Configuring the CMC Network." This initial configuration assigns the TCP/IP networking parameters that enable access to the CMC.

Once 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:** Dell strongly recommends the best practice of isolating/separating the management network in the chassis, used by iDRAC and CMC, from your production network(s). Mixing management and production/application traffic on this management network could cause congestion/saturation, which will result in CMC and iDRAC communication delays. The 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 if present, to 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 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.

### **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 in the secondary CMC slot, make two connections to the management network.

Each CMC has two RJ-45 Ethernet ports, labeled **GB1** (the *uplink* port) and **STK** (the *stacking* port). With basic cabling, you connect the GB1 port to the management network and leave the STK port unused.

 **CAUTION: Connecting the STK port to the management network can have unpredictable results.**

### **Daisy-chain CMC Network Connection**

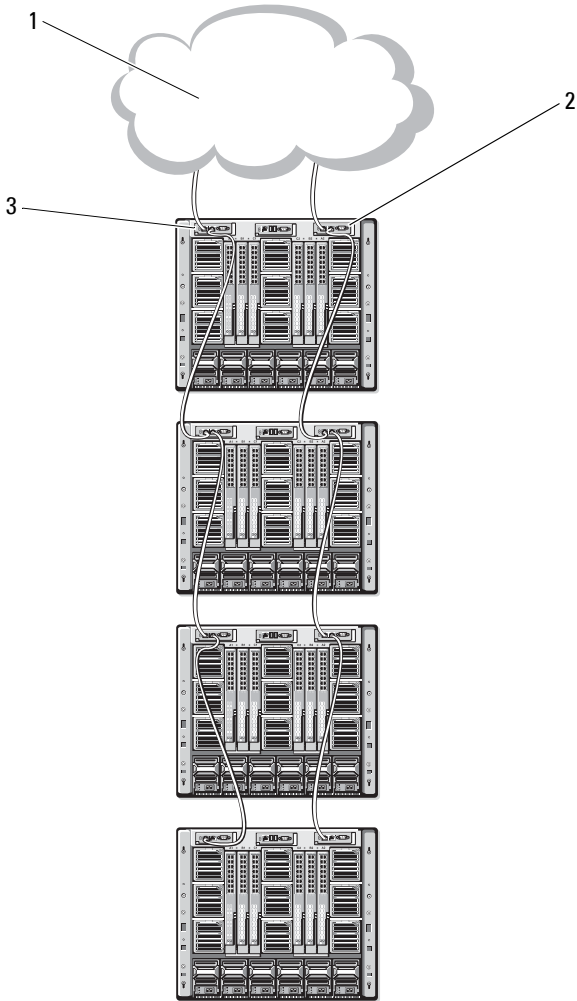
If you have multiple chassis in a rack, you can reduce the number of connections to the management network by daisy-chaining up to four chassis together. If each of four chassis contains a redundant CMC, by daisy-chaining you reduce the number of management network connections required from eight to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

When daisy-chaining chassis together, GB1 is the uplink port and STK is the stacking port. A GB1 port must connect to the management network or to the STK port of the CMC in a chassis that is closer to network. The STK port must only receive a connection from a GB1 port further from the chain or network.

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

Figure 2-1 illustrates the arrangement of cables for four daisy-chained chassis, each with CMCs in the primary and secondary slots.

**Figure 2-1. Daisy-chained CMC Network Connection**



1 management network

2 secondary CMC

3 primary CMC

Follow these steps to daisy-chain up to four chassis:

- 1 Connect the GB1 port of the primary CMC in the first chassis to the management network.
- 2 Connect the GB1 port of the primary CMC in the second chassis to the STK port of the primary CMC in the first chassis.
- 3 If you have a third chassis, connect the GB1 port of its primary CMC to the STK port of the primary CMC in the second chassis.
- 4 If you have a fourth chassis, connect the GB1 port of its primary 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 GB1 port on another chassis. Connecting a STK port to the management network can disrupt the network and cause a loss of data.**



**NOTE:** Never connect a primary CMC to a secondary CMC.



**NOTE:** Resetting a CMC whose STK port is chained to another CMC can disrupt the network for CMCs 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.

## 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:

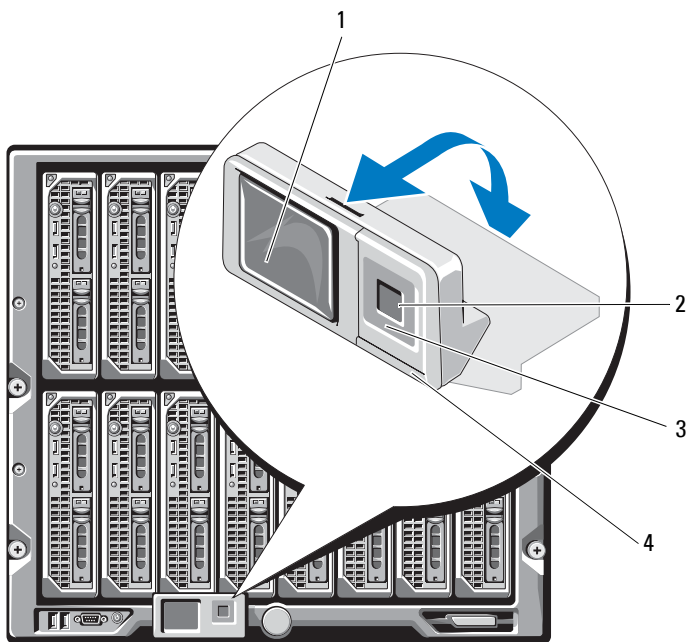
- Command line interfaces (CLIs) such as a serial console, Telnet, SSH, or the Dell CMC Console via iKVM
- Remote RACADM
- The CMC Web interface

## 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 2-2 illustrates the LCD panel.

**Figure 2-2. 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 *Dell Chassis Management Controller Administrator Reference Guide*.

### **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 will result 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:

<b>Dynamic Host Configuration Protocol (DHCP)</b>	The CMC retrieves IP configuration (IP address, mask, and gateway) automatically from a DHCP server on your network. The CMC will be assigned a unique IP address allotted over your network. If you have selected the DHCP option, press the center button. The <b>Configure iDRAC?</b> screen appears; go to step 10.
<b>Static</b>	<p>You manually enter the IP address, gateway, and subnet mask in the screens immediately following.</p> <p>If you have selected the <b>Static</b> option, press the center button to continue to the next <b>CMC Network Settings</b> screen, then:</p> <ol style="list-style-type: none"><li>Set the <b>Static IP Address</b> 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 <b>Static IP Address</b>, press the center button to continue.</li><li>Set the subnet mask, and then press the center button.</li><li>Set the gateway, and then press the center button. The <b>Network Summary</b> screen displays.  The <b>Network Summary</b> screen lists the <b>Static IP Address</b>, <b>Subnet Mask</b>, and <b>Gateway</b> 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.</li><li>When you have confirmed the accuracy of the settings you entered, press the center button. The <b>Register DNS?</b> screen appears.</li></ol>

 **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.
- 11** Select the Internet Protocol (IPv4, IPv6, or both) that you want to use for the blades.

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

<b>Static</b>	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 will be 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 will prompt 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 will not be 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

Telnet is enabled via one of the other interfaces; telnet is not as secure as the other interfaces so it is disabled by default.

Table 2-1 describes each CMC network interface.

**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 <a href="http://support.dell.com/manuals">support.dell.com/manuals</a>.</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>
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><b>NOTE:</b> Telnet is an unsecure 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 NIC 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](http://support.dell.com/manuals). To access the CMC using a supported Web browser, see "Accessing the CMC Web Interface." For information on Dell OpenManage IT Assistant, see "Installing Remote Access Software on a Management Station."

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."

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

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."




## 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](http://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, some or all of the fan units in the chassis will spin at 100%. This is normal.
-  **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 *Dell Chassis Management Controller Administrator Reference Guide*) or the **Chassis Summary** page (see "Viewing the Current Firmware Versions") 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 primary CMC and the CMC with the older firmware becomes the standby. (See the `cmchangeover` command section in the *Dell Chassis Management Controller Firmware Administrator Reference Guide* for help swapping roles.) This allows you to verify that the update 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.

## Updating CMC Firmware Using the Web Interface

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

## 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 *Dell Chassis Management Controller Administrator Reference Guide*.

## 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." For more information about using RACADM, see "Using the RACADM Command Line Interface."



**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."

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

### 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 — see "Configuring Multiple CMCs in Multiple Chassis"



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

- Web interface — see "Configuring CMC Network Properties"

### 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." For instructions on adding and configuring users using the Web interface, see "Adding and Configuring CMC Users." For instructions on using Active Directory with your CMC, see "Using the CMC With Microsoft Active Directory."

## Adding SNMP and E-mail Alerts

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

## Configuring Remote Syslog

The *remote syslog* feature is activated/configured through either the CMC GUI or through 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 the CMC on whether the log entries were received successfully.

To configure CMC services:

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

For more information on configuring the remote syslog, see Table 5-27.



# Understanding the Redundant CMC Environment

You can install a standby CMC that takes over if your primary CMC fails.

Failovers can occur when you:

- Run the RACADM **cmcchangeover** command. (See the **cmcchangeover** command section in the *Dell Chassis Management Controller Administrator Reference Guide*.)
- Run the RACADM **racreset** command on the active CMC. (See the **racreset** command section in the *Dell Chassis Management Controller Administrator Reference Guide*.)
- 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.")
- Remove the network cable from the active CMC
- Remove the active CMC from the chassis
- Initiate a CMC firmware flash on the active CMC
- Primary CMC is no longer functional



**NOTE:** In the event of a CMC failover, all iDRAC connections and all active CMC sessions will be lost. Users with lost sessions must reconnect to the new primary 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 will report as redundancy degraded.

The standby CMC assumes the same settings and properties of the primary 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."

## **Primary 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 Graphics and Component Health Status."

# 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."

## 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 <b>racadm</b> and are followed by a subcommand, such as <b>getconfig</b> , <b>serveraction</b> , or <b>getsensorinfo</b> . See "Using the RACADM Command Line Interface" 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" for help using the <b>connect</b> command. <b>NOTE:</b> The <b>racadm connect</b> 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](http://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. 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 *Dell Chassis Management Controller Administrator Reference Guide*) or from the **Services Management** page in the Web interface (see "Configuring Services.")

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."

## 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 *Dell Chassis Management Controller Administrator Reference Guide*. For instructions on enabling SSH connections on the CMC using the Web interface, see "Configuring Services."

## Changing the SSH Port

To change the SSH port, use 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 *Dell Chassis Management Controller Administrator Reference Guide*.

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

**Table 3-2. Cryptography Schemes**

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

## **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 your 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" 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, type:  
`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 14.
- 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.
- 9 Press `<Enter>` to save each blank value.
- 10 When all specified fields are clear, press `<Enter>` to exit the **Modem Dialing and Parameter Setup** menu.

- 11 Select **Save setup as config\_name** and press <Enter>.
- 12 Select **Exit From Minicom** and press <Enter>.
- 13 At the command shell prompt, type `minicom <Minicom config file name>`.
- 14 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 <b>init</b> , <b>reset</b> , <b>connect</b> , and <b>hangup</b> 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 *Dell Chassis Management Controller Administrator Reference Guide*.
- 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, type:


```
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 10-1 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 will 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 will be able to 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 will be garbled.

 **NOTE:** Not all keys will work in the BIOS setup screens, so you should 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”), or establish a vKVM session from the iDRAC web GUI (see the *iDRAC User's Guide* on [support.dell.com/manuals](http://support.dell.com/manuals)), and perform the following steps:

Serial communication in the BIOS is OFF by default. To redirect host text console data to Serial over LAN, you must enable console redirection through COM1. To change the BIOS setting:

- 1 Boot the managed server.
- 2 Press <F2> to enter the BIOS setup utility during POST.
- 3 Scroll down to Serial Communication and press <Enter>. In the pop-up dialog box, the serial communication list displays these options:
  - off
  - on without console redirection
  - on with console redirection via COM1

Use the arrow keys to navigate between these options.

- 4 Ensure that **On with console redirection via COM1** is enabled.

- 5 Enable **Redirection After Boot** (default value is **disabled**). This option enables BIOS console redirection across subsequent reboots.
- 6 Save the changes and exit.
- 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 will receive information from the BIOS, and enable the Special Administration Console (SAC) console on 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 `/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 s
    initrd /boot/initrd-2.4.9-e.3.im

```

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

- Disable GRUB's graphical interface and use the text-based interface; otherwise, the GRUB screen will not be 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 "local" or "remote," depending on the location of the `racadm` executable program you are using:



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

- Remote RACADM — you execute RACADM commands on a management station with the `-r` option and the DNS name or IP address of the CMC.
- Local RACADM — you log into the CMC using Telnet, SSH, a serial connection, or the iKVM. With local RACADM, you are executing 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 execute scripts directly on the CMC. For more information about configuring multiple CMCs, see "Configuring Multiple CMCs in Multiple Chassis."

## Using a Serial, Telnet, or SSH Console

You can log in to the CMC either 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." 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 *Dell Chassis Management Controller Administrator Reference Guide*.

## 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 into 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 into 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 on to the CMC.

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

## 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 of the *Dell Chassis Management Controller Administrator Reference Guide*.



**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. See "Connecting to Servers or I/O Modules With the Connect Command" for information about using these commands.

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

```
racadm help
```

**Table 4-1. RACADM Subcommands**

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

**Table 4-1. RACADM Subcommands (continued)**

<b>Command</b>	<b>Description</b>
deploy	Deploys a server by specifying required properties.
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.

**Table 4-1. RACADM Subcommands (continued)**

<b>Command</b>	<b>Description</b>
getsvctag	Displays service tags.
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.
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)**

<b>Command</b>	<b>Description</b>
setslotname	Sets the name of a slot in the chassis.
setsysinfo	Sets the name and location of the chassis.
sshpkauth	Enables you to upload up to 6 different SSH public keys, delete existing keys, and view 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 NIC.
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 lists the options for the remote RACADM subcommands.

**Table 4-2. Remote RACADM Subcommand Options**

Option	Description
<code>-r &lt;racIpAddr&gt;</code>	Specifies the controller's remote IP address.
<code>-r &lt;racIpAddr&gt;:&lt;port&gt;</code>	Use <i>&lt;port number&gt;</i> if the CMC port number is not the default port (443)
<code>-i</code>	Instructs RACADM to interactively query the user for user name and password.
<code>-u &lt;usrName&gt;</code>	Specifies the user name that is used to authenticate the command transaction. If the <code>-u</code> option is used, the <code>-p</code> option must be used, and the <code>-i</code> option (interactive) is not allowed.
<code>-p &lt;password&gt;</code>	Specifies the password used to authenticate the command transaction. If the <code>-p</code> option is used, the <code>-i</code> 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."

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](http://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 will not be 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."

## 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 that will give him or her the permission to configure the CMC.


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

## Configuring CMC IPv4 Network Properties

### Setting Up Initial Access to the CMC

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.

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."

 **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 *Dell Chassis Management Controller Administrator Reference Guide*.

 **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 (primary 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 primary CMC.

### Enabling the CMC NIC


To enable/disable the CMC IPv4 NIC, type:

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

-  **NOTE:** The CMC IPv4 NIC is enabled by default.

To enable/disable the CMC IPv6 addressing, type:

```
racadm config -g cfgIpv6LanNetworking -o cfgNicEnable 1
racadm config -g cfgIpv6LanNetworking -o cfgNicEnable 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 NIC 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."

### **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. 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:** These 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 Only)

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

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



**NOTE:** Some DNS servers will 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**

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

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

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

where:

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

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

where:

<speed> is 10 or 100(default).

### **Setting the Maximum Transmission Unit (MTU)**

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 will use an MTU of 1280.

## Setting the SMTP Server IP Address

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  
cfgRhostsFwUpdateIpAddr <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 will be a duration when this property setting will not work due to change in the specified SMTP server IP address. In such cases, use the DNS name.

## Configuring the Network Security Settings



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

### Enabling IP Range Checking

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:


- a `cfgRacTuneIpRangeMask` bit-wise and with incoming IP address
- b `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 will reset *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:

```
racadm getconfig -u <username>
```

or

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 the user privileges. For information about user privileges, see Table 5-18, Table 5-19, and Table 3-1 in the database property chapter of the *Dell Chassis Management Controller Administrator Reference Guide*.
- 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 *Dell Chassis Management Controller Firmware 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.

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

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

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

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

To verify that the user was added successfully with the correct privileges, use one of the following commands:

```
racadm getconfig -u john
```

or

```
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 will not have to enter username or passwords when logging into the CMC. This can be very useful for setting up automated scripts to perform various functions.

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

- 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 *Dell Chassis Management Controller Administrator Reference Guide*.

## Generating Public Keys for Windows

Before adding an account, a public key is required from the system that will access 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 either 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 will fail.

- 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
```



**NOTE:** The options are case sensitive.

where,

-t option could either 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.

## 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 options, 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 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." Next, type the following command lines with the new user name and password.



**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.

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

## 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" and "Configuring E-mail Alerts."

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.

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.

- 2 Modify the configuration file using a plain-text editor (optional). Any special formatting characters in the configuration file may corrupt the RACADM database.
- 3 Use the newly created configuration file to modify a target CMC.

At the command prompt, type:

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

- 4 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 primary 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 an *.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 *Dell Chassis Management Controller Administrator Reference Guide*.

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.

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

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

The parser reads in all of the indexes from the 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 *Dell Chassis Management Controller Administrator Reference Guide* for a complete list of objects and groups.

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

## Parsing Rules

- 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.

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 *Dell Chassis Management Controller Administrator Reference Guide*.

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 will stop 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, use the following command:

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

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

```
[cfgUserAdmin]
```

```
cfgUserAdminUserName=<USER_NAME>
```

If you type `racadm getconfig -f <myexample>.cfg`, the command builds a `.cfg` file for the current 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 will be updated as follows:

