



Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide, Release 1.5

First Published: March 04, 2013

Last Modified: December 12, 2013

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-28993-03

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2009-2013 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface

Preface **xiii**

Audience **xiii**

Conventions **xiii**

New and Changed Information for this Release **xv**

Related Cisco UCS Documentation **xvii**

CHAPTER 1

Overview **1**

Overview of the Cisco UCS C-Series Rack-Mount Servers **1**

Overview of the Server Software **1**

Cisco Integrated Management Controller **2**

CIMC CLI **3**

Command Modes **3**

Command Mode Table **5**

Complete a Command **8**

Command History **8**

Committing, Discarding, and Viewing Pending Commands **8**

Command Output Formats **8**

Online Help for the CLI **9**

CHAPTER 2

Installing the Server OS **11**

OS Installation Methods **11**

KVM Console **11**

Installing an OS Using the KVM Console **12**

PXE Installation Servers **12**

Installing an OS Using a PXE Installation Server **12**

Booting an Operating System from a USB Port **13**

CHAPTER 3**Managing the Server 15**

- Overview to DHCP User Friendliness 15
- Toggling the Locator LED 16
- Toggling the Locator LED for a Hard Drive 16
- Managing the Server Boot Order 17
 - Server Boot Order 17
 - Configuring the Server Boot Order 17
 - Viewing the Actual Server Boot Order 18
- Resetting the Server 19
- Shutting Down the Server 19
- Managing Server Power 20
 - Powering On the Server 20
 - Powering Off the Server 20
 - Power Cycling the Server 21
- Configuring Power Policies 22
 - Viewing the Power Statistics 22
 - Power Capping Policy 23
 - Configuring the Power Cap Policy 23
 - Configuring the Power Restore Policy 25
- Configuring Fan Policies 26
 - Fan Control Policies 26
 - Configuring a Fan Policy 27
- Managing the Flexible Flash Controller 28
 - Cisco Flexible Flash 28
 - Upgrading from Single Card to Dual Card Mirroring with FlexFlash 30
 - Configuring the Flexible Flash Controller Properties 31
 - Booting from the Flexible Flash 32
 - Resetting the Flexible Flash Controller 33
 - Resetting the Configuration of the Cards in the Cisco Flexible Flash Controller 34
 - Retaining the Configuration of the Flexible Flash Controller 35
- Configuring BIOS Settings 36
 - Viewing BIOS Status 36
 - Configuring Main BIOS Settings 37
 - Configuring Advanced BIOS Settings 38

Configuring Server Management BIOS Settings	39
Restoring BIOS Defaults	39
Restoring BIOS Manufacturing Custom Defaults	40
Updating Firmware on Server Components	41

CHAPTER 4

Viewing Server Properties 43

Viewing Server Properties	43
Viewing CIMC Properties	44
Viewing CPU Properties	44
Viewing Memory Properties	45
Viewing Power Supply Properties	46
Viewing Storage Properties	46
Viewing Storage Adapter Properties	46
Viewing the Flexible Flash Controller Properties	48
Viewing Physical Drive Properties	49
Viewing Virtual Drive Properties	50
Viewing Nvidia GPU Card Information	51
Viewing PCI Adapter Properties	52
Viewing Network Related Properties	52
Viewing LOM Properties	52

CHAPTER 5

Viewing Server Sensors 55

Viewing Power Supply Sensors	55
Viewing Fan Sensors	56
Viewing Temperature Sensors	56
Viewing Voltage Sensors	57
Viewing Current Sensors	58
Viewing Storage Sensors	58

CHAPTER 6

Managing Remote Presence 61

Managing the Virtual KVM	61
KVM Console	61
Enabling the Virtual KVM	62
Disabling the Virtual KVM	62
Configuring the Virtual KVM	63

Configuring Virtual Media	64
Configuring a CIMC-Mapped vMedia Volume	65
Viewing CIMC-Mapped vMedia Volume Properties	66
Removing a CIMC-Mapped Mounted vMedia Volume	67
Managing Serial over LAN	68
Serial Over LAN	68
Guidelines and Restrictions for Serial Over LAN	68
Configuring Serial Over LAN	68
Launching Serial Over LAN	70

CHAPTER 7

Managing User Accounts	71
Configuring Local Users	71
LDAP Servers	72
Configuring the LDAP Server	73
Configuring LDAP in CIMC	74
Configuring LDAP Groups in CIMC	75
Viewing User Sessions	77
Terminating a User Session	77

CHAPTER 8

Configuring Network-Related Settings	79
Server NIC Configuration	79
Server NICs	79
Configuring Server NICs	80
Configuring Common Properties	81
Configuring IPv4	82
Configuring the Server VLAN	84
Connecting to a Port Profile	85
Network Interface Configuration	86
Overview to Network Interface Configuration	86
Configuring Interface Properties	86
Network Security Configuration	87
Network Security	87
Configuring Network Security	87
Network Time Protocol Configuration	88
Configuring Network Time Protocol Settings	88

CHAPTER 9**Managing Network Adapters 91**[Overview of the Cisco UCS C-Series Network Adapters 91](#)[Viewing Network Adapter Properties 93](#)[Configuring Network Adapter Properties 93](#)[Managing vHBAs 94](#)[Guidelines for Managing vHBAs 94](#)[Viewing vHBA Properties 95](#)[Modifying vHBA Properties 96](#)[Creating a vHBA 100](#)[Deleting a vHBA 101](#)[vHBA Boot Table 102](#)[Viewing the Boot Table 102](#)[Creating a Boot Table Entry 102](#)[Deleting a Boot Table Entry 103](#)[vHBA Persistent Binding 104](#)[Enabling Persistent Binding 105](#)[Disabling Persistent Binding 105](#)[Rebuilding Persistent Binding 106](#)[Managing vNICs 107](#)[Guidelines for Managing vNICs 107](#)[Viewing vNIC Properties 107](#)[Modifying vNIC Properties 108](#)[Creating a vNIC 113](#)[Deleting a vNIC 114](#)[Creating Cisco usNIC Using the CIMC CLI 115](#)[Modifying a Cisco usNIC using the CIMC CLI 118](#)[Viewing usNIC Properties 120](#)[Deleting Cisco usNIC from a vNIC 121](#)[Configuring iSCSI Boot Capability 122](#)[Configuring iSCSI Boot Capability for vNICs 122](#)[Configuring iSCSI Boot Capability on a vNIC 122](#)[Deleting an iSCSI Boot Configuration for a vNIC 123](#)[Managing VM FEX 124](#)[Virtual Machine Fabric Extender 124](#)

Viewing VM FEX Properties	124
VM FEX Settings	126
Managing Storage Adapters	129
Create Virtual Drive from Unused Physical Drives	129
Create Virtual Drive from an Existing Drive Group	131
Clearing Foreign Configuration	132
Deleting a Virtual Drive	133
Initializing a Virtual Drive	133
Set as Boot Drive	134
Modifying Attributes of a Virtual Drive	135
Making a Dedicated Hot Spare	136
Making a Global Hot Spare	136
Preparing a Drive for Removal	137
Removing a Drive from Hot Spare Pools	138
Undo Preparing a Drive for Removal	138
Enabling Auto Learn Cycles for the Battery Backup Unit	139
Disabling Auto Learn Cycles for the Battery Backup Unit	139
Starting a Learn Cycle for a Battery Backup Unit	140
Toggling the Locator LED for a Physical Drive	141
Viewing Storage Controller Logs	141
Backing Up and Restoring the Adapter Configuration	142
Exporting the Adapter Configuration	142
Importing the Adapter Configuration	143
Restoring Adapter Defaults	144
Managing Adapter Firmware	144
Adapter Firmware	144
Installing Adapter Firmware	144
Activating Adapter Firmware	145
Resetting the Adapter	146

CHAPTER 10

Configuring Communication Services	147
Configuring HTTP	147
Configuring SSH	148
Configuring XML API	149
XML API for CIMC	149

Enabling XML API	149
Configuring IPMI	150
IPMI Over LAN	150
Configuring IPMI over LAN	150
Configuring SNMP	151
SNMP	151
Configuring SNMP Properties	151
Configuring SNMP Trap Settings	153
Sending a Test SNMP Trap Message	154
Configuring SNMPv3 Users	154

CHAPTER 11

Managing Certificates 157

Managing the Server Certificate	157
Generating a Certificate Signing Request	157
Creating a Self-Signed Certificate	159
Uploading a Server Certificate	161

CHAPTER 12

Configuring Platform Event Filters 163

Platform Event Filters	163
Enabling Platform Event Alerts	163
Disabling Platform Event Alerts	164
Configuring Platform Event Filters	164
Configuring Platform Event Trap Settings	166
Interpreting Platform Event Traps	167

CHAPTER 13

CIMC Firmware Management 171

Overview of Firmware	171
Obtaining Firmware from Cisco	172
Installing CIMC Firmware from a Remote Server	173
Activating Installed CIMC Firmware	174
Installing BIOS Firmware from a Remote Server	176

CHAPTER 14

Viewing Faults and Logs 179

Viewing the Faults and Logs Summary	179
CIMC Log	180

Viewing the CIMC Log	180
Clearing the CIMC Log	181
Configuring the CIMC Log Threshold	181
Sending the CIMC Log to a Remote Server	182
System Event Log	184
Viewing the System Event Log	184
Clearing the System Event Log	185

CHAPTER 15

Server Utilities 187

Exporting Technical Support Data	187
Rebooting the CIMC	189
Clearing the BIOS CMOS	189
Recovering from a Corrupted BIOS	190
Resetting the CIMC to Factory Defaults	191
Exporting and Importing the CIMC Configuration	192
Exporting and Importing the CIMC Configuration	192
Exporting the CIMC Configuration	192
Importing a CIMC Configuration	193
Generating Non maskable Interrupts to the Host	194

APPENDIX A

BIOS Parameters by Server Model 197

C22 and C24 Servers	197
Main BIOS Parameters for C22 and C24 Servers	197
Advanced BIOS Parameters for C22 and C24 Servers	198
Server Management BIOS Parameters for C22 and C24 Servers	214
C220 and C240 Servers	217
Main BIOS Parameters for C220 and C240 Servers	217
Advanced BIOS Parameters for C220 and C240 Servers	217
Server Management BIOS Parameters for C220 and C240 Servers	234
C260 Servers	237
Main BIOS Parameters for C260 Servers	237
Advanced BIOS Parameters for C260 Servers	237
Server Management BIOS Parameters for C260 Servers	247
C420 Servers	250
Main BIOS Parameters for C420 Servers	250

Advanced BIOS Parameters for C420 Servers	251
Server Management BIOS Parameters for C420 Servers	267
C460 Servers	270
Main BIOS Parameters for C460 Servers	270
Advanced BIOS Parameters for C460 Servers	270
Server Management BIOS Parameters for C460 Servers	280



Preface

This preface includes the following sections:

- [Audience, page xiii](#)
- [Conventions, page xiii](#)
- [New and Changed Information for this Release, page xv](#)
- [Related Cisco UCS Documentation, page xvii](#)

Audience

This guide is intended primarily for data center administrators with responsibilities and expertise in one or more of the following:

- Server administration
- Storage administration
- Network administration
- Network security

Conventions

Text Type	Indication
GUI elements	GUI elements such as tab titles, area names, and field labels appear in this font . Main titles such as window, dialog box, and wizard titles appear in this font .
Document titles	Document titles appear in <i>this font</i> .
TUI elements	In a Text-based User Interface, text the system displays appears in <i>this font</i> .
System output	Terminal sessions and information that the system displays appear in <i>this font</i> .

Text Type	Indication
CLI commands	CLI command keywords appear in this font . Variables in a CLI command appear in <i>this font</i> .
[]	Elements in square brackets are optional.
{x y z}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x y z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
< >	Nonprinting characters such as passwords are in angle brackets.
[]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

**Note**

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the document.

**Tip**

Means *the following information will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.

**Caution**

Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.

**Timesaver**

Means *the described action saves time*. You can save time by performing the action described in the paragraph.

**Warning****IMPORTANT SAFETY INSTRUCTIONS**

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

New and Changed Information for this Release

The following tables provide an overview of the significant changes to this guide for the current release. The tables do not provide an exhaustive list of all changes made to the configuration guides or of the new features in this release.

For a complete list of all C-Series documentation, see the *Cisco UCS C-Series Servers Documentation Roadmap* available at the following URL: <http://www.cisco.com/go/unifiedcomputing/c-series-doc>.

New Features and Significant Behavioral Changes in Cisco Integrated Management Controller software, Release 1.5(4)

Release notes for Cisco Integrated Management Controller, Release 1.5, is available at:

http://www.cisco.com/en/US/products/ps10739/prod_release_notes_list.html

Feature	Description	Where Documented
Modified CIMC port settings.	Support for setting autonegotiate and duplex modes on CIMC dedicated network ports.	Configuring Network-Related Settings, on page 79
Support for single hypervisor (HV) partition configuration.	The SD storage is available to CIMC as a single hypervisor (HV) partition configuration.	Managing the Server, on page 15

New Features and Significant Behavioral Changes in Cisco Integrated Management Controller software, Release 1.5(3)

Release notes for Cisco Integrated Management Controller, Release 1.5, is available at:

http://www.cisco.com/en/US/products/ps10739/prod_release_notes_list.html

Feature	Description	Where Documented
BIOS tokens	Following new tokens were added: <ul style="list-style-type: none"> • Out-of-Band Mgmt Port • Onboard SCU Storage SW Stack 	BIOS Parameters by Server Model, on page 197

New Features and Significant Behavioral Changes in Cisco Integrated Management Controller software, Release 1.5(2)

Release notes for Cisco Integrated Management Controller, Release 1.5, is available at:

http://www.cisco.com/en/US/products/ps10739/prod_release_notes_list.html

Feature	Description	Where Documented
Fan policy	Support for configuring a fan policy for servers through CIMC	Managing the Server, on page 15
DHCP-enhanced registration	Support for modifying the host name of the server	Managing the Server, on page 15
LDAP	Support extended to include RedHat Directory Server, Novell eDirectory, OpenLDAP, Microsoft Active Directory, and Oracle OpenDS.	Managing User Accounts, on page 71
Cisco usNIC	Support for Cisco usNIC for low-latency Open MPI applications using the Cisco VIC 1225 and 1225T adapters	Managing Network Adapters, on page 91

New Features and Significant Behavioral Changes in Cisco Integrated Management Controller software, Release 1.5(1)

Release notes for Cisco Integrated Management Controller, Release 1.5, is available at:

http://www.cisco.com/en/US/products/ps10739/prod_release_notes_list.html

Feature	Description	Where Documented
Enhanced fault reporting	Enhanced fault reporting capabilities in the CIMC UI.	Viewing Faults and Logs, on page 179
Dual SD Card and Cisco Flexible Flash Card	Support for dual SD card configuration and enhanced configuration options with Cisco Flexible Flash cards.	Managing the Server, on page 15
Nvidia GPU information	Support for viewing Nvidia GPU card information	Viewing Server Properties, on page 43
Storage Adapters	Support added for configuration tasks for storage adapters	Managing Network Adapters, on page 91
NTP Configuration	Support for Network Time Protocol	Configuring Network-Related Settings, on page 79

Feature	Description	Where Documented
vNICs	Support for iSCSI boot capability on a vNIC	Managing Network Adapters, on page 91
Virtual Media	Support for configuring network mounted vmedia volumes	Managing Remote Presence, on page 61
Enhanced SNMP features	Enhanced SNMPv3 and SNMP trap configuration is relocated in the user interface.	Configuring Communication Services, on page 147
XML API	Support added for CIMC control by an XML API.	Configuring Communication Services, on page 147

Related Cisco UCS Documentation

Documentation Roadmaps

For a complete list of all B-Series documentation, see the *Cisco UCS B-Series Servers Documentation Roadmap* available at the following URL: <http://www.cisco.com/go/unifiedcomputing/b-series-doc>.

For a complete list of all C-Series documentation, see the *Cisco UCS C-Series Servers Documentation Roadmap* available at the following URL: <http://www.cisco.com/go/unifiedcomputing/c-series-doc>.

Other Documentation Resources

An ISO file containing all B and C-Series documents is available at the following URL: <http://www.cisco.com/cisco/software/type.html?mdfid=283853163&flowid=25821>. From this page, click **Unified Computing System (UCS) Documentation Roadmap Bundle**.

The ISO file is updated after every major documentation release.

Follow [Cisco UCS Docs on Twitter](#) to receive document update notifications.