```
#  
#   Object Group "cfgLanNetworking"  
#  
[cfgLanNetworking]  
cfgNicIpAddress=10.35.9.143  
# comment, the rest of this line is ignored  
cfgNicGateway=10.35.9.1
```

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

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

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 blade 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 blade 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 the Serial and RACADM Commands: Frequently Asked Questions**

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

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

<b>Question</b>	<b>Answer</b>
While I was using remote RACADM, the prompt changed to a ">" and I cannot get the "\$" prompt to return.	If you type a double quotation mark (") in the command, the CLI will change 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

The CMC provides a Web interface that enables you to configure the 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." For information on using command line consoles, see "Configuring CMC to Use Command Line Consoles."



**NOTE:** If you are using Microsoft® Internet Explorer®, connecting through a proxy, and see the error "The XML page cannot be displayed," you will 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](http://support.dell.com).

- 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, type:

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

where <CMC IP address> is the IP address for the 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](http://support.dell.com).

- 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 the CMC and <port number> is the HTTPS port number.


The CMC **Login** page appears.

## Logging In

 **NOTE:** To log in to the 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 the CMC. For added security, Dell strongly recommends that you change the default password of the root account during initial setup.


 **NOTE:** The CMC does not support extended ASCII characters, such as ß, å, 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 Microsoft® Active 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>`.

 **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 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 will be 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 will return the name you configure.

To set the chassis name:

- 1 Log in to the CMC Web interface. The **Component 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 the 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 **Component Health** page displays.
- 2 Click the **Setup** tab. The **General Chassis Settings** page displays.
- 3 Click the **Date/Time** sub-tab. 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**.

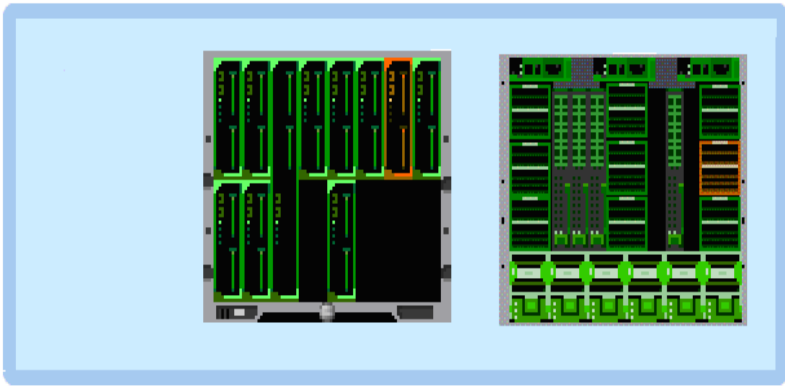
To set the date and time using the command line interface, see the `config` command and `cfgRemoteHosts` database property group sections in the *Dell Chassis Management Controller Administrator Reference Guide*.

## Monitoring System Health Status

### Viewing Chassis and Component Summaries

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

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



The **Component Health** page provides an overall health status for the chassis, primary and stand-by CMCs, sever modules, IO Modules (IOMs), fans, iKVM, power supplies (PSUs), and temperature sensors. The **Chassis Summary** page provides a text-based overview of the chassis, primary and stand-by CMCs, iKVM, and IOMs. For instructions on viewing chassis and components summaries, see "Viewing Chassis Summaries" on page 341.

### **Viewing Chassis Graphics and Component Health Status**

The **Chassis Graphics** page 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.

The **Component Health** page provides an overall health status for all chassis components. For instructions on viewing chassis graphics and component health status, see "Viewing Chassis and Component Health Status."

### **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." For more information about CMC power management, see "Power Management."

## 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 will have its name grayed out.
- Use the cursor to hover over the slot name or slot number of a server, a tool tip is prompted with the servers' model name and service tag number (if available).

## Viewing the Health Status of All Servers

The health status for all servers can be viewed in two ways: from the **Chassis Graphics** section on the **Chassis Status** page or the **Servers Status** page. **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.
- 2 The **Chassis Status** page is displayed. The center 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 color of the server subgraphic:
  - Green - server is present, powered on and communicating with the CMC; there is no indication of an adverse condition.
  - Amber - server is present, but may or may not be powered on, or may or may not be communicating with the CMC; an adverse condition may exist.
  - Gray - server is present and not powered on. It is not communicating with the 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:


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

Table 5-1 provides descriptions of the information provided on the **Servers Status** page.

**Table 5-1. 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	Indicates the name of the server, which by default is identified by its <b>slot name</b> (SLOT-01 to SLOT-16). <b>NOTE:</b> You can change the server name from the default. For instructions, see "Editing Slot Names".															
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.															
Health	<table border="0"><tr><td data-bbox="303 612 348 659"></td><td data-bbox="348 612 505 659">OK</td><td data-bbox="505 612 1006 659">Indicates that the server is present and communicating with the CMC.</td></tr><tr><td data-bbox="303 659 348 746"></td><td data-bbox="348 659 505 746">Informational</td><td data-bbox="505 659 1006 746">Displays information about the server when no change in health status has occurred.</td></tr><tr><td data-bbox="303 746 348 938"></td><td data-bbox="348 746 505 938">Warning</td><td data-bbox="505 746 1006 938">Indicates that only warning alerts have been issued, and <i>corrective action must be taken</i>. If corrective actions are not taken within the administrator-specified time, critical or severe failures that can affect the integrity of the device may occur.</td></tr><tr><td data-bbox="303 938 348 1074"></td><td data-bbox="348 938 505 1074">Severe</td><td data-bbox="505 938 1006 1074">Indicates at least one Failure alert has been issued. Severe status represents a system failure on the server, and <b>corrective action must be taken immediately</b>.</td></tr><tr><td data-bbox="303 1074 348 1141"></td><td data-bbox="348 1074 505 1141">No Value</td><td data-bbox="505 1074 1006 1141">When the server is absent from the slot, health information is not provided.</td></tr></table>		OK	Indicates that the server is present and communicating with the CMC.		Informational	Displays information about the server when no change in health status has occurred.		Warning	Indicates that only warning alerts have been issued, and <i>corrective action must be taken</i> . If corrective actions are not taken within the administrator-specified time, critical or severe failures that can affect the integrity of the device may occur.		Severe	Indicates at least one Failure alert has been issued. Severe status represents a system failure on the server, and <b>corrective action must be taken immediately</b> .		No Value	When the server is absent from the slot, health information is not provided.
	OK	Indicates that the server is present and communicating with the CMC.														
	Informational	Displays information about the server when no change in health status has occurred.														
	Warning	Indicates that only warning alerts have been issued, and <i>corrective action must be taken</i> . If corrective actions are not taken within the administrator-specified time, critical or severe failures that can affect the integrity of the device may occur.														
	Severe	Indicates at least one Failure alert has been issued. Severe status represents a system failure on the server, and <b>corrective action must be taken immediately</b> .														
	No Value	When the server is absent from the slot, health information is not provided.														

**Table 5-1. All Servers Status Information (continued)**

Item	Description
Launch iDRAC GUI	 Left click the icon 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 true: <ol style="list-style-type: none"><li data-bbox="337 405 549 429">1 The server is present</li><li data-bbox="337 440 577 464">2 The chassis power is on</li><li data-bbox="337 475 766 499">3 The LAN interface on the server is enabled</li></ol> <p><b>NOTE:</b> 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 <b>Launch iDRAC GUI</b> icon may display an error page on the iDRAC LAN interface.</p>
Power State	Indicates the power status of the server: <ul style="list-style-type: none"><li data-bbox="297 687 855 740">• <b>N/A</b> - The CMC has not yet determined the power state of the server.</li><li data-bbox="297 756 773 780">• <b>Off</b> - Either the server is off or the chassis is off.</li><li data-bbox="297 796 654 820">• <b>On</b> - Both chassis and server are on.</li><li data-bbox="297 836 934 888">• <b>Powering On</b> - Temporary state between Off and On. When the action completes successfully, the <b>Power State</b> will be <b>On</b>.</li><li data-bbox="297 904 934 957">• <b>Powering Off</b> - Temporary state between On and Off. When the action completes successfully, the <b>Power State</b> will be <b>Off</b>.</li></ul>
Service Tag	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.

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

### 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** printable ASCII characters (ASCII codes 32 through 126), excluding the double quote (" , ASCII 34). If using the RACADM command to change the slot name using any special characters, (~!@#\$\$%^&\*), the name string must be enclosed in double quotes for the environment to pass them correctly to the CMC.
- 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 the 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 **Servers** in the **Chassis** menu in the system tree.
- 3 Click the **Setup** tab - the **Slot Names** subtab. 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**.

### 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 the 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 5-2 lists the boot devices that you can specify.

**Table 5-2. Boot Devices**

<b>Boot Device</b>	<b>Description</b>
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.

**Table 5-2. Boot Devices (continued)**

<b>Boot Device</b>	<b>Description</b>
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** privilege or **Chassis Configuration Administrator** privilege and a login on the iDRAC.

To set the first boot device for some or all servers in the chassis:

- 1 Log in to the CMC Web interface.
- 2 Click **Servers** in the system tree and then click **Setup**→**Deploy First Boot Device**. A list of servers is displayed, 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, uncheck 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 Status** page or the **Server Status** page.

The **Chassis Graphics** 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.
- 2 The **Chassis Status** page is displayed. The center 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 color of the server subgraphic:
  - Green - server is present, powered on and communicating with the CMC; there is no indication of an adverse condition.
  - Amber - server is present, but may or may not be powered on, or may or may not be communicating with the CMC; an adverse condition may exist.
  - Gray - server is present and not powered on. It is not communicating with the CMC and there is no indication of an adverse condition.
- 3 Use the cursor to hover over an individual server subgraphic and a corresponding text hint or screen tip is displayed. The text hint provides additional information on that server.
- 4 The server subgraphic is hyperlinked to the corresponding CMC GUI page to provide immediate navigation to the **Server Status** page for that server.

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 **Servers** 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.

Table 5-3 through Table 5-8 provide descriptions of the information on the **Server Status** page.






**Table 5-3. Individual Server Status - Properties**

Item	Description															
Slot	Indicates 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	Indicates the name of the slot where the server resides.															
Present	Indicates 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).															
Health	<table><tbody><tr><td></td><td>OK</td><td>Indicates that the server is present and communicating with the CMC. In the event of a communication failure between the CMC and the server, the CMC cannot obtain or display health status for the server.</td></tr><tr><td></td><td>Informational</td><td>Displays information about the server when no change in health status (OK, Warning, Severe) has occurred.</td></tr><tr><td></td><td>Warning</td><td>Indicates that only warning alerts have been issued, and <i>corrective action must be taken</i>. If corrective actions are not taken within the administrator-specified time, critical or severe failures that can affect the integrity of the server may occur.</td></tr><tr><td></td><td>Severe</td><td>Indicates at least one Failure alert has been issued. Severe status represents a system failure on the server, and <i>corrective action must be taken immediately</i>.</td></tr><tr><td></td><td>No Value</td><td>When the server is absent from the slot, health information is not provided.</td></tr></tbody></table>		OK	Indicates that the server is present and communicating with the CMC. In the event of a communication failure between the CMC and the server, the CMC cannot obtain or display health status for the server.		Informational	Displays information about the server when no change in health status (OK, Warning, Severe) has occurred.		Warning	Indicates that only warning alerts have been issued, and <i>corrective action must be taken</i> . If corrective actions are not taken within the administrator-specified time, critical or severe failures that can affect the integrity of the server may occur.		Severe	Indicates at least one Failure alert has been issued. Severe 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.
	OK	Indicates that the server is present and communicating with the CMC. In the event of a communication failure between the CMC and the server, the CMC cannot obtain or display health status for the server.														
	Informational	Displays information about the server when no change in health status (OK, Warning, Severe) has occurred.														
	Warning	Indicates that only warning alerts have been issued, and <i>corrective action must be taken</i> . If corrective actions are not taken within the administrator-specified time, critical or severe failures that can affect the integrity of the server may occur.														
	Severe	Indicates at least one Failure alert has been issued. Severe 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	Indicates the model of the server in the chassis. Examples: <b>PowerEdge M600</b> , <b>PowerEdge M605</b> .															
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.															

**Table 5-3. Individual Server Status - Properties (continued)**

Item	Description
iDRAC Firmware	Indicates 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	Indicates the BIOS version on the server.
Operating System	Indicates the operating system on the server.

**Table 5-4. 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.
		Severe	Indicates a critical event requiring immediate corrective actions to avoid system failures.
Date/Time	Indicates 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 5-5. Individual Server Status - iDRAC Network Settings**

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

**Table 5-6. Individual Server Status - IPv4 iDRAC Network Settings**

<b>Item</b>	<b>Description</b>
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 will always have 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 5-7. Individual Server Status - IPv6 iDRAC Network Settings**

<b>Item</b>	<b>Description</b>
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 will always have a unique IPv6 address over your network, and may be given up to 16 IPv6 addresses.

**Table 5-7. Individual Server Status - IPv6 iDRAC Network Settings (continued)**

Item	Description
Link Local Address	IPv6 address assigned to the CMC based upon the MAC address of the 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 5-8. 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.  <b>NOTE:</b> A green check mark in the <b>Server-Assigned</b> and <b>Chassis-Assigned</b> columns indicates the type of active addresses.  <b>NOTE:</b> 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 will be 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."



## Viewing the Health Status of IOMs

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 the 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 the CMC; an adverse condition may exist.
  - Gray - IOM is present and not powered on. It is not communicating with the 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.

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."

## 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 Graphics** section on the **Chassis Status** page or the **Fans Status** page. The **Chassis Graphics** 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.
- 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 all fans. Fan health status is indicated by the color of the fan subgraphic:
  - Green - fan is present, powered on and communicating with the CMC; there is no indication of an adverse condition.
  - Amber - fan is present, but may or may not be powered on, or may or may not be communicating with the CMC; an adverse condition may exist.
  - Gray - fan is present and not powered on. It is not communicating with the CMC and there is no indication of an adverse condition.
- 3 Use the cursor to hover over the an individual fan subgraphic and a corresponding text hint or screen tip is displayed. The text hint provides additional information on that fan.
- 4 The fan subgraphic is hyperlinked to the corresponding CMC GUI page to provide immediate navigation to the **Fans Status** page.

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.

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




- The 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.

Table 5-9 provides descriptions of the information provided on the **Fans Status** page.

**Table 5-9. 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 ( <b>Yes</b> or <b>No</b> ).
Health	 OK Indicates that the fan unit is present and communicating with the CMC. In the event of a communication failure between the CMC and the fan unit, the CMC cannot obtain or display health status for the fan unit.
	 Severe Indicates at least one Failure alert has been issued. Severe status represents a system failure on the fan unit, and <b>corrective action must be taken immediately</b> to prevent overheating and system shutdown.
	 Unknown Displayed when the chassis is first powered on. In the event of a communication failure between the CMC and the fan unit, the 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 Graphics** page.

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 the CMC; an adverse condition may exist.
  - Gray - iKVM is present and not powered on. It is not communicating with the 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 additional instructions on viewing iKVM status and setting properties for the iKVM, see:

- "Viewing the iKVM Status and Properties"
- "Enabling or Disabling the Front Panel"
- "Enabling the Dell CMC Console Through iKVM"
- "Updating the iKVM Firmware"

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

## 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 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 right 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 the CMC; there is no indication of an adverse condition.
  - Amber - PSU is present, but may or may not be powered on or may or may not be communicating with the CMC; an adverse condition may exist.
  - Gray - PSU is present and not powered on. It is not communicating with the CMC and 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.




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."

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.

Table 5-10 and Table 5-11 provide descriptions of the information provided on the **Power Supply Status** page.

**Table 5-10. Power Supply Health Status Information**

Item	Description	
Name	Displays the name of the PSU: PS- <i>n</i> , where <i>n</i> is the power supply number.	
Present	Indicates whether the power supply is present ( <b>Yes</b> or <b>No</b> ).	
Health	 OK	Indicates that the PSU is present and communicating with the CMC. Indicates that the health of the PSU is OK. In the event of a communication failure between the CMC and the fan unit, the CMC cannot obtain or display health status for the PSU.
	 Severe	Indicates that the PSU has a failure and the health is critical. <b>Corrective action must be taken immediately.</b> 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 the CMC and the PSU, the CMC cannot obtain or display health status for the PSU.
Power Status	Indicates the power state of the PSU: <b>Online</b> , <b>Off</b> , or <b>Slot Empty</b> .	
Capacity	Displays the power capacity in watts.	

**Table 5-11. System Power Status**

<b>Item</b>	<b>Description</b>
Overall Power Health	Indicates the health status ( <b>OK, Non-Critical, Critical, Non-Recoverable, Other, Unknown</b> ) of the power management for the entire chassis.
System Power Status	Displays the power status ( <b>On, Off, Powering On, Powering Off</b> ) of the chassis.
Redundancy	Indicates the power supply redundancy status. Values include: <b>No:</b> Power Supplies are not redundant. <b>Yes:</b> Full Redundancy in effect.

### **Viewing Status of the Temperature Sensors**

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






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

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 Information** page displays.

Table 5-12 provides descriptions of the information provided on the **Temperature Sensors Information** page.

**Table 5-12. Temperature Sensors Health Status Information**

Item	Description	
ID	Displays the numeric ID of the temperature probe.	
Name	Displays the name of each temperature probe on the chassis, servers, IOMs, and iKVM. Examples: Ambient Temp, Server 1 Temp, I/O Module 1, iKVM Temp.	
Present	Indicates whether the sensor is present (Yes) or absent (No) in the chassis.	
Health	 OK	Indicates that the temperature probe unit is present and communicating with the CMC. Indicates that the health of the temperature probe unit is OK.
	 Severe	Indicates that the temperature sensor has a failure and the health is critical. <b>Corrective action must be taken immediately.</b>
	 Unknown	Displayed with the chassis is first powered on. In the event of a communication failure between the CMC and the temperature probe unit, the CMC cannot obtain or display health status for the temperature probe.
Reading	Indicates the current temperature in degrees Centigrade and Fahrenheit.	
Threshold Maximum	Indicates the highest temperature, in degrees Centigrade and Fahrenheit, at which a Failure alert is issued.	
Threshold Minimum	Indicates the lowest temperature, in degrees Centigrade and Fahrenheit, at which a Failure alert is issued.	



# 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" 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 will be 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 the CMC


Before you begin configuring the CMC, you must first configure the CMC network settings to allow the CMC to be managed remotely. This initial configuration assigns the TCP/IP networking parameters that enable access to the CMC.


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

- 1 Log in to the Web interface.
- 2 Select **Chassis** in the system tree.
- 3 Click the **Network/Security** tab. The **Network Configuration** page appears.
- 4 Enable or disable DHCP for the CMC by selecting or clearing the **Use DHCP (For CMC NIC 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:** To perform the following steps, you must have **Chassis Configuration Administrator** privilege.

 **NOTE:** The settings on the **Network Configuration** page, 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 (primary 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 primary CMC.

- 1 Log in to the Web interface.
- 2 Click the **Network/Security** tab.

- 3 Configure the CMC network settings described in Table 5-13 through Table 5-15.
- 4 Click **Apply Changes**.

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

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

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

**Table 5-13. Network Settings**

<b>Setting</b>	<b>Description</b>
CMC MAC Address	Displays the chassis' MAC address, which is a unique identifier for the chassis over the computer network.
Enable CMC NIC	<p>Enables the NIC of the CMC.</p> <p><b>Default:</b> Enabled. If this option is checked:</p> <ul style="list-style-type: none"> <li>• The CMC communicates with and is accessible over the computer network.</li> <li>• The Web interface, CLI (remote RACADM), WSMAN, Telnet, and SSH associated with the CMC are available.</li> </ul> <p>If this option is not checked:</p> <ul style="list-style-type: none"> <li>• The CMC NIC cannot communicate over the network.</li> <li>• Communication to the chassis through CMC is not available.</li> <li>• The Web interface, CLI (remote RACADM), WSMAN, Telnet, and SSH associated with the CMC are not available.</li> <li>• The server iDRAC Web interface, local CLI, I/O modules, and iKVM are still accessible.</li> <li>• Network addresses for the iDRAC and CMC can be obtained, in this case, from the chassis' LCD.</li> </ul> <p><b>NOTE:</b> Access to the other network-accessible components in the chassis is not affected when the network on the chassis is disabled (or lost).</p>

**Table 5-13. Network Settings (continued)**

<b>Setting</b>	<b>Description</b>
Register CMC on DNS	This property registers the CMC name on the DNS Server. <b>Default:</b> Unchecked (disabled) by default <b>NOTE:</b> Some DNS Servers will only register names of 31 characters or fewer. Make sure the designated name is within the DNS required limit.
DNS CMC Name	Displays the CMC name only when <b>Register CMC on DNS</b> is selected. The default CMC name is <i>CMC_service_tag</i> , where <i>service tag</i> is the service tag number 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 <b>Use DHCP (For NIC IP Address)</b> is selected. <b>Default:</b> Enabled
DNS Domain Name	The default DNS Domain Name is a blank character. This field can be edited only when the <b>Use DHCP for DNS Domain Name</b> check box is selected.
Auto Negotiation (1 Gb)	Determines whether the CMC automatically sets the duplex mode and network speed by communicating with the nearest router or switch ( <b>On</b> ) or allows you to set the duplex mode and network speed manually ( <b>Off</b> ). <b>Default:</b> On <b>If Auto Negotiation is On,</b> CMC automatically communicates with the nearest router or switch and operates at 1 Gb speed. <b>If Auto Negotiation is Off,</b> you must set the duplex mode and network speed manually.

**Table 5-13. 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><b>NOTE:</b> 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. <b>Determine whether your network supports the above network speeds and set it accordingly.</b> If your network configuration does not match any of these values, Dell recommends that you use <b>Auto Negotiation</b> or refer to your network equipment manufacturer.</p> <p><b>NOTE:</b> To use 1000 Mb or 1 Gb speeds, select <b>Auto Negotiation</b>.</p>
Duplex Mode	<p>Set the duplex mode to full or half to match your network environment.</p> <p><b>Implications:</b> If <b>Auto Negotiation</b> 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 will result in a slow network connection.</p> <p><b>NOTE:</b> 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><b>Configuration range:</b> 576–1500.</p> <p><b>Default:</b> 1500.</p> <p><b>NOTE:</b> IPv6 requires a minimum MTU of 1280. If IPv6 is enabled, and <b>cfgNetTuningMtu</b> is set to a lower value, the CMC will use an MTU of 1280.</p>

**Table 5-14. IPv4 Settings**

<b>Setting</b>	<b>Description</b>
Enable IPv4	Allow the 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 the 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, the CMC retrieves IPv4 configuration (IP Address, subnet mask, and gateway) automatically from a DHCP server on your network. The CMC will always have a unique IP Address allotted over your network.</p> <p><b>NOTE:</b> When this feature is enabled, the <b>Static IP Address, Static Subnet Mask, and Static Gateway</b> property fields (located immediately following this option on the <b>Network Configuration</b> 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 <b>Static IP Address, Static Subnet Mask, and Static Gateway</b> in the text fields immediately following this option in the <b>Network Configuration</b> page.</p>
Static IP Address	Specifies the IPv4 address for the CMC NIC.
Static Subnet Mask	Specifies the static IPv4 subnet mask for the CMC NIC.
Static Gateway	<p>Specifies the IPv4 gateway for the CMC NIC.</p> <p><b>NOTE:</b> The <b>Static IP Address, Static Subnet Mask, and Static Gateway</b> fields are active only if <b>DHCP Enable</b> (the property field preceding these fields) is disabled (unchecked). In that case, you must manually type the <b>Static IP Address, Static Subnet Mask, and Static Gateway</b> for the CMC to use over the network.</p> <p><b>NOTE:</b> The <b>Static IP Address, Static Subnet Mask, and Static Gateway</b> 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 5-14. IPv4 Settings (continued)**

<b>Setting</b>	<b>Description</b>
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><b>NOTE:</b> If <b>Use DHCP (For NIC IP Address)</b> is enabled, then enable the <b>Use DHCP to Obtain DNS Server Addresses</b> property.</p> <p>If this option is checked, the CMC retrieves its DNS IP address automatically from a DHCP server on your network.</p> <p><b>NOTE:</b> 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 <b>not</b> selected, the 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 <b>Network Configuration</b> page.</p>
Static Preferred DNS Server	<p>Specifies the static IP address for the preferred DNS Server. The Static Preferred DNS Server is implemented only when <b>Use DHCP to Obtain DNS Server Addresses</b> is disabled.</p>
Static Alternate DNS Server	<p>Specifies the static IP address for the alternate DNS Server. The Static Alternate DNS Server is implemented only when <b>Use DHCP to obtain DNS Server addresses</b> is disabled. If you do not have an alternate DNS Server, type an IP address of 0.0.0.0.</p>

**Table 5-15. IPv6 Settings**

<b>Setting</b>	<b>Description</b>
Enable IPv6	Allows the 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 the CMC to use the IPv6 protocol to obtain IPv6 related address and gateway settings from an IPv6 router configured to provide this information. The CMC will then have a unique IPv6 address on your network. Default: Checked (enabled)</p> <p><b>NOTE:</b> When this feature is enabled, the <b>Static IPv6 Address</b>, <b>Static Prefix Length</b>, and <b>Static Gateway</b> property fields (located immediately following this option on the <b>Network Configuration</b> 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 <b>Network Configuration</b> page.</p>
Static IPv6 Address	Specifies the IPv6 address for the CMC NIC when Autoconfiguration is not enabled.
Static Prefix Length	Specifies the IPv6 prefix length for the CMC NIC when Autoconfiguration is not enabled.
Static Gateway	<p>Specifies the static IPv6 gateway for the CMC NIC when Autoconfiguration is not enabled.</p> <p><b>NOTE:</b> The <b>Static IPv6 Address</b>, <b>Static Prefix Length</b>, and <b>Static Gateway</b> fields are active only if <b>AutoConfiguration Enable</b> (the property field preceding these fields) is disabled (unchecked). In that case, you must manually type the <b>Static IPv6 Address</b>, <b>Static Prefix Length</b>, and <b>Static Gateway</b> for the CMC to use over the IPv6 network.</p> <p><b>NOTE:</b> The <b>Static IPv6 Address</b>, <b>Static Prefix Length</b>, and <b>Static Gateway</b> 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 5-15. 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 <b>Use DHCP to Obtain DNS Server Addresses</b> 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 <b>Use DHCP to Obtain DNS Server Addresses</b> 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/Security** 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 5-16 describes the **settings** on the **Network Security** page.



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

**Table 5-16. Network Security Page Settings**

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

**Table 5-16. 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 the 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><b>NOTE:</b> 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/Security** 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 5-17 describes the **settings** on the **Network Security** page.

**Table 5-17. 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**→**Servers**→**Setup** tab→**VLAN** subtab.

## Adding and Configuring CMC Users

To manage your system with the 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 Active Directory users. iDRAC users can also be local users or Active Directory 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 User Configuration Administrator must log into the server directly. The User Configuration Administrator cannot create a server user from CMC or vice versa. This rule protects the security and integrity of the servers.

Table 5-18, Table 5-19, and Table 5-20 describe CMC user privileges (local or Active Directory), and what operations a CMC user can execute on the chassis and on the servers based on the privileges he is granted. The term user or users, therefore, should be understood as CMC users. Server users will be explicitly specified.

**Table 5-18. User Types**

<b>Privilege</b>	<b>Description</b>
<b>CMC Login User</b>	<p>Users who have the <b>CMC Login User</b> privilege can log in to CMC. A user with only the login privilege can view all of the CMC data but cannot add or modify data or execute commands.</p> <p>It is possible for a user to have other privileges without the login privilege. This feature is useful when a user is temporarily disallowed to login. When that user's login privilege is restored, the user retains all the other privileges previously granted.</p>
<b>Chassis Configuration Administrator</b>	<p>Users who have the Chassis Configuration Administrator privilege can add or change data that:</p> <ul style="list-style-type: none"><li>• Identifies the chassis, such as chassis name and chassis location</li><li>• Is assigned specifically to the chassis, such as IP mode (static or DHCP), static IP address, static gateway, and static subnet mask</li><li>• Provides services to the chassis, such as date and time, firmware update, and CMC reset.</li><li>• 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.</li></ul> <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>
<b>User Configuration Administrator</b>	<p>Users who have the User Configuration Administrator privilege can:</p> <ul style="list-style-type: none"><li>• Add a new user</li><li>• Delete an existing user</li><li>• Change a user's password</li><li>• Change a user's privileges</li><li>• Enable or disable a user's login privilege but retain the user's name and other privileges in the database.</li></ul>
<b>Clear Logs Administrator</b>	<p>CMC users who have the Clear Administrator privilege can clear the hardware log and CMC log.</p>


**Table 5-18. User Types (continued)**

<b>Privilege</b>	<b>Description</b>
<b>Chassis Control Administrator (Power Commands)</b>	<p>CMC users with the Chassis Power Administrator privilege can perform all power-related operations:</p> <ul style="list-style-type: none"><li>• Control chassis power operations, including power on, power off, and power cycle.</li></ul>
<b>Server Administrator</b>	<p>The Server Administrator privilege is a blanket privilege granting a CMC user all rights to perform any operation on any servers present in the chassis.</p> <p>When a user with CMC 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 CMC Server Administrator privilege overrides any lack of administrator privileges on the server.</p> <p>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 style="list-style-type: none"><li>• The same user name exists on the server</li><li>• The same user name must have the exact same password on the server</li><li>• The user must have the privilege to execute the command</li></ul> <p>When a CMC user who does not have Server Administrator privilege issues an action to be performed on a server, the CMC will send 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> <p>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>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 5-18. User Types (continued)**

<b>Privilege</b>	<b>Description</b>
Server Administrator (continued)	Server Configuration Administrator: <ul style="list-style-type: none"><li>• Set IP address</li><li>• Set gateway</li><li>• Set subnet mask</li><li>• Set first boot device</li></ul> User Configuration Administrator: <ul style="list-style-type: none"><li>• Set iDRAC root password</li><li>• iDRAC reset</li></ul> Server Control Administrator: <ul style="list-style-type: none"><li>• Power on</li><li>• Power off</li><li>• Power cycle</li><li>• Graceful shutdown</li><li>• Server Reboot</li></ul>
Test Alert User	CMC users who have the Test Alert User privilege can send test alert messages.
Debug Command Administrator	CMC users who have the Debug Administrator privilege can execute system diagnostic commands.
Fabric A Administrator	CMC users who have the Fabric A Administrator privilege 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	CMC users who have the Fabric B Administrator privilege 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	CMC users who have the Fabric C Administrator privilege can set and configure the Fabric C IOM, which resides in either slot C1 or slot C2 of the I/O slots.

The CMC user groups provide a series of user groups that have pre-assigned user privileges. The privileges are listed and described in Table 5-18. The following table lists the user groups and the pre-defined 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 5-19. CMC Group Privileges**

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



**Table 5-19. CMC Group Privileges (continued)**

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

**Table 5-20. 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 5-20. 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 the Microsoft® Active Directory® service software, you can configure Active Directory to provide access to the CMC. Active Directory configuration would allow 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 With Microsoft Active Directory" on page 207.

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, Dell strongly recommends that you change the default password of the root (User 1) account. The root account is the default administrative account that ships with the 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 **User Configuration Administrator** privilege to perform the following steps.

- 1 Log in to the Web interface.
- 2 Click the **Network/Security** tab, and then click the **Users** sub-tab. The **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 will 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 5-21 describes the **General** settings for configuring a new or existing CMC username and password.

**Table 5-21. General User Settings**

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 the CMC.

**Table 5-21. General User Settings (continued)**

<b>Property</b>	<b>Description</b>
<b>User Name</b>	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. <b>NOTE:</b> 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 will be able to see the change immediately.
<b>Change Password</b>	Allows an existing user's password to be changed. Set the new password in the <b>New Password</b> field.  The <b>Change Password</b> check box is not selectable if you are configuring a new user. You can select it only when changing an existing user setting.
<b>Password</b>	Sets a new password for an existing user. To change the password, you must also select the <b>Change Password</b> check box. The password can contain up to 20 characters, which display as dots as you type.
<b>Confirm Password</b>	Verifies the password you entered in the <b>New Password</b> field. <b>NOTE:</b> The <b>New Password</b> and <b>Confirm New Password</b> fields are editable only when you are (1) configuring a new user; or (2) editing the settings for an existing user, and the <b>Change Password</b> check box is selected.

- 5 Assign the user to a CMC user group. Table 5-18 describes CMC user privileges. Table 5-19 describes the **user group permissions** for the **CMC User Privileges** settings. Table 5-20 provides a comparison of privileges between Administrators, Power Users, and Guest Users.

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 the 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 With Microsoft Active Directory" on page 207.

You can use the Microsoft Active Directory service to configure your software to provide access to the 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 **Network/Security** tab, and then click the **Active Directory** sub-tab. The **Active Directory Main Menu** page appears.

Table 5-22 lists the Active Directory Main Menu page options.


**Table 5-22. Active Directory Main Menu Page Options**


<b>Field</b>	<b>Description</b>
Configure	Configure and manage the following Active Directory settings for CMC: CMC Name, ROOT Domain Name, CMC Domain Name, Active Directory Authentication Timeout, Active Directory Schema Selection (Extended or Standard), and Role Group settings.
Upload AD Certificate	Upload a certificate authority-signed certificate for Active Directory to the CMC. This certificate, which you obtain from Active Directory, grants access to the CMC.
Download Certificate	Downloads a CMC server certificate to your management station or shared network using Windows Download Manager. When you select this option and click <b>Next</b> , a <b>File Download</b> dialog box appears. Use this dialog box to specify a location on your management station or shared network for the server certificate.

**Table 5-22. Active Directory Main Menu Page Options (continued)**

Field	Description
View Certificate	Displays the certificate authority-signed server certificate for Active Directory that has been uploaded to the CMC. <b>NOTE:</b> 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.
Upload Kerberos Keytab	Uploads a Kerberos Keytab for Active Directory to the CMC. You can generate the Kerberos Keytab from the Active Directory Server by executing the <code>ktpass.exe</code> utility. This keytab establishes a trust relationship between the Active Directory Server and the CMC. <b>NOTE:</b> The CMC does not have a Kerberos Keytab for Active Directory. You must upload a currently generated Kerberos Keytab. See "Configuring Single Sign-On" for detailed information.

### Configuring Active Directory (Standard Schema and Extended Schema)

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

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

- 1 Ensure that all Secure Socket Layer (SSL) certificates for the Active Directory servers are signed by the same certificate authority and have been uploaded to the CMC.
- 2 Log in to the Web interface and navigate to the **Active Directory Main Menu**.
- 3 Select **Configure**, and then click **Next**. The **Active Directory Configuration and Management** page displays.
- 4 Select the **Enable Active Directory** check box under the **Common Settings** heading.
- 5 Type the required information into the remaining fields. See Table 5-23.

**Table 5-23. Active Directory Common Settings Properties**

<b>Setting</b>	<b>Description</b>
Root Domain Name	<p>Specifies the domain name used by Active Directory. The root domain name is the fully qualified root domain name for the forest.</p> <p><b>NOTE:</b> The root domain name must be a valid domain name using the <i>x.y</i> naming convention, where <i>x</i> is a 1–256 character ASCII string with no spaces between characters, and <i>y</i> is a valid domain type such as com, edu, gov, int, mil, net, or org.</p> <p><b>Default:</b> null (empty)</p>
AD Timeout	<p>The time in seconds to wait for Active Directory queries to complete. The minimum value is equal to or greater than 15 seconds.</p> <p><b>Default:</b> 120 seconds</p>
Specify AD Server to search (Optional)	<p>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.</p> <p><b>NOTE:</b> The name on the Active Directory CA Certificate will not be matched against the specified Active Directory server or the Global Catalog server.</p>
Domain Controller	<p>Specifies the server where your Active Directory service is installed.</p> <p>This option is valid only if <b>Specify AD Server to search (OPTIONAL)</b> is enabled.</p>
Global Catalog	<p>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.</p> <p>This option is valid only if <b>Specify AD Server to search (OPTIONAL)</b> is enabled.</p>

- 6 Select an Active Directory schema under the Active Directory Schema Selection heading. See Table 5-24.
- 7 If you selected **Extended Schema**, type the following required information in the Extended Schema Settings section, and then proceed directly to step 9. If you selected Standard Schema, proceed to step 8.
  - **CMC Device Name** – The name that 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 name must be a 1–256 character ASCII string with no spaces between characters. Default: null (empty).
  - **CMC Domain Name** – The DNS name (string) of the domain where the Active Directory CMC object resides (example: cmc.com). 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. Default: null (empty).



**NOTE:** Do not use the NetBIOS name. The CMC Domain Name is the fully qualified domain name of the sub-domain where the CMC Device Object is located.


**Table 5-24. Active Directory Schema Options**

Setting	Description
Use Standard Schema	<p>Uses Standard Schema with Active Directory, which uses Active Directory group objects only.</p> <p>Before configuring CMC to use the Active Directory Standard Schema option, you must first configure the Active Directory software:</p> <ol style="list-style-type: none"> <li>1 On an Active Directory server (domain controller), open the Active Directory Users and Computers Snap-in.</li> <li>2 Create a group or select an existing group. The name of the group and the name of this domain must be configured on the CMC either with the Web interface or RACADM.</li> </ol>



**Table 5-24. Active Directory Schema Options (continued)**


<b>Setting</b>	<b>Description</b>
Use <b>Extended Schema</b>	Uses Extended Schema with Active Directory, which uses Dell-defined Active Directory objects.  Before configuring CMC to use the Active Directory Extended Schema option, you must first configure the Active Directory software: <ol style="list-style-type: none"><li>1 Extend the Active Directory schema.</li><li>2 Extend the Active Directory Users and Computers Snap-in.</li><li>3 Add CMC users and their privileges to Active Directory.</li><li>4 Enable SSL on each of your domain controllers.</li><li>5 Configure the CMC Active Directory properties using either the CMC Web interface or the RACADM.</li></ol>

- 8 If you selected Standard Schema, type the following information in the Standard Schema Settings section. If you selected Extended Schema, proceed to step 9.
  - **Role Groups** – The role groups associated with the CMC. To change the settings for a role group, click the role group number in the Role Groups list. The **Configure Role Group** page displays.  
 **NOTE:** If you click a role group link prior to applying any new settings you have made, you will lose those settings. To avoid losing any new settings, click **Apply** before clicking a role group link.
  - **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.
- 9 Click **Apply** to save the settings.

To refresh the contents of the **Active Directory Configuration and Management** page, click **Refresh**.

To print the contents of the **Active Directory Configuration and Management** page, click **Print**.


To configure the Role Groups for Active Directory, click the individual Role Group (1–5). See Table 5-19 and Table 5-18.

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

### **Uploading an Active Directory Certificate Authority-Signed Certificate**

From the **Active Directory Main Menu** page:

- 1 Select **Upload AD Certificate**, 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.


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

- 3 Click **Apply**. If the certificate is invalid, an error message displays.

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

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

### **Viewing an Active Directory Certificate Authority-Signed Certificate**

 **NOTE:** If you uploaded an Active Directory server certificate on the CMC, make sure the certificate is still valid and has not expired.

From the **Active Directory Main Menu** page:

- 1 Select **View Certificate**, and then click **Next**.
- 2 Click the appropriate **View Active Directory CA Certificate** page button to continue.

**Table 5-16. Active Directory CA Certificate Information**

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

- 3 To refresh the contents of the **View Active Directory CA Certificate** page, click **Refresh**.  
To print the contents of the **View Active Directory CA Certificate** page, click **Print**.

## 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)

The 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. The 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 the 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 the 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/Security** tab, and then click the **SSL sub-tab**. 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, Dell strongly recommends that you obtain and upload a secure server certificate to the 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, the CMC is vulnerable to access from unauthorized users.

**Table 5-17. SSL Main Menu Options**

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

**Table 5-17. SSL Main Menu Options (continued)**

Field	Description
Upload Webserver key and Certificate	Select this option and click <b>Next</b> to open the <b>Webserver Key and Certificate Upload</b> 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 the CMC.  <b>NOTE:</b> Only X.509, Base64 encoded certificates are accepted by the 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 <b>Next</b> button to open the <b>View Server Certificate</b> page where you can view the current server certificate.

To obtain a secure server certificate for the 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 the 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 the CMC.



**NOTE:** For the 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 the CMC when the CSR was generated.



**CAUTION:** When a new CSR is generated, it overwrites any previous CSR on the CMC. If a pending CSR is overwritten before its server certificate is granted from a certificate authority, the CMC will 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.  
Table 5-18 describes the **Generate Certificate Signing Request (CSR)** page options.
- 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 will later submit this file to a certificate authority.

**Table 5-18. Generate Certificate Signing Request (CSR) Page Options**

<b>Field</b>	<b>Description</b>
<b>Common Name</b>	<p>The exact name being certified (usually the Web server's domain name, for example, <b>www.xyzcompany.com/</b>).</p> <p><b>Valid:</b> Alphanumeric characters (A–Z, a–z, 0–9); hyphens, underscores, and periods.</p> <p><b>Not valid:</b> Non-alphanumeric characters not noted above (such as, but not limited to, @ # \$ % &amp; *); characters used primarily in non-English languages, such as ß, â, é, ü.</p>
<b>Organization Name</b>	<p>The name associated with your organization (example: <b>XYZ Corporation</b>).</p> <p><b>Valid:</b> Alphanumeric characters (A–Z, a–z, 0–9); hyphens, underscores, periods, and spaces.</p> <p><b>Not valid:</b> Non-alphanumeric characters not noted above (such as, but not limited to, @ # \$ % &amp; *).</p>
<b>Organization Unit</b>	<p>The name associated with an organizational unit, such as a department (example: <b>Enterprise Group</b>).</p> <p><b>Valid:</b> Alphanumeric characters (A–Z, a–z, 0–9); hyphens, underscores, periods, and spaces.</p> <p><b>Not valid:</b> Non-alphanumeric characters not noted above (such as, but not limited to, @ # \$ % &amp; *).</p>

**Table 5-18. Generate Certificate Signing Request (CSR) Page Options (continued)**

<b>Field</b>	<b>Description</b>
<b>Locality</b>	<p>The city or other location of your organization (examples: <b>Atlanta, Hong Kong</b>).</p> <p><b>Valid:</b> Alphanumeric characters (A–Z, a–z, 0–9) and spaces.</p> <p><b>Not Valid:</b> Non-alphanumeric characters not noted above (such as, but not limited to, @ # \$ % &amp; *).</p>
<b>State</b>	<p>The state, province, or territory where the entity that is applying for a certification is located (examples: <b>Texas, New South Wales, Andhra Pradesh</b>).</p> <p><b>NOTE:</b> Do not use abbreviations.</p> <p><b>Valid:</b> Alphanumeric characters (upper- and lower-case letters; 0–9); and spaces.</p> <p><b>Not valid:</b> Non-alphanumeric characters not noted above (such as, but not limited to, @ # \$ % &amp; *).</p>
<b>Country</b>	<p>The country where the organization applying for certification is located.</p>
<b>Email</b>	<p>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: <b>name@xyzcompany.com</b>).</p> <p><b>NOTE:</b> This e-mail address is an optional field.</p>

## Uploading a Server Certificate

- 1 From the **SSL Main Menu** page, select **Upload Server Certificate**, 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**.



## 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 5-19 describes the fields and associated descriptions listed in the **Certificate** window.

**Table 5-19. Certificate Information**

<b>Field</b>	<b>Description</b>
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 terminate a session:


- 1 Log into the CMC through the Web.
- 2 Click the **Network/Security** tab then click the **Sessions** sub-tab.
- 3 On the **Sessions** page, locate the session you want to terminate and click the trash can icon.

To manage sessions:

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

- 3 Click the **Network/Security** tab.
- 4 Click the **Sessions** sub-tab. The **Sessions** page appears.

**Table 5-20. Sessions Properties**

<b>Property</b>	<b>Description</b>
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 trash can icon  . This column is displayed only if you have <b>Chassis Configuration Administrator</b> privileges.


To terminate the session, click the trash can icon on the line that describes the session.


## Configuring Services

The 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 the 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; the 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/Security** tab.
- 3 Click the **Services** sub-tab. The **Services** page appears.
- 4 Configure the following services as required:
  - CMC serial console (Table 5-21)
  - Web server (Table 5-22)
  - SSH (Table 5-23)
  - Telnet (Table 5-24)
  - Remote RACADM (Table 5-25)
  - SNMP (Table 5-26)
  - Remote Syslog (Table 5-27)
- 5 Click **Apply**; update all default time outs and maximum time out limits.

**Table 5-21. CMC Serial Console Settings**

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

**Table 5-21. CMC Serial Console Settings (continued)**

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

**Table 5-21. CMC Serial Console Settings (continued)**

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

**Table 5-22. Web Server Settings**

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

**Table 5-22. Web Server Settings (continued)**

<b>Setting</b>	<b>Description</b>
Idle Timeout	<p>Indicates the number of seconds before an idle Web user interface session is automatically disconnected. A change to the <b>Timeout</b> setting takes effect at the next login; it does not affect the current session.</p> <p><b>Timeout range:</b> 60 to 10800 seconds.</p> <p><b>Default:</b> 1800 seconds</p>
HTTP Port Number	<p>Indicates the default port used by the CMC that listens for a server connection.</p> <p><b>NOTE:</b> 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://&lt;IP address&gt;:&lt;port number&gt;</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><b>Configuration range:</b> 10–65535</p> <p><b>Default:</b> 80</p>
HTTPS Port Number	<p>Indicates the default port used by the 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://&lt;IP address&gt;:&lt;port number&gt;</code></p> <p>where <i>&lt;IP address&gt;</i> is the IP address for the chassis, and <i>&lt;port number&gt;</i> is the HTTPS port number other than the default of 443.</p> <p><b>Configuration range:</b> 10–65535</p> <p><b>Default:</b> 443</p>

**Table 5-23. SSH Settings**

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

**Table 5-24. Telnet Settings**

<b>Setting</b>	<b>Description</b>
Enabled	Enables Telnet console interface on the CMC. <b>Default:</b> Unchecked (disabled)
Max Sessions	Indicates 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). <b>Allowed range:</b> 1–4 <b>Default:</b> 4 <b>NOTE:</b> 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.
Idle Timeout	Indicates 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. <b>Timeout Range:</b> 0 or 60–10800 seconds. To disable the Timeout feature, enter 0. <b>Default:</b> 1800 seconds
Port Number	Indicates the port used by the CMC that listens for a server connection. <b>Default:</b> 23



**Table 5-25. Remote RACADM Settings**

<b>Setting</b>	<b>Description</b>
Enabled	Enables the remote RACADM utility access to the CMC. <b>Default:</b> Checked (enabled)
Max Sessions	Indicates 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 <b>Active Sessions</b> (including your own). <b>Allowed range:</b> 1–4 <b>Default:</b> 4 <b>NOTE:</b> 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.
Idle Timeout	Indicates 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. <b>Timeout Range:</b> 0, or 10 to 1920 seconds. To disable the Timeout feature, enter 0. <b>Default:</b> 30 seconds

**Table 5-26. SNMP Configuration**

<b>Setting</b>	<b>Description</b>
Enabled	Enables SNMP on the CMC. <b>Legal Values:</b> Checked (enabled), unchecked (disabled) <b>Default:</b> unchecked (disabled)
Community Name	Indicates the community string used to get data from CMC's SNMP daemon.

**Table 5-27. Remote Syslog Configuration**

<b>Setting</b>	<b>Description</b>
Enabled	Enables the transmission and remote capture of the System Log on the specified server(s). <b>Legal Values:</b> Checked (enabled), unchecked (disabled) <b>Default:</b> unchecked (disabled)
Syslog Server 1	The first of three possible servers to host a copy of the syslog. Specified as a hostname, an IPv6 address, or an IPv4 address.
Syslog Server 2	The second of three possible servers to host a copy of the syslog. Specified as a hostname, an IPv6 address, or an IPv4 address.
Syslog Server 3	The third of three possible servers to host a copy of the syslog. Specified as a hostname, an IPv6 address, or an IPv4 address.
Syslog Port Number	Specifies the port number on the remote server for receiving a copy of the syslog. The same port number is used for all three servers. A valid syslog port number is in the 10-65535 range. <b>Default:</b> 514

## Configuring Power Budgeting

The 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 the CMC, see "Configuring and Managing Power" on page 263.

For more information on the CMC's power management service, see "Power Management" on page 247.

# Managing Firmware Updates

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

- CMC - primary and standby.
- iKVM
- iDRAC
- IOM infrastructure devices

When you update firmware, follow the recommended process to prevent a loss of service if the update fails. See "Installing or Updating the CMC Firmware" for guidelines to follow before using the instructions in this section.

## Viewing the Current Firmware Versions




The **Update** page displays the current version of all the components in the chassis that can be updated. These may include the iKVM firmware, primary CMC firmware, (if applicable) the standby CMC firmware, the iDRAC firmware, and the IOM infrastructure device firmware; see "Updating the IOM Infrastructure Device Firmware" for additional details. Clicking on either the device name or the **Select/Deselect All** check box and then the **Apply Update** button will display an update page for the selected devices.

If the chassis contains an earlier generation server whose iDRAC is in recovery mode or if the CMC detects that an iDRAC has corrupted firmware, then the earlier generation iDRAC is also listed on the **Updatable Components** page. See "Recovering iDRAC Firmware Using the CMC" for the steps to recover iDRAC firmware using the CMC.

To view the components that can be updated:


- 1 Log in to the Web interface (see "Accessing the CMC Web Interface").
- 2 Click **Chassis** in the system tree.
- 3 Click the **Update** tab. The **Updatable Components** page appears.

## Updating Firmware




-  **NOTE:** To update firmware on the 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."


The **Updatable Components** 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.


## Updating the CMC Firmware

-  **NOTE:** During updates of the CMC firmware or the iDRAC firmware on a server, some or all of the fan units in the chassis will spin at 100%. This is normal.
-  **NOTE:** The Active (primary) CMC resets and becomes temporarily unavailable after the firmware has been uploaded successfully. If a standby CMC is present, the standby and active roles will swap; the standby (secondary) CMC becomes the active (primary) CMC. If an update is applied only to the active (primary) CMC, after the reset is complete the primary CMC will not be running the updated image, only the standby (secondary) will have that image.
-  **NOTE:** To avoid disconnecting other users during a reset, notify authorized users who might log in to the CMC and check for active sessions by viewing the **Sessions** page. To open the **Sessions** page, select **Chassis** in the tree, click the **Network/Security** tab, and then click the **Sessions** sub-tab. 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 the 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 34 for instructions.

 **NOTE:** If you experience problems downloading files from the CMC using Internet Explorer, enable the **Do not save encrypted pages to disk** option. See "Downloading Files From CMC With Internet Explorer" on page 33 for instructions.

- 1 On the **Updatable Components** page, select the CMC or CMCs to update by selecting the **Update Targets** check box for the 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**. The 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 items to note:
  - 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 the CMC.

- 5 For a standby (secondary) CMC, when the update is complete the Update State field displays "Done". For an active (primary) CMC, during the final phases of the firmware update process, the browser session and connection with the CMC will be lost temporarily as the active (primary) CMC is taken off line. You must log in again after a few minutes, when the active (primary) CMC has rebooted.


After the CMC resets, the new firmware is displayed on the **Updatable Components** 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 the CMC Web interface.
- 2 Select **Chassis** in the system tree.
- 3 Click the **Update** tab. The **Updatable Components** 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.

- 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 items to note:

- 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 **Updatable Components** 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 the 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 the CMC do not match.

- 1 Log back in to the CMC Web interface.
- 2 Select **Chassis** in the system tree.
- 3 Click the **Update** tab. The **Updatable Components** 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 the CMC. The CMC firmware should be updated first, before updating IOMINF firmware.

IOMINF updates are allowed by the CMC if it detects that the IOMINF firmware is out-of-date with the image contained in the CMC file system. If the IOMINF firmware is up-to-date, the CMC will prevent IOMINF updates. Up-to-date IOMINF devices are 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 items to note:
  - 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 restarts when the update is complete.


When the update is complete, the new firmware is displayed on the **Updatable Components** page and the updated system will no longer be present on that page.

### Updating the Server iDRAC Firmware

 **NOTE:** The iDRAC (on a Server) will reset 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** in the system tree.
- 3 Click the **Update** tab. The **Updatable Components** 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 items to note:
  - 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 the CMC or server.



## Recovering iDRAC Firmware Using the 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](http://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 newly-updated iDRAC firmware process. When the CMC detects corrupted iDRAC firmware, it lists the server on the **Updatable Components** page.

Follow these steps to update the iDRAC firmware.

- 1 Download the latest iDRAC firmware to your management computer from [support.dell.com](http://support.dell.com).
- 2 Log in to the Web interface (see "Accessing the CMC Web Interface").
- 3 Click **Chassis** in the system tree.
- 4 Click the **Update** tab. The **Updatable Components** 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**.

- 8 Click **Begin Firmware Update**. Additional items to note:
  - 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

The 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 will be installed later; these default settings are the **iDRAC QuickDeploy** settings.

For more information on the iDRAC behavior, see the *iDRAC User's Guides* on the Dell Support website at [support.dell.com](http://support.dell.com).

## 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.

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

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

**Table 5-28. QuickDeploy Settings**

<b>Setting</b>	<b>Description</b>
QuickDeploy Enabled	Enables/disables the <b>QuickDeploy</b> 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. <b>NOTE:</b> This includes the root user password if the <b>Set iDRAC Root Password on Server Insertion</b> box is checked. <b>Default:</b> 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 <b>iDRAC Root Password</b> text box when the server is inserted.
iDRAC Root Password	When <b>Set iDRAC Root Password on Server Insertion</b> and <b>QuickDeploy Enabled</b> 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 <b>iDRAC Root Password</b> field.
Enable iDRAC LAN	Enables/disables the iDRAC LAN channel. <b>Default:</b> 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. <b>Default:</b> Unchecked (disabled)
Enable iDRAC DHCP	Enables/disables DHCP for each iDRAC present in the chassis. If this option is enabled, the fields <b>QuickDeploy IP</b> , <b>QuickDeploy Subnet Mask</b> , and <b>QuickDeploy Gateway</b> are disabled, and can not be modified since DHCP will be used to automatically assign these settings for each iDRAC. <b>Default:</b> Unchecked (disabled)

**Table 5-28. 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><b>NOTE:</b> 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 iDRACs 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 LAN over IPMI 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 the CMC to an 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 **Servers** 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 5-29. 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 (for the 16 available slots on the chassis), that help identify the location of the server in the chassis. <b>NOTE:</b> 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 <b>SLOT-01</b> to <b>SLOT-16</b> . <b>NOTE:</b> The slot name cannot be blank or NULL.
Enable LAN	Enables (checked) or disables (unchecked) the LAN channel. <b>NOTE:</b> When LAN is not selected (disabled), all other network configuration settings, ( <b>IPMI over LAN, DHCP, IP Address Subnet Mask</b> and <b>Gateway</b> ) are not used. These fields are not accessible.


**Table 5-29. iDRAC Network Settings (continued)**

<b>Setting</b>	<b>Description</b>
<b>Change Root Password</b>	Enables (when checked) the ability to change the password of the iDRAC root user. The <b>iDRAC Root Password</b> and <b>Confirm iDRAC Root Password</b> fields must be provided for this operation to be successful.
<b>DHCP</b>	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
<b>IPMI over LAN</b>	Enables (checked) or disables (unchecked) the IPMI LAN channel. LAN must be enabled to set this field.
<b>IP Address</b>	The static IPv4 or IPv6 address assigned to the iDRAC located in this slot.
<b>Subnet Mask</b>	Specifies the subnet mask assigned to the iDRAC installed in this slot.
<b>Gateway</b>	Specifies the default gateway assigned to the iDRAC which will be installed in this slot.
<b>Enable IPv4</b>	Enables the iDRAC in the slot to use the IPv4 protocol on the network. You must select the <b>Enable LAN</b> option for this option to be active. Default setting is enabled.
<b>Enable IPv6</b>	Enables the iDRAC in the slot to use the IPv6 protocol on the network. You must select the <b>Enable LAN</b> option and deselect the <b>Autoconfiguration</b> option for this option to be active. Default setting is disabled. <b>NOTE:</b> This option is available only if the server is IPv6 capable.
<b>Autoconfiguration</b>	Enables the iDRAC to obtain IPv6 settings (Address and prefix length) from a DHCPv6 server and also enables stateless address auto configuration. <b>NOTE:</b> This option is available only if the server is IPv6 capable.
<b>Prefix Length</b>	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 will also be saved.
- 7 To restore the iDRAC Network settings to the current values for each installed blade, 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 blades 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 the CMC to an iDRAC. Pressing the **Refresh** button too soon may display only partially correct data for a one or more iDRAC servers.

## Launching iDRAC using Single Sign-On

The CMC provides limited management of individual chassis components, such as servers. For complete management of these individual components, the 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, use the following steps:

- 1 Log in to the CMC Web interface.
- 2 Select **Servers** in the system tree. The **Servers Status** page appears.
- 3 Click the **Launch iDRAC GUI** icon 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 **Servers** 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** icon.



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, will automatically be 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 will automatically be 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, will **NOT** be 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, will not be 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 will be 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](http://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."

## 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 blade.

Use the following steps to view whether FlexAddress is active for the chassis:

- 1 Log in to the Web interface (see "Accessing the CMC Web Interface").
- 2 Click **Chassis** in the system tree.
- 3 Click the **Setup** tab. The **General Setup** page appears. The FlexAddress entry will have 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.

Use the following steps to display a FlexAddress status overview for each server module:

- 1 Log in to the Web interface (see "Accessing the CMC Web Interface").
- 2 Click **Servers** in the system tree. Click the **Properties** tab, **WWN/MAC** sub-tab.
- 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:

---

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

---

- 4 For additional information, click the **Help** link and review "Using FlexAddress."

## 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 blade.

Use the following steps to view FlexAddress server information:

- 1 Log in to the Web interface (see "Accessing the CMC Web Interface" on page 97).
- 2 Expand **Servers** 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** sub-tab. The **FlexAddress Status** 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:

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"><li>• <b>Chassis-Assigned</b> - 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.</li><li>• <b>Server-Assigned</b> - server uses the server-assigned address or the default address embedded into the controller hardware.</li></ul>
Power State	Displays the current power status of the servers; values are: <b>On</b> , <b>Powering On</b> , <b>Powering Off</b> , <b>Off</b> , and <b>N/A</b> (if a server is not present).

Health		OK	Indicates that FlexAddress is present and providing status to the CMC. In the event of a communication failure between the CMC and FlexAddress, the CMC cannot obtain or display health status for FlexAddress.
		Informational	Displays information about FlexAddress when no change in health status (OK, Warning, Severe) has occurred.
		Warning	Indicates that only warning alerts have been issued, and <b>corrective action must be taken</b> . If corrective actions are not taken within the administrator-specified time, critical or severe failures that can affect the integrity of the server could occur.
		Severe	Indicates at least one Failure alert has been issued. Severe status represents a system failure on the server, and <b>corrective action must be taken immediately</b> .
		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 the **Help** link and review "Using FlexAddress" on page 189.

## Configuring FlexAddress

If you purchase FlexAddress with your chassis, it will be 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](http://support.dell.com) 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 will have FlexAddress enabled only on Fabric-A. All other fabrics will use the factory-assigned WWN/MAC on the server.

Selected slots will be 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 189.

## 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 will be 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").
- 2 Click **Servers** 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** section 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 will 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 blade 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 will not be enabled for the selected fabrics.

- 7 Click **Apply** to save the changes.

For additional information, click the **Help** link and review "Using FlexAddress."

## Server-Level Slot FlexAddress Configuration

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

Use the following steps 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").
- 2 Expand **Servers** 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** sub-tab. 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 the **Help** link and review "Using FlexAddress."

# Remote File Sharing

The Remote Virtual Media File Share option maps a file from a share drive on the network to one or more blades through the 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").
- 2 Click **Servers** in the system tree.
- 3 Click the **Setup** tab, and the **Remote File Sharing** sub-tab. The **Deploy Remote File Share** page is displayed.
- 4 Set the Remote File Sharing settings.

**Table 5-30. 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, type: <code>//&lt;IP to connect for CIFS file system&gt;/&lt;file path&gt;/&lt;image name&gt;</code></p> <p>To connect to NFS, type: <code>//&lt;IP to connect for NFS file system&gt;:/&lt;file path&gt;/&lt;image name&gt;</code></p> <p>File names that end with <code>.img</code> are connected as virtual floppies. File names that end with <code>.iso</code> 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>
Slot	<p>Identifies the location of the slot. Slot numbers are sequential from 1 to 16 (for the 16 available slots in the chassis).</p>




**Table 5-30. Remote File Sharing Settings (continued)**

Setting	Description
Name	Indicates 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 – The 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 5-31 lists frequently asked questions and answers.

**Table 5-31. Managing and Recovering a Remote System: Frequently Asked Questions**

Question	Answer
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 the CMC.	<p>The 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 <b>CMC default certificate</b> which does not match the host name of the CMC (for example, the IP address).</p> <p>To address this security concern, upload a CMC server certificate issued to the IP address of the 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 the 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"><li data-bbox="471 963 804 987">1 In the <b>System</b> tree, click <b>Chassis</b>.</li><li data-bbox="471 999 938 1082">2 Click the <b>Network/Security</b> tab, and then click <b>Network</b>. The <b>Network Configuration</b> page appears.</li><li data-bbox="471 1093 930 1117">3 Select the <b>Register CMC on DNS</b> check box.</li><li data-bbox="471 1128 885 1179">4 Enter the CMC name In the <b>DNS CMC Name</b> field.</li><li data-bbox="471 1190 698 1214">5 Click <b>Apply Changes</b>.</li></ol> <p>For more information about generating CSRs and issuing certificates, see "Securing CMC Communications Using SSL and Digital Certificates" on page 147.</p>

**Table 5-31. Managing and Recovering a Remote System: Frequently Asked Questions (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"><li>• When changing the network configuration or network security properties using the CMC Web user interface</li><li>• When the <code>cfgRacTuneHttpsPort</code> property is changed (including when a <code>config -f &lt;config file&gt;</code> changes it)</li><li>• When <code>racresetcfg</code> is used</li><li>• When the CMC is reset</li><li>• When a new SSL server certificate is uploaded</li></ul>
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 147.</p>

**Table 5-31. Managing and Recovering a Remote System: Frequently Asked Questions (*continued*)**

Question	Answer
The following message is displayed for unknown reasons: Remote Access: SNMP Authentication Failure Why does this happen?	<p data-bbox="460 312 958 571">As part of discovery, IT Assistant attempts to verify the device's get and set community names. In IT Assistant, you have the get <b>community name = public</b> and the set <b>community name = private</b>. 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 will only accept requests from <b>community = public</b>.</p> <p data-bbox="460 587 958 639">You can change the CMC community name using RACADM.</p> <p data-bbox="460 655 958 708">To see the CMC community name, use the following command:</p> <pre data-bbox="460 724 958 751">racadm getconfig -g cfgOobSnmp</pre> <p data-bbox="460 767 958 820">To set the CMC community name, use the following command:</p> <pre data-bbox="460 836 958 932">racadm config -g cfgOobSnmp -o cfgOobSnmpAgentCommunity &lt;community name&gt;</pre> <p data-bbox="460 948 958 1129">To prevent SNMP authentication traps from being generated, you must input community names that will be accepted by the agent. Since the CMC only allows one community name, you must input the same <b>get</b> and <b>set</b> community name for IT Assistant discovery setup.</p>

## Troubleshooting the 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 had to be reconfigured to be aware of the new server module.

FlexAddress allows the 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 will be 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 will contain an XML tag `mac_start` that is the first starting hex MAC address that will be 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:  $(\text{starting\_mac})00188BFFDCFA + 0\text{xCF} = (\text{ending\_mac})00188BFFDDC9$ .



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

## Activating FlexAddress

FlexAddress is delivered on a Secure Digital (SD) card that must be inserted into the 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
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 will have 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 the 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 the CMC restarts, verify the activation process by using the steps in the next section, "Verifying FlexAddress Activation."

## 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
```