Overview

This chapter includes the following sections:

- [Overview of the Cisco UCS C-Series Rack-Mount Servers, page 1](#)
- [Overview of the Server Software, page 1](#)
- [Cisco Integrated Management Controller, page 2](#)
- [CIMC CLI, page 3](#)

Overview of the Cisco UCS C-Series Rack-Mount Servers

The Cisco UCS C-Series rack-mount servers include the following models:

- Cisco UCS C200 Rack-Mount Server
- Cisco UCS C210 Rack-Mount Server
- Cisco UCS C220 Rack-Mount Server
- Cisco UCS C240 Rack-Mount Server
- Cisco UCS C250 Rack-Mount Server
- Cisco UCS C260 Rack-Mount Server
- Cisco UCS C460 Rack-Mount Server



Note

To determine which Cisco UCS C-Series rack-mount servers are supported by this firmware release, see the associated *Release Notes*. The C-Series release notes are available at the following URL: http://www.cisco.com/en/US/products/ps10739/prod_release_notes_list.html

Overview of the Server Software

The Cisco UCS C-Series Rack-Mount Server ships with the CIMC firmware.

CIMC Firmware

CIMC is a separate management module built into the motherboard. A dedicated ARM-based processor, separate from the main server CPU, runs the CIMC firmware. The system ships with a running version of the CIMC firmware. You can update the CIMC firmware, but no initial installation is needed.

Server OS

The Cisco UCS C-Series rack servers support operating systems such as Windows, Linux, Oracle and so on. For more information on supported operating systems, see the *Hardware and Software Interoperability for Standalone C-series servers* at http://www.cisco.com/en/US/products/ps10477/prod_technical_reference_list.html. You can use CIMC to install an OS on the server using the KVM console and vMedia.

**Note**

You can access the available OS installation documentation from the *Cisco UCS C-Series Servers Documentation Roadmap* at <http://www.cisco.com/go/unifiedcomputing/c-series-doc>.

Cisco Integrated Management Controller

The CIMC is the management service for the C-Series servers. CIMC runs within the server.

**Note**

The CIMC management service is used only when the server is operating in Standalone Mode. If your C-Series server is integrated into a UCS system, you must manage it using UCS Manager. For information about using UCS Manager, see the configuration guides listed in the *Cisco UCS B-Series Servers Documentation Roadmap* at <http://www.cisco.com/go/unifiedcomputing/b-series-doc>.

Management Interfaces

You can use a web-based GUI or SSH-based CLI to access, configure, administer, and monitor the server. Almost all tasks can be performed in either interface, and the results of tasks performed in one interface are displayed in another. However, you cannot do the following:

- Use CIMC GUI to invoke CIMC CLI
- View a command that has been invoked through CIMC CLI in CIMC GUI
- Generate CIMC CLI output from CIMC GUI

Tasks You Can Perform in CIMC

You can use CIMC to perform the following server management tasks:

- Power on, power off, power cycle, reset and shut down the server
- Toggle the locator LED
- Configure the server boot order
- View server properties and sensors
- Manage remote presence

- Create and manage local user accounts, and enable remote user authentication through Active Directory
- Configure network-related settings, including NIC properties, IPv4, VLANs, and network security
- Configure communication services, including HTTP, SSH, and IPMI Over LAN
- Manage certificates
- Configure platform event filters
- Update CIMC firmware
- Monitor faults, alarms, and server status

No Operating System or Application Provisioning or Management

CIMC provisions servers, and as a result, exists below the operating system on a server. Therefore, you cannot use it to provision or manage operating systems or applications on servers. For example, you cannot do the following:

- Deploy an OS, such as Windows or Linux
- Deploy patches for software, such as an OS or an application
- Install base software components, such as anti-virus software, monitoring agents, or backup clients
- Install software applications, such as databases, application server software, or web servers
- Perform operator actions, including restarting an Oracle database, restarting printer queues, or handling non-CIMC user accounts
- Configure or manage external storage on the SAN or NAS storage

CIMC CLI

The CIMC CLI is a command-line management interface for Cisco UCS C-Series servers. You can launch the CIMC CLI and manage the server over the network by SSH or Telnet. By default, Telnet access is disabled.

A user of the CLI will be one of three roles: admin, user (can control, cannot configure), and read-only.

**Note**

To recover from a lost admin password, see the Cisco UCS C-Series server installation and service guide for your platform.

Command Modes

The CLI is organized into a hierarchy of command modes, with the EXEC mode being the highest-level mode of the hierarchy. Higher-level modes branch into lower-level modes. You use the **scope** command to move from higher-level modes to modes in the next lower level, and the **exit** command to move up one level in the mode hierarchy. The **top** command returns to the EXEC mode.

**Note**

Most command modes are associated with managed objects. The **scope** command does not create managed objects and can only access modes for which managed objects already exist.

Each mode contains a set of commands that can be entered in that mode. Most of the commands available in each mode pertain to the associated managed object. Depending on your assigned role, you may have access to only a subset of the commands available in a mode; commands to which you do not have access are hidden.

The CLI prompt for each mode shows the full path down the mode hierarchy to the current mode. This helps you to determine where you are in the command mode hierarchy and can be an invaluable tool when you need to navigate through the hierarchy.

Command Mode Table

The following table lists the first four levels of command modes, the commands used to access each mode, and the CLI prompt associated with each mode.

Mode Name	Command to Access	Mode Prompt
EXEC	top command from any mode	#
bios	scope bios command from EXEC mode	/bios #
advanced	scope advanced command from bios mode	/bios/advanced #
main	scope main command from bios mode	/bios/main #
server-management	scope server-management command from bios mode	/bios/server-management #
certificate	scope certificate command from EXEC mode	/certificate #
chassis	scope chassis command from EXEC mode	/chassis #
adapter	scope adapter <i>index</i> command from chassis mode	/chassis/adapter #
host-eth-if	scope host-eth-if command from adapter mode	/chassis/adapter/host-eth-if #
host-fc-if	scope host-fc-if command from adapter mode	/chassis/adapter/host-fc-if #
port-profiles	scope port-profiles command from adapter mode	/chassis/adapter/port-profiles #
vmfex	scope vmfex <i>index</i> command from adapter mode	/chassis/adapter/vmfex #
dimmm-summary	scope dimm-summary <i>index</i> command from chassis mode	/chassis/dimm-summary #
flexflash	scope flexflash <i>index</i> command from chassis mode	/chassis/flexflash #
operational-profiles	scope operational-profile command from flexflash mode	/chassis/flexflash/operational-profile #

Mode Name	Command to Access	Mode Prompt
storageadapter	scope storageadapter <i>slot</i> command from chassis mode	/chassis/storageadapter #
physical-drive	scope physical-drive command from storageadapter mode	/chassis/storageadapter/physical-drive #
virtual-drive	scope virtual-drive command from storageadapter mode	/chassis/storageadapter/virtual-drive #
cimc	scope cimc command from EXEC mode	/cimc #
firmware	scope firmware command from cimc mode	/cimc/firmware #
import-export	scope import-export command from cimc mode	/cimc/import-export #
log	scope log command from cimc mode	/cimc/log #
server	scope server <i>index</i> command from log mode	/cimc/log/server #
network	scope network command from cimc mode	/cimc/network #
ipblocking	scope ipblocking command from network mode	/cimc/network/ipblocking #
tech-support	scope tech-support command from cimc mode	/cimc/tech-support #
fault	scope fault command from EXEC mode	/fault #
pef	scope pef command from fault mode	/fault/pef #
http	scope http command from EXEC mode	/http #
ipmi	scope ipmi command from EXEC mode	/ipmi #
kvm	scope kvm command from EXEC mode	/kvm #
ldap		/ldap #

Mode Name	Command to Access	Mode Prompt
	scope ldap command from EXEC mode	
role-group	scope role-group command from ldap mode	/ldap/role-group #
power-cap	scope power-cap command from EXEC mode	/power-cap #
sel	scope sel command from EXEC mode	/sel #
sensor	scope sensor command from EXEC mode	/sensor #
snmp	scope snmp command from EXEC mode	/snmp #
trap-destinations	scope trap-destinations command from snmp mode	/snmp/trap-destinations #
v3users	scope v3users command from snmp mode	/snmp/v3users #
sol	scope sol command from EXEC mode	/sol #
ssh	scope ssh command from EXEC mode	/ssh #
user	scope user <i>user-number</i> command from EXEC mode	/user #
user-session	scope user-session <i>session-number</i> command from EXEC mode	/user-session #
vmedia	scope vmedia command from EXEC mode	/vmedia #
xmlapi	scope xmlapi command from EXEC mode	/xmlapi #

Complete a Command

You can use the Tab key in any mode to complete a command. Partially typing a command name and pressing Tab causes the command to be displayed in full or to the point where another keyword must be chosen or an argument value must be entered.

Command History

The CLI stores all commands used in the current session. You can step through the previously used commands by using the Up Arrow or Down Arrow keys. The Up Arrow key steps to the previous command in the history, and the Down Arrow key steps to the next command in the history. If you get to the end of the history, pressing the Down Arrow key does nothing.

All commands in the history can be entered again by simply stepping through the history to recall the desired command and pressing Enter. The command is entered as if you had manually typed it. You can also recall a command and change it before you press Enter.

Committing, Discarding, and Viewing Pending Commands

When you enter a configuration command in the CLI, the command is not applied until you enter the **commit** command. Until committed, a configuration command is pending and can be discarded by entering a **discard** command. When any command is pending, an asterisk (*) appears before the command prompt. The asterisk disappears when you enter the **commit** command, as shown in this example:

```
Server# scope chassis
Server /chassis # set locator-led off
Server /chassis *# commit
Server /chassis #
```

You can accumulate pending changes in multiple command modes and apply them together with a single **commit** command. You can view the pending commands by entering the **show configuration pending** command in any command mode.

**Note**

Committing multiple commands together is not an atomic operation. If any command fails, the successful commands are applied despite the failure. Failed commands are reported in an error message.

Command Output Formats

Most CLI **show** commands accept an optional **detail** keyword that causes the output information to be displayed as a list rather than a table. You can configure either of two presentation formats for displaying the output information when the **detail** keyword is used. The format choices are as follows:

- Default—For easy viewing, the command output is presented in a compact list.

This example shows command output in the default format:

```
Server /chassis # set cli output default
Server /chassis # show hdd detail
Name HDD_01_STATUS:
    Status : present
```

```
Name HDD_02_STATUS:
  Status : present
Name HDD_03_STATUS:
  Status : present
Name HDD_04_STATUS:
  Status : present

Server /chassis #
```

- **YAML**—For easy parsing by scripts, the command output is presented in the YAML (YAML Ain't Markup Language) data serialization language, delimited by defined character strings.

This example shows command output in the YAML format:

```
Server /chassis # set cli output yaml
Server /chassis # show hdd detail
---
  name: HDD_01_STATUS
  hdd-status: present
---
  name: HDD_02_STATUS
  hdd-status: present
---
  name: HDD_03_STATUS
  hdd-status: present
---
  name: HDD_04_STATUS
  hdd-status: present
...

Server /chassis #
```

For detailed information about YAML, see <http://www.yaml.org/about.html>.

In most CLI command modes, you can enter **set cli output default** to configure the default format, or **set cli output yaml** to configure the YAML format.

Online Help for the CLI

At any time, you can type the ? character to display the options available at the current state of the command syntax.

If you have not typed anything at the prompt, typing ? lists all available commands for the mode you are in. If you have partially typed a command, typing ? lists all available keywords and arguments available at your current position in the command syntax.



Installing the Server OS

This chapter includes the following sections:

- [OS Installation Methods, page 11](#)
- [KVM Console, page 11](#)
- [PXE Installation Servers, page 12](#)
- [Booting an Operating System from a USB Port, page 13](#)

OS Installation Methods

C-Series servers support several operating systems. Regardless of the OS being installed, you can install it on your server using one of the following tools:

- KVM console
- PXE installation server

KVM Console

The KVM console is an interface accessible from CIMC that emulates a direct keyboard, video, and mouse (KVM) connection to the server. The KVM console allows you to connect to the server from a remote location.

Instead of using CD/DVD or floppy drives physically connected to the server, the KVM console uses virtual media, which are actual disk drives or disk image files that are mapped to virtual CD/DVD or floppy drives. You can map any of the following to a virtual drive:

- CD/DVD or floppy drive on your computer
- Disk image files (ISO or IMG files) on your computer
- USB flash drive on your computer
- CD/DVD or floppy drive on the network
- Disk image files (ISO or IMG files) on the network

- USB flash drive on the network

You can use the KVM console to install an OS on the server.

**Note**

The KVM Console is operated only through the GUI. To launch the KVM Console, see the instructions in the *Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide*.

Installing an OS Using the KVM Console

Because the KVM console is operated only through the GUI, you cannot install a server OS using the CLI. To install an OS using the KVM console, follow the instructions in the "Installing an OS Using the KVM Console" section of the *Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide*.

**Note**

Detailed guides for installing Linux, VMware, and Windows can be found at this URL: http://www.cisco.com/en/US/products/ps10493/products_installation_and_configuration_guides_list.html.

PXE Installation Servers

A Preboot Execution Environment (PXE) installation server allows a client to boot and install an OS from a remote location. To use this method, a PXE environment must be configured and available on your VLAN, typically a dedicated provisioning VLAN. Additionally, the server must be set to boot from the network. When the server boots, it sends a PXE request across the network. The PXE installation server acknowledges the request, and starts a sequence of events that installs the OS on the server.

PXE servers can use installation disks, disk images, or scripts to install an OS. Proprietary disk images can also be used to install an OS, additional components, or applications.

**Note**

PXE installation is an efficient method for installing an OS on a large number of servers. However, considering that this method requires setting up a PXE environment, it might be easier to use another installation method.

Installing an OS Using a PXE Installation Server

Before You Begin

- Verify that the server can be reached over a VLAN.
- You must log in as a user with admin privileges to install an OS.

Procedure

Step 1 Set the boot order to **PXE** first.

Step 2 Reboot the server.

If a PXE install server is available on the VLAN, the installation process begins when the server reboots. PXE installations are typically automated and require no additional user input. Refer to the installation guide for the OS being installed to guide you through the rest of the installation process.

What to Do Next

After the OS installation is complete, reset the LAN boot order to its original setting.

Booting an Operating System from a USB Port

All Cisco UCS C-series servers support booting an operating system from any USB port on the server. However, there are a few guidelines that you must keep in mind, prior to booting an OS from a USB port.

- To maintain the boot order configuration, it is recommended that you use an internal USB port for booting an OS.
- The USB port must be enabled prior to booting an OS from it.

By default, the USB ports are enabled. If you have disabled a USB port, you must enable it prior to booting an OS from it. For information on enabling a disabled USB ports, see topic *Enabling or Disabling the Internal USB Port* in the server-specific installation and service guide available at the following link:

http://www.cisco.com/en/US/products/ps10493/prod_installation_guides_list.html.

- After you boot the OS from the USB port, you must set the second-level boot order so that the server boots from that USB source every time.

For information on setting the boot order, see [Configuring the Server Boot Order](#), on page 17.



Managing the Server

This chapter includes the following sections:

- [Overview to DHCP User Friendliness, page 15](#)
- [Toggling the Locator LED, page 16](#)
- [Toggling the Locator LED for a Hard Drive, page 16](#)
- [Managing the Server Boot Order, page 17](#)
- [Resetting the Server, page 19](#)
- [Shutting Down the Server, page 19](#)
- [Managing Server Power, page 20](#)
- [Configuring Power Policies, page 22](#)
- [Configuring Fan Policies, page 26](#)
- [Managing the Flexible Flash Controller, page 28](#)
- [Configuring BIOS Settings, page 36](#)
- [Updating Firmware on Server Components, page 41](#)

Overview to DHCP User Friendliness

The Dynamic Host Configuration Protocol (DHCP) enhancement ships with the addition of the hostname to the DHCP packet, which can either be interpreted or displayed at the DHCP server side. The hostname is now added in the options field of the DHCP packet, and sent in the DHCP DISCOVER packet which was initially sent to the DHCP server.

The default hostname of the server is changed from ucs-c2XX to CXXX-YYYYYY. Where XXX is the model number and YYYYYY is the serial number of the server. This unique string acts as a client identifier, and helps you track and map the IP addresses leased out to the CIMC from the DHCP server. The default serial number is provided by the manufacturer as a sticker/label on the server which helps you physically identify the server.

Toggling the Locator LED

Before You Begin

You must log in with user or admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server # scope chassis	Enters chassis command mode.
Step 2	Server /chassis # set locator-led {on off}	Enables or disables the chassis locator LED.
Step 3	Server /chassis # commit	Commits the transaction to the system configuration.