The following table lists the status messages returned by the command.

**Table 6-1. Status Messages Returned by featurecard -s Command**

Status Message	Actions
No feature card inserted.	Check the CMC to verify that the SD card was properly inserted. In a redundant CMC configuration, make sure 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 will return 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 will return a message:

```
racadm feature -s
```

```
No features active on the chassis.
```

For further information on the RACADM commands, see the **feature** and **featurecard** command sections of the *Dell Chassis Management Controller Administrator Reference Guide*.

## 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 the 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 will be deactivated and no change will be 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 will return 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 will fail 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 *Dell Chassis Management Controller Administrator Reference Guide*.

## 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."

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 will have FlexAddress enabled only on Fabric-A. All other fabrics will 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 *Dell Chassis Management Controller Administrator Reference Guide*.

## 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(RHEL) and RHEL 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" for additional details on FlexAddress configuration. For additional information on the command, see the **getflexaddr** command section of the *Dell Chassis Management Controller Administrator Reference Guide*.

# 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 If a feature card is removed, what will happen?

Nothing will happen. Feature cards can be removed and stored or may be left in place.

- 2 If a feature card that was used in one chassis is removed and put into another chassis, what will happen?

The Web interface will display 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 = XXXXXXXX

Feature Card Chassis Service Tag = YYYYYYYY

An entry will be 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 will be ignored by CMC. In this situation, the `$racadm featurecard -s` will return 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 = XXXXXXXX
```

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

The original feature card is no longer eligible for deactivation on that or any other chassis, unless Dell Service re-programs the original chassis service tag back into a chassis, and the 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 What if I have two feature cards installed in my redundant CMC system? Will I get an error?

The feature card in the active CMC will be active and installed in the chassis. The second card will be 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 will return this message:

```
No features active on the chassis. ERROR: read
only file system
```

**7** What will happen if there isn't an SD card in the active CMC module?

The `$racadm featurecard -s` command will return this message:

```
No feature card inserted.
```


**8** What will happen to my FlexAddress feature if the server BIOS is updated from version 1.xx to version 2.xx?

The server module will need to be powered down before it can be used with FlexAddress. After the server BIOS update is complete, the server module will not get chassis-assigned addresses until the server has been power cycled.

**9** What will happen if a chassis with a single CMC is downgraded with firmware prior to 1.10?

- The FlexAddress feature and configuration will be removed from the chassis.
- The feature card used to activate the feature on this chassis is unchanged, and remains bound to the chassis. When the CMC firmware of the chassis is subsequently upgraded to 1.10 or later, the FlexAddress feature is reactivated by reinserting the original feature card (if necessary), resetting the CMC (if feature card was inserted after firmware upgrade was completed), and reconfiguring the feature.

- 10** 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 will 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 will 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 the 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 will still be activated and ready to use. All fabrics and slots will be 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
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



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

<b>Situation</b>	<b>Command</b>	<b>Output</b>
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 &lt;fabricName&gt; &lt;slotState&gt;] OR \$racadm setflexaddr [-i &lt;slot#&gt; &lt;slotState&gt;]</code>	ERROR: Flexaddress feature is not active on the chassis
Guest user attempts to set FlexAddress on slots/fabrics	<code>\$racadm setflexaddr [-f &lt;fabricName&gt; &lt;slotState&gt;] \$racadm setflexaddr [-i &lt;slot#&gt; &lt;slotState&gt;]</code>	ERROR: Insufficient user privileges to perform operation
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 will exceed 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 will be 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 will be 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 will meet your requirements or that operation of the Software will be 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 will terminate 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, will be 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 the CMC With Microsoft Active Directory

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, you can configure the software to provide access to the CMC. This allows you to add and control CMC user privileges to your existing users in your Active Directory software.



**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 extended schema solution, which uses Active Directory objects defined by Dell.
- The standard schema solution, which uses Active Directory group objects only.

### Extended Schema Versus Standard Schema

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

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.

With the standard schema solution:

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

## Extended Schema Overview

There are two ways to enable Extended Schema Active Directory:

- Using the CMC Web interface. For instructions, see "Configuring the CMC With Extended Schema Active Directory and the Web Interface" on page 223.
- Using the RACADM CLI tool. For instructions, see "Configuring the CMC With Extended Schema Active Directory and RACADM" on page 226.

### 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.

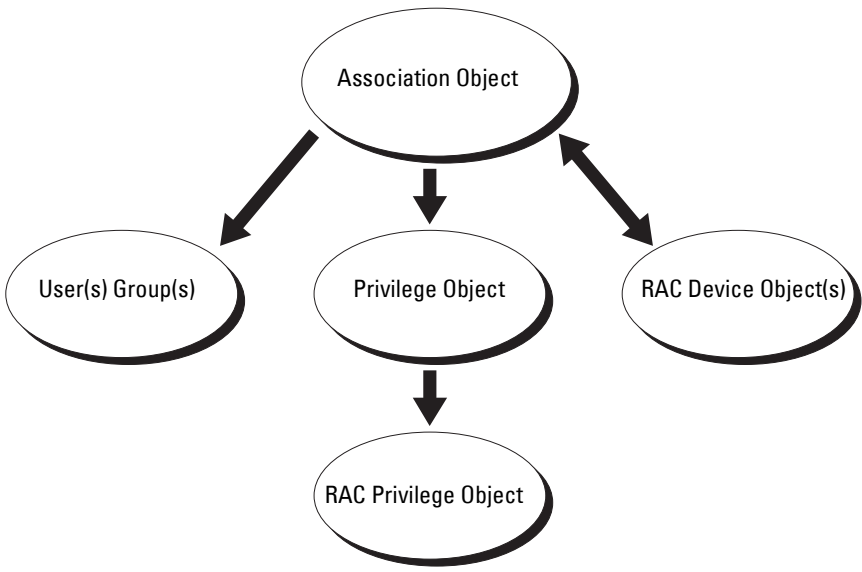
Figure 7-1 illustrates that the Association Object provides the connection that is needed for all of the Authentication and Authorization.



**NOTE:** The RAC privilege object applies to DRAC 4, DRAC 5, and the 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 7-1. Typical Setup for Active Directory Objects**

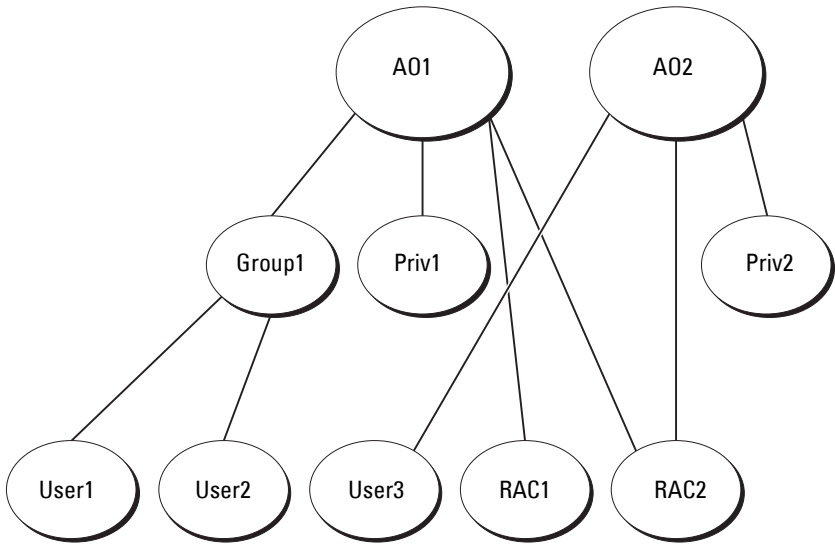


The Association Object allows for as many or as few users and/or groups as well as RAC Device Objects. However, the Association Object only includes one Privilege Object per Association Object. The Association Object connects the "Users" who have "Privileges" on the RACs (CMCs).

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 7-2 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 will not work with Universal Groups from other domains.

**Figure 7-2. Setting Up Active Directory Objects in a Single Domain**



To configure the objects for the single domain scenario:

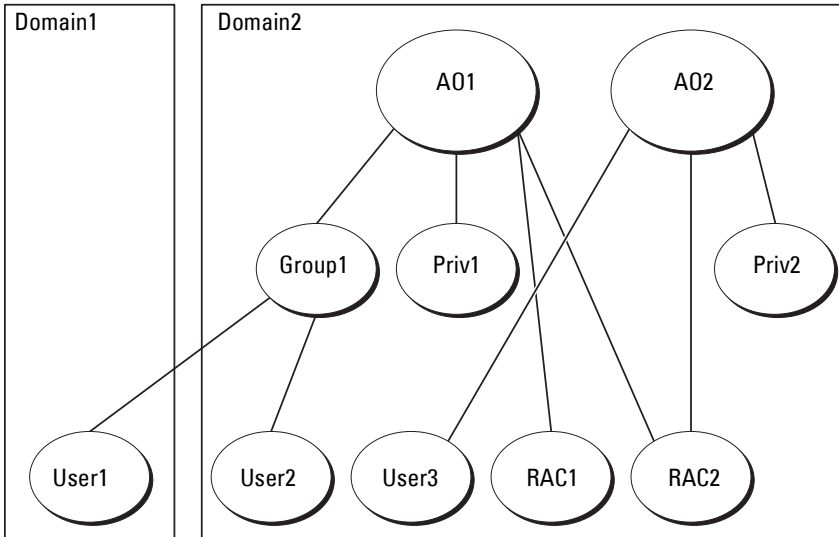
- 1** Create two Association Objects.
- 2** Create two RAC Device Objects, RAC1 and RAC2, to represent the two CMCs.
- 3** Create two Privilege Objects, Priv1 and Priv2, in which Priv1 has all privileges (administrator) and Priv2 has login privilege.
- 4** Group user1 and user2 into Group1.
- 5** Add 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."

Figure 7-3 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 7-3. 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 7-3 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 the CMC:

- 1 Extend the Active Directory schema (see "Extending the Active Directory Schema").
- 2 Extend the Active Directory Users and Computers Snap-In (see "Installing the Dell Extension to the Active Directory Users and Computers Snap-In").
- 3 Add CMC users and their privileges to Active Directory (see "Adding CMC Users and Privileges to Active Directory").
- 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 the CMC With Extended Schema Active Directory and the Web Interface" or "Configuring the CMC With Extended Schema Active Directory and RACADM").

## **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 will not be added to the schema.

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

- <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." 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 7-1 through Table 7-6
- Attributes — see Table 7-7

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

**Table 7-1. Class Definitions for Classes Added to the Active Directory Schema**

<b>Class Name</b>	<b>Assigned Object Identification Number (OID)</b>
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 7-2. dellRacDevice Class**

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

**Table 7-3. 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 7-4. 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 7-5. 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 7-6. dellProduct Class**

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



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

<b>Assigned OID/Syntax Object Identifier</b>	<b>Single Valued</b>
<b>Attribute: dellPrivilegeMember</b>	
<b>Description:</b> List of dellPrivilege objects that belong to this attribute.	
<b>OID:</b> 1.2.840.113556.1.8000.1280.1.1.2.1	FALSE
<b>Distinguished Name:</b> (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	
<b>Attribute: dellProductMembers</b>	
<b>Description:</b> List of dellRacDevices objects that belong to this role. This attribute is the forward link to the dellAssociationMembers backward link.	
<b>Link ID:</b> 12070	
<b>OID:</b> 1.2.840.113556.1.8000.1280.1.1.2.2	FALSE
<b>Distinguished Name:</b> (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	
<b>Attribute: dellIsCardConfigAdmin</b>	
<b>Description:</b> TRUE if the user has Card Configuration rights on the device.	
<b>OID:</b> 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)	
<b>Attribute: dellIsLoginUser</b>	
<b>Description:</b> TRUE if the user has Login rights on the device.	
<b>OID:</b> 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)	
<b>Attribute: dellIsCardConfigAdmin</b>	
<b>Description:</b> TRUE if the user has Card Configuration rights on the device.	
<b>OID:</b> 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)	

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

<b>Assigned OID/Syntax Object Identifier</b>	<b>Single Valued</b>
<b>Attribute: dellIsUserConfigAdmin</b>	
<b>Description:</b> TRUE if the user has User Configuration Administrator rights on the device.	
<b>OID:</b> 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)	
<b>Attribute: dellIsLogClearAdmin</b>	
<b>Description:</b> TRUE if the user has Clear Logs Administrator rights on the device.	
<b>OID:</b> 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)	
<b>Attribute: dellIsServerResetUser</b>	
<b>Description:</b> TRUE if the user has Server Reset rights on the device.	
<b>OID:</b> 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)	
<b>Attribute: dellIsTestAlertUser</b>	
<b>Description:</b> TRUE if the user has Test Alert User rights on the device.	
<b>OID:</b> 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)	
<b>Attribute: dellIsDebugCommandAdmin</b>	
<b>Description:</b> TRUE if the user has Debug Command Admin rights on the device.	
<b>OID:</b> 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)	
<b>Attribute: dellSchemaVersion</b>	
<b>Description:</b> The Current Schema Version is used to update the schema.	
<b>OID:</b> 1.2.840.113556.1.8000.1280.1.1.2.12	TRUE
Case Ignore String(LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	

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

Assigned OID/Syntax Object Identifier	Single Valued
<b>Attribute: dellRacType</b>	
<b>Description:</b> This attribute is the Current Rac Type for the dellRacDevice object and the backward link to the dellAssociationObjectMembers forward link.	
<b>OID:</b> 1.2.840.113556.1.8000.1280.1.1.2.13	TRUE
Case Ignore String(LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	
<b>Attribute: dellAssociationMembers</b>	
<b>Description:</b> List of dellAssociationObjectMembers that belong to this Product. This attribute is the backward link to the dellProductMembers Linked attribute.	
Link ID: 12071	
<b>OID:</b> 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)	
<b>Attribute: dellPermissionsMask1</b>	
<b>OID:</b> 1.2.840.113556.1.8000.1280.1.6.2.1 Integer (LDAPTYPE_INTEGER)	
<b>Attribute: dellPermissionsMask2</b>	
<b>OID:</b> 1.2.840.113556.1.8000.1280.1.6.2.2 Integer (LDAPTYPE_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 Software Quick Installation Guide* for additional instructions about installing systems management software.

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

### **Installing the Administrator Pack**

You must install the Administrator Pack on each system that is managing the Active Directory 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, you will:

- 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 the CMC Name that you will type in step 8a of "Configuring the CMC With Extended Schema Active Directory and the Web Interface."
- 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."

### Creating an Association Object

The Association Object is derived from a Group and must contain a Group Type. The Association Scope specifies the Security Group Type for the Association Object. When you create an Association Object, choose the Association Scope that applies to the type of objects you intend to add.

For example, if you select **Universal**, the association objects are only available when the Active Directory Domain is functioning in Native Mode or above.

- 1 In the **Console Root** (MMC) window, right-click a container.
- 2 Select **New**→**Dell RAC Object**.  
This opens the **New Object** window.
- 3 Type a name for the new object.
- 4 Select **Association Object**.
- 5 Select the scope for the **Association Object**.
- 6 Click **OK**.

### **Adding Objects to an Association Object**

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

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

### **Adding Users or User Groups**

- 1 Right-click the **Association Object** and select **Properties**.
- 2 Select the **Users** tab and click **Add**.
- 3 Type the user or User Group name and click **OK**.

Click the **Privilege Object** tab to add the privilege object to the association that defines the user's or user group's privileges when authenticating to a RAC device. Only one privilege object can be added to an Association Object.

### **Adding Privileges**

- 1 Select the **Privileges Object** tab and click **Add**.
- 2 Type the Privilege Object name and click **OK**.


Click the **Products** tab to add one or more RAC devices to the association. The associated devices specify the RAC devices connected to the network that are available for the defined users or user groups. Multiple RAC devices can be added to an Association Object.

### **Adding RAC Devices or RAC Device Groups**


To add RAC devices or RAC device groups:


- 1** Select the **Products** tab and click **Add**.
- 2** Type the RAC device or RAC device group name and click **OK**.
- 3** In the **Properties** window, click **Apply** and click **OK**.


### **Configuring the 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 the **Network/Security** tab, and then click the **Active Directory** sub-tab. The **Active Directory Main Menu** page appears.
- 4** Select the **Configure** radio button, and then click **Next**. The **Active Directory Configuration and Management** page appears.
- 5** In the **Common Settings** section:
  - a** Select the **Enable Active Directory** check box so that it is checked.
  - b** Type the **Root Domain Name**. 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 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 the CMC from searching for a server.

 **NOTE:** You can specify a list of domain controller or global catalog servers separated by commas. The 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 existing applications/domains.
- 7 Select the **Use Extended Schema** radio button in the **Active Directory Schema Selection** area.
- 8 In the **Extended Schema Settings** section:
  - a Type the **CMC 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`.
- 9 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 will lose the settings you entered when you navigate to the next page.



- 10 Click **Go Back To Active Directory Main Menu**.
- 11 Select the **Upload AD Certificate** radio button, and then click **Next**. The **Certificate Upload** page appears.
- 12 Type the file path of the certificate in the text field, or click **Browse** to select the certificate file.



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

The 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 the CMC.

- 13 Click **Apply**. The CMC Web server automatically restarts after you click **Apply**.
- 14 Log back in to the CMC Web interface.
- 15 Select **Chassis** in the system tree, click the **Network/Security** tab, then click the **Network** sub-tab. The **Network Configuration** page appears.
- 16 If **Use DHCP (for NIC 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.
- 17 Click **Apply Changes**.


The CMC Extended Schema Active Directory feature configuration is complete.

## Configuring the 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 the 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
```