This example disables the chassis locator LED and commits the transaction:

```
Server# scope chassis
Server /chassis # set locator-led off
Server /chassis *# commit

Server /chassis #
```

Toggling the Locator LED for a Hard Drive

Before You Begin

You must log in with user or admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server # scope chassis	Enters chassis command mode.
Step 2	Server/chassis # scope hdd	Enters hard disk drive (HDD) command mode.
Step 3	Server /chassis/hdd # set locateHDD <i>drivenum</i> {1 2}	Where <i>drivenum</i> is the number of the hard drive whose locator LED you want to set. A value of 1 turns the LED on while a value of 2 turns the LED off.

This example turns on the locator LED on HDD 2:

```
Server# scope chassis
Server /chassis # scope hdd
Server /chassis/hdd # locateHDD 2 1
HDD Locate LED Status changed to 1
Server /chassis/hdd # show
Name                               Status                               LocateLEDStatus
```

```

-----
HDD1_STATUS      present      TurnOFF
HDD2_STATUS      present      TurnON
HDD3_STATUS      absent       TurnOFF
HDD4_STATUS      absent       TurnOFF

Server /chassis/hdd #

```

Managing the Server Boot Order

Server Boot Order

Using CIMC, you can configure the order in which the server attempts to boot from available boot device types.

When you change the boot order configuration, CIMC sends the configured boot order to the BIOS the next time the server is rebooted. To implement the new boot order, reboot the server after making the configuration change. The new boot order will take effect on any subsequent reboot. The configured boot order is not sent again until the configuration is changed again.



Note

The actual boot order will differ from the configured boot order if either of the following conditions occur:

- The BIOS encounters issues while trying to boot using the configured boot order.
- A user changes the boot order directly through the BIOS.

Configuring the Server Boot Order



Note

Do not change the boot order while the host is performing BIOS power-on self test (POST).

Before You Begin

You must log in with user or admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope bios	Enters bios command mode.
Step 2	Server /bios # set boot-order <i>device1[,device2[,device3</i> <i>[,device4[,device5]]]</i>	Specifies the boot device options and order. You can select one or more of the following: <ul style="list-style-type: none"> • cdrom—Bootable CD-ROM • fdd—Floppy disk drive • hdd—Hard disk drive

	Command or Action	Purpose
		<ul style="list-style-type: none"> • pxe—PXE boot • efi—Extensible Firmware Interface
Step 3	Server /bios # commit	Commits the transaction to the system configuration.

The new boot order will be used on the next BIOS boot.

This example sets the boot order and commits the transaction:

```
Server# scope bios
Server /bios # set boot-order hdd,cdrom,fdd,pxe,efi
Server /bios *# commit
Server /bios # show detail
BIOS:
    Boot Order: HDD,CDROM,FDD,PXE,EFI

Server /bios #
```

What to Do Next

Reboot the server to boot with your new boot order.

Viewing the Actual Server Boot Order

The actual server boot order is the boot order actually used by the BIOS when the server last booted. The actual boot order can differ from the boot order configured in CIMC.

Procedure

	Command or Action	Purpose
Step 1	Server# scope bios	Enters bios command mode.
Step 2	Server /bios # show actual-boot-order [detail]	Displays the boot order actually used by the BIOS when the server last booted.

This example displays the actual boot order from the last boot:

```
Server# scope bios
Server /bios # show actual-boot-order

Boot Order  Type                               Boot Device
-----
1           CD/DVD                               CD-ROM
2           CD/DVD                               Cisco  Virtual CD/DVD  1.18
3           Network Device (PXE)               Cisco  NIC 23:0.0
4           Network Device (PXE)               MBA v5.0.5  Slot 0100
5           Network Device (PXE)               MBA v5.0.5  Slot 0101
6           Network Device (PXE)               MBA v5.0.5  Slot 0200
7           Network Device (PXE)               MBA v5.0.5  Slot 0201
8           Network Device (PXE)               Cisco  NIC 22:0.0
9           Internal EFI Shell                 Internal EFI Shell
10          FDD                               Cisco  Virtual HDD      1.18
```

```

11          FDD          Cisco  Virtual Floppy  1.18
Server /bios #

```

Resetting the Server



Important

If any firmware or BIOS updates are in progress, do not reset the server until those tasks are complete.

Before You Begin

You must log in with user or admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters chassis command mode.
Step 2	Server /chassis # power hard-reset	After a prompt to confirm, resets the server.

This example resets the server:

```

Server# scope chassis
Server /chassis # power hard-reset
This operation will change the server's power state.
Continue?[y|N]

```

Shutting Down the Server



Important

If any firmware or BIOS updates are in progress, do not shut down the server until those tasks are complete.

Before You Begin

You must log in with user or admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters chassis mode.
Step 2	Server /chassis # power shutdown	Shuts down the server.

The following example shuts down the server:

```
Server# scope chassis
Server /chassis # power shutdown
```

Managing Server Power

Powering On the Server



Note

If the server was powered off other than through the CIMC, the server will not become active immediately when powered on. In this case, the server will enter standby mode until the CIMC completes initialization.



Important

If any firmware or BIOS updates are in progress, do not change the server power until those tasks are complete.

Before You Begin

You must log in with user or admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters chassis command mode.
Step 2	Server /chassis # power on	Turns on the server.

This example turns on the server:

```
Server# scope chassis
Server /chassis # power on
This operation will change the server's power state.
Continue?[y|N]y

Server /chassis # show
Power Serial Number Product Name  UUID
-----
on      Not Specified Not Specified 208F0100020F000000BEA80000DEAD00
```

Powering Off the Server



Important

If any firmware or BIOS updates are in progress, do not power off the server until those tasks are complete.

Before You Begin

You must log in with user or admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters chassis command mode.
Step 2	Server /chassis # power off	Turns off the server.

This example turns off the server:

```
Server# scope chassis
Server /chassis # power off
This operation will change the server's power state.
Continue?[y|N]y

Server /chassis # show
Power Serial Number Product Name  UUID
-----
off   Not Specified Not Specified 208F0100020F000000BEA80000DEAD00
```

Power Cycling the Server



Important

If any firmware or BIOS updates are in progress, do not power cycle the server until those tasks are complete.

Before You Begin

You must log in with user or admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters chassis command mode.
Step 2	Server /chassis # power cycle	Power cycles the server.

This example power cycles the server:

```
Server# scope chassis
Server /chassis # power cycle
```

Configuring Power Policies

Viewing the Power Statistics

Procedure

	Command or Action	Purpose
Step 1	Server# show power-cap [detail]	Displays the server power consumption statistics and the power cap policy.

The displayed fields are described in the following table:

Name	Description
Current Consumption	The power currently being used by the server, in watts.
Maximum Consumption	The maximum number of watts consumed by the server since the last time it was rebooted.
Minimum Consumption	The minimum number of watts consumed by the server since the last time it was rebooted.
Minimum Configurable Limit	The minimum amount of power that can be specified as the peak power cap for this server, in watts.
Maximum Configurable Limit	The maximum amount of power that can be specified as the peak power cap for this server, in watts.

Additional fields are described in the following table:

Name	Description
Enable Power Capping	If power capping is enabled, the system monitors how much power is allocated to the server and takes the specified action if the server goes over its maximum allotment.
Peak Power	The maximum number of watts that can be allocated to this server. If the server requests more power than specified in this field, the system takes the action defined in the Non-Compliance Action field. Enter a number of watts within the range defined by the Minimum Configurable Limit field and the Maximum Configurable Limit field.

Name	Description
Non-Compliance Action	<p>The action the system should take if power capping is enabled and the server requests more than its peak power allotment. This can be one of the following:</p> <ul style="list-style-type: none"> • force-power-reduction—The server is forced to reduce its power consumption by any means necessary. This option is available only on some C-Series servers. • none—No action is taken and the server is allowed to use more power than specified in the Peak Power field. • power-off-host—The server is shut down. • throttle—Processes running on the server are throttled to bring the total power consumption down.

This example displays the detailed power statistics:

```
Server# show power-cap detail
  Cur Consumption (W): 247
  Max Consumption (W): 286
  Min Consumption (W): 229
  Minimum Configurable Limit (W): 285
  Maximum Configurable Limit (W): 1250
  Power Cap Enabled: yes
  Peak Power: 0
  Non Compliance Action: throttle

Server#
```

Power Capping Policy

The power capping policy determines how server power consumption is actively managed. When power capping is enabled, the system monitors how much power is allocated to the server and attempts to keep the power consumption below the allocated power. If the server exceeds its maximum allotment, the power capping policy triggers the specified non-compliance action.

Configuring the Power Cap Policy



Note

This feature is not available on some servers.

Before You Begin

You must log in with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope power-cap	Enters the power cap command mode.
Step 2	Server /power-cap # set enabled {yes no}	Enables or disables the capping of power to the server.
Step 3	Server /power-cap # set peak-power watts	Specifies the maximum number of watts that can be allocated to this server. Enter a number of <i>watts</i> within the range defined by the Minimum Configurable Limit field and the Maximum Configurable Limit field of the show power-cap detail command output. These fields are determined by the server model. If the server requests more power than specified in this command, the system takes the action defined by the set non-compliance-action command.
Step 4	Server /power-cap # set non-compliance-action {force-power-reduction none power-off-host throttle}	Specifies the action the system should take if power capping is enabled and the server requests more than its peak power allotment. This can be one of the following: <ul style="list-style-type: none"> • force-power-reduction—The server is forced to reduce its power consumption by any means necessary. This option is not available on some server models. • none—No action is taken and the server is allowed to use more power than specified in the peak power setting. • power-off-host—The server is shut down. • throttle—Processes running on the server are throttled to bring the total power consumption down.
Step 5	Server /power-cap # commit	Commits the transaction to the system configuration.

This example enables and configures a power cap policy and commits the transaction:

```

Server# scope power-cap
Server /power-cap # set enabled yes
Server /power-cap *# set peak-power 1000
Server /power-cap *# set non-compliance-action throttle
Server /power-cap *# commit
Server /power-cap # show detail
    Cur Consumption (W): 688
    Max Consumption (W): 1620
    Min Consumption (W): 48
    Minimum Configurable Limit (W): 500
    Maximum Configurable Limit (W): 2000
    Power Cap Enabled: yes
    Peak Power: 1000
    Non Compliance Action: throttle

Server /power-cap #

```

Configuring the Power Restore Policy

The power restore policy determines how power is restored to the server after a chassis power loss.

Before You Begin

You must log in with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # set policy { power-off power-on restore-last-state }	Specifies the action to be taken when chassis power is restored. Select one of the following: <ul style="list-style-type: none"> • power-off—Server power will remain off until manually turned on. This is the default action. • power-on—Server power will be turned on when chassis power is restored. • restore-last-state—Server power will return to the state before chassis power was lost. When the selected action is power-on , you can select a delay in the restoration of power to the server.
Step 3	Server /chassis # set delay { fixed random }	(Optional) Specifies whether server power will be restored after a fixed or random time. The default is fixed . This command is accepted only if the power restore action is power-on .
Step 4	Server /chassis # set delay-value <i>delay</i>	(Optional) Specifies the delay time in seconds. The range is 0 to 240; the default is 0.
Step 5	Server /chassis # commit	Commits the transaction to the system configuration.

This example sets the power restore policy to power-on with a fixed delay of 180 seconds (3 minutes) and commits the transaction:

```
Server# scope chassis
Server /chassis # set policy power-on
Server /chassis *# set delay fixed
Server /chassis *# set delay-value 180
Server /chassis *# commit
Server /chassis # show detail
Chassis:
  Power: on
  Serial Number: QCI1404A1IT
  Product Name: UCS C200 M1
  PID : R200-1120402
  UUID: 01A6E738-D8FE-DE11-76AE-8843E138AE04
  Locator LED: off
```

```
Description: Testing power restore
Power Restore Policy: power-on
Power Delay Type: fixed
Power Delay Value(sec): 180
```

```
Server /chassis #
```

Configuring Fan Policies

Fan Control Policies

Fan Control Policies enable you to control the fan speed to bring down server power consumption and noise levels. Prior to these fan policies, the fan speed increased automatically when the temperature of any server component exceeded the set threshold. To ensure that the fan speeds were low, the threshold temperatures of components are usually set to high values. While this behavior suited most server configurations, it did not address the following situations:

- **Maximum CPU performance**

For high performance, certain CPUs must be cooled substantially below the set threshold temperature. This required very high fan speeds which resulted in higher power consumption and increased noise levels.

- **Low power consumption**

To ensure the lowest power consumption, fans must run very slowly, and in some cases, stop completely on servers that support it. But slow fan speeds resulted in servers overheating. To avoid this situation, it is necessary to run fans at a speed that is moderately faster than the lowest possible speed.

With the introduction of fan policies, you can determine the right fan speed for the server, based on the components in the server. In addition, it allows you to configure the fan speed to address problems related to maximum CPU performance and low power consumption.

Following are the fan policies that you can choose from:

- **Balanced**

This is the default policy. This setting can cool almost any server configuration, but may not be suitable for servers with PCIe cards, since these cards overheat easily.

- **Performance**

This setting can be used for server configurations where maximum fan speed is required for high performance. With this setting, the fan speeds will run at the same speed or higher speed than that of the Balanced fan policy.

- **Low Power**

This setting is ideal for minimal configuration servers that do not contain any PCIe cards.

- **High Power**

This setting can be used for server configurations that require fan speeds ranging from 60 to 85%. This policy is ideal for servers that contain PCIe cards that easily overheat and have high temperatures. The minimum fan speed set with this policy varies for each server platform, but is approximately in the range of 60 to 85%.

- **Maximum Power**

This setting can be used for server configurations that require extremely high fan speeds ranging between 70% to 100%. This policy is ideal for servers that contain PCIe cards that easily overheat and have extremely high temperatures. The minimum fan speed set with this policy varies for each server platform, but is approximately in the range of 70 to 100%.

**Note**

Although you set a fan policy in CIMC, the actual speed that the fan runs at is determined by the configuration requirements of the server. For example, if you set the fan policy to **Balanced**, but the server includes PCIe cards that overheat easily, then the speed of the fans on the server is adjusted automatically. But the policy defined is retained as **Balanced**.

Configuring a Fan Policy

The fan policy determines the cooling requirements for your server. Prior to setting the fan policy, you must determine if your server includes PCIe cards that overheat easily.

Before You Begin

You must log in with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope fan-policy	Enters the fan policy command mode.
Step 3	Server /chassis/fan-policy # set fan-policy	<p>Sets the fan policy for the server. It can be one of the following:</p> <ul style="list-style-type: none"> • balanced This is the default policy. This setting can cool almost any server configuration, but may not be suitable for servers with PCIe cards, since these cards overheat easily. • performance This setting can be used for server configurations where maximum fan speed is required for high performance. With this setting, the fan speeds will run at the same speed or higher speed than that of the balanced fan policy. • low-power This setting is ideal for minimal configuration servers that do not contain any PCIe cards. • high-power This setting can be used for server configurations that require fan speeds ranging from 60 to 85%. This policy is ideal for servers that contain PCIe cards that easily overheat and have high temperatures.

	Command or Action	Purpose
		<p>The minimum fan speed set with this policy varies for each server platform, but is approximately in the range of 60 to 85%.</p> <ul style="list-style-type: none"> • maximum-power <p>This setting can be used for server configurations that require extremely high fan speeds ranging between 70% to 100%. This policy is ideal for servers that contain PCIe cards that easily overheat and have extremely high temperatures. The minimum fan speed set with this policy varies for each server platform, but is approximately in the range of 70 to 100%.</p>
Step 4	Server /chassis/fan-policy # commit	Commits the changes to the server.

This example shows how to set the fan policy to maximum power for a server:

```
server # scope chassis
server /chassis # scope fan-policy
server /chassis/fan-policy # set fan-policy maximum-power
server /chassis/fan-policy* # commit
server /chassis/fan-policy # show detail
Fan policy: maximum-power
server /chassis/fan-policy #
```

Managing the Flexible Flash Controller

Cisco Flexible Flash

Some C-Series Rack-Mount Servers support an internal Secure Digital (SD) memory card for storage of server software tools and utilities. The SD card is hosted by the Cisco Flexible Flash storage adapter.

The SD storage is available to CIMC as a single hypervisor (HV) partition configuration. Prior versions had four virtual USB drives. Three were preloaded with Cisco UCS Server Configuration Utility, Cisco drivers and Cisco Host Upgrade Utility, and the fourth as user-installed hypervisor. A single HV partition configuration is also created when you upgrade to the latest version of CIMC or downgrade to the prior version, and reset the configuration.

For information about the Cisco software utilities and packages, see the *Cisco UCS C-Series Servers Documentation Roadmap* at this URL:

<http://www.cisco.com/go/unifiedcomputing/c-series-doc>

Card Management Feature in the Cisco Flexible Flash Controller

The Cisco Flexible Flash controller supports management of both single and two SD cards as a RAID-1 pair. With the introduction of card management, you can perform the following tasks:

Action	Description
Reset Cisco Flex Flash	Allows you to reset the controller.
Reset Partition Defaults	Allows you to reset the configuration in the selected slot to the default configuration.
Synchronize Card Configuration	Allows you to retain the configuration for an SD card that supports firmware version 253 and later.
Configure Operational Profile	Allows you to configure the SD cards on the selected Cisco Flexible Flash controller.

RAID Partition Enumeration

Non-RAID partitions are always enumerated from the primary card and the enumeration does not depend on the status of the primary card.

Following is the behavior of the RAID partition enumeration when there are two cards in the Cisco Flexible Flash controller:

Scenario	Behavior
Single card	RAID partitions are enumerated if the card is healthy, and if the mode is either Primary or Secondary-active .
Dual paired cards	RAID partitions are enumerated if one of the cards is healthy. When only one card is healthy, all read/write operations occur on this healthy card. You must use UCS SCU to synchronize the two RAID partitions.
Dual unpaired cards	If this scenario is detected when the server is restarting, then neither one of the RAID partitions is enumerated. If this scenario is detected when the server is running, when a user connects a new SD card, then the cards are not managed by the Cisco Flexible Flash controller. This does not affect the host enumeration. You must pair the cards to manage them. You can pair the cards using the Reset Partition Defaults or Synchronize Card Configuration options.

Upgrading from Single Card to Dual Card Mirroring with FlexFlash

You can upgrade from a single card mirroring to dual card mirroring with FlexFlash in one of the following methods:

- Add an empty FlexFlash to the server, and then upgrade the SD firmware version from prior versions to the latest version

For information on how to complete this task, see

- Upgrade the FlexFlash firmware to the latest version and then add an empty card to the server.

Prior to using either of these methods, you must keep in mind the following guidelines:

- To create RAID1 mirroring, the empty card that you want to add to the server must be of the exact size of the card that is already in the server. Identical card size is a must to set up RAID1 mirroring.
- Ensure that the card with valid data in the Hypervisor partition is marked as the primary healthy card. You can determine this state either in the CIMC GUI or from the CIMC CLI. To mark the state of the card as primary healthy, you can either use the **Reset Configuration** option in the CIMC GUI or run the **reset-config** command in the CIMC CLI. When you reset the configuration of a particular card, the secondary card is marked as secondary active unhealthy.
- In a Degraded RAID health state all read-write transactions are done on the healthy card. In this scenario, data mirroring does not occur. Data mirroring occurs only in the Healthy RAID state.
- Data mirroring is only applicable to RAID partitions. In the C-series servers, only Hypervisor partitions operate in the RAID mode.
- If you have not configured SD cards for use with prior versions, then upgrading to the latest version loads the latest 253 firmware and enumerates all four partitions to the host.

While upgrading versions of the FlexFlash, you may see the following error message:

```
Unable to communicate with Flexible Flash controller: operation ffCardsGet, status
CY_AS_ERROR_INVALID_RESPONSE"
```

In addition, the card status may be shown as **missing**. This error occurs because you accidentally switched to an alternate release or a prior version, such as 1.4(x). In this scenario, you can either revert to the latest version, or you can switch back to the FlexFlash 1.4(x) configuration. If you choose to revert to the latest CIMC version, then the Cisco FlexFlash configuration remains intact. If you choose to switch back to the prior version configuration, you must reset the Flexflash configuration. In this scenario, you must be aware of the following:

- If multiple cards are present, and you revert to a prior version, then the second card cannot be discovered or managed.
- If the card type is SD253, then you must run the **reset-config** command twice from the CIMC CLI - once to reload the old firmware on the controller and to migrate SD253 to SD247 type, and the second time to start the enumeration.

Configuring the Flexible Flash Controller Properties

Before You Begin

- You must log in with admin privileges to perform this task.
- Cisco Flexible Flash must be supported by your platform.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope flexflash index	Enters the Cisco Flexible Flash controller command mode for the specified controller. At this time, the only permissible <i>index</i> value is FlexFlash-0 .
Step 3	Server /chassis/flexflash # scope operational-profile	Enters the operational profile command mode.
Step 4	Server /chassis/flexflash/operational-profile # set raid-primary-member {slot1 slot2}	Specifies the slot in which the primary copy of the data resides. Important Currently, Cisco Flexible Flash cards are supported in slot 1 and slot 2. Therefore, you can specify slot1 or slot2 .
Step 5	Server /chassis/flexflash/operational-profile # set raid-secondary-role {active initializing}	The role of the secondary RAID. The currently supported value is active .
Step 6	Server /chassis/flexflash/operational-profile # set read-error-count-threshold	Specifies the number of read errors that are permitted while accessing the Cisco Flexible Flash card. If the number of errors exceeds this threshold, the Cisco Flexible Flash card is disabled and you must reset it manually before CIMC attempts to access it again. To specify a read error threshold, enter an integer between 1 and 255. To specify that the card should never be disabled regardless of the number of errors encountered, enter 0 (zero).
Step 7	Server /chassis/flexflash/operational-profile # set write-error-count-threshold	Specifies the number of write errors that are permitted while accessing the Cisco Flexible Flash card. If the number of errors exceeds this threshold, the Cisco Flexible Flash card is disabled and you must reset it manually before CIMC attempts to access it again. To specify a write error threshold, enter an integer between 1 and 255. To specify that the card should never be disabled regardless of the number of errors encountered, enter 0 (zero).

	Command or Action	Purpose
Step 8	<pre>Server /chassis/flexflash/operational-profile # set virtual-drives-enabled <i>list</i></pre>	<p>Specifies a list of virtual drives to be made available to the server as a USB-style drive. The options are as follows:</p> <ul style="list-style-type: none"> • SCU—The server can access the Cisco UCS Server Configuration Utility. • DRIVERS—The server can access the Cisco drivers volume. • HV—The server can access a user-installed hypervisor. • HUU—The server can access the Cisco Host Upgrade Utility. <p>When specifying more than one option, you must enclose the list in quotation marks (").</p>
Step 9	<pre>Server /chassis/adaptor # commit</pre>	Commits the transaction to the system configuration.

This example shows how to configure the properties of the Flash controller:

```
Server# scope chassis
Server /chassis # scope flexflash FlexFlash-0
Server /chassis/flexflash # scope operational-profile
Server /chassis/flexflash/operational-profile # set read-error-count-threshold 100
Server /chassis/flexflash/operational-profile # set write-error-count-threshold 100
Server /chassis/flexflash/operational-profile *# set raid-primary-member slot1
Server /chassis/flexflash/operational-profile # set raid-secondary-role active
Server /chassis/flexflash/operational-profile *# set virtual-drives-enabled "SCU HUU"
Server /chassis/flexflash/operational-profile *# commit
Server /chassis/flexflash/operational-profile #
```

Booting from the Flexible Flash

You can specify a bootable virtual drive on the Cisco Flexible Flash card that will override the default boot priority the next time the server is restarted, regardless of the default boot order defined for the server. The specified boot device is used only once. After the server has rebooted, this setting is ignored.



Note

Before you reboot the server, ensure that the virtual drive you select is enabled on the Cisco Flexible Flash card.

After you upgrade to the latest version of CIMC or downgrade to a prior version, and reset the configuration, the server boots through the HV partition only. If the prior version has valid SCU data, then the server will boot through SCU in spite of single HV partition.

Before You Begin

- You must log in with admin privileges to perform this task.
- Cisco Flexible Flash must be supported by your platform.

Procedure

	Command or Action	Purpose
Step 1	Server# scope bios	Enters the BIOS command mode.
Step 2	Server /bios # set boot-override {None SCU HV HUU}	The virtual drive from which the server attempts to boot the next time it is restarted. This can be one of the following: <ul style="list-style-type: none"> • None—The server uses the default boot order • SCU—The server boots from the Cisco UCS Server Configuration Utility • HV—The server boots from the hypervisor virtual drive • HUU—The server boots from the Cisco Host Upgrade Utility
Step 3	Server /bios # commit	Commits the transaction to the system configuration.

This example specifies that the server boots from the Cisco UCS Server Configuration Utility the next time it is restarted:

```
Server# scope bios
Server /bios # set boot-override SCU
Committing the boot override BIOS will try boot to
the specified boot device first. Failure to detect
the boot device BIOS will boot from the list
configured in the BIOS boot order.
Server /bios *# commit
Server /bios #
```

Resetting the Flexible Flash Controller

In normal operation, it should not be necessary to reset the Cisco Flexible Flash. We recommend that you perform this procedure only when explicitly directed to do so by a technical support representative.

**Note**

This operation will disrupt traffic to the virtual drives on the Cisco Flexible Flash controller.

Before You Begin

- You must log in with admin privileges to perform this task.
- Cisco Flexible Flash must be supported by your platform.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope flexflash <i>index</i>	Enters the Cisco Flexible Flash controller command mode for the specified controller. At this time, the only permissible <i>index</i> value is FlexFlash-0 .
Step 3	Server /chassis/flexflash # reset	Resets the Cisco Flexible Flash controller.

This example resets the flash controller:

```
Server# scope chassis
Server /chassis # scope flexflash FlexFlash-0
Server /chassis/flexflash # reset
This operation will reset Cisco Flexible Flash controller.
Host traffic to VDs on this device will be disrupted.
Continue?[y|N] y

Server /chassis/flexflash #
```

Resetting the Configuration of the Cards in the Cisco Flexible Flash Controller

You can reset the configuration of a selected slot in the Cisco Flexible Flash controller to the default configuration.

When you reset the configuration of the slots in the Cisco Flexible Flash card, the following situations occur:

- The card in the selected slot is marked as primary healthy.
- The card in the other slot is marked as secondary-active unhealthy.
- One RAID partition is created.
- The card read/write error counts and read/write threshold are set to 0.
- Host connectivity could be disrupted.

If you upgrade to the latest version and select reset configuration option, a single hypervisor (HV) partition is created, and the existing four partition configurations are erased. This may also result in data loss. You can retrieve the lost data only if you have not done any data writes into HV partition, and downgrade to prior version.

Before You Begin

- You must log in with admin privileges to perform this task.
- Cisco Flexible Flash must be supported on your server.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope flexflash index	Enters the Cisco Flexible Flash controller command mode for the specified controller. At this time, the only permissible <i>index</i> value is FlexFlash-0 .
Step 3	Server /chassis/flexflash # reset-partition-defaults primary slot ID	Resets the configuration of the selected slot to the default configuration.

This example shows how to reset the configuration from a slot to the default configuration:

```
Server# scope chassis
Server /chassis # scope flexflash FlexFlash-0
Server /chassis/flexflash # reset-partition-defaults slot1
```

This action will mark the slot1 as the healthy primary slot, and slot2 (if card exists) as unhealthy secondary active.

This operation may disturb the host connectivity as well.
Continue? [y|N] y

```
Server /chassis/flexflash/operational-profile #
```

Retaining the Configuration of the Flexible Flash Controller

You can copy the configuration of a given slot in the Cisco Flexible Flash card to the other slot. However, the slot from which the configuration is copied from must be of the SDK523 type. You can retain the configuration in the following situations:

- There are two unpaired FlexFlash
- The server is operating from a single FlexFlash, and an unpaired FlexFlash is in the other slot.
- One FlexFlash supports firmware version 253, and the other FlexFlash is unpartitioned.

Before You Begin

- You must log in with admin privileges to perform this task.
- Cisco Flexible Flash must be supported on your server.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.

	Command or Action	Purpose
Step 2	Server /chassis # scope flexflash index	Enters the Cisco Flexible Flash controller command mode for the specified controller. At this time, the only permissible <i>index</i> value is FlexFlash-0 .
Step 3	Server /chassis/flexflash # synchronize-card-configuration <i>primary slot ID</i>	Copies the configuration from the primary slot to the secondary slot.

This example shows how to copy the configuration from one slot to the other:

```
Server# scope chassis
Server /chassis # scope flexflash FlexFlash-0
Server /chassis/flexflash # synchronize-card-configuration slot1
```

This action will copy the config of slot1 to both the slots, mark slot1 as healthy, primary slot and slot2 (card must be present) as unhealthy secondary active. This operation may disturb the host connectivity as well.
Continue? [y|N] y

```
Server /chassis/flexflash/operational-profile #
```

Configuring BIOS Settings

Viewing BIOS Status

Procedure

	Command or Action	Purpose
Step 1	Server# scope bios	Enters the BIOS command mode.
Step 2	Server /bios # show detail	Displays details of the BIOS status.

The BIOS status information contains the following fields:

Name	Description
BIOS Version	The version string of the running BIOS.
Boot Order	The order of bootable target types that the server will attempt to use.
Boot Override Priority	This can be None, SCU, HV, or HUU.
FW Update/Recovery Status	The status of any pending firmware update or recovery action.

Name	Description
FW Update/Recovery Progress	The percentage of completion of the most recent firmware update or recovery action.

This example displays the BIOS status:

```
Server# scope bios
Server /bios # show detail
  BIOS Version: "C460M1.1.2.2a.0 (Build Date: 01/12/2011)"
  Boot Order: EFI,CDROM,HDD
  Boot Override Priority:
  FW Update/Recovery Status: NONE
  FW Update/Recovery Progress: 100

Server /bios #
```

Configuring Main BIOS Settings

Before You Begin

You must log in with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope bios	Enters the BIOS command mode.
Step 2	Server /bios # scope main	Enters the main BIOS settings command mode.
Step 3	Configure the BIOS settings.	The BIOS parameters available depend on the model of the server that you are using. For descriptions and information about the options for each BIOS setting, see one the following topics: <ul style="list-style-type: none"> • Main BIOS Parameters for C22 and C24 Servers , on page 197 • Main BIOS Parameters for C200 and C210 Servers • Main BIOS Parameters for C250 Servers • Main BIOS Parameters for C260 Servers , on page 237 • Main BIOS Parameters for C460 Servers , on page 270
Step 4	Server /bios/main # commit	Commits the transaction to the system configuration. Changes are applied on the next server reboot. If server power is on, you are prompted to choose whether to reboot now.

This example configures the BIOS to pause the boot upon a critical POST error and commits the transaction:

```
Server# scope bios
Server /bios # scope main
```

```

Server /bios/main # set POSTErrorPause Enabled
Server /bios/main *# commit
Changes to BIOS set-up parameters will require a reboot.
Do you want to reboot the system?[y|N] n
Changes will be applied on next reboot.
Server /bios/main #

```

Configuring Advanced BIOS Settings



Note

Depending on your installed hardware, some configuration options described in this topic may not appear.

Before You Begin

You must log in with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope bios	Enters the BIOS command mode.
Step 2	Server /bios # scope advanced	Enters the advanced BIOS settings command mode.
Step 3	Configure the BIOS settings.	<p>The BIOS parameters available depend on the model of the server that you are using. For descriptions and information about the options for each BIOS setting, see one the following topics:</p> <ul style="list-style-type: none"> • Advanced BIOS Parameters for C22 and C24 Servers , on page 198 • Advanced BIOS Parameters for C200 and C210 Servers • Advanced BIOS Parameters for C250 Servers • Advanced BIOS Parameters for C260 Servers , on page 237 • Advanced BIOS Parameters for C460 Servers , on page 270
Step 4	Server /bios/advanced # commit	<p>Commits the transaction to the system configuration.</p> <p>Changes are applied on the next server reboot. If server power is on, you are prompted to choose whether to reboot now.</p>

This example enables low voltage DDR memory mode and commits the transaction:

```

Server# scope bios
Server /bios # scope advanced
Server /bios/advanced # set LvDDRMode Enabled
Server /bios/advanced *# commit
Changes to BIOS set-up parameters will require a reboot.
Do you want to reboot the system?[y|N] n
Changes will be applied on next reboot.
Server /bios/advanced #

```


Configuring Server Management BIOS Settings

Before You Begin

You must log in with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope bios	Enters the BIOS command mode.
Step 2	Server /bios # scope server-management	Enters the server management BIOS settings command mode.
Step 3	Configure the BIOS settings.	<p>The BIOS parameters available depend on the model of the server that you are using. For descriptions and information about the options for each BIOS setting, see one the following topics:</p> <ul style="list-style-type: none"> • Server Management BIOS Parameters for C22 and C24 Servers , on page 214 • Server Management BIOS Parameters for C200 and C210 Servers • Server Management BIOS Parameters for C250 Servers • Server Management BIOS Parameters for C260 Servers , on page 247 • Server Management BIOS Parameters for C460 Servers , on page 280
Step 4	Server /bios/server-management # commit	<p>Commits the transaction to the system configuration.</p> <p>Changes are applied on the next server reboot. If server power is on, you are prompted to choose whether to reboot now.</p>

This example enables automatic detection of the BMC and commits the transaction:

```
Server# scope bios
Server /bios # scope server-management
Server /bios/server-management # set BMCpNP Enabled
Server /bios/server-management *# commit
Changes to BIOS set-up parameters will require a reboot.
Do you want to reboot the system?[y|N] n
Changes will be applied on next reboot.
Server /bios/server-management #
```

Restoring BIOS Defaults

Before You Begin

You must log in as a user with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope bios	Enters the BIOS command mode.
Step 2	Server /bios # bios-setup-default	Restores BIOS default settings. This command initiates a reboot.