 **NOTE:** You can use this command through remote RACADM only.

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

 **NOTE:** You can use this command through remote RACADM only.

**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 the CMC from searching for a server.

 **NOTE:** You can specify a list of LDAP or global catalog servers separated by commas. The 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 the 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 the 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.

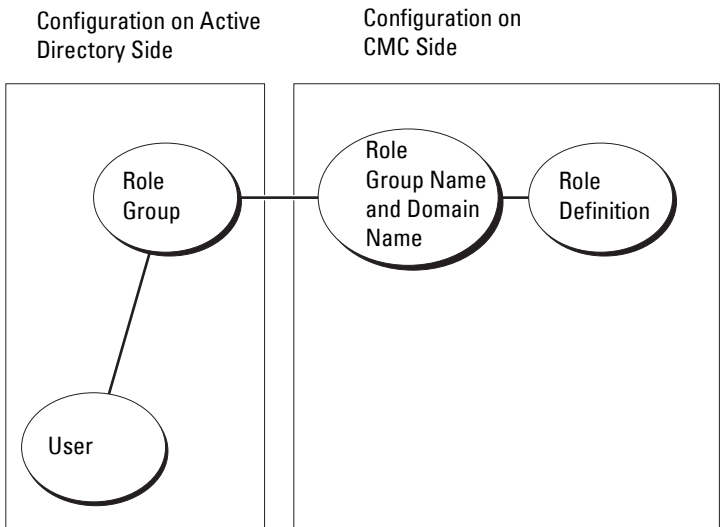
# Standard Schema Active Directory Overview

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

On the Active Directory side, a standard group object is used as a role group. A user who has CMC access will be 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 5-19 shows the privileges level of the role groups and Table 7-8 shows the default role group settings.


**Figure 7-4. Configuration of CMC with Active Directory and Standard Schema**



**Table 7-8. Default Role Group Privileges**

<b>Role Group</b>	<b>Default Privilege Level</b>	<b>Permissions Granted</b>	<b>Bit Mask</b>
1	None	<ul style="list-style-type: none"><li>• CMC Login User</li><li>• Chassis Configuration Administrator</li><li>• User Configuration Administrator</li><li>• Clear Logs Administrator</li><li>• Chassis Control Administrator (Power Commands)</li><li>• Super User</li><li>• Server Administrator</li><li>• Test Alert User</li><li>• Debug Command User</li><li>• Fabric A Administrator</li><li>• Fabric B Administrator</li><li>• Fabric C Administrator</li></ul>	0x00000fff
2	None	<ul style="list-style-type: none"><li>• CMC Login User</li><li>• Clear Logs Administrator</li><li>• Chassis Control Administrator (Power Commands)</li><li>• Server Administrator</li><li>• Test Alert User</li><li>• Fabric A Administrator</li><li>• Fabric B Administrator</li><li>• Fabric C Administrator</li></ul>	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 132.

There are two ways to enable Standard Schema Active Directory:

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

### **Configuring Standard Schema Active Directory to Access Your CMC**

You need to perform the following steps to configure the Active Directory before an Active Directory user can access the 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 will need to be configured on the CMC either with the Web interface or RACADM.

For more information, see "Configuring the CMC With Standard Schema Active Directory and Web Interface" or "Configuring the CMC With Standard Schema Active Directory and RACADM."

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

### **Configuring the 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 the **Network/Security** tab, and then click the **Active Directory** sub-tab. The **Active Directory Main Menu** page appears.
- 4 Select the **Configure** option, and then click **Next**. 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**. 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 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.

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

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 will lose the settings you entered when you navigate to the next page.

9 In the **Standard Schema Settings** section, click a **Role Group**. The **Configure Role Group** page appears.

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

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

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

If you modify any of the privileges, the existing **Role Group Privilege** (Administrator, Power User, or Guest User) will change to either the Custom group or the appropriate Role Group Privilege. See Table 5-19.

- 13 Click **Apply** to save the Role Group settings.
- 14 Click **Go Back To Active Directory Configuration and Management**.
- 15 Click **Go Back To Active Directory Main Menu**.
- 16 Upload your domain forest Root certificate authority-signed certificate into the CMC.
  - a Select the **Upload Active Directory CA Certificate** check box and then click **Next**.
  - b In the **Certificate Upload** page, type the file path of the certificate or browse to the certificate file.



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

The 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 the CMC.

- c Click **Apply**. The CMC Web server automatically restarts after you click **Apply**.
- 17 Log out and then log in to the CMC to complete the CMC Active Directory feature configuration.
- 18 Select **Chassis** in the system tree.
- 19 Click the **Network/Security** tab.
- 20 Click the **Network** sub-tab. The **Network Configuration** page appears.
- 21 If **Use DHCP (for NIC IP Address)** is selected under **Network Settings**, select **Use DHCP to obtain DNS server address**.

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

- 22 Click **Apply Changes**.

The CMC Standard Schema Active Directory feature configuration is complete.



## Configuring the 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, log in, 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 the 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 the 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>
```

## Frequently Asked Questions

Table 7-9 lists frequently asked questions and answers about using Active Directory with the CMC.

**Table 7-9. Using CMC With Active Directory: Frequently Asked Questions**

Question	Answer
Can I log into the 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 the 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.

**Table 7-9. Using CMC With Active Directory: Frequently Asked Questions (continued)**

<b>Question</b>	<b>Answer</b>
Does using the 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.
I created and uploaded a new RAC certificate and now the Web interface does not launch.	If you use Microsoft Certificate Services to generate the RAC certificate, you may have inadvertently chose <b>User Certificate</b> instead of <b>Web Certificate</b> when creating the certificate. To recover, generate a CSR, and then create a new Web certificate from Microsoft Certificate Services and upload it using the following RACADM commands: <pre>racadm sslcsrigen [-g] [-f {filename}] racadm sslcertupload -t 1 -f {web_sslcert}</pre>


**Table 7-9. Using CMC With Active Directory: Frequently Asked Questions (continued)**

Question	Answer
What can I do if I cannot log into the CMC using Active Directory authentication? How do I troubleshoot the issue?	<p><b>1</b> Ensure that you use the correct user domain name during a login and not the NetBIOS name.</p> <p><b>2</b> If you have a local CMC user account, log into the CMC using your local credentials. After you are logged in, perform the following steps:</p> <ul style="list-style-type: none"><li><b>a</b> Ensure that you have checked the <b>Enable Active Directory</b> check box on the CMC Active Directory configuration page.</li><li><b>b</b> Ensure that the DNS setting is correct on the CMC Networking configuration page.</li><li><b>c</b> Ensure that you have uploaded the Active Directory certificate from your Active Directory root certificate authority-signed certificate to the CMC.</li><li><b>d</b> Check the Domain Controller SSL certificates to ensure that they have not expired.</li><li><b>e</b> Ensure that your <b>CMC Name</b>, <b>Root Domain Name</b>, and <b>CMC Domain Name</b> match your Active Directory environment configuration.</li><li><b>f</b> Ensure that the CMC password has a maximum of 127 characters. While the CMC can support passwords of up to 256 characters, Active Directory only supports passwords that have a maximum length of 127 characters.</li></ul>

## Configuring Single Sign-On

Microsoft® Windows® 2000, Windows XP, Windows Server® 2003, Windows Vista®, 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, the CMC can use Kerberos to support two additional types of login mechanisms—single sign-on and Smart Card login. For single sign-on login, the 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:** 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](http://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**

- The CMC must have firmware version 2.10 or later
- Each CMC must have an Active Directory account
- The 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 the 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 the 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 the CMC supports the DES-CBC-MD5 type of cryptography for Kerberos authentication.

This procedure produces a keytab file that you must upload to the 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.aspx?mfr=true](http://technet2.microsoft.com/windowsserver/en/library/64042138-9a5a-4981-84e9-d576a8db0d051033.aspx?mfr=true).

## Configuring the CMC

 **NOTE:** The configuration steps described in this section apply only to the CMC's Web access.

Configure the 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 Your CMC."

## 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 **Remote Access**→**Configuration** tab→**Active Directory** subtab.
- 2 Select **Upload Kerberos Keytab** and click **Next**.
- 3 On the **Kerberos Keytab Upload** page, navigate to the folder where the keytab file is saved and click **Apply**.

When the upload is complete, a message box is displayed indicating a successful or failed upload.

- 4 When the keytab file uploads successfully, click **Go Back To Active Directory Main Menu**.

## Enabling Single Sign-On

- 1 Navigate to **Chassis Management Controller Network Security** tab→**Active Directory** subtab and select **Configure Active Directory**.
- 2 On the **Active Directory Configuration and Management** page, select:
  - **Single Sign-On** — this option enables you to log in to the 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.

Type:

```
testfeature -f adkrb -u <user>@<domain>
```

where user is a valid Active Directory user account.

A command success indicates that the 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 *Chassis Management Controller Administrator Reference Guide* on [support.dell.com/manuals](http://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 the CMC uses Single Sign-On with Kerberos authentication.

### Internet Explorer

- 1 In 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 the 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 the 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 the 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.

The 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, the 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" for Smart Card are the same as Single Sign-On.

### Configuring Settings

The "Prerequisites" 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 the CMC).

## Configuring the CMC



**NOTE:** The configuration steps described in this section apply only to the CMC's Web access.

Configure the 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 Your CMC."

## 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 **Remote Access**→**Configuration** tab→**Active Directory** subtab.
- 2 Select **Upload Kerberos Keytab** and click **Next**.
- 3 On the **Kerberos Keytab Upload** page, navigate to the folder where the keytab file is saved and click **Apply**.

When the upload is complete, a message box is displayed indicating a successful or failed upload.

- 4 When the keytab file uploads successfully, click **Go Back To Active Directory Main Menu**.

## Enabling Smart Card Authentication

- 1 Navigate to **Chassis Management Controller Network Security** tab→ **Active Directory** subtab and select **Configure Active Directory**.
- 2 On the **Active Directory Configuration and Management** page, select:
  - **Smart Card** — this option requires inserting a Smart Card into reader and entering 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 the 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 *Chassis Management Controller Administrator Reference Guide*.

## 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 the 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 change 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 the 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** 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 will be able to help you get a new Smart Card.

### **Unable to Log into CMC as an Active Directory User**

If you cannot log into the CMC as an Active Directory user, try logging into the 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
```

# Power Management

## Overview

The Dell™ PowerEdge™ M1000e server enclosure is the most power-efficient modular server 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 7928 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 matched sets (or grids): PSU slots 1, 2, and 3 in the first grid (Grid A) and PSU slots 4, 5, and 6 in the second grid (Grid B). Each PSU in a matched set

belongs to a different AC power grid and must be cabled as such for proper AC Redundant mode of operation. The load is shared across all active PSUs. The load on a single PSU never exceeds 50 percent of its capacity. With AC redundancy, the system can tolerate the loss of an entire AC power grid or up to 50 percent of its capacity with failures of individual PSUs. The system continues to supply adequate power to the modular enclosure system. The AC Redundancy mode is the factory-default setting for 6 PSU configuration and indicates the chassis is configured for AC Redundancy.

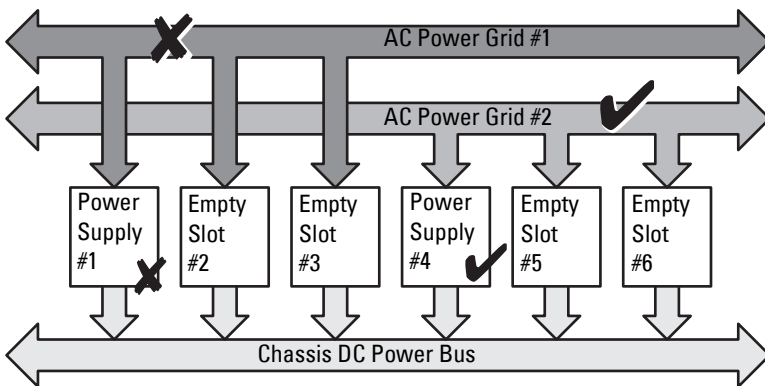
**NOTE:** A system will operate in an AC Redundant mode only if the required conditions have been met. Specifically, each AC power grid must be populated with matched PSUs and the overall load must not exceed the capacity of a single grid.

### AC Redundancy Levels

CMC supports three levels of N+N AC Redundancy—1+1, 2+2, and 3+3. In AC redundancy, the CMC reports all active power supplies as online. This is done to ensure that the system does not experience downtime in the event of a power failure to a grid. If any of the N PSUs in a grid fail, the CMC reports the Enclosure Redundancy Status as **No Redundancy**. E-mail and/or SNMP alerts are sent to administrators if you have configured the **Redundancy Lost** event for alerting.

- 1+1 AC Redundancy Level — at least one PSU is connected to each AC grid.

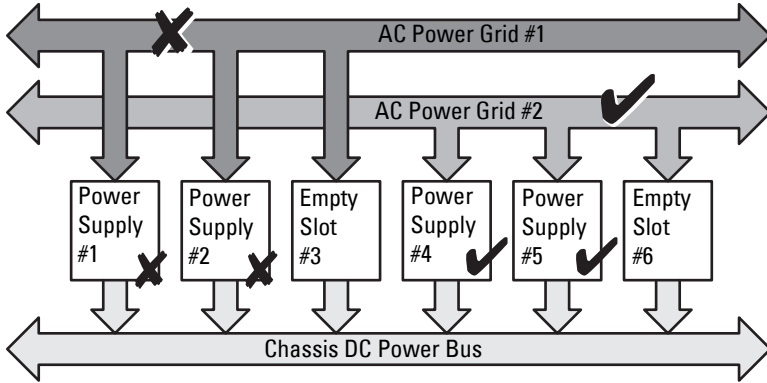
**Figure 8-1. 1+1 Redundancy Level**





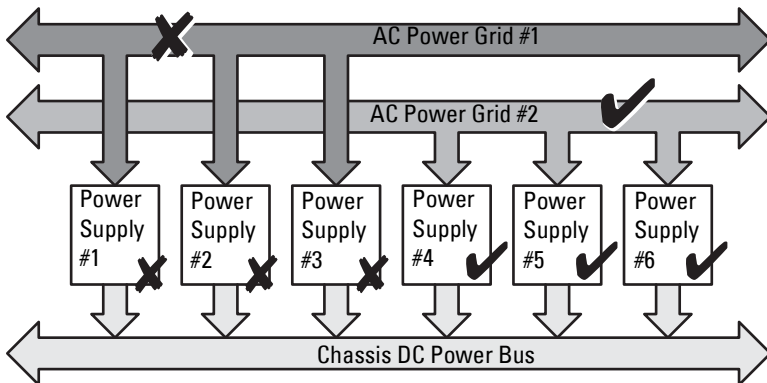
- 2+2 AC Redundancy Level — at least two PSUs are connected to each AC grid.


**Figure 8-2. 2+2 Redundancy Level**




- 3+3 AC Redundancy Level — three PSUs are connected to each power grid. Since three PSUs can power the entire enclosure, this configuration is unaffected by the complete failure of one AC grid without loss of power to the enclosure.

**Figure 8-3. 3+3 Redundancy Level**



 **NOTE:** In the event of a single PSU failure in this configuration, the two remaining PSUs in the failing grid are marked as **Online**. In this state, either 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, AC redundancy status is reported as **No Redundancy** and Chassis health is displayed as **Critical**.

 **NOTE:** The chassis needs only 3 PSUs to operate all blades. However, there must be a balanced set of PSUs to support AC Redundancy; half of them are considered when calculating power capacities; the other half are marked for AC redundancy. If you install less than the number of PSUs required to operate your servers, redundancy may be reported as **No Redundancy** or servers may not be allowed to power on.

## 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. One PSU's capacity over the allocation requirements is kept in online reserve for this purpose. This forms a Power Supply redundancy pool.

Any PSU installed outside this pool is not used. These PSUs join the redundancy pool if any PSU in the pool fails.

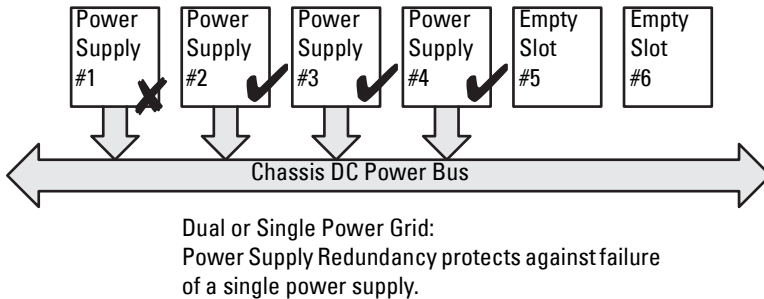
## Power Supply Redundancy Levels

CMC supports three levels of Power Supply Redundancy—1+1, 2+1, and 3+1. This option keeps the additional PSU engaged at all times to ensure that the failure of a single PSU can always be tolerated. Although Figure 8-4 illustrates a configuration of four PSU present in the first four PSU slots, CMC does not require the four PSU units to be present in any specific PSU slot positions.

Dynamic Power Supply Engagement (DPSE) allows PSUs to be placed in standby.

The *standby* state indicates a physical state (OFF). When you enable DPSE, the extra PSUs are placed in Standby mode to increase efficiency and save power.


**Figure 8-4. Power Supply Redundancy: 3+1 PSU Redundancy**



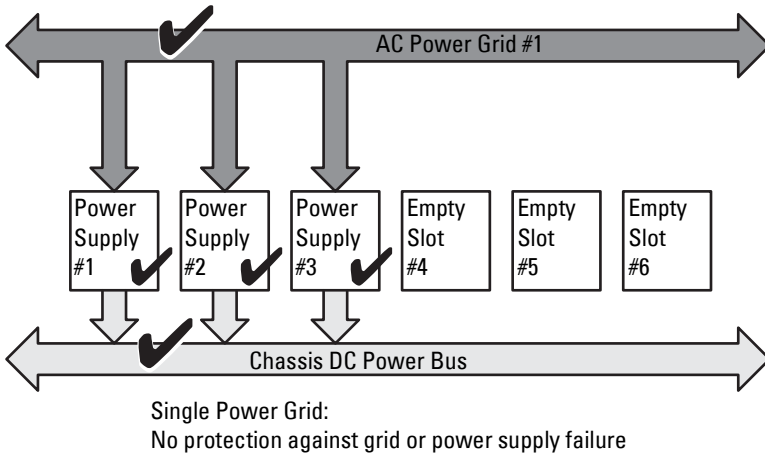
### No Redundancy Mode

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**.

Although Figure 8-5 illustrates the three PSUs present in the first three PSU slots, CMC does not require the three PSU units to be present in any specific PSU slot positions.

 **NOTE:** All active PSU in the chassis are listed as **Online** and any additional PSU may be turned off for increasing power efficiency and is marked as **Standby** if DPSE is enabled. All PSUs in the chassis are listed as **Online** if DPSE is disabled in **No Redundancy** mode.

**Figure 8-5. No Redundancy**



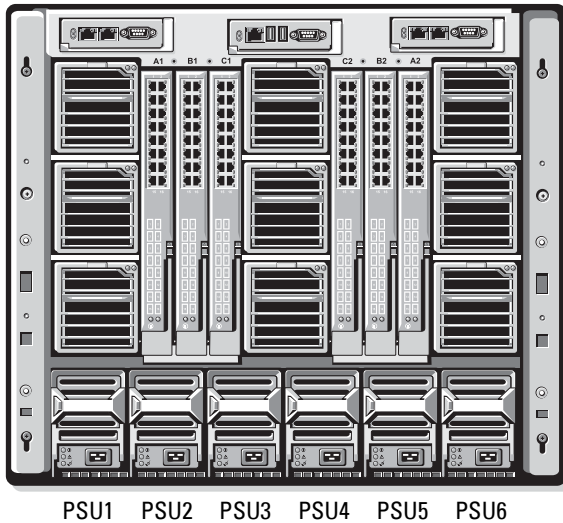
A PSU failure brings the other PSUs out of Standby mode, as needed, to support the chassis power allocations. If you have 4 PSUs and one fails, the fourth PSU is brought online. A chassis can have a maximum of 6 PSUs online.