This example restores BIOS default settings:

```
Server# scope bios
Server /bios # bios-setup-default
This operation will reset the BIOS set-up tokens to factory defaults.
All your configuration will be lost.
Changes to BIOS set-up parameters will initiate a reboot.
Continue?[y|N]y
```

Restoring BIOS Manufacturing Custom Defaults

In instances where the components of the BIOS no longer function as desired, you can restore the BIOS set up tokens to the manufacturing default values.

**Note**

This action is only available for some C-Series servers.

Before You Begin

- You must log in with admin privileges to perform this task.
- The server must be powered off.

Procedure

	Command or Action	Purpose
Step 1	Server# scope bios	Enters the BIOS command mode.
Step 2	Server /bios # restore-mfg-defaults	Restores the set up tokens to the manufacturing default values.

This example shows how to restore the BIOS set up tokens to the manufacturing default values:

```
Server # scope bios
Server /bios # restore-mfg-defaults
This operation will reset the BIOS set-up tokens to manufacturing defaults.
The system will be powered on.
Continue? [y|n] N
Server /bios #
```

Updating Firmware on Server Components



Important If any firmware or BIOS updates are in progress, do not reset the server until those tasks are complete.

Before You Begin

You must log in with user or admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters chassis command mode.
Step 2	Server /chassis # scope firmware	Enters chassis command mode.
Step 3	Server /chassis/firmware # show detail	Displays the firmware update required on some components message.
Step 4	Server /chassis/firmware # update-all	Updates the firmware on the server components.

This example resets the server:

```
Server# scope chassis
Server /chassis # scope firmware
Server /chassis / firmware # show detail

Firmware update required on some components,
please run update-all (under chassis/firmware scope).

Server /chassis / firmware # update-all
```




Viewing Server Properties

This chapter includes the following sections:

- [Viewing Server Properties, page 43](#)
- [Viewing CIMC Properties, page 44](#)
- [Viewing CPU Properties, page 44](#)
- [Viewing Memory Properties, page 45](#)
- [Viewing Power Supply Properties, page 46](#)
- [Viewing Storage Properties, page 46](#)
- [Viewing PCI Adapter Properties, page 52](#)
- [Viewing Network Related Properties, page 52](#)

Viewing Server Properties

Procedure

	Command or Action	Purpose
Step 1	Server# show chassis [detail]	Displays server properties.

This example displays server properties:

```
Server# show chassis detail
Chassis:
  Power: on
  Serial Number: QCI140205ZG
  Product Name: UCS C210 M2
  PID : R210-2121605W
  UUID: FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFFFF
  Locator LED: off
  Description:
  Power Restore Policy: power-off
  Power Delay Type: fixed
  Power Delay Value(sec): 0
```

Server#

Viewing CIMC Properties


Note

CIMC gets the current date and time from the server BIOS. To change this information, reboot the server and press **F2** when prompted to access the BIOS configuration menu. Then change the date or time using the options on the main BIOS configuration tab.

Procedure

	Command or Action	Purpose
Step 1	Server# show cimc [detail]	Displays CIMC properties.

This example displays CIMC properties:

```
Server# show cimc detail
CIMC:
  Firmware Version: 1.4(2.18)
  Current Time: Wed Jan 11 07:01:50 2012
  Boot-loader Version: 1.4(2.18).16
```

Server#

Viewing CPU Properties

Before You Begin

The server must be powered on, or the properties will not display.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters chassis command mode.
Step 2	Server /chassis # show cpu [detail]	Displays CPU properties.

This example displays CPU properties:

```
Server# scope chassis
Server /chassis # show cpu
Name          Cores    Version
-----
CPU1          4        Intel(R) Xeon(R) CPU           E5520  @ 2.27GHz
CPU2          4        Intel(R) Xeon(R) CPU           E5520  @ 2.27GHz
```

Server /chassis #

Viewing Memory Properties

Before You Begin

The server must be powered on, or the properties will not display.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters chassis command mode.
Step 2	Server /chassis # show dimm [detail]	Displays memory properties.
Step 3	Server /chassis # show dimm-summary	Displays DIMM summary information.

This example displays memory properties:

```
Server# scope chassis
Server /chassis # show dimm
Name Capacity Channel Speed (MHz) Channel Type
-----
DIMM_A1 2048 MB 1067 Other
DIMM_A2 2048 MB 1067 Other
DIMM_B1 2048 MB 1067 Other
DIMM_B2 2048 MB 1067 Other
DIMM_C1 Not Installed Unknown Other
DIMM_C2 Not Installed Unknown Other
DIMM_D1 2048 MB 1067 Other
DIMM_D2 2048 MB 1067 Other
DIMM_E1 2048 MB 1067 Other
DIMM_E2 2048 MB 1067 Other
DIMM_F1 Not Installed Unknown Other
DIMM_F2 Not Installed Unknown Other
```

```
Server /chassis #
```

This example displays detailed information about memory properties:

```
Server# scope chassis
Server /chassis # show dimm detail
Name DIMM_A1:
  Capacity: 2048 MB
  Channel Speed (MHz): 1067
  Channel Type: Other
  Memory Type Detail: Synchronous
  Bank Locator: NODE 0 CHANNEL 0 DIMM 0
  Visibility: Yes
  Operability: Operable
  Manufacturer: 0x802C
  Part Number: 18JSF25672PY-1G1D1
  Serial Number: 0xDA415F3F
  Asset Tag: Unknown
  Data Width: 64 bits
Name DIMM_A2:
  Capacity: 2048 MB
--More--
```

```
Server /chassis #
```

This example displays DIMM summary information:

```
Server# scope chassis
Server /chassis # show dimm-summary
```

```

DIMM Summary:
  Memory Speed: 1067 MHz
  Total Memory: 16384 MB
  Effective Memory: 16384 MB
  Redundant Memory: 0 MB
  Failed Memory: 0 MB
  Ignored Memory: 0 MB
  Number of Ignored Dimms: 0
  Number of Failed Dimms: 0
  Memory RAS possible: Memory configuration can support mirroring
  Memory Configuration: Maximum Performance

Server /chassis #

```

Viewing Power Supply Properties

Before You Begin

The server must be powered on, or the properties will not display.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters chassis command mode.
Step 2	Server /chassis # show psu [detail]	Displays power supply properties.

This example displays power supply properties:

```

Server# scope chassis
Server /chassis # show psu
Name          In. Power (Watts)  Out. Power (Watts)  Firmware  Status
-----
PSU1          74              650                R0E       Present
PSU2          83              650                R0E       Present

Server /chassis #

```

Viewing Storage Properties

Viewing Storage Adapter Properties

Before You Begin

The server must be powered on, or the properties will not display.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # show storageadapter [slot] [detail]	Displays installed storage cards. Note This command displays all MegaRAID controllers on the server that can be managed through CIMC. If an installed controller or storage device is not displayed, then it cannot be managed through CIMC.
Step 3	Server /chassis # scope storageadapter slot	Enters command mode for an installed storage card.
Step 4	Server /chassis/storageadapter # show bbu [detail]	Displays battery backup unit information for the storage card.
Step 5	Server /chassis/storageadapter # show capabilites [detail]	Displays RAID levels supported by the storage card.
Step 6	Server /chassis/storageadapter # show error-counters [detail]	Displays number of errors seen by the storage card.
Step 7	Server /chassis/storageadapter # show firmware-versions [detail]	Displays firmware version information for the storage card.
Step 8	Server /chassis/storageadapter # show hw-config [detail]	Displays hardware information for the storage card.
Step 9	Server /chassis/storageadapter # show mfg-data [detail]	Displays manufacturer data for the storage card.
Step 10	Server /chassis/storageadapter # show pci-info [detail]	Displays adapter PCI information for the storage card.
Step 11	Server /chassis/storageadapter # show running-firmware-images [detail]	Displays running firmware information for the storage card.
Step 12	Server /chassis/storageadapter # show settings [detail]	Displays adapter firmware settings for the storage card.
Step 13	Server /chassis/storageadapter # show startup-firmware-images [detail]	Displays firmware images to be activated on startup for the storage card.

This example displays storage properties:

```

Server# scope chassis
Server /chassis # show storageadapter
PCI Slot Product Name                Serial Number  Firmware Package Build
-----
SAS          LSI MegaRAID SAS 9260-8i  SV93404392    12.12.0-0038

```

```

      Product ID      Battery Status Cache Memory Size
-----
LSI Logic           fully charged  0 MB

```

Server /chassis #

This example displays battery backup unit information for the storage card named SAS:

Server# **scope chassis**

Server /chassis # **scope storageadapter SAS**

Server /chassis/storageadapter # **show bbu**

```

Controller Battery Type Battery Present Voltage      Current      Charge Charging State
-----
SAS          iBBU          true          4.051 V      0.000 A      100%      fully charged

```

Server /chassis/storageadapter #

Viewing the Flexible Flash Controller Properties

Before You Begin

- Cisco Flexible Flash must be supported by your platform.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # show flexflash [detail]	(Optional) Displays the available Cisco Flexible Flash controllers.
Step 3	Server /chassis # scope flexflash index	Enters the Cisco Flexible Flash controller command mode for the specified controller. At this time, the only permissible <i>index</i> value is FlexFlash-0 .
Step 4	Server /chassis/flexflash # show operational-profile [detail]	Displays the operational profile properties.

This example displays the properties of the flash controller:

Server# **scope chassis**

Server /chassis # **show flexflash**

```

Controller  Product Name      Has Error  Firmware Version  Vendor      Internal State
-----
FlexFlash-0 Cisco FlexFlash  No         1.2 build 247     Cypress     Connected

```

Server /chassis # **scope flexflash FlexFlash-0**

Server /chassis # **show operational-profile**

```

Primary Member Slot I/O Error Threshold Host Accessible VDs
-----
slot1              100                      SCU Drivers

```

Server /chassis/flexflash #

Viewing Physical Drive Properties

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope storageadapter slot	Enters command mode for an installed storage card.
Step 3	Server /chassis/storageadapter # show physical-drive [<i>drive-number</i>] [<i>detail</i>]	Displays physical drive information for the storage card.
Step 4	Server /chassis/storageadapter # show physical-drive-count [<i>detail</i>]	Displays the number of physical drives on the storage card.
Step 5	Server /chassis/storageadapter # scope physical-drive <i>drive-number</i>	Enters command mode for the specified physical drive.
Step 6	Server /chassis/storageadapter/physical-drive # show general [<i>detail</i>]	Displays general information about the specified physical drive.
Step 7	Server /chassis/storageadapter/physical-drive # show inquiry-data [<i>detail</i>]	Displays inquiry data about the specified physical drive.
Step 8	Server /chassis/storageadapter/physical-drive # show status [<i>detail</i>]	Displays status information about the specified physical drive.

This example displays general information about physical drive number 1 on the storage card named SAS:

```

Server# scope chassis
Server /chassis # scope storageadapter SAS
Server /chassis/storageadapter # scope physical-drive 1
Server /chassis/storageadapter/physical-drive # show general
Slot Number 1:
  Controller: SAS
  Enclosure Device ID: 27
  Device ID: 34
  Sequence Number: 2
  Media Error Count: 0
  Other Error Count: 0
  Predictive Failure Count: 0
  Link Speed: 6.0 Gb/s
  Interface Type: SAS
  Media Type: HDD
  Block Size: 512
  Block Count: 585937500
  Raw Size: 286102 MB
  Non Coerced Size: 285590 MB
  Coerced Size: 285568 MB
  SAS Address 0: 500000e112693fa2
  SAS Address 1:
  Connected Port 0:
  Connected Port 1:
  Connected Port 2:
  Connected Port 3:
  Connected Port 4:
  Connected Port 5:

```

```

Connected Port 6:
Connected Port 7:
Power State: powersave

```

```
Server /chassis/storageadapter/physical-drive #
```

This example displays inquiry data about physical drive number 1 on the storage card named SAS:

```

Server# scope chassis
Server /chassis # scope storageadapter SAS
Server /chassis/storageadapter # scope physical-drive 1
Server /chassis/storageadapter/physical-drive # show inquiry-data
Slot Number 1:
  Controller: SAS
  Product ID: MBD2300RC
  Drive Firmware: 5701
  Drive Serial Number: D010P9A0016D

```

```
Server /chassis/storageadapter/physical-drive #
```

This example displays status information about physical drive number 1 on the storage card named SAS:

```

Server# scope chassis
Server /chassis # scope storageadapter SAS
Server /chassis/storageadapter # scope physical-drive 1
Server /chassis/storageadapter/physical-drive # show inquiry-data
Slot Number 1:
  Controller: SAS
  State: online
  Online: true
  Fault: false

```

```
Server /chassis/storageadapter/physical-drive #
```

Viewing Virtual Drive Properties

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope storageadapter slot	Enters command mode for an installed storage card.
Step 3	Server /chassis/storageadapter # show virtual-drive [drive-number] [detail]	Displays virtual drive information for the storage card.
Step 4	Server /chassis/storageadapter # show virtual-drive-count [detail]	Displays the number of virtual drives configured on the storage card.
Step 5	Server /chassis/storageadapter # scope virtual-drive drive-number	Enters command mode for the specified virtual drive.
Step 6	Server /chassis/storageadapter/virtual-drive # show physical-drive [detail]	Displays physical drive information about the specified virtual drive.

This example displays information about virtual drives on the storage card named SAS:

```

Server# scope chassis
Server /chassis # scope storageadapter SAS
Server /chassis/storageadapter # show virtual-drive

```

Virtual Drive	Status	Name	Size	RAID Level
0	Optimal	SLES1SP1beta5	30720 MB	RAID 0
1	Optimal	RHEL5.5	30720 MB	RAID 0
2	Optimal	W2K8R2_DC	30720 MB	RAID 0
3	Optimal	VD_3	30720 MB	RAID 0
4	Optimal	ESX4.0u2	30720 MB	RAID 0
5	Optimal	VMs	285568 MB	RAID 0
6	Optimal	RHEL6-35GB	35840 MB	RAID 0
7	Optimal	OS_Ins_Test_DR	158720 MB	RAID 0
8	Optimal		285568 MB	RAID 1

Server /chassis/storageadapter #

This example displays physical drive information about virtual drive number 1 on the storage card named SAS:

```

Server# scope chassis
Server /chassis # scope storageadapter SAS
Server /chassis/storageadapter # scope virtual-drive 1
Server /chassis/storageadapter/virtual-drive # show physical-drive
Span  Physical Drive Status    Starting Block Number Of Blocks
-----
0      12                online      62914560      62914560

Server /chassis/storageadapter/virtual-drive #

```

Viewing Nvidia GPU Card Information

These commands are not available on all UCS C-series servers.

Before You Begin

The server must be powered on to view information on the Nvidia GPU cards.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # show gpu	Displays the available Nvidia GPU cards on the system.
Step 3	Server /chassis # scope gpu <i>slot-number</i>	Enters the GPU card command mode. Specify the slot number of the GPU card.
Step 4	Server /chassis/gpu # show gpu-list	Displays temperature information on the GPU cards.

This example shows how to view the temperature information of the available GPU cards on the system:

```

Server # scope chassis
Server /chassis # show gpu

Slot      Product Name          Num of GPUs
-----
5         Nvidia GRID K2 @ BD      2

Server /chassis # scope gpu 5
Server /chassis/gpu # show gpu-list

```

```

GPU ID      Temperature
-----
0           32
1           33

Server /chassis/gpu #

```

Viewing PCI Adapter Properties

Before You Begin

The server must be powered on, or the properties will not display.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # show pci-adapter [detail]	Displays PCI adapter properties.

This example displays PCI adapter properties:

```

Server# scope chassis
Server /chassis # show pci-adapter
Name                Slot  Vendor ID  Device ID  Product Name
-----
PCIe Adapter1       1    0x1137    0x0042     Cisco UCS P81E Virtual...
PCIe Adapter2       5    0x1077    0x2432     Qlogic QLE2462 4Gb dua...

Server /chassis #

```

Viewing Network Related Properties

Viewing LOM Properties

You can view the MAC addresses of the LAN On Motherboard (LOM) Ethernet ports.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope network-adapter slot ID	Enters the specific network adapter command mode.
Step 3	Server /chassis/network-adapter # show mac-list [detail]	Displays the MAC addresses of the LOM ports.

This example shows how to display the MAC addresses of the LOM ports:

```
Server# scope chassis
Server /chassis # scope network-adapter 1
Server /chassis/network-adapter # show mac-list
Interface ID      MAC Address
-----
eth0              010000002000
eth1              010000002000

Server /chassis/network-adapter #
```




Viewing Server Sensors

This chapter includes the following sections:

- [Viewing Power Supply Sensors, page 55](#)
- [Viewing Fan Sensors, page 56](#)
- [Viewing Temperature Sensors, page 56](#)
- [Viewing Voltage Sensors, page 57](#)
- [Viewing Current Sensors, page 58](#)
- [Viewing Storage Sensors, page 58](#)

Viewing Power Supply Sensors

Procedure

	Command or Action	Purpose
Step 1	Server# scope sensor	Enters sensor command mode.
Step 2	Server /sensor # show psu [detail]	Displays power supply sensor statistics for the server.
Step 3	Server /sensor # show psu-redundancy [detail]	Displays power supply redundancy sensor status for the server.

This example displays power supply sensor statistics:

```
Server# scope sensor
Server /sensor # show psu
Name           Sensor Status   Reading   Units   Min. Warning   Max. Warning
  Min. Failure   Max. Failure
-----
PSU1_STATUS      Normal           present
```

```

PSU2_STATUS          Normal          present

Server /sensor # show psu-redundancy
Name                  Reading        Sensor Status
-----
PSU_REDUNDANCY        full          Normal

Server /sensor #

```

Viewing Fan Sensors

Procedure

	Command or Action	Purpose
Step 1	Server# scope sensor	Enters sensor command mode.
Step 2	Server /sensor # show fan [detail]	Displays fan sensor statistics for the server.

This example displays fan sensor statistics:

```

Server# scope sensor
Server /sensor # show fan
Name                  Sensor Status  Reading    Units      Min. Warning  Max. Warning
Min. Failure          Max. Failure
-----
W793_FAN2_TACH1      Normal        2400       RPM        N/A           N/A
800                  N/A
W793_FAN2_TACH2      Normal        2400       RPM        N/A           N/A
800                  N/A
W793_FAN3_TACH1      Normal        2300       RPM        N/A           N/A
800                  N/A
W793_FAN3_TACH2      Normal        2300       RPM        N/A           N/A
800                  N/A
W793_FAN4_TACH1      Normal        2400       RPM        N/A           N/A
800                  N/A
W793_FAN4_TACH2      Normal        1600       RPM        N/A           N/A
800                  N/A

Server /sensor #

```

Viewing Temperature Sensors

Procedure

	Command or Action	Purpose
Step 1	Server# scope sensor	Enters sensor command mode.
Step 2	Server /sensor # show temperature [detail]	Displays temperature sensor statistics for the server.

This example displays temperature sensor statistics:

```

Server# scope sensor
Server /sensor # show temperature
Name                               Sensor Status  Reading  Units  Min. Warning Max. Warning
Min. Failure Max. Failure
-----
IOH_TEMP_SENS                     Normal        32.0    C      N/A      80.0
N/A                               85.0
P2_TEMP_SENS                      Normal        31.0    C      N/A      80.0
N/A                               81.0
P1_TEMP_SENS                      Normal        34.0    C      N/A      80.0
N/A                               81.0
DDR3_P2_D1_TMP                   Normal        20.0    C      N/A      90.0
N/A                               95.0
DDR3_P1_A1_TMP                   Normal        21.0    C      N/A      90.0
N/A                               95.0
FP_AMBIENT_TEMP                  Normal        28.0    C      N/A      40.0
N/A                               45.0

Server /sensor #

```

Viewing Voltage Sensors

Procedure

	Command or Action	Purpose
Step 1	Server# scope sensor	Enters sensor command mode.
Step 2	Server /sensor # show voltage [detail]	Displays voltage sensor statistics for the server.

This example displays voltage sensor statistics:

```

Server# scope sensor
Server /sensor # show voltage
Name                               Sensor Status  Reading  Units  Min. Warning Max. Warning
Min. Failure Max. Failure
-----
P3V_BAT_SCALED                   Normal        3.022    V      N/A      N/A
2.798                           3.088
P12V_SCALED                      Normal        12.154   V      N/A      N/A
11.623                          12.331
P5V_SCALED                      Normal        5.036    V      N/A      N/A
4.844                           5.157
P3V3_SCALED                     Normal        3.318    V      N/A      N/A
3.191                           3.381
P5V_STBY_SCALED                 Normal        5.109    V      N/A      N/A
4.844                           5.157
PV_VCCP_CPU1                   Normal        0.950    V      N/A      N/A
0.725                           1.391
PV_VCCP_CPU2                   Normal        0.891    V      N/A      N/A
0.725                           1.391
P1V5_DDR3_CPU1                 Normal        1.499    V      N/A      N/A
1.450                           1.548
P1V5_DDR3_CPU2                 Normal        1.499    V      N/A      N/A
1.450                           1.548
P1V1_IOH                       Normal        1.087    V      N/A      N/A
1.068                           1.136
P1V8_AUX                       Normal        1.773    V      N/A      N/A

```

```

1.744          1.852
Server /sensor #

```

Viewing Current Sensors

Procedure

	Command or Action	Purpose
Step 1	Server# scope sensor	Enters sensor command mode.
Step 2	Server /sensor # show current [detail]	Displays current sensor statistics for the server.

This example displays current sensor statistics:

```

Server# scope sensor
Server /sensor # show current
Name                               Sensor Status  Reading    Units      Min. Warning Max. Warning
Min. Failure Max. Failure
-----
VR_P2_IMON                         Normal         16.00     AMP        N/A         147.20
N/A                               164.80
VR_P1_IMON                         Normal         27.20     AMP        N/A         147.20
N/A                               164.80
Server /sensor #

```

Viewing Storage Sensors

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters chassis command mode.
Step 2	Server /chassis # show hdd [detail]	Displays storage sensor information.

The displayed fields are described in the following table:

Name	Description
Name column	The name of the storage device.
Status column	A brief description of the storage device status.

Name	Description
LED Status column	<p>The current LED color, if any.</p> <p>To make the physical LED on the storage device blink, select Turn On from the drop-down list. To let the storage device control whether the LED blinks, select Turn Off.</p> <p>Note This information is only available for some C-Series servers.</p>

This example displays storage sensor information:

```
Server# scope chassis
Server /chassis # show hdd
Name                               Status
-----
HDD_01_STATUS                     present
HDD_02_STATUS                     present
HDD_03_STATUS                     present
HDD_04_STATUS                     present

Server /chassis #
```




Managing Remote Presence

This chapter includes the following sections:

- [Managing the Virtual KVM, page 61](#)
- [Configuring Virtual Media, page 64](#)
- [Managing Serial over LAN, page 68](#)

Managing the Virtual KVM

KVM Console

The KVM console is an interface accessible from CIMC that emulates a direct keyboard, video, and mouse (KVM) connection to the server. The KVM console allows you to connect to the server from a remote location.

Instead of using CD/DVD or floppy drives physically connected to the server, the KVM console uses virtual media, which are actual disk drives or disk image files that are mapped to virtual CD/DVD or floppy drives. You can map any of the following to a virtual drive:

- CD/DVD or floppy drive on your computer
- Disk image files (ISO or IMG files) on your computer
- USB flash drive on your computer
- CD/DVD or floppy drive on the network
- Disk image files (ISO or IMG files) on the network
- USB flash drive on the network

You can use the KVM console to install an OS on the server.



Note

The KVM Console is operated only through the GUI. To launch the KVM Console, see the instructions in the *Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide*.

Enabling the Virtual KVM

Before You Begin

You must log in as a user with admin privileges to enable the virtual KVM.

Procedure

	Command or Action	Purpose
Step 1	Server# scope kvm	Enters KVM command mode.
Step 2	Server /kvm # set enabled yes	Enables the virtual KVM.
Step 3	Server /kvm # commit	Commits the transaction to the system configuration.
Step 4	Server /kvm # show [detail]	(Optional) Displays the virtual KVM configuration.

This example enables the virtual KVM:

```
Server# scope kvm
Server /kvm # set enabled yes
Server /kvm *# commit
Server /kvm # show
Encryption Enabled Local Video    Active Sessions Enabled KVM Port
-----
no                               yes          0          yes          2068

Server /kvm #
```

Disabling the Virtual KVM

Before You Begin

You must log in as a user with admin privileges to disable the virtual KVM.

Procedure

	Command or Action	Purpose
Step 1	Server# scope kvm	Enters KVM command mode.
Step 2	Server /kvm # set enabled no	Disables the virtual KVM. Note Disabling the virtual KVM disables access to the virtual media feature, but does not detach the virtual media devices if virtual media is enabled.

	Command or Action	Purpose
Step 3	Server /kvm # commit	Commits the transaction to the system configuration.
Step 4	Server /kvm # show [detail]	(Optional) Displays the virtual KVM configuration.

This example disables the virtual KVM:

```
Server# scope kvm
Server /kvm # set enabled no
Server /kvm *# commit
Server /kvm # show
Encryption Enabled Local Video      Active Sessions Enabled KVM Port
-----
no                               yes          0                no          2068

Server /kvm #
```

Configuring the Virtual KVM

Before You Begin

You must log in as a user with admin privileges to configure the virtual KVM.

Procedure

	Command or Action	Purpose
Step 1	Server# scope kvm	Enters KVM command mode.
Step 2	Server /kvm # set enabled {yes no}	Enables or disables the virtual KVM.
Step 3	Server /kvm # set encrypted {yes no}	If encryption is enabled, the server encrypts all video information sent through the KVM.
Step 4	Server /kvm # set kvm-port port	Specifies the port used for KVM communication.
Step 5	Server /kvm # set local-video {yes no}	If local video is yes , the KVM session is also displayed on any monitor attached to the server.
Step 6	Server /kvm # set max-sessions sessions	Specifies the maximum number of concurrent KVM sessions allowed. The <i>sessions</i> argument is an integer between 1 and 4.
Step 7	Server /kvm # commit	Commits the transaction to the system configuration.
Step 8	Server /kvm # show [detail]	(Optional) Displays the virtual KVM configuration.

This example configures the virtual KVM and displays the configuration:

```
Server# scope kvm
Server /kvm # set enabled yes
Server /kvm *# set encrypted no
```

```

Server /kvm *# set kvm-port 2068
Server /kvm *# set max-sessions 4
Server /kvm *# set local-video yes
Server /kvm *# commit
Server /kvm # show detail
KVM Settings:
  Encryption Enabled: no
  Max Sessions: 4
  Local Video: yes
  Active Sessions: 0
  Enabled: yes
  KVM Port: 2068

Server /kvm #

```

What to Do Next

Launch the virtual KVM from the GUI.

Configuring Virtual Media

Before You Begin

You must log in as a user with admin privileges to configure virtual media.

Procedure

	Command or Action	Purpose
Step 1	Server# scope vmedia	Enters virtual media command mode.
Step 2	Server /vmedia # set enabled {yes no}	Enables or disables virtual media. By default, virtual media is disabled. Note Disabling virtual media detaches the virtual CD, virtual floppy, and virtual HDD devices from the host.
Step 3	Server /vmedia # set encryption {yes no}	Enables or disables virtual media encryption.
Step 4	Server /vmedia # set low-power-usb-enabled {yes no}	Enables or disables low power USB. Note While mapping an ISO to a server which has a UCS VIC P81E card and the NIC is in Cisco Card mode: <ul style="list-style-type: none"> • If the low power USB is enabled, after mapping the ISO and rebooting the host the card resets and ISO mapping is lost. The virtual drives are not visible on the boot selection menu. • If the low power USB is disabled, after mapping the ISO, and rebooting the host and the CIMC, the virtual drivers appear on the boot selection menu as expected.
Step 5	Server /vmedia # commit	Commits the transaction to the system configuration.

	Command or Action	Purpose
Step 6	Server /vmedia # show [detail]	(Optional) Displays the virtual media configuration.

This example configures virtual media encryption:

```
Server# scope vmedia
Server /vmedia # set enabled yes
Server /vmedia *# set encryption yes
Server /vmedia *# set low-power-use-enabled no
Server /vmedia *# commit
Server /vmedia # show detail
vMedia Settings:
  Encryption Enabled: yes
  Enabled: yes
  Max Sessions: 1
  Active Sessions: 0
  Low Power USB Enabled: no

Server /vmedia #
```

What to Do Next

Use the KVM to attach virtual media devices to a host.

Configuring a CIMC-Mapped vMedia Volume

Before You Begin

You must log in with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server # scope vmedia	Enters the virtual media command mode.
Step 2	Server /vmedia # map-cifs { volume-name remote-share remote-file-path [<i>mount options</i>]	Maps a CIFS file for vMedia. You must specify the following: <ul style="list-style-type: none"> • Name of the volume to create • Remote share including IP address and the exported directory • Path of the remote file corresponding to the exported directory. • (Optional) Mapping options • Username and password to connect to the server
Step 3	Server /vmedia # map-nfs { volume-name remote-share remote-file-path } [<i>mount options</i>]	Maps an NFS file for vMedia. You must specify the following: <ul style="list-style-type: none"> • Name of the volume to create

	Command or Action	Purpose
		<ul style="list-style-type: none"> • Remote share including IP address and the exported directory • Path of the remote file corresponding to the exported directory. • (Optional) Mapping options
Step 4	Server /vmedia # map-www { volume-name remote-share remote-file-path [<i>mount options</i>]	Maps an HTTPS file for vMedia. You must specify the following: <ul style="list-style-type: none"> • Name of the volume to create • Remote share including IP address and the exported directory • Path of the remote file corresponding to the exported directory. • (Optional) Mapping options • Username and password to connect to the server

This example shows how to create a CIFS CIMC-mapped vmedia settings:

```

Server # scope vmedia
Server /vmedia # map-cifs sample-volume //10.10.10.10/project /test/sample
Server username:
Server password: ****
Confirm password: ****

Server /vmedia #

```

Viewing CIMC-Mapped vMedia Volume Properties

Before You Begin

You must log in with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server # scope vmedia	Enters the virtual media command mode.
Step 2	Server /vmedia # show mappings detail	Displays information on all the vmedia mapping that are configured.

This example shows how to view the properties of all the configured vmedia mapping:

```
Server # scope vmedia
Server /vmedia # show mappings
```

Volume	Map-status	Drive-type	remote-share	remote-file	mount-type
Huu	OK	removable	http://10.104.236.99/	rhel-server-6.1-x86_6.iso	www
Rhel	OK	CD	http://10.104.236.99/	rhel-server-6.1-x86_6.iso	www

Removing a CIMC-Mapped Mounted vMedia Volume

Before You Begin

You must log in with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server # scope vmedia	Enters the virtual media command mode.
Step 2	Server /vmedia # unmap volume_name	Specifies the volume name to unmap.

This example shows how to unmap a CIMC-mapped vmedia volume:

```
Server # scope vmedia
Server /vmedia # show mappings
```

Volume	Map-status	Drive-type	remote-share	remote-file	mount-type
Huu	OK	removable	http://10.104.236.99/	rhel-server-6.1-x86_6.iso	www
Rhel	OK	CD	http://10.104.236.99/	rhel-server-6.1-x86_6.iso	www

```
Server /vmedia # unmap huu
Server /vmedia # show mappings
```

Volume	Map-status	Drive-type	remote-share	remote-file	mount-type
Rhel	OK	CD	http://10.104.236.99/	rhel-server-6.1-x86_6.iso	www

```
Server /vmedia #
```

Managing Serial over LAN

Serial Over LAN

Serial over LAN (SoL) is a mechanism that enables the input and output of the serial port of a managed system to be redirected via an SSH session over IP. SoL provides a means of reaching the host console via CIMC.