When you enable DPSE, the extra PSUs are placed in Standby mode to increase efficiency and save power.

### **Power Budgeting for Hardware Modules**

Figure 8-6 illustrates a chassis that contains a six-PSU configuration. The PSUs are numbers 1-6, starting on the left-side of the enclosure.

**Figure 8-6. Chassis With Six-PSU Configuration**



The CMC maintains a power budget for the enclosure that reserves the necessary wattage for all installed servers and components.

The CMC allocates power to the CMC infrastructure and the blade servers in the chassis. The 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 blade servers that communicate to the chassis through the iDRAC. For more information, see the *iDRAC User's Guide* at [support.dell.com/manuals](http://support.dell.com/manuals).

The iDRAC provides the CMC with its power envelope requirements before powering up the blade server. The power envelope consists of the maximum and minimum power requirements that could keep the server operating. iDRAC's initial estimate is based on a worst-case model where all components in the blade server draw maximum power and are often higher than the actual blade 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 (usually a reduced power envelope).

The CMC grants the requested power to the blade 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.

However, under heavy load the performance of the server's processors may be degraded to ensure power consumption stays below or if the user-configured **System Input Power Cap** if the Cap has been lowered from the factory default setting.

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. The CMC first ensures enough power is available to run the fans, IO Modules, iKVM (if present), and the CMC itself. This power allocation is called the **Input Power Allocated to Chassis Infrastructure**. Once the servers in an enclosure are powered up, any attempt to set a lower **System Input Power Cap** that would require a server to power off to fulfill this requirement will fail.

If necessary for the total power budget to stay below the value of the **System Input Power Cap**, the CMC will allocate servers a value less than their maximum requested power. Servers are allocated power based on their **Server Priority** setting, with priority 1 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 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 modular enclosure only

if sufficient power is available. The **System Input Power Cap** can be increased any time up to a maximum value of 7928 watts to allow the power up of additional servers.

Changes in the modular enclosure that reduce power allocation are server power off, server, I/O module, or iKVM removal, and 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

The 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. The 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 be not be allocated enough power to run at their maximum performance or they may not even power on at all, depending on how low the limit is set and the server power requirements.

If an administrator manually powers on the low priority server modules before the higher priority ones, the low priority server modules will be the first modules to have their power allocation lowered to the minimum value. Once the available power allocation is exhausted, CMC reclaims power from lower or equal priority servers up to their minimum power level.



**NOTE:** I/O modules, fans, and iKVM (if present) are designated the highest priority. CMC reclaims power only 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 using the minimum PSUs needed to power the chassis, resulting in increased utilization of online PSUs and thus increasing their efficiency. This results in increased PSU life, reduced heat generation, and power savings by operating power supplies at more efficient power levels.

The CMC monitors total enclosure power allocation, and moves the PSUs that are not required 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.

The system runs most efficiently with as few active PSUs as possible, therefore:

- **No Redundancy** mode with DPSE is highly power efficient, with only the minimum PSUs online. Unneeded PSUs are placed in standby mode.
- **PSU Redundancy** mode with DPSE also provides power efficiency. At least two supplies are active, 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 six 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 will be placed in Standby and stay unutilized to improve power efficiency. Removal or failure of an online PSU in this configuration will 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 in pairs—one from each AC grid (except in the 1+1 redundancy level). 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 will cause the engagement of PSUs from the **Standby** state in pairs—one from each AC grid (except in the 1+1 redundancy level). 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 the 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 8-1.

**Table 8-1. 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 PSUs properly cabled to separate AC grids.**

If one AC grid fails, the three PSUs on the functioning AC grid take over without interruption to the servers or infrastructure.

**⚠ CAUTION: In AC redundancy mode, you must have a balanced set of PSUs (at least one PSU in each grid). If this condition is not met, there is a possibility of a loss of redundancy.**

## 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, will be 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 from up to three PSUs is used to power the entire chassis. So in a 6-PSU chassis, a chassis continues to operate at full capacity if any 3 PSUs fail.



**CAUTION:** The No Redundancy mode uses only three PSUs without a backup. Failure of one of the three PSUs being used could cause servers to lose power and data.

## Power Conservation and Power Budget Changes

The 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**, the 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, the 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."

You can assign server priority using the GUI:

- 1 Click **Servers** in the system tree.
- 2 Select the **Power Management** tab→**Priority** sub-tab.

## PSU Failure With Degraded or No Redundancy Policy

The CMC decreases power to servers when an insufficient power event occurs, such as a PSU failure. After decreasing power on servers, the CMC re-evaluates the power needs of the chassis. If power requirements are still not met, CMC may also power off the lower priority blade 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."

## New Server Engagement Policy

When a new server is powered on, the 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 8-2 describes the actions taken by the CMC when a new server is powered on in the scenario described above.

**Table 8-2. CMC Response When a Server Power-On is Attempted**

<b>Worst Case Power is Available</b>	<b>CMC Response</b>	<b>Server Power On</b>
Yes	No power conservation is required	Allowed
No	Perform power conservation: <ul style="list-style-type: none"><li>• Power required for new server is available</li><li>• Power required for new server is not available</li></ul>	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 will 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 8-3 describes the firmware response to a PSU power down or removal as it applies to various PSU redundancy configurations.

**Table 8-3. Chassis Impact from PSU Failure or Removal**

<b>PSU Configuration</b>	<b>Dynamic PSU Engagement</b>	<b>Firmware Response</b>
AC Redundancy	Disabled	CMC alerts you of loss of AC Redundancy.
Power Supply Redundancy	Disabled	CMC alerts you of loss of Power Supply Redundancy.
No Redundancy	Disabled	Decrease power to low priority servers, if needed.
AC Redundancy	Enabled	CMC alerts you of loss of AC Redundancy. PSUs in standby mode (if any) are turned on to compensate for power budget lost from the PSU failure or removal.
Power Supply Redundancy	Enabled	CMC alerts you of loss of Power Supply Redundancy. PSUs in standby mode (if any) are turned on to compensate for power budget lost from PSU failure or removal.
No Redundancy	Enabled	Decrease power to low priority servers, if needed.

### **PSU Removals With Degraded or No Redundancy Policy**

The CMC may begin conserving power when you remove a PSU or a PSU AC cord. The 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, the 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 blade servers.

## Limits

- The 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. The M1000e chassis ships with one of two configurations: three PSUs or six PSUs. You can select any of the three PSU redundancy configuration settings listed in "Redundancy Policies."

## 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 8-4 lists the SEL entries that are related to power supply changes.

**Table 8-4. 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

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. A modular enclosure that is configured in the **Non Redundant** power policy records a SEL entry for insufficient resources, **Non Redundant** power policy is recorded when the functional power supply count drops below the enclosure minimum of three power supplies. Similarly, when the functional power supply count is restored, a SEL entry for sufficient resources, **Non Redundant** power policy, is recorded. Table 8-5 lists the SEL entries related to power redundancy policy changes.

**Table 8-5. SEL Events for Power Redundancy Status Changes**

<b>Power Policy Event</b>	<b>System Event Log (SEL) Entry</b>
Redundancy lost	redundancy lost was asserted
Redundancy regained	redundancy regained was 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 will typically be **OK**. However, if the conditions for operating with AC redundancy cannot be met, the redundancy status will be **No**, and the overall power health will be **Critical**. This is because the system is not able to operate in accordance with the configured redundancy policy.



**NOTE:** The 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 the 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 right 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 the 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 usually during Chassis power up or PSU insertion. PSU is present and not powered on. It is not communicating with the CMC and 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 8-6 and Table 8-7 provide descriptions of the information provided on the **Power Supply Status** page.



**Table 8-6. Power Supply Health Status Information**

<b>Item</b>	<b>Description</b>	
Name	Displays the name of the power supply unit: PS-[n], where [n] is the power supply number.	
Present	Indicates whether the PSU is <b>Present</b> or <b>Absent</b> .	
Health	 OK	Indicates that the PSU is present and communicating with the CMC. In the event of a communication failure between the CMC and the power supply, the 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 within the administrator-specified time, it could lead to critical or severe power failures that can affect the integrity of the chassis.
	 Severe	Indicates at least one Failure alert has been issued for the power supply. Severe status indicates a power failure on the chassis, and <b>corrective action must be taken immediately</b> .
Power Status	Indicates the power state of the power supplies (one of the following): <b>Initializing, Online, Stand By, In Diagnostics, Failed, Offline, Unknown, or Absent</b> .	
Capacity	Displays the power supply's capacity in watts.	

**Table 8-7. System Power Health Status Information**

<b>Item</b>	<b>Description</b>
Overall Power Health	Indicates the health status ( <b>OK, Non-Critical, Critical, Non-Recoverable, Other, Unknown</b> ) of the power management for the entire chassis.
System Power Status	Displays the power status ( <b>On, Off, Powering On, Powering Off</b> ) of the chassis.
Redundancy	Indicates the power supply redundancy status. Values include: <b>No:</b> Power Supplies are not redundant. <b>Yes:</b> Full Redundancy in effect.

## Using RACADM

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


```
racadm getpminfo
```

For more information about `getpminfo`, including output details, see the *Chassis Management Controller Administrator Reference Guide* on the Dell Support website at [support.dell.com](http://support.dell.com).

## Viewing Power Consumption Status


The 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** in the system tree.
- 3 Click the **Power Management** tab - **Power Consumption** subtab. The **Power Consumption** page displays.

Table 8-8 through Table 8-11 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 the CMC, log in, and type:

```
racadm getpminfo
```

**Table 8-8. Real-Time Power Statistics**

<b>Item</b>	<b>Description</b>
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 <b>Configuration</b> sub-tab on the <b>Budget Status</b> page 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 <b>hh:mm:ss MM/DD/YYYY</b> , where <b>hh</b> is hours (0-24), <b>mm</b> is minutes (00-60), <b>ss</b> is seconds (00-60), <b>MM</b> is the month (1-12), <b>DD</b> is the day (1-31), and <b>YYYY</b> is the year. This value is reset with the <b>Reset Peak/Min Power Statistics</b> button and also when the 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 <b>hh:mm:ss MM/DD/YYYY</b> , where <b>hh</b> is hours (0-24), <b>mm</b> is minutes (00-60), <b>ss</b> is seconds (00-60), <b>MM</b> is the month (1-12), <b>DD</b> is the day, 1-31, and <b>YYYY</b> 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 <b>Configuration</b> sub-tab on the <b>Budget Status</b> page to clear this value. The value for minimum system power is displayed in both the watts and BTU/h units. This value is reset with the <b>Reset Peak/Min Power Statistics</b> button and also when the CMC resets or fails over.

**Table 8-8. 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 <b>hh:mm:ss MM/DD/YYYY</b> , where <b>hh</b> is hours (0-24), <b>mm</b> is minutes (00-60), <b>ss</b> is seconds (00-60), <b>MM</b> is the month (1-12), <b>DD</b> is the day (1-31), and <b>YYYY</b> is the year. This value is reset with the <b>Reset Peak/Min Power Statistics</b> button and also when the 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 <b>Peak System Power Timestamp</b> .
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 8-9. Real-Time Energy Statistics Status**

<b>Item</b>	<b>Description</b>
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 <b>hh:mm:ss MM/DD/YYYY</b> , where <b>hh</b> is hours (0-24), <b>mm</b> is minutes (00-60), <b>ss</b> is seconds (00-60), <b>MM</b> is the month (1-12), <b>DD</b> is the day (1-31), and <b>YYYY</b> is the year. This value is reset with the <b>Reset Energy Statistics</b> button, but will persist 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 <b>hh:mm:ss MM/DD/YYYY</b> , where <b>hh</b> is hours (0-24), <b>mm</b> is minutes (00-60), <b>ss</b> is seconds (00-60), <b>MM</b> is the month (1-12), <b>DD</b> is the day (1-31), and <b>YYYY</b> is the year.

**Table 8-10. System Power Status**

<b>Item</b>	<b>Description</b>
Overall Power Health	Indicates the health status ( <b>OK</b> , <b>Non-Critical</b> , <b>Critical</b> , <b>Non-Recoverable</b> , <b>Other</b> , <b>Unknown</b> ) of the chassis' power subsystem.
System Power Status	Displays the power status ( <b>On</b> , <b>Off</b> , <b>Powering On</b> , <b>Powering Off</b> ) of the chassis.
Redundancy	Indicates the redundancy status. Valid values are: <b>No</b> — PSUs are not redundant <b>Yes</b> — full redundancy in effect

**Table 8-11. Server Modules**

<b>Item</b>	<b>Description</b>
Slot	Displays the location of the server module. The <b>Slot</b> 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 ( <b>Yes</b> or <b>No</b> ). If this field displays <b>Extension of #</b> (where the <b>#</b> will be 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 <b>Start Time</b> 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 <b>Time Stamp</b> field. The measurement is displayed in watts.

## Viewing Power Budget Status

The 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** in the system tree.
- 3 Click the **Power Management** tab. The **Power Budget Status** page displays.

Table 8-12 through Table 8-15 describe the information displayed on the **Power Budget Status** page.

See "Configuring Power Budget and Redundancy" for information about configuring the settings for this information.

### Using RACADM

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


```
racadm getpbinfo
```

For more information about **getpbinfo**, including output details, see the **getpbinfo** command section in the *Chassis Management Controller Administrator Reference Guide*.

**Table 8-12. 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). The CMC will enforce 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 <b>System Input Power Cap</b>, 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 <b>same</b> 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 8-12. System Power Policy Configuration (continued)**

Item	Description
Redundancy Policy	<p>Indicates the current redundancy configuration: <b>AC Redundancy</b>, <b>Power Supply Redundancy</b>, and <b>No Redundancy</b>.</p> <p><b>AC Redundancy</b>—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 at 100% capacity.</p> <p><b>Power Supply Redundancy</b> — 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><b>Power Supply Redundancy</b> does not use all six PSUs; it uses a maximum of four PSUs and the other PSUs may be placed in Standby mode if DPSE is enabled.</p> <p><b>No Redundancy</b> — The power from all three PSUs on one AC circuit (grid) is used to power the entire chassis, including the chassis, servers, I/O modules, iKVM, and CMC.</p> <p> <b>CAUTION: The No Redundancy mode uses only three PSUs at a time, with no backup. Failure of one of the three PSUs in use could cause the server modules to lose power and data.</b></p>
Dynamic Power Supply Engagement	<p>Indicates whether <b>Dynamic Power Supply Engagement</b> is enabled or disabled. Enabling this feature allows the 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 8-13. Power Budgeting**

<b>Item</b>	<b>Description</b>
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 <b>AC Redundancy</b> mode, the <b>Input Redundancy Reserve</b> 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 <b>Power Supply Redundancy</b> mode, the <b>Input Redundancy Reserve</b> is the amount of reserve power that can be utilized in the event of a specific PSU failure.</p>
Input Power Allocated to Servers	Displays (in watts) the cumulative input power the CMC is allocating to servers based on their configuration.
Input Power Allocated to Chassis Infrastructure	Displays (in watts) the cumulative input power the CMC is allocating to the chassis infrastructure (Fans, IO modules, iKVM, CMC, Standby CMC and iDRAC on servers).
Total Input Power Available for Allocation	Indicates the total chassis power budget, in watts, available for chassis operation.
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 four or more power supplies and the Dynamic Power Supply Engagement is enabled.</p> <p><b>NOTE:</b> 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 <b>Total Input Power Available for Allocation</b> value.</p>

**Table 8-14. Server Modules**

<b>Item</b>	<b>Description</b>
<b>Slot</b>	Displays the location of the server module. The <b>Slot</b> is a sequential number (1–16) that identifies the server module by its location within the chassis.
<b>Name</b>	Displays the server name. The server name can be redefined by the user.
<b>Type</b>	Displays the type of the server.
<b>Priority</b>	<p>Indicates the priority level allotted to the server slot in the chassis for power budgeting. The 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><b>Priority levels:</b> 1 (highest) through 9 (lowest)</p> <p><b>Default:</b> 1</p> <p><b>NOTE:</b> 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>
<b>Power State</b>	<p>Displays the power status of the server:</p> <ul style="list-style-type: none"><li>• <b>N/A:</b> The CMC has not determined the power state of the server.</li><li>• <b>Off:</b> Either the server or chassis is off.</li><li>• <b>On:</b> Both chassis and server are on.</li><li>• <b>Powering On:</b> Temporary state between Off and On. When the powering on cycle completes, the Power State will change to On.</li><li>• <b>Powering Off:</b> Temporary state between On and Off. When the powering off cycle completes, the Power State will change to Off.</li></ul>
<b>Budget Allocation - Actual</b>	<p>Displays the power budget allocation for the server module.</p> <ul style="list-style-type: none"><li>• <b>Actual:</b> Current power budget allocation for each server.</li></ul>

**Table 8-15. System Power Supplies**

<b>Item</b>	<b>Description</b>
Name	Displays the name of the PSU in the format PS- <i>n</i> , where <i>n</i> , is the PSU number.
Power State	Indicates the power state of the PSU — <b>Initializing, Online, Stand By, In Diagnostics, Failed, Unknown, or Absent</b> (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

The 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** in the system tree.
- 3** Click the **Power Management** tab→**Configuration** sub-tab. The **Budget/Redundancy Configuration** page displays.
- 4** Set any or all of the properties described in Table 8-16 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 8-16. Configurable Power Budget/Redundancy Properties**

Item	Description
System Input Power Cap	<p data-bbox="350 304 960 504">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 <b>exceeds</b> 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 will fail.</p> <p data-bbox="350 520 960 663">The power allocated to Servers and Chassis Infrastructure can be found in the User Interface on the <b>Chassis→Power Management→Power Budget</b> status page under <b>Power Budgeting</b> section or by using the CLI RACADM utility command (<code>racadm getpbinfo</code>).</p> <p data-bbox="350 679 960 791">Users can power off one or more server(s) to lower the current power allocation, and re-attempt setting a lower value for <b>System Input Power Cap</b> (if desired) or simply configure the cap prior to powering on the servers.</p> <p data-bbox="350 807 960 919">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="350 935 960 983"><b>NOTE:</b> See the Datacenter Capacity Planner (DCCP) tool at <a href="http://www.dell.com/calc">www.dell.com/calc</a> for capacity planning.</p> <p data-bbox="350 999 960 1206"><b>NOTE:</b> 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 will be susceptible to some rounding error.</p>

**Table 8-16. 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"><li data-bbox="398 320 1006 432">• <b>No Redundancy:</b> Power from all three power supplies on one AC circuit (grid) is used to power-on the entire chassis, including the chassis, servers, I/O modules, iKVM, the and CMC.</li></ul> <p><b>NOTE:</b> The <b>No Redundancy</b> mode uses only three power supplies at a time. If 3 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 three 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"><li data-bbox="398 667 1006 778">• <b>Power Supply Redundancy:</b> The capacity of the highest-rated power supply in the chassis is kept in reserve, ensuring that a failure of any one power supply will not cause the server modules or chassis to power down (hot spare).</li></ul> <p><b>Power Supply Redundancy</b> mode does not utilize all six power supplies, but rather a <b>maximum of four</b> and a <b>minimum of two</b> power supplies. Any additional power supplies, if present, may be placed in Standby mode for improving power efficiency if DPSE is enabled.</p> <p><b>Power Supply Redundancy</b> mode prevents server modules from powering up if the power consumption of the chassis exceeds the rated power. Failure of <b>two</b> 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"><li data-bbox="398 1129 1006 1300">• <b>AC Redundancy:</b> This mode divides half the PSUs into two power grids (for example, PSUs 1-3 making up power grid 1 and PSUs 4-6 making up power grid 2). In this configuration, all six PSUs are online. Failure of a PSU or loss of AC power to one grid will report the redundancy status as lost.</li></ul>

**Table 8-16. Configurable Power Budget/Redundancy Properties (continued)**

Item	Description
Enable Dynamic Power Supply Engagement	<p>Enables (when checked) dynamic power management. In <b>Dynamic Engagement</b> mode, the power supplies are turned <b>ON</b> (online) or <b>OFF</b> (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. The 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>Disables (when checked) 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>

### Using RACADM

To enable redundancy 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 the CMC and log in.

2 Set properties as needed:

- To select a redundancy policy, type:

```
racadm config -g cfgChassisPower -o  
cfgChassisRedundancyPolicy <value>
```

where <value> can be 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> can be 0 (disable), 1 (enable). The default is 1.

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 *CMC Administrator Reference Guide*.

## 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** in the system tree. The **Servers Status** page appears.
- 3 Click the **Power Management** tab. 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 the 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** in the system tree. The **Component Health** page appears.
- 3 Click the **Power Management** tab. The **Power Budget Status** page appears.
- 4 Click the **Configuration** sub-tab. The **Budget/Redundancy Configuration** page appears.



- 5 Type a budget value of up to 7928 watts in the **System Input Power Cap** text field.

 **NOTE:** The power budget is limited to a maximum of three PSUs out of a total of six PSUs. If you attempt to set a AC power budget value that exceeds the power capacity of your chassis, the CMC will display 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 will be susceptible to some rounding error.

- 6 Click **Apply** to save your changes.

### Using RACADM

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


```
racadm config -g cfgChassisPower -o  
cfgChassisPowerCap <value>
```

where <value> is a number between 2715–7928 representing the maximum power limit in watts. The default is 7928.

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 a maximum of three PSUs out of a total of six PSUs. If you attempt to set a AC power budget value that exceeds the power capacity of your chassis, the CMC displays a failure message.

## Server Power Reduction to Maintain Power Budget

The 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, the 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, the CMC will lower 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.")
- 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."

## 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." For power control operations on servers, see "Executing Power Control Operations on a Server."

The 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** in the system tree.
- 3 Click the **Power Management** tab. The **Power Budget Status** page displays.
- 4 Click the **Control** sub-tab. The **Power Management** page displays.

- 5 Select one of the following **Power Control Operations** by clicking its radio button:
    - **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 will 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). The CMCs remain powered on, but in virtual standby state; a power supply unit and fans provide cooling for the CMCs in this state. The power supply will also provide power to the fans that will be running 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 the CMC without powering off (warm reboot). (This option is disabled if the CMC is already powered off).
  -  **NOTE:** This action only resets the 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 the 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. The I/O Modules Status page displays.
- 3 Click the Power Management 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 the 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.

The 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 **Servers** 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 Management** tab. The **Server Power Management** page displays.
- 4 **Power Status** displays the power status of the server (one of the following):
  - **N/A** - The 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** will be **On**.
  - **Powering Off** - Temporary state between On and Off. When the action completes successfully, the **Power State** will be **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 Management**→**Control** page.

## Using RACADM

Open a serial/Telnet/SSH text console to the 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*.

## Troubleshooting

For power supply and power-related issue troubleshooting, see "Troubleshooting and Recovery."

# 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

The 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, the CMC assigned names take precedence, and any new names you assign to servers using OSCAR will be overwritten.

The 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 *Dell Chassis Management Controller Administrator Reference Guide*.

## 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 the CMC."

## Physical Connection Interfaces

You can connect to a server or the CMC CLI console via 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<sup>®</sup> software. The iKVM supports ACI connections from the following products:

- 180AS, 2160AS, 2161DS\*, 2161DS-2, or 4161DS Dell Remote Console Switches™
- Avocent AutoView<sup>®</sup> switching system
- Avocent DSR<sup>®</sup> switching system
- Avocent AMX<sup>®</sup> 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 9-1 describes navigating the OSCAR interface using the keyboard and mouse.

**Table 9-1. OSCAR Keyboard and Mouse Navigation**

Key or Key Sequence	Result
<ul style="list-style-type: none"><li>• &lt;Print Screen&gt;-&lt;Print Screen&gt;</li><li>• &lt;Shift&gt;-&lt;Shift&gt;</li><li>• &lt;Alt&gt;-&lt;Alt&gt;</li><li>• &lt;Ctrl&gt;-&lt;Ctrl&gt;</li></ul>	Any of these key sequences can open OSCAR, depending on your <b>Invoke OSCAR</b> settings. You can enable two, three, or all of these key sequences by selecting boxes in the <b>Invoke OSCAR</b> section of the <b>Main</b> dialog box, and then clicking <b>OK</b> .
<F1>	Opens the <b>Help</b> screen for the current dialog box.
<Esc>	Closes the current dialog box without saving changes and returns to the previous dialog box.  In the <b>Main</b> 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 <b>OK</b> button, then returns to the previous dialog box.
<Enter>	Completes a switch operation in the <b>Main</b> 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.

**Table 9-1. OSCAR Keyboard and Mouse Navigation (continued)**

Key or Key Sequence	Result
<Print Screen>, <Backspace>	Toggles back to previous selection if there were no other keystrokes.
<Print Screen>, <Alt> + <0>	Immediately disconnects a user from a server; no server is selected. Status flag displays Free. (This action only applies to the = <0> on the keyboard and not the keypad.)
<Print Screen>, <Pause>	Immediately turns on screen saver mode and prevents access to that specific console, if it is password protected.
Up/Down Arrow keys	Moves the cursor from line to line in lists.
Right/Left Arrow keys	Moves the cursor within the columns when editing a text box.
<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 9-2 describes the features available from the OSCAR Setup menu for configuring your servers.

**Table 9-2. 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"> <li>• Sets a password to restrict access to servers.</li> <li>• Enables a screen saver and set an inactivity time before the screen saver appears and set the screen save mode.</li> </ul>
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."

## 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 9-3. 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 the 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 the 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."







**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 9-4. OSCAR Interface Status Symbols**

<b>Symbols</b>	<b>Description</b>
	(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."

## 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 will be 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 will be 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 will put 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 will bounce 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 the 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 *Dell Chassis Management Controller Administrator Reference Guide*.

### 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 the 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 the 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 *Dell Chassis Management Controller Administrator Reference Guide*.

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 the 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 the CMC; an adverse condition may exist.
  - Gray - iKVM is present and not powered on. It is not communicating with the 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 9-5 provides descriptions of the information provided on the **iKVM Status** page.

**Table 9-5. iKVM Status Information**

<b>Item</b>	<b>Description</b>
Presence	Indicates whether the iKVM module is <b>Present</b> or <b>Absent</b> .
Power State	Indicates the power status of the iKVM: <b>On</b> , <b>Off</b> , or <b>N/A (Absent)</b> .
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	Indicates the firmware version of the iKVM.
Hardware Version	Indicates the hardware version of the iKVM.

**Table 9-5. iKVM Status Information (continued)**

<b>Item</b>	<b>Description</b>
Front Panel Connected	Indicates whether the monitor is <b>connected</b> to the front panel VGA connector ( <b>Yes</b> or <b>No</b> ). This information is provided to the CMC so it can determine whether a local user has front-panel access to the chassis.
Rear Panel Connected	Indicates whether the monitor is <b>connected</b> to the rear panel VGA connector ( <b>Yes</b> or <b>No</b> ). This information is provided to the 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 ( <b>Yes</b> or <b>No</b> ).
Allow access to CMC from iKVM	Indicates whether the CMC command console through iKVM is enabled ( <b>Yes</b> or <b>No</b> ).

### 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 items to note:
  - 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 the CMC, log in, and type:


```
racadm fwupdate -g -u -a <TFTP server IP address> -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 *Dell Chassis Management Controller Administrator Reference Guide*.

# 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 will switch Linux to a text console.

**Table 9-6. 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 the 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"><li>1 Log in to the CMC Web interface.</li><li>2 Select iKVM in the system tree.</li><li>3 Click the <b>Setup</b> tab.</li><li>4 Select the <b>Front Panel USB/Video Enabled</b> check box.</li><li>5 Click <b>Apply</b> to save the setting.</li></ol> <p>To enable the front panel using RACADM, open a serial/Telnet/SSH text console to the CMC, log in, and type:</p> <pre>racadm config -g cfgKVMInfo -o cfgKVMAccesToCMCEnable 1</pre>
The rear panel access does not work.	<p>The front panel setting is enabled by the 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 9-6. Troubleshooting iKVM (continued)**

<b>Problem</b>	<b>Likely Cause and Solution</b>
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><b>There is problem with the iKVM,</b> for which the iKVM requires reprogramming. To fix the problem, follow the instructions for updating iKVM firmware (see "Updating the iKVM Firmware").</p> <p><b>The iKVM is reprogramming the CMC Console Interface.</b> 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><b>The iKVM firmware has detected a hardware error.</b> For additional information, view the iKVM status.</p> <p>To view iKVM status using the Web interface:</p> <ol style="list-style-type: none"><li>1 Log in to the CMC Web interface.</li><li>2 Select iKVM in the system tree.</li></ol> <p>To view iKVM status using RACADM, open a serial/Telnet/SSH text console to the CMC, log in, and type:</p> <pre>racadm getkvminfo</pre>

**Table 9-6. Troubleshooting iKVM (continued)**

<b>Problem</b>	<b>Likely Cause and Solution</b>
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 will become active and accessible.  To disable the front panel using the Web interface: <ol style="list-style-type: none"><li><b>1</b> Log in to the CMC Web interface.</li><li><b>2</b> Select iKVM in the system tree.</li><li><b>3</b> Click the <b>Setup</b> tab.</li><li><b>4</b> Clear (un-check) the <b>Front Panel USB/Video Enabled</b> check box.</li><li><b>5</b> Click <b>Apply</b> to save the setting.</li></ol> To disable the front panel using RACADM, open a serial/Telnet/SSH text console to the CMC, log in, and type: <pre>racadm config -g cfgKVMInfo -o cfgKVMFrontPanelEnable 0</pre>



**Table 9-6. Troubleshooting iKVM (continued)**

<b>Problem</b>	<b>Likely Cause and Solution</b>
<p>In the OSCAR menu, the Dell CMC connection is displaying a red X, and I cannot connect to the CMC.</p>	<p>There are two possible causes:</p> <p><b>The Dell CMC console has been disabled.</b> 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"><li>1 Log in to the CMC Web interface.</li><li>2 Select <b>iKVM</b> in the system tree.</li><li>3 Click the <b>Setup</b> tab.</li><li>4 Select the <b>Allow access to CMC CLI from iKVM</b> check box.</li><li>5 Click <b>Apply</b> to save the setting.</li></ol> <p>To enable the Dell CMC connection using RACADM, open a serial/Telnet/SSH text console to the CMC, log in, and type:</p> <pre>racadm config -g cfgKVMInfo -o cfgKVMAccessToCMCEnable 1</pre> <p><b>The CMC is unavailable because it is initializing, switching over to the standby CMC, or reprogramming.</b> In this case, simply wait until the CMC finishes initializing.</p>
<p>The slot name for a server is displayed as "Initializing" in OSCAR, and I cannot select it.</p>	<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 will appear 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 will allow 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.

The chassis supports three fabric or protocol types. The IOMs and MCs 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 will always be 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.

Each MC can support two external links. For example, in the first MC, the first link is permanently connected to the IOM in slot 1 of Group B, and the second link is permanently connected to the IOM in slot 2 of Group B.



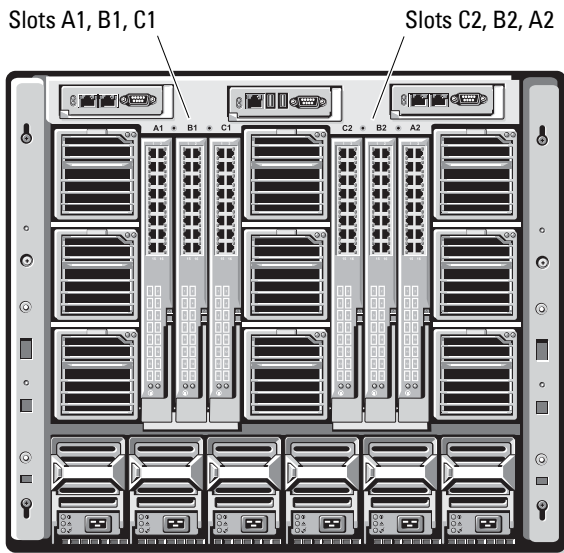
**NOTE:** In the CMC CLI, IOMs are referred to by the convention, switch-*n*: A1=switch-1, A2=switch-2, B1=switch-3, B2=switch-4, C1=switch-5, and C2=switch-6.

# 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 will prevent invalid configurations from powering on.

Figure 10-1 shows the location of IOMs in the chassis. The location of each IOM is indicated by its group number (A, B, or C) and slot number (1 or 2). On the chassis, the IOM slot names are marked A1, A2, B1, B2, C1, and C2.

**Figure 10-1. Rear View of a Chassis, Showing the Location of the IOMs**



The 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, the CMC will power-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 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.

## Invalid Configurations

There are three types of invalid configurations:

- Invalid MC configuration, where a newly installed MC'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 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 will not be allowed to power on.

## **Invalid IOM-Mezzanine Card (MC) Configuration**

The mismatched IOM will be held in the power-off state. The CMC adds an entry to the CMC and hardware logs noting the invalid configuration and specifying the IOM name. The CMC will also cause the error LED on the offending IOM to blink. If the CMC is configured to send alerts, it sends e-mail and/or SNMP alerts for this event.

For information about the CMC and hardware logs, see "Viewing the Event Logs."

## **Invalid IOM-IOM Configuration**

The CMC holds the newly installed IOM in powered-off state, causes the IOM's error LED to blink, and creates entries in the CMC and hardware logs about the mismatch.

For information about the CMC and hardware logs, see "Viewing the Event Logs."

## **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 the 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 the 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 the CMC; an adverse condition may exist.
  - Gray - IOM is present and not powered on. It is not communicating with the 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** sub-tab. The **I/O Modules Status** page displays. Table 10-1 provides descriptions of the information provided on the **I/O Modules Status** page.


**Table 10-1. I/O Modules Status Information**

Item	Description	
Slot	Indicates the location of the I/O module in the chassis by group number (A, B, or C) and slot number (1 or 2). Slot names: <b>A1, A2, B1, B2, C1, or C2.</b>	
Present	Indicates whether the IOM is present ( <b>Yes</b> or <b>No</b> ).	
Health	 <b>OK</b>	Indicates that the IOM is present and communicating with the CMC. In the event of a communication failure between the CMC and the server, the CMC cannot obtain or display health status for the IOM.
	 <b>Informational</b>	Displays information about the IOM when no change in health status ( <b>OK, Warning, Severe</b> ) has occurred.
	 <b>Warning</b>	<p>Indicates that warning alerts have been issued, and <b>corrective action must be taken</b>. 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>
	 <b>Severe</b>	<p>Indicates at least one Failure alert has been issued. Severe status represents a system failure on the IOM, and <b>corrective action must be taken immediately</b>.</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."



**Table 10-1. I/O Modules Status Information (continued)**

Item	Description
Fabric	<p>Indicates 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><b>NOTE:</b> 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."</p>
Name	Displays the IOM product name.
Launch IOM Management Console	<p>If the icon 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><b>NOTE:</b> 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><b>NOTE:</b> 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><b>NOTE:</b> You will be prompted to log in to I/O module management interface.</p> <p><b>NOTE:</b> You can configure the I/O module IP address using the CMC GUI, as described in "Configuring Network Settings for an Individual IOM."</p>
Role	<p>When linking I/O modules together, the Role displays the I/O Module stacking membership. <b>Member</b> means the module is part of a stack set. <b>Master</b> indicates the module is a primary access point.</p>
Power Status	Indicates the power status of the IOM: <b>On</b> , <b>Off</b> , or <b>N/A</b> (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."</p> <p><b>NOTE:</b> 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** sub-tab. The **I/O Modules Status** page displays.

Table 10-2 provides descriptions of the information provided on the **I/O Module Status** page.

**Table 10-2. I/O Module Health Status Information**

Item	Description
Location	Indicates the location of the IOM in the chassis by group number (A, B, or C) and slot number (1 or 2). Slot names: <b>A1, A2, B1, B2, C1, or C2</b> .
Name	Displays name of the IOM.
Present	Indicates whether the IOM is <b>Present</b> or <b>Absent</b> .
Health	 <b>OK</b> Indicates that the IOM is present and communicating with the CMC. In the event of a communication failure between the CMC and the server, the CMC cannot obtain or display health status for the IOM.
	 <b>Informational</b> 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 10-2. I/O Module Health Status Information (continued)**


Item	Description
 Warning	<p>Indicates that warning alerts have been issued, and <b>corrective action must be taken</b>. 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 at least one Failure alert has been issued. Severe status represents a system failure on the IOM, and <b>corrective action must be taken immediately</b>.</p> <p>Examples of conditions causing Severe status: Failure in IOM detected; IOM was removed.</p> <p><b>NOTE:</b> Any change in health is logged to both the hardware and CMC log. For information on viewing logs, see "Viewing the Hardware Log" and "Viewing the CMC Log."</p>
Power Status	Indicates the power status of the IOM: <b>On</b> , <b>Off</b> , or <b>N/A</b> (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>Indicates 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><b>NOTE:</b> 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."</p>


**Table 10-2. 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. <b>NOTE:</b> 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>• <b>Member</b> - the module is part of a stack set</li><li>• <b>Master</b> - the module is a primary access point.</li></ul>


### 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 will result 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** sub-tab. 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 the 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 10-3. Configure I/O Module Network Settings**

Item	Description
Slot	Indicates 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.)
DHCP Enabled	<p>Enables the IOM on the chassis to request and obtain an IP address from the Dynamic Host Configuration Protocol (DHCP) server automatically.</p> <p>Default: Checked (enabled).</p> <p>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><b>NOTE:</b> 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>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:

- The CMC can read the IP address setting too quickly after a configuration change; it will display **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 will not set the IP address and will return 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.

- 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
- Disabling forgotten password
- Error codes and logs

## Chassis Monitoring Tools

### 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** sub-tab. 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 the CMC, log in, and type:

```
racadm setled -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 the CMC.



You can configure the CMC to generate event traps. Table 11-1 provides an overview of the events that trigger SNMP and e-mail alerts. For information on e-mail alerts, see "Configuring E-mail Alerts."



**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 11-1. Chassis Events That Can Generate SNMP**

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 11-1. Chassis Events That Can Generate SNMP***(continued)*

<b>Event</b>	<b>Description</b>
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.

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, Dell strongly recommends that you change the default password of the root (User 1) account. The root account is the default administrative account that ships with the 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 **Alert Management** 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** sub-tab. 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/Security→Services** page. The SNMP traps community string is the community that the CMC uses for outbound traps destined to management stations. The community string on the **Chassis→Network/Security→Services** page is the community string that management stations use to query the SNMP daemon on the 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 **Alert Management** tab. The **Chassis Events** page appears.
- 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 **testtrap** 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 the 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 the CMC to generate by typing:

```
racadm config -g cfgAlerting -o  
cfgAlertingFilterMask <mask value>
```

where *<mask value>* is a hex value between 0x0 and 0x017ffdf.

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 11-2. Event Traps Filter Masks**

<b>Event</b>	<b>Filter Mask Value</b>
Fan Probe Failure	0x1
Battery Probe Warning	0x2
Temperature Probe Warning	0x8
Temperature Probe Failure	0x10
Redundancy Degraded	0x40
Redundancy Lost	0x80
Power Supply Warning	0x800
Power Supply Failure	0x1000
Power Supply Absent	0x2000
Hardware Log Failure	0x4000
Hardware Log Warning	0x8000
Server Absent	0x10000
Server Failure	0x20000
KVM Absent	0x40000
KVM Failure	0x80000
IOM Absent	0x100000
IOM Failure	0x200000
Firmware Version Mismatch	0x00400000
Chassis Power Threshold Error	0x01000000

- 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 the 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 will 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 cfgTraps -i <index>**. If the index is configured, values will appear for the **cfgTrapsAlertDestIPAddr** and **cfgTrapsCommunityName** objects.

To test an event trap for an alert destination:

```
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 the 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 11-1 provides an overview of the events that trigger e-mail and SNMP alerts. For information on SNMP alerts, see "Configuring SNMP Alerts."

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 **Alert Management** 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** sub-tab. 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 the CMC. If you choose 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 the CMC is used (for example, `emailname@[IP_address]`).
  - c Click **Apply** to save your changes.
- 7** Specify the e-mail address(es) that will 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 **Alert Management** tab. The **Chassis Events** page appears.
- 4** Click the **Email Alert Settings** sub-tab. 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 the 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 the CMC to generate by typing:

```
racadm config -g cfgAlerting -o  
cfgAlertingFilterMask <mask value>
```

where <mask value> is a hexadecimal value between 0x0 and 0x017ffdf and must be expressed with the leading 0x characters.

Table 11-2 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."

- 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 the 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 steps 4 and 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 `cfgRhostsSmtplibServerIpAddr` database property by typing:

```
racadm config -g cfgRemoteHosts -o  
cfgRhostsSmtplibServerIpAddr 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 steps 2–6.



**NOTE:** The commands in steps 2–6 will 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 will 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 the CMC and configuring power budget, redundancy, and power control, see "Power Management."

### 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."

## 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," "Executing Power Control Operations on an IOM," and "Executing Power Control Operations on a Server."

## Power Supply Troubleshooting

Use the items below to assist in troubleshooting power supply and power-related issues:

- **Problem:** Attempted to configure the **Power Redundancy Policy** to **AC Redundancy**, but it failed.
  - **Resolution A:** This operation requires 2, 4, or 6 power supplies (1, 2, or 3 in each grid) receiving input power to be present and functional in the modular enclosure. For full **AC Redundancy** operation, ensure that a full PSU configuration of six power supplies is available before an attempt is made to change the redundancy policy to **AC Redundancy**.
  - **Resolution B:** Check if all power supplies are properly connected to the two AC grids; the left three power supplies need to be connected to an AC grid and the right three power supplies need to be connected to the other AC grid, and both AC grids are working. You cannot configure power redundancy to **AC Redundancy** when one of the AC grid 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:** 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.

- **Problem:** Dynamic Power Supply Engagement is enabled, but none of the power supplies display in the **Standby** state.
  - **Resolution:** This will occur if there is a six power supply configuration for **AC Redundancy**, and enclosure operation requires power capacity of at least three power supplies. Only when the surplus power available in the enclosure exceeds the capacity of at least one power supply that a pair of power supplies, one power supply from each of the **Online** and **Redundant** power supply sets, is moved to the **Standby** state.
- **Problem:** Inserted a new server into the enclosure with six power supplies, but the server won't 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 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 will 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 will allow for additional power allocation to the fans without an impact on server performance.

# Viewing Chassis Summaries

The CMC provides rollup overviews of the chassis, primary 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 11-3, Table 11-4, Table 11-5, and Table 11-6 describe the information provided.

**Table 11-3. 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 104.
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	Indicates ( <b>Yes</b> , <b>No</b> ) 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 11-4. CMC Summary**

<b>Item</b>	<b>Description</b>
<b>Primary CMC Information</b>	
Name	Displays the name of the CMC. For example, Primary CMC or Standby CMC.
Description	Provides a brief description of the purpose of the CMC.
Date/Time	Indicates the date and time set on the active or primary CMC.
Active CMC Location	Indicates the slot location of the active or primary CMC.
Redundancy Mode	Displays if the standby CMC is present in the chassis.
Primary Firmware Version	Indicates the firmware version of the active or primary CMC.
Firmware Last Updated	Indicates when the firmware was last updated. If no updates have occurred, this property displays as N/A.
Hardware Version	Indicates the hardware version of the active or primary CMC.
MAC Address	Indicates the MAC address for the CMC NIC. The MAC address is a unique identifier for the CMC over the network.
IP Address	Indicates the IP address of the CMC NIC.
Gateway	Indicates the gateway of the CMC NIC.
Subnet Mask	Indicates the subnet mask of the CMC NIC.
Use DHCP (for NIC IP Address)	Indicates whether the 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	Indicates the primary DNS server name.
Alternate DNS Server	Indicates the alternate DNS server name.
Use DHCP for DNS Domain Name	Indicates use of DHCP to acquire the DNS Domain name (Yes, No).
DNS Domain Name	Indicates the DNS Domain name.

**Table 11-4. CMC Summary (continued)**

<b>Item</b>	<b>Description</b>
<b>Standby CMC Information</b>	
<b>Present</b>	Displays ( <b>Yes</b> , <b>No</b> ) whether a second (standby) CMC is installed.
<b>Standby Firmware Version</b>	Displays the CMC firmware version installed on the standby CMC.

**Table 11-5. iKVM Summary**

<b>Item</b>	<b>Description</b>
<b>Present</b>	Indicates whether the iKVM module is present ( <b>Yes</b> or <b>No</b> ).
<b>Name</b>	<b>Displays the name of the iKVM. The name identifies the iKVM on the network.</b>
<b>Manufacturer</b>	Displays the iKVM model or manufacturer.
<b>Part Number</b>	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.
<b>Firmware Version</b>	Indicates the firmware version of the iKVM.
<b>Hardware Version</b>	Indicates the hardware version of the iKVM.
<b>Power Status</b>	Indicates the power status of the iKVM: <b>On</b> , <b>Off</b> , <b>N/A</b> ( <b>Absent</b> ).
<b>Front Panel USB/Video Enabled</b>	Indicates whether the front panel VGA and USB connectors are enabled ( <b>Yes</b> or <b>No</b> ).
<b>Allow Access to CMC CLI from iKVM</b>	Indicates that CLI access is enabled on the iKVM ( <b>Yes</b> or <b>No</b> ).

**Table 11-6. IOM Summary**

<b>Item</b>	<b>Description</b>
<b>Location</b>	Indicates 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.
<b>Present</b>	Indicates whether the IOM is present ( <b>Yes</b> or <b>No</b> ).
<b>Name</b>	Displays the name of the IOM.
<b>Fabric</b>	Displays the type of fabric.
<b>Power Status</b>	Indicates the power status of the IOM: <b>On</b> , <b>Off</b> , or <b>N/A</b> (Absent).
<b>Service Tag</b>	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 the CMC and log in.

**2** To view chassis and CMC summaries, type:

```
racadm getsysinfo
```

To view the iKVM summary, type:

```
racadm getkvminfo
```

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 Status** 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 color of the component subgraphic.






- Green - the component is present, powered on and communicating with the CMC; there is no indication of an adverse condition.
- Amber - the component is present, but may or may not be powered on, or may or may not be communicating with the CMC; an adverse condition may exist.
- Gray - the component is present and not powered on. It is not communicating with the 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.

The component subgraphic is also hyperlinked to the corresponding CMC GUI page to provide immediate navigation to the status page for that component.

The **Component Health** section displays status for each component with an icon. Table 11-7 provides descriptions of each icon.

**Table 11-7. Health Status Indicators**

Item	Description
	OK Indicates that the component is present and communicating with the CMC.
	Informational Displays information about the component when there is no change in health status.
	Warning Indicates that only Warning alerts have been issued, and <b>corrective action must be taken</b> . If corrective actions are not taken within administrator-specified time, it could lead to a component failure, communication failure between the component and the CMC, and a critical or severe failure that could affect the integrity of the chassis.
	Severe Indicates that at least one failure alert has been issued. This means that the CMC can still communicate with the component and that the health status reported is critical. <b>Corrective action must be taken immediately</b> . Failure to do so may cause the component to fail and stop communicating with the CMC.
	Unknown Displays when the chassis is first powered on. All chassis components initially are indicated as "unknown" until they are fully powered on.
	No Value Indicates that the component is absent from the slot, or the CMC cannot communicate with the component. <b>NOTE:</b> It is not possible for the chassis to be absent.

### Using RACADM

Open a serial/Telnet/SSH text console to the 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

The 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 the CMC to send e-mail or SNMP traps when specific events occur. For information on configuring CMC to send alerts, see "Configuring SNMP Alerts" and "Configuring E-mail Alerts."