Guidelines and Restrictions for Serial Over LAN

For redirection to SoL, the server console must have the following configuration:

- console redirection to serial port A
- no flow control
- baud rate the same as configured for SoL
- VT-100 terminal type
- legacy OS redirection disabled

The SoL session will display line-oriented information such as boot messages, and character-oriented screen menus such as BIOS setup menus. If the server boots an operating system or application with a bitmap-oriented display, such as Windows, the SoL session will no longer display. If the server boots a command-line-oriented operating system (OS), such as Linux, you may need to perform additional configuration of the OS in order to properly display in an SoL session.

In the SoL session, your keystrokes are transmitted to the console except for the function key F2. To send an F2 to the console, press the Escape key, then press 2.

Configuring Serial Over LAN

Before You Begin

You must log in as a user with admin privileges to configure serial over LAN (SoL).

Procedure

	Command or Action	Purpose
Step 1	Server# scope sol	Enters SoL command mode.
Step 2	Server /sol # set enabled {yes no}	Enables or disables SoL on this server.
Step 3	Server /sol # set baud-rate {9600 19200 38400 57600 115200}	Sets the serial baud rate the system uses for SoL communication. Note The baud rate must match the baud rate configured in the server serial console.

	Command or Action	Purpose
Step 4	Server /sol # set comport {com0 com1}	<p>(Optional) Sets the serial port through which the system routes SoL communications.</p> <p>Note This field is only available on some C-Series servers. If it is not available, the server always uses COM port 0 for SoL communication.</p> <p>You can specify:</p> <ul style="list-style-type: none"> • com0—SoL communication is routed through COM port 0, an externally accessible serial port that supports either a physical RJ45 connection to an external device or a virtual SoL connection to a network device. <p>If you select this option, the system enables SoL and disables the RJ45 connection, which means that the server can no longer support an external serial device.</p> <ul style="list-style-type: none"> • com1—SoL communication is routed through COM port 1, an internal port accessible only through SoL. <p>If you select this option, you can use SoL on COM port 1 and the physical RJ45 connection on COM port 0.</p> <p>Note Changing the comport setting disconnects any existing SoL sessions.</p>
Step 5	Server /sol # commit	Commits the transaction to the system configuration.
Step 6	Server /sol # show [detail]	(Optional) Displays the SoL settings.

This example configures SoL:

```

Server# scope sol
Server /sol # set enabled yes
Server /sol *# set baud-rate 115200
Server /sol *# commit
Server /sol # show
Enabled Baud Rate(bps)  Com Port
-----
yes      115200          com2
Server /sol # show detail
Serial Over LAN:
  Enabled: yes
  Baud Rate(bps): 115200
  Com Port: com2
Server /sol #

```

Launching Serial Over LAN

Procedure

	Command or Action	Purpose
Step 1	Server# connect host	Opens a serial over LAN (SoL) connection to the redirected server console port. You can enter this command in any command mode.

What to Do Next

To end the SoL session, you must close the CLI session. For example, to end an SoL session over an SSH connection, disconnect the SSH connection.



Managing User Accounts

This chapter includes the following sections:

- [Configuring Local Users, page 71](#)
- [LDAP Servers, page 72](#)
- [Configuring the LDAP Server, page 73](#)
- [Configuring LDAP in CIMC, page 74](#)
- [Configuring LDAP Groups in CIMC, page 75](#)
- [Viewing User Sessions, page 77](#)
- [Terminating a User Session, page 77](#)

Configuring Local Users

Before You Begin

You must log in as a user with admin privileges to configure or modify local user accounts.

Procedure

	Command or Action	Purpose
Step 1	Server# scope user <i>usernumber</i>	Enters user command mode for user number <i>usernumber</i> .
Step 2	Server /user # set enabled { yes no }	Enables or disables the user account on the CIMC.
Step 3	Server /user # set name <i>username</i>	Specifies the username for the user.
Step 4	Server /user # set password	You are prompted to enter the password twice.

	Command or Action	Purpose
Step 5	Server /user # set role {readonly user admin}	Specifies the role assigned to the user. The roles are as follows: <ul style="list-style-type: none"> • readonly—This user can view information but cannot make any changes. • user—This user can do the following: <ul style="list-style-type: none"> • View all information • Manage the power control options such as power on, power cycle, and power off • Launch the KVM console and virtual media • Clear all logs • Toggle the locator LED • admin—This user can perform all actions available through the GUI, CLI, and IPMI.
Step 6	Server /user # commit	Commits the transaction to the system configuration.

This example configures user 5 as an admin:

```

Server# scope user 5
Server /user # set enabled yes
Server /user *# set name john
Server /user *# set password
Please enter password:
Please confirm password:
Server /user *# set role readonly
Server /user *# commit
Server /user # show
User   Name           Role      Enabled
-----
5      john              readonly yes

```

LDAP Servers

CIMC supports directory services that organize information in a directory, and manage access to this information. CIMC supports Lightweight Directory Access Protocol (LDAP), which stores and maintains directory information in a network. In addition, CIMC supports Microsoft Active Directory (AD). Active Directory is a technology that provides a variety of network services including LDAP-like directory services, Kerberos-based authentication, and DNS-based naming. The CIMC utilizes the Kerberos-based authentication service of LDAP.

When LDAP is enabled in the CIMC, user authentication and role authorization is performed by the LDAP server for user accounts not found in the local user database. The LDAP user authentication format is username@domain.com.

By enabling encryption in the configuration of Active Directory on the server, you can require the server to encrypt data sent to the LDAP server.

Configuring the LDAP Server

The CIMC can be configured to use LDAP for user authentication and authorization. To use LDAP, configure users with an attribute that holds the user role and locale information for the CIMC. You can use an existing LDAP attribute that is mapped to the CIMC user roles and locales or you can modify the LDAP schema to add a new custom attribute, such as the CiscoAVPair attribute, which has an attribute ID of 1.3.6.1.4.1.9.287247.1.



Important

For more information about altering the schema, see the article at <http://technet.microsoft.com/en-us/library/bb727064.aspx>.



Note

This example creates a custom attribute named CiscoAVPair, but you can also use an existing LDAP attribute that is mapped to the CIMC user roles and locales.

The following steps must be performed on the LDAP server.

Procedure

Step 1 Ensure that the LDAP schema snap-in is installed.

Step 2 Using the schema snap-in, add a new attribute with the following properties:

Properties	Value
Common Name	CiscoAVPair
LDAP Display Name	CiscoAVPair
Unique X500 Object ID	1.3.6.1.4.1.9.287247.1
Description	CiscoAVPair
Syntax	Case Sensitive String

Step 3 Add the CiscoAVPair attribute to the user class using the snap-in:

- Expand the **Classes** node in the left pane and type U to select the user class.
- Click the **Attributes** tab and click **Add**.
- Type C to select the CiscoAVPair attribute.
- Click **OK**.

Step 4 Add the following user role values to the CiscoAVPair attribute, for the users that you want to have access to CIMC:

Role	CiscoAVPair Attribute Value
admin	shell:roles="admin"
user	shell:roles="user"
read-only	shell:roles="read-only"

Note For more information about adding values to attributes, see the article at <http://technet.microsoft.com/en-us/library/bb727064.aspx>.

What to Do Next

Use the CIMC to configure the LDAP server.

Configuring LDAP in CIMC

Configure LDAP in CIMC when you want to use an LDAP server for local user authentication and authorization.

Before You Begin

You must log in as a user with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope ldap	Enters the LDAP command mode.
Step 2	Server /ldap # set enabled {yes no}	Enables or disables LDAP security. When enabled, user authentication and role authorization is performed by LDAP for user accounts not found in the local user database.
Step 3	Server /ldap # set domain <i>LDAP domain name</i>	Specifies an LDAP domain name.
Step 4	Server /ldap # set timeout <i>seconds</i>	Specifies the number of seconds the CIMC waits until the LDAP search operation times out. The value must be between 0 and 1800 seconds.
Step 5	Server /ldap # set encrypted {yes no}	If encryption is enabled, the server encrypts all information sent to AD.
Step 6	Server /ldap # set base-dn <i>domain-name</i>	Specifies the Base DN that is searched on the LDAP server.
Step 7	Server /ldap # set attribute <i>name</i>	Specify an LDAP attribute that contains the role and locale information for the user. This property is always a name-value pair. The system queries the user record for the value that matches this attribute name.

	Command or Action	Purpose
		<p>You can use an existing LDAP attribute that is mapped to the CIMC user roles and locales or you can create a custom attribute, such as the CiscoAVPair attribute, which has the following attribute ID:</p> <p>1.3.6.1.4.1.9.287247.1</p> <p>Note If you do not specify this property, user access is denied.</p>
Step 8	Server /ldap # set filter-attribute	Specifies the account name attribute. If Active Directory is used, then specify sAMAccountName for this field.
Step 9	Server /ldap # commit	Commits the transaction to the system configuration.
Step 10	Server /ldap # show [detail]	(Optional) Displays the LDAP configuration.

This example configures LDAP using the CiscoAVPair attribute:

```
Server# scope ldap
Server /ldap # set enabled yes
Server /ldap *# set domain sample-domain
Server /ldap *# set timeout 60
Server /ldap *# set encrypted yes
Server /ldap *# set base-dn example.com
Server /ldap *# set attribute CiscoAVPair
Server /ldap *# set filter-attribute sAMAccountName
Server /ldap *# commit
Server /ldap # show detail
LDAP Settings:
  Enabled: yes
  Encrypted: yes
  Domain: sample-domain
  BaseDN: example.com
  Timeout: 60
  Filter-Attribute: sAMAccountName
  Attribute: CiscoAvPair
Server /ldap #
```

What to Do Next

If you want to use LDAP groups for group authorization, see *Configuring LDAP Groups in CIMC*.

Configuring LDAP Groups in CIMC



Note

When Active Directory (AD) group authorization is enabled and configured, user authentication is also done on the group level for users that are not found in the local user database or who are not individually authorized to use CIMC in the Active Directory.

Before You Begin

- You must log in as a user with admin privileges to perform this task.

- Active Directory (or LDAP) must be enabled and configured.

Procedure

	Command or Action	Purpose
Step 1	Server# scope ldap	Enters the LDAP command mode for AD configuration.
Step 2	Server /ldap# scope ldap-group-rule	Enters the LDAP group rules command mode for AD configuration.
Step 3	Server /ldap/ldap-group-rule # set group-auth {yes no}	Enables or disables LDAP group authorization.
Step 4	Server /ldap # scope role-group index	Selects one of the available group profiles for configuration, where <i>index</i> is a number between 1 and 28.
Step 5	Server /ldap/role-group # set name group-name	Specifies the name of the group in the AD database that is authorized to access the server.
Step 6	Server /ldap/role-group # set domain domain-name	Specifies the AD domain the group must reside in.
Step 7	Server /ldap/role-group # set role {admin user readonly}	Specifies the permission level (role) assigned to all users in this AD group. This can be one of the following: <ul style="list-style-type: none"> • admin—The user can perform all actions available. • user—The user can perform the following tasks: <ul style="list-style-type: none"> ◦ View all information ◦ Manage the power control options such as power on, power cycle, and power off ◦ Launch the KVM console and virtual media ◦ Clear all logs ◦ Toggle the locator LED • readonly—The user can view information but cannot make any changes.
Step 8	Server /ldap/role-group # commit	Commits the transaction to the system configuration.

This example shows how to configure LDAP group authorization:

```

Server# scope ldap
Server /ldap # scope ldap-group-rule
Server /ldap/ldap-group-rule # set group-auth yes
Server /ldap *# scope role-group 5
Server /ldap/role-group # set name Training
Server /ldap/role-group* # set domain example.com
Server /ldap/role-group* # set role readonly
Server /ldap/role-group* # commit
ucs-c250-M2 /ldap # show role-group

```

Group	Group Name	Domain Name	Assigned Role
1	(n/a)	(n/a)	admin
2	(n/a)	(n/a)	user
3	(n/a)	(n/a)	readonly
4	(n/a)	(n/a)	(n/a)
5	Training	example.com	readonly

```
Server /ldap/role-group #
```

Viewing User Sessions

Procedure

	Command or Action	Purpose
Step 1	Server# show user-session	Displays information about current user sessions.

The command output displays the following information about current user sessions:

Name	Description
Session ID column	The unique identifier for the session.
Username column	The username for the user.
IP Address column	The IP address from which the user accessed the server.
Type column	The method by which the user accessed the server.
Action column	<p>If your user account is assigned the admin user role, this column displays Terminate if you can force the associated user session to end. Otherwise it displays N/A.</p> <p>Note You cannot terminate your current session from this tab.</p>

This example displays information about current user sessions:

```
Server# show user-session
ID      Name      IP Address      Type      Killable
-----
15      admin      10.20.30.138    CLI       yes

Server /user #
```

Terminating a User Session

Before You Begin

You must log in as a user with admin privileges to terminate a user session.

Procedure

	Command or Action	Purpose
Step 1	Server# show user-session	Displays information about current user sessions. The user session to be terminated must be eligible to be terminated (killable) and must not be your own session.
Step 2	Server /user-session # scope user-session <i>session-number</i>	Enters user session command mode for the numbered user session that you want to terminate.
Step 3	Server /user-session # terminate	Terminates the user session.

This example shows how the admin at user session 10 terminates user session 15:

```

Server# show user-session
ID      Name      IP Address      Type      Killable
-----
10      admin      10.20.41.234    CLI       yes
15      admin      10.20.30.138    CLI       yes
Server# scope user-session 15
Server /user-session # terminate
User session 15 terminated.

Server /user-session #

```




Configuring Network-Related Settings

This chapter includes the following sections:

- [Server NIC Configuration, page 79](#)
- [Configuring Common Properties, page 81](#)
- [Configuring IPv4, page 82](#)
- [Configuring the Server VLAN, page 84](#)
- [Connecting to a Port Profile, page 85](#)
- [Network Interface Configuration, page 86](#)
- [Network Security Configuration, page 87](#)
- [Network Time Protocol Configuration, page 88](#)

Server NIC Configuration

Server NICs

NIC Mode

The NIC mode setting determines which ports can reach the CIMC. The following network mode options are available, depending on your platform:

- **Dedicated**—The management port is used to access the CIMC.
- **Shared LOM**—Any LOM (LAN On Motherboard) port can be used to access the CIMC.
- **Shared LOM 10G**—Any 10G LOM port can be used to access the CIMC. This option is only available for some adapter cards.
- **Cisco Card**—Any port on the adapter card can be used to access the CIMC. The Cisco adapter card has to be installed in a slot with Network Communications Services Interface protocol (NCSI) support.

- **Shared LOM Extended**—Any LOM port or adapter card port can be used to access the CIMC. The Cisco adapter card has to be installed in a slot with NCSI support.

NIC Redundancy

The following NIC redundancy options are available, depending on the selected NIC mode and your platform:

- **none**—Each port associated with the configured NIC mode operates independently. The ports do not fail over if there is a problem.
- **active-active**—If supported, all ports associated with the configured NIC mode operate simultaneously. This increases throughput and provides multiple paths to the CIMC.
- **active-standby**—If a port associated with the configured NIC mode fails, traffic will fail over to one of the other ports associated with the NIC mode.



Note If you select this option, make sure all ports associated with the configured NIC mode are connected to the same subnet to ensure that traffic is secure regardless of which port is used.

The available redundancy modes vary depending on the selected network mode and your platform. For the available modes, see the *Hardware Installation Guide* (HIG) for the type of server you are using. The C-Series HIGs are available at the following URL: http://www.cisco.com/en/US/products/ps10493/prod_installation_guides_list.html

Configuring Server NICs

Configure a server NIC when you want to set the NIC mode and NIC redundancy.

Before You Begin

You must log in as a user with admin privileges to configure the NIC.

Procedure

	Command or Action	Purpose
Step 1	Server# scope cimc	Enters the CIMC command mode.
Step 2	Server /cimc # scope network	Enters the CIMC network command mode.
Step 3	Server /cimc/network # set mode {dedicated shared_lom shared_lom_10g shipping cisco_card}	Sets the NIC mode to one of the following: <ul style="list-style-type: none"> • Dedicated—The management Ethernet port is used to access the CIMC. • Shared LOM—The LAN On Motherboard (LOM) Ethernet host ports are used to access the CIMC. <p>Note If you select Shared LOM, make sure that all host ports belong to the same subnet.</p>

	Command or Action	Purpose
		<ul style="list-style-type: none"> • Shared LOM 10G—The 10G LOM Ethernet host ports are used to access the CIMC. • Shipping—A limited configuration for initial connection. Select another mode for normal operation. • Cisco card—The ports on the adapter card are used to access the CIMC.
Step 4	Server /cimc/network # set redundancy {none active-active active-standby}	Sets the NIC redundancy mode when the NIC mode is Shared LOM. The redundancy mode can be one of the following: <ul style="list-style-type: none"> • none—The LOM Ethernet ports operate independently and do not fail over if there is a problem. • active-active—If supported, all LOM Ethernet ports are utilized. • active-standby—If one LOM Ethernet port fails, traffic fails over to another LOM port.
Step 5	Server /cimc/network # commit	Commits the transaction to the system configuration. Note The available NIC mode and NIC redundancy mode options may vary depending on your platform. If you select a mode not supported by your server, an error message displays when you save your changes.

This example configures the CIMC network interface:

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set mode dedicated
Server /cimc/network *# commit
Server /cimc/network #
```

Configuring Common Properties

Use common properties to describe your server.

Before You Begin

You must log in as a user with admin privileges to configure common properties.

Procedure

	Command or Action	Purpose
Step 1	Server# scope cimc	Enters the CIMC command mode.

	Command or Action	Purpose
Step 2	Server /cimc # scope network	Enters the CIMC network command mode.
Step 3	Server /cimc/network # set hostname <i>host-name</i>	Specifies the name of the host. On modifying the hostname, you are prompted to confirm whether you want to create a new self-signed certificate with CN as the new hostname. If you enter y at the prompt, a new self-signed certificate will be created with CN as the new hostname. If you enter n at the prompt, only hostname will be changed and no certificate will be generated.
Step 4	Server /cimc/network # commit	Commits the transaction to the system configuration.

This example configures the common properties:

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set hostname Server
Create new certificate with CN as new hostname? [y|N]
y
New certificate will be generated on committing changes.
All HTTPS and SSH sessions will be disconnected.
Server /cimc/network *# commit
Server /cimc/network #
```

What to Do Next

Changes to the network will be applied immediately. You may lose connectivity to the CIMC and may have to log in again. Because of the new SSH session created, you may be prompted to confirm the host key.

Configuring IPv4

Before You Begin

You must log in as a user with admin privileges to configure IPv4 network settings.

Procedure

	Command or Action	Purpose
Step 1	Server# scope cimc	Enters the CIMC command mode.
Step 2	Server /cimc # scope network	Enters the CIMC network command mode.

	Command or Action	Purpose
Step 3	Server /cimc/network # set dhcp-enabled {yes no}	Selects whether the CIMC uses DHCP. Note If DHCP is enabled, we recommend that the DHCP server be configured to reserve a single IP address for the CIMC. If the CIMC is reachable through multiple ports on the server, the single IP address must be reserved for the full range of MAC addresses of those ports.
Step 4	Server /cimc/network # set v4-addr <i>ipv4-address</i>	Specifies the IP address for the CIMC.
Step 5	Server /cimc/network # set v4-netmask <i>ipv4-netmask</i>	Specifies the subnet mask for the IP address.
Step 6	Server /cimc/network # set v4-gateway <i>gateway-ipv4-address</i>	Specifies the gateway for the IP address.
Step 7	Server /cimc/network # set dns-use-dhcp {yes no}	Selects whether the CIMC retrieves the DNS server addresses from DHCP.
Step 8	Server /cimc/network # set preferred-dns-server <i>dns1-ipv4-address</i>	Specifies the IP address of the primary DNS server.
Step 9	Server /cimc/network # set alternate-dns-server <i>dns2-ipv4-address</i>	Specifies the IP address of the secondary DNS server.
Step 10	Server /cimc/network # commit	Commits the transaction to the system configuration.
Step 11	Server /cimc/network # show [detail]	(Optional) Displays the IPv4 network settings.

This example configures and displays the IPv4 network settings:

```

Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set dhcp-enabled yes
Server /cimc/network *# set v4-addr 10.20.30.11
Server /cimc/network *# set v4-netmask 255.255.248.0
Server /cimc/network *# set v4-gateway 10.20.30.1
Server /cimc/network *# set dns-use-dhcp-enabled no
Server /cimc/network *# set preferred-dns-server 192.168.30.31
Server /cimc/network *# set alternate-dns-server 192.168.30.32
Server /cimc/network *# commit
Server /cimc/network # show detail
Network Setting:
  IPv4 Address: 10.20.30.11
  IPv4 Netmask: 255.255.248.0
  IPv4 Gateway: 10.20.30.1
  DHCP Enabled: yes
  Obtain DNS Server by DHCP: no
  Preferred DNS: 192.168.30.31
  Alternate DNS: 192.168.30.32
  VLAN Enabled: no
  VLAN ID: 1
  VLAN Priority: 0
  Hostname: Server
  MAC Address: 01:23:45:67:89:AB

```

```

NIC Mode: dedicated
NIC Redundancy: none

Server /cimc/network #

```

Configuring the Server VLAN

Before You Begin

You must be logged in as admin to configure the server VLAN.

Procedure

	Command or Action	Purpose
Step 1	Server# scope cimc	Enters the CIMC command mode.
Step 2	Server /cimc # scope network	Enters the CIMC network command mode.
Step 3	Server /cimc/network # set vlan-enabled {yes no}	Selects whether the CIMC is connected to a VLAN.
Step 4	Server /cimc/network # set vlan-id <i>id</i>	Specifies the VLAN number.
Step 5	Server /cimc/network # set vlan-priority <i>priority</i>	Specifies the priority of this system on the VLAN.
Step 6	Server /cimc/network # commit	Commits the transaction to the system configuration.
Step 7	Server /cimc/network # show [detail]	(Optional) Displays the network settings.

This example configures the server VLAN:

```

Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set vlan-enabled yes
Server /cimc/network *# set vlan-id 10
Server /cimc/network *# set vlan-priority 32
Server /cimc/network *# commit
Server /cimc/network # show detail
Network Setting:
  IPv4 Address: 10.20.30.11
  IPv4 Netmask: 255.255.248.0
  IPv4 Gateway: 10.20.30.1
  DHCP Enabled: yes
  Obtain DNS Server by DHCP: no
  Preferred DNS: 192.168.30.31
  Alternate DNS: 192.168.30.32
  VLAN Enabled: yes
  VLAN ID: 10
  VLAN Priority: 32
  Hostname: Server
  MAC Address: 01:23:45:67:89:AB
  NIC Mode: dedicated
  NIC Redundancy: none

Server /cimc/network #

```

Connecting to a Port Profile


Note

You can configure a port profile or a VLAN, but you cannot use both. If you want to use a port profile, make sure the **set vlan-enabled** command is set to no.

Before You Begin

You must be logged in as admin to connect to a port profile.

Procedure

	Command or Action	Purpose
Step 1	Server# scope cimc	Enters the CIMC command mode.
Step 2	Server /cimc # scope network	Enters the CIMC network command mode.
Step 3	Server /cimc/network # set port-profile <i>port_profile_name</i>	Specifies the port profile CIMC should use to configure the management interface, the virtual Ethernet, and the VIF on supported adapter cards such as the Cisco UCS VIC1225 Virtual Interface Card. Enter up to 80 alphanumeric characters. You cannot use spaces or other special characters except for - (hyphen) and _ (underscore). In addition, the port profile name cannot begin with a hyphen. Note The port profile must be defined on the switch to which this server is connected.
Step 4	Server /cimc/network # commit	Commits the transaction to the system configuration.
Step 5	Server /cimc/network # show [detail]	(Optional) Displays the network settings.

This example connects to port profile abcde12345:

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set port-profile abcde12345
Server /cimc/network # commit
Server /cimc/network # show detail
Network Setting:
  IPv4 Address: 10.193.66.174
  IPv4 Netmask: 255.255.248.0
  IPv4 Gateway: 10.193.64.1
  DHCP Enabled: no
  Obtain DNS Server by DHCP: no
  Preferred DNS: 0.0.0.0
  Alternate DNS: 0.0.0.0
  VLAN Enabled: no
  VLAN ID: 1
  VLAN Priority: 0
  Port Profile: abcde12345
  Hostname: Server
```

```
MAC Address: 50:3D:E5:9D:63:3C
NIC Mode: dedicated
NIC Redundancy: none
```

```
Server /cimc/network #
```

Network Interface Configuration

Overview to Network Interface Configuration

This support is added to configure network speed and duplex mode for the CIMC management port. Auto negotiate mode and duplex mode can be set for dedicated mode only. When auto negotiate mode is enabled the settings for duplex is ignored by the system and the network speed is set to either 1000 Mbps or 100 Mbps as per the speed configured on the switch. When auto negotiate mode is disabled, you can set the duplex to either **Full** or **Half**, a default speed of 100 Mbps is set, and the duplex retains its previous value.

When you reset CIMC to factory defaults, **Shared LOM Extended** mode is configured to **Full** duplex mode with 100 Mbps speed, and auto negotiate mode is disabled. You can enable auto negotiate mode when you change the settings to **Dedicated** mode.

Configuring Interface Properties

The settings on the switch must match with the CIMC settings to avoid any speed or duplex mismatch.

Procedure

	Command or Action	Purpose
Step 1	Server # scope cimc	Enters the CIMC command mode.
Step 2	Server/cimc # scope network	Enters the network command mode.
Step 3	Server/cimc/network* # set mode dedicated	Enters dedicated command mode.
Step 4	Server/cimc/network # set auto-negotiate {yes no}	Enables or disables auto negotiation command mode. <ul style="list-style-type: none"> • If you enter yes, the setting for duplex will be ignored by the system. The CIMC retains the speed at which the switch is configured. • If you enter no, you can set duplex. Else, a default speed of 100 Mbps will be applied, and duplex will retain its previous value.
Step 5	Server/cimc/network* # set duplex {full half}	Sets specified duplex mode type. By default, the duplex mode is set to Full

This example shows how to configure the interface properties and commit the transaction:

```
Server # scope cimc
Server/cimc # scope network
```



```

Server/cimc/network* # set mode dedicated
Server/cimc/network # set auto-negotiate no
Warning: You have chosen to set auto negotiate to no
If speed and duplex are not set then a default speed of 100Mbps will be applied
Duplex will retain its previous value
Server/cimc/network* # commit
Server/cimc/network # set duplex full
Server/cimc/network* # commit
Server/cimc/network #

```

Network Security Configuration

Network Security

The CIMC uses IP blocking as network security. IP blocking prevents the connection between a server or website and certain IP addresses or ranges of addresses. IP blocking effectively bans undesired connections from those computers to a website, mail server, or other Internet servers.

IP banning is commonly used to protect against denial of service (DoS) attacks. CIMC bans IP addresses by setting up an IP blocking fail count.

Configuring Network Security

Configure network security if you want to set up an IP blocking fail count.

Before You Begin

You must log in as a user with admin privileges to configure network security.

Procedure

	Command or Action	Purpose
Step 1	Server# scope cimc	Enters the CIMC command mode.
Step 2	Server /cimc # scope network	Enters the CIMC network command mode.
Step 3	Server /cimc/network # scope ipblocking	Enters the IP blocking command mode.
Step 4	Server /cimc/network/ipblocking # set enabled {yes no}	Enables or disables IP blocking.
Step 5	Server /cimc/network/ipblocking # set fail-count <i>fail-count</i>	<p>Sets the number of times a user can attempt to log in unsuccessfully before the system locks that user out for a specified length of time.</p> <p>The number of unsuccessful login attempts must occur within the time frame specified in the IP Blocking Fail Window field.</p> <p>Enter an integer between 3 and 10.</p>

	Command or Action	Purpose
Step 6	Server /cimc/network/ipblocking # set fail-window <i>fail-seconds</i>	Sets the length of time, in seconds, in which the unsuccessful login attempts must occur in order for the user to be locked out. Enter an integer between 60 and 120.
Step 7	Server /cimc/network/ipblocking # set penalty-time <i>penalty-seconds</i>	Sets the number of seconds the user remains locked out if they exceed the maximum number of login attempts within the specified time window. Enter an integer between 300 and 900.
Step 8	Server /cimc/network/ipblocking # commit	Commits the transaction to the system configuration.

This example configures IP blocking:

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # scope ipblocking
Server /cimc/network/ipblocking # set enabled yes
Server /cimc/network/ipblocking *# set fail-count 5
Server /cimc/network/ipblocking *# set fail-window 90
Server /cimc/network/ipblocking *# set penalty-time 600
Server /cimc/network/ipblocking *# commit
Server /cimc/network/ipblocking #
```

Network Time Protocol Configuration

Configuring Network Time Protocol Settings

By default, when CIMC is reset, it synchronizes the time with the host. With the introduction of the NTP service, you can configure CIMC to synchronize the time with an NTP server. The NTP server does not run in CIMC by default. You must enable and configure the NTP service by specifying the IP/DNS address of at least one server or a maximum of four servers that function as NTP servers or time source servers. When you enable the NTP service, CIMC synchronizes the time with the configured NTP server. The NTP service can be modified only through CIMC.



Note

To enable the NTP service, it is preferable to specify the IP address of a server rather than the DNS address.

Before You Begin

You must log in with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server # scope cimc	Enters CIMC command mode.
Step 2	Server /cimc # scope network	Enters network command mode.
Step 3	Server /cimc/network # scope ntp	Enters NTP service command mode.
Step 4	Server /cimc/network/ntp # set enabled yes	Enables the NTP service on the server.
Step 5	Server /cimc/network/ntp* # commit	Commits the transaction.
Step 6	Server /cimc/network/ntp # set server-1 10.120.33.44	Specifies the IP/DNS address of one of the four servers that act as an NTP server or the time source server.
Step 7	Server /cimc/network/ntp # set server-2 10.120.34.45	Specifies the IP/DNS address of one of the four servers that act as an NTP server or the time source server.
Step 8	Server /cimc/network/ntp # set server-3 10.120.35.46	Specifies the IP/DNS address of one of the four servers that act as an NTP server or the time source server.
Step 9	Server /cimc/network/ntp # set server-4 10.120.36.48	Specifies the IP/DNS address of one of the four servers that act as an NTP server or the time source server.
Step 10	Server /cimc/network/ntp # commit	Commits the transaction.

This example shows how to configure the NTP service:

```

Server # scope cimc
Server /cimc # scope network
Server /cimc/network # scope ntp
Server /cimc/network/ntp # set enabled yes
Warning: IPMI Set SEL Time Command will be
disabled if NTP is enabled.
Do you wish to continue? [y|N]
y
Server /cimc/network/ntp* # commit
Server /cimc/network/ntp # set server-1 10.120.33.44
Server /cimc/network/ntp* # set server-2 10.120.34.45
Server /cimc/network/ntp* # set server-3 10.120.35.46
Server /cimc/network/ntp* # set server-4 10.120.36.48
Server /cimc/network/ntp* # commit
Server /cimc/network/ntp #

```




Managing Network Adapters

This chapter includes the following sections:

- Overview of the Cisco UCS C-Series Network Adapters, page 91
- Viewing Network Adapter Properties, page 93
- Configuring Network Adapter Properties, page 93
- Managing vHBAs, page 94
- Managing vNICs, page 107
- Managing VM FEX, page 124
- Managing Storage Adapters, page 129
- Backing Up and Restoring the Adapter Configuration, page 142
- Managing Adapter Firmware, page 144
- Resetting the Adapter, page 146

Overview of the Cisco UCS C-Series Network Adapters



Note

The procedures in this chapter are available only when a Cisco UCS C-Series network adapter is installed in the chassis.

A Cisco UCS C-Series network adapter can be installed to provide options for I/O consolidation and virtualization support. The following adapters are available:

- Cisco UCS P81E Virtual Interface Card
- Cisco UCS VIC1225 Virtual Interface Card

The interactive *UCS Hardware and Software Interoperability Utility* lets you view the supported components and configurations for a selected server model and software release. The utility is available at the following URL: <http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html>

Cisco UCS P81E Virtual Interface Card

The Cisco UCS P81E Virtual Interface Card is optimized for virtualized environments, for organizations that seek increased mobility in their physical environments, and for data centers that want reduced costs through NIC, HBA, cabling, and switch reduction and reduced management overhead. This Fibre Channel over Ethernet (FCoE) PCIe card offers the following benefits:

- Allows up to 16 virtual Fibre Channel and 16 virtual Ethernet adapters to be provisioned in virtualized or nonvirtualized