### Examples of hardware log entries

```
critical System Software event: redundancy lost
```

```
Wed May 09 15:26:28 2007 normal System Software  
event: log cleared was asserted
```

```
Wed May 09 16:06:00 2007 warning System Software  
event: predictive failure was asserted
```

```
Wed May 09 15:26:31 2007 critical System Software  
event: log full was asserted
```

```
Wed May 09 15:47:23 2007 unknown System Software  
event: unknown event
```

### Using the Web Interface


You can view, save a text file version of, and clear the hardware log in the CMC Web interface.

Table 11-8 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** sub-tab. The **Hardware Log** page displays.






To save a copy of the hardware log to your managed station or network:  
Click **Save Log**. A dialog box opens; 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:** The CMC creates a new log entry indicating that the log was cleared.

**Table 11-8. Hardware Log Information**

Item	Description
Severity	<p> OK Indicates a normal event that does not require corrective actions.</p> <p> Informational Indicates an informational entry on an event in which the Severity status has not changed.</p> <p> Unknown Indicates a noncritical event for which <b>corrective actions should be taken soon</b> to avoid system failures.</p> <p> Warning Indicates a critical event requiring immediate corrective actions to avoid system failures.</p> <p> Severe Indicates a critical event that <b>requires immediate corrective actions</b> to avoid system failures.</p>
Date/Time	Indicates 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 the CMC, of the event (for example, Redundancy lost, Server inserted).

## Using RACADM

1 Open a serial/Telnet/SSH text console to the CMC and log in.

2 To view the hardware log, type:

```
racadm getssel
```

To clear the hardware log, type:

```
racadm clrssel
```

## Viewing the CMC Log

The 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 11-9 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** sub-tab. The **CMC Log** page displays.

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 11-9. CMC Log Information**

<b>Command</b>	<b>Result</b>
Source	Indicates the interface (such as the CMC) that caused the event.
Date/Time	Indicates 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 the CMC.

### Using RACADM

**1** Open a serial/Telnet/SSH text console to the CMC and log in.

**2** To view the hardware log, type:

```
racadm getraclog
```

To clear the hardware log, type:

```
racadm clrraclog
```

### Firmware Update Error Codes

The CMC log can also display error codes as part of the log information. The table below contains the firmware update CMC log error codes.

**Table 11-10. Firmware Update Error Codes**

<b>Error Class</b>	<b>Error Value (Hex)</b>	<b>Error Value (Decimal)</b>
ERR_NO_PRIVILEGE	0x1400	5120
ERR_LOC_CMC_STATE	0x1401	5121
ERR_INV_TARG_LINK	0x1402	5122
ERR_ILLEGAL_CMC_STATE	0x1403	5123
ERR_MX_NULL_PARAM	0x1404	5124
ERR_CLASS_UNSUPPORTED	0x1405	5125
ERR_INAPPROPRIATE_REQUEST	0x1406	5126
ERR_MX_BAD_PARAM	0x1407	5127
ERR_INVALID_TARGET	0x1408	5128
ERR_URL_NOT_FOUND	0x1409	5129

**Table 11-10. Firmware Update Error Codes (continued)**

<b>Error Class</b>	<b>Error Value (Hex)</b>	<b>Error Value (Decimal)</b>
ERR_CANCEL_PID_KILL	0x140A	5130
ERR_REROUTE_PEER	0x140B	5131
ERR_BAD_URL	0x140C	5132
ERR_PAYLOAD_TOO_BIG	0x140D	5133
ERR_BAD_IP_CONV	0x140E	5134
ERR_BAD_HDR_PARAM	0x140F	5135
ERR_BAD_FILENAME	0x1410	5136
ERR_TARGET_NOT_READY	0x1411	5137
ERR_TFTP_GET_FAIL	0x1412	5138
ERR_WAITPID_FAIL	0x1413	5139
ERR_REBOOT_FAIL	0x1414	5140
ERR_UNSUPPORTED_PROTOCOL	0x1415	5141
BAD_FTP_PASSWORD	0x1416	5142
ERR_FORK_FAILED	0x1417	5143
ERR_MALLOC_ERROR	0x1418	5144
ERR_PEER_ABSENT	0x1419	5145
ERR_UPDATE_FAIL	0x141A	5146
ERR_OPEN_FILE_FAIL	0x141B	5147
ERR_IMAGE_FILE_NOT_ACCESSIBLE	0x141C	5148
ERR_FCNTL_GET_FAIL	0x141D	5149
ERR_FCNTL_SET_FAIL	0x141E	5150
ERR_POLL_FAIL	0x141F	5151
ERR_SEND_FAIL	0x1420	5152
ERR_CONNECT_FAIL	0x1421	5153
ERR_SOCKET_FAIL	0x1422	5154
ERR_RESOLVE_REMOTE_IP_ADDR_FAIL	0x1423	5155
ERR_TIMEOUT	0x1424	5156
ERR_RECV_FAIL	0x1425	5157
ERR_INVENTORY_COUNT	0x1426	5158

**Table 11-10. Firmware Update Error Codes (continued)**

<b>Error Class</b>	<b>Error Value (Hex)</b>	<b>Error Value (Decimal)</b>
ERR_FWUPD_INIT_CALL	0x1427	5159
ERR_FWUPD_START_UPDATE_CALL	0x1428	5160
ERR_OP_NOT_CANCELABLE	0x1429	5161
BAD_FTP_USERNAME	0x142A	5162
DEVICE_NOT_AVAILABLE	0x142B	5163

## 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** sub-tab. 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 11-11 as well as the RACADM commands.



**Table 11-11. 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 the 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 <b>gettracelog -i</b> command returns the number of records in the trace log. <b>NOTE:</b> For more information about the <b>gettracelog</b> command, see the <b>gettracelog</b> command section in the <i>Dell Chassis Management Controller Administrator Reference Guide</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 will cause a failover and the standby CMC will become 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** sub-tab. The **Reset Components** page displays. The **CMC Summary** section of the **Reset Components** page displays the following information:

**Table 11-12. CMC Summary**

Attribute	Description
Health	<div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;">  OK    Informational    Warning    Severe         </div> <div> <p>The CMC is present and communicating with its components.</p> <p>Displays information about the CMC when no change in health status (OK, Warning, Severe) has occurred.</p> <p>Warning alerts have been issued, and <b>corrective action must be taken</b>. If corrective actions are not taken within the administrator-specified time, critical or severe failures that can affect the integrity of the CMC can occur.</p> <p>At least one failure alert has been issued. Severe status represents a CMC system failure, and <b>corrective action must be taken immediately</b>.</p> </div> </div>
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 primary CMC.
Redundancy Mode	Displays <b>Redundant</b> if a standby CMC is present in the chassis, and <b>No Redundancy</b> if no standby CMC is present in the chassis.

5 The **Virtual Reseat Server** section of the **Reset Components** page displays the following information:

**Table 11-13. Virtual Reseat Server**

<b>Attribute</b>	<b>Description</b>
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 ( <b>Yes</b> or <b>No</b> ).
Health	 OK The server is present and communicating with the CMC. In the event of a communication failure between the 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 <b>corrective action must be taken</b> . If corrective actions are not taken within the administrator-specified time, 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 <b>corrective action must be taken immediately</b> .

**Table 11-13. Virtual Reseat Server**

Attribute	Description
iDRAC Status	<p data-bbox="292 284 799 336">Displays the status of the server iDRAC embedded management controller:</p> <ul data-bbox="292 352 934 722" style="list-style-type: none"><li data-bbox="292 352 897 376">• <b>N/A</b> - Server is not present, or the chassis is not powered on.</li><li data-bbox="292 392 781 416">• <b>Ready</b> - iDRAC is ready and operating normally.</li><li data-bbox="292 432 891 485">• <b>Corrupted</b> - iDRAC firmware is corrupted. Use the iDRAC firmware update utility to repair the firmware.</li><li data-bbox="292 501 922 584">• <b>Failed</b> - 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.</li><li data-bbox="292 600 900 652">• <b>FW Update</b> - iDRAC firmware update in progress; allow the update to complete before attempting any action.</li><li data-bbox="292 668 934 722">• <b>Initializing</b> - iDRAC reset in progress; wait for the controller to complete powering-on before attempting any action.</li></ul>
Power State	<p data-bbox="292 743 613 767">Displays the server power status:</p> <ul data-bbox="292 783 956 1026" style="list-style-type: none"><li data-bbox="292 783 956 807">• <b>N/A</b> - The CMC has not determined the power state of the server.</li><li data-bbox="292 823 669 847">• <b>Off</b> - The server or the chassis is off.</li><li data-bbox="292 863 656 887">• <b>On</b> - The chassis and server are on.</li><li data-bbox="292 903 945 957">• <b>Powering On</b> - Temporary state between Off and On. Once the powering on cycle completes, the Power State will change to On.</li><li data-bbox="292 973 945 1026">• <b>Powering Off</b> - Temporary state between On and Off. Once the powering off cycle completes, the Power State will change to Off.</li></ul>
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 the 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. The 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 the 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.

The CMC provides tools to troubleshoot these problems, with the primary source of troubleshooting information being the CMC trace log. This log will contain an error message for NTP related failures. If the CMC is unable to synchronize with any of the remote NTP servers that have been configured, then it will derive its timing from the local system clock.

If the CMC is synchronized to the local system clock rather than a remote time server, the trace log will contain the 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 you believe that the NTP servers are correctly configured and this entry is present in the trace log, then it is a confirmation that the CMC is not able 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" 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").

Table 11-14 lists common LED patterns on the chassis.

**Table 11-14. LED Color and Blinking Patterns**

<b>Component</b>	<b>LED Color, Blinking Pattern</b>	<b>Meaning</b>
CMC	Green, glowing steadily	Powered on
	Green, blinking	Firmware is being uploaded
	Green, dark	Powered off
	Blue, glowing steadily	Master/primary
	Blue, blinking	User-enabled module identifier
	Amber, glowing steadily	Not used
	Amber, blinking	Fault
	Blue, dark	Slave/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 11-14. LED Color and Blinking Patterns (continued)**

<b>Component</b>	<b>LED Color, Blinking Pattern</b>	<b>Meaning</b>
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 11-14. 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 the 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 the 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 the CMC as it is installed in the chassis, you will 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 the CMC, reinstall the CMC making sure the board is inserted all the way and the latch closes correctly.

Bottom LED — The bottom LED is multi-colored. When the 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 the 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 the CMC.

To obtain recovery information:

- 1 Install a NULL modem cable between the 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 will display an error message every 5 seconds.
- 3 Press <Enter>. If a **recovery** prompt appears, additional information is available. The prompt will indicate 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 the CMC. The CMC is bad and must be returned to Dell.
- If the prompt indicates **Bad FW Images**, then follow the steps in "Recovering the Firmware Image" to fix the problem.

## Recovering the Firmware Image

The 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 the 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 *Dell Chassis Management Controller Administrator Reference Guide*).

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.

## Disabling a Forgotten 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 11-1. 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 will be reset regardless if the account has been removed, or if the password was changed.



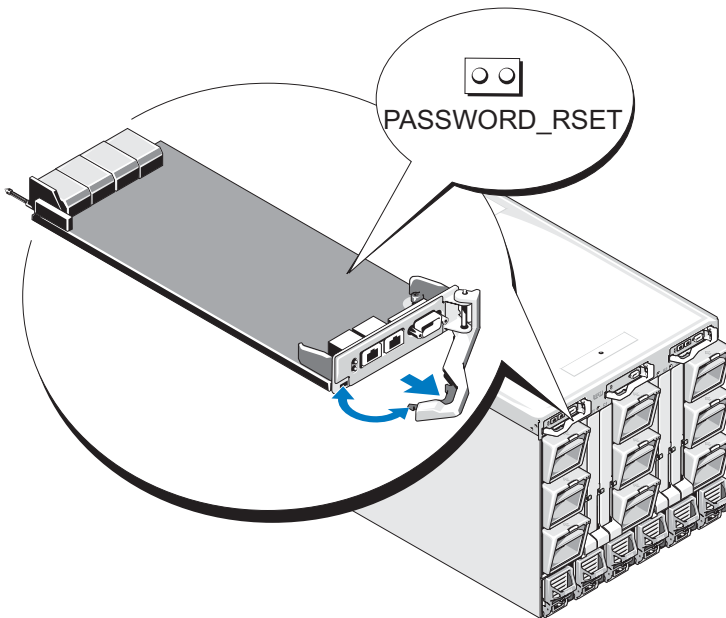
**NOTE:** Ensure the CMC module is in a passive state before you begin.

- 1 Press in the CMC release latch on the handle and rotate the handle away from the module front panel. Slide the CMC module out of the enclosure.



**NOTE:** Electrostatic discharge (ESD) events can harm electronic components inside your equipment. Under certain conditions, ESD may build up on your body or an object, and then discharge into another object, such as your CMC. To prevent ESD damage, you should discharge static electricity from your body before you interact with any of your equipment’s internal electronic components.

- 2 Remove the jumper plug from the password reset connector, and insert a 2-pin jumper to enable the default administrator account. See Figure 11-1 to locate the password jumper on the CMC board.

**Figure 11-1. Password Reset Jumper Location**



**Table 11-15. CMC Password Jumper Settings**

PASSWORD_RESET		(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.
- 4 Initiate a changeover to make the module active using the GUI interface to perform the following steps:
  - a Navigate to the **Chassis** page, click the **Power Management** tab - **Control** sub tab.
  - b Select the **Reset CMC (warm boot)** button.
  - c Click **Apply**.
- 5 The CMC automatically fails over to the redundant module, and that module now becomes active. Log into the active CMC using the default administrator username of **root** and password of **calvin**, and restore any necessary user account settings. The existing accounts and passwords are not disabled and are still active.

After you have completed any account updates, remove the 2-pin jumper and replace the jumper plug.



**NOTE:** Make sure the CMC module is in a passive state before you begin.

- 1 Press in the CMC release latch on the handle and rotate the handle away from the module front panel. Slide the CMC module out of the enclosure.
- 2 Remove the 2-pin jumper and replace the jumper plug.
- 3 Slide the CMC module into the enclosure. Reattach any cables that were disconnected.

## 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."

# Glossary

## **Active Directory**

Active Directory is a centralized and standardized system that automates network management of user data, security, and distributed resources, and enables interoperation with other directories. Active Directory is designed especially for distributed networking environments.

## **ARP**

Address resolution protocol, a method for finding a host's Ethernet address from its Internet address.

## **ASCII**

American Standard Code for Information Interchange, a code representation used for displaying or printing letters, numbers, and other characters.

## **blade**

A self-contained server designed for high density racks.

## **BIOS**

Basic input/output system, the part of system software that provides the lowest-level interface to peripheral devices and which controls the first stage of the system boot process, including installation of the operating system into memory.

## **CMC**

The Dell Chassis Management Controller, providing remote management capabilities and power control functions for Dell PowerEdge™ systems.

## **bus**

A set of conductors connecting the various functional units in a computer. Busses are named by the type of data they carry, such as data bus, address bus, or PCI bus.

**CA**

A certificate authority (CA) is a business entity that is recognized in the IT industry for meeting high standards of reliable screening, identification, and other important security criteria. Examples of CAs include Thawte and VeriSign. After the CA receives your CSR, they review and verify the information the CSR contains. If the applicant meets the CA's security standards, the CA issues a certificate to the applicant that uniquely identifies that applicant for transactions over networks and on the Internet.

**CD**

Compact disc

**Certificate Signing Request (CSR)**

A digital request to a certificate authority for a secure server certificate.

**CLI**

Command Line interface

**DHCP**

Dynamic host configuration protocol, a means of dynamically allocating IP addresses to computers on a network.

**DLL**

Dynamic link library, a library of functions, any of which can be called when needed by a larger program that is running in the system. The smaller functions let the larger program communicate with a specific device such as a printer or scanner.

**DNS**

Domain name system

**iDRAC**

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

**delay time (OSCAR user interface)**

The number of seconds before the OSCAR Main dialog box is displayed after <Print Screen> is pressed.



**extended schema**

A solution used with Active Directory to determine user access to the CMC; uses Dell-defined Active Directory objects.

**FQDN**

Fully qualified domain name, a domain name that specifies a module's absolute position in the DNS tree hierarchy. Microsoft® Active Directory® only supports an FQDN of 64 bytes or fewer.

**FSMO**

Flexible single master operation, a Microsoft Active Directory domain controller task that guarantees atomicity of an extension operation.

**GB1**

The uplink port on the chassis.

**GMT**

Greenwich Mean Time. GMT is the standard time common to every place in the world. GMT nominally reflects the mean solar time along the prime meridian (0 longitude) that runs through the Greenwich Observatory outside of London, UK.

**GUI**

Graphical user interface, which refers to a computer display interface that uses elements such as windows, dialog boxes, and buttons as opposed to a command prompt interface, in which all user interaction is displayed and typed in text.

**hardware log**

A CMC-generated record of events relating to hardware on the chassis.

**ICMP**

Internet control message protocol, a way for operating systems to send error messages.

**ID**

Identifier, commonly used when referring to a user identifier (user ID) or object identifier (object ID).

**iKVM**

Avocent® Integrated KVM Switch Module, an optional, hot-pluggable module to the chassis providing local access to keyboard, mouse, and video to any of the 16 servers in the chassis, as well as the additional Dell CMC Console option that connects to the chassis' active CMC.

**IOMINF**

I/O module infrastructure device.

**IP**

Internet Protocol. IP is the network layer for TCP/IP. IP provides packet routing, fragmentation, and reassembly.

**IPMB**

Intelligent platform management bus, which is used in systems management technology.

**Kbps**

Kilobits per second, a data transfer rate.

**LAN**

Local area network

**LDAP**

Lightweight directory access protocol

**LED**

Light-emitting diode

**LOM**

Local area network on motherboard

**MAC**

Media access control, a network sublayer between a network node and the network physical layer.

**MAC address**

Media access control address, a unique address embedded in the physical components of a NIC.

**management station**

A system that remotely accesses the CMC.

**Mbps**

Megabits per second, which is a data transfer rate.

**MC**

Mezzanine card

**Microsoft Active Directory**

A centralized, standardized system that automates network management of user data, security, and distributed resources, and enables interoperability with other directories. Active Directory is designed especially for distributed networking environments.

**NIC**

Network interface card, an adapter circuit board installed in a computer to provide a physical connection to a network.

**Non-Persistent Log**

A log that is cleared when the CMC reboots.

**OID**

Object identifier

**OSCAR**

On Screen Configuration and Reporting, a graphical user interface used for iKVM access.

**PCI**

Peripheral component interconnect, a standard interface and bus technology for connecting peripherals to a system and for communicating with those peripherals.

**POST**

Power-on self-test, a sequence of diagnostic tests that are run automatically by a system when it is powered on.

**RAC**

Remote access controller

**RAM**

Random-access memory. RAM is general-purpose readable and writable memory on systems.

**RAM disk**

A memory-resident program which emulates a hard drive.

**ROM**

Read-only memory, from which data may be read, but to which data cannot be written.

**RPM**

Red Hat Package Manager, a package-management system for the Red Hat Enterprise Linux operating system. RPM manages the installation of software packages. It is similar to an installation program.

**SEL**

System event log or hardware log

**SMTP**

Simple mail transfer protocol, used to transfer electronic mail between systems—usually over an Ethernet.

**SNMP**

Simple network management protocol, designed to manage nodes on an IP network. iDRACs are SNMP-managed devices (nodes).

**SNMP trap**

A notification (event) generated by the CMC that contains information about state changes on the managed system or about potential hardware problems.

**SSH**

Secure Shell, a network protocol that allows data to be exchanged over a secure channel between two computers.

**SSL**

Secure sockets layer, a protocol that provides secure communications over networks for data transfers.

**standard schema**

A solution used with Active Directory to determine user access to the CMC; uses Active Directory group objects only.

**STK**

The staking port on the chassis

**TCP/IP**

Transmission control protocol/Internet protocol, representing the set of standard Ethernet protocols that includes the network layer and transport layer protocols.

**TFTP**

Trivial file transfer protocol, a simple file transfer protocol used for downloading boot code to diskless devices or systems.

**UDP**

User Datagram Protocol

**UPS**

Uninterruptible power supply

**USB**

Universal serial bus, a serial bus standard to interface devices.

**UTC**

Universal Coordinated Time. *See* GMT.

**vKVM**

Virtual keyboard-video-mouse console

**VLAN**

Virtual local area network

**VNC**

Virtual network computing

**VT-100**

Video Terminal 100, which is used by the most common terminal emulation programs.

**WAN**

Wide area network

**WWN**

World Wide Name, a unique value that represents Fibre Channel node in the physical layer.

# Index

## A

- ACI, 289
- Active Directory, 207
  - adding CMC users, 220
  - configuring access to the CMC, 213
  - configuring and managing certificates, 141
  - extending schemas, 213
  - objects, 209
  - schema extensions, 208
  - using with standard schema, 228
- adding
  - SNMP alerts, 328
- alerts
  - troubleshooting, 366
- Analog Console Interface, 287

## C

- Certificate Signing Request (CSR)
  - about, 148
  - generating a new certificate, 149
- certificates
  - Active Directory, 141
  - SSL and digital, 147
  - uploading a server certificate, 152
  - viewing a server certificate, 153

## CMC

- configuring, 223, 230
- creating a configuration file, 89
- downloading firmware, 45
- feature sets, 18
- installing, 29
- log, 349
- redundant environment, 49
- setting up, 29
- command line console
  - features, 51
- configuration file
  - creating, 89
- configuring
  - CMC from the LCD panel, 45
  - CMC remote RACADM, 44
  - power budgeting, 45
  - remote RACADM, 44
  - SNMP alerts, 328
- connect command
  - CMC command line connection, 56

## F

- fabric management, 315
- feature sets of CMC, 18
- featurecard, 191

- firmware
  - downloading, 45
  - managing, 163
  - updating, CMC, 164
  - updating, iKVM, 166
  - updating, IOM infrastructure device, 167
  - updating, Server iDRAC, 168

- FlexAddress, 189
  - activating, 190
  - activation verification, 191
  - configuring using CLI, 194
  - deactivating, 193
  - license agreement, 202
  - Linux configuration, 195
  - troubleshooting, 196
  - viewing status using CLI, 195
  - Wake-On-LAN, 196

- frequently asked questions
  - managing and recovering a remote system, 186
  - using the CMC with Active Directory, 234

## H

- hardware log, 347
- hardware specifications, 21

## I

- I/O fabric, 315
- iDRAC
  - recovering firmware, 169
- iKVM, 287
- installing CMC, 29

## L

- LDC panel
  - configuring CMC from, 45
- logs
  - CMC, 349
  - hardware, 347

## M

- managed system
  - accessing through the local serial port, 52
- management station
  - configuring terminal emulation, 54
- MC
  - definition, 371
- mezzanine card. See also MC
- Microsoft Active Directory, 207



## **N**

- network properties
  - configuring manually, 74
  - configuring using racadm, 74

## **O**

- OSCAR, 287

## **P**

- parsing rules, 90
- password
  - disabling, 364
  - reset jumper location, 365
- power budgeting
  - configuring, 45
- power conservation, 259
- proxy server, 32

## **R**

- RAC
  - see Remote Access Connection, 23
- RACADM
  - uninstalling from Linux management station, 31
- racadm utility
  - configuring network properties, 74
  - parsing rules, 90

- Red Hat Enterprise Linux
  - configuring for serial console redirection, 59

- redundant environment, 49
- remote access connection (RAC), 23

- remote RACADM
  - configuring, 44

## **S**

- Secure Sockets Layer (SSL)
  - about, 147
- security
  - using SSL and digital certificates, 147
- serial console
  - using, 52
- server certificate
  - uploading, 152
  - viewing, 153
- services
  - configuring, 154
- setting up CMC, 29
- Single Sign-On, 236
- slot names
  - editing, 104
  - naming rules, 104
- snap-in
  - installing the Dell extension, 219

- SNMP alerts
  - adding and configuring, 328
- specifications
  - hardware, 21
- standard schema
  - using with Active Directory, 228

## **T**

- telnet console
  - using, 52

## **W**

- web browser
  - configuring, 31
  - supported browsers, 24
- web interface
  - accessing, 97
  - configuring email alerts, 334
- WS-Management, 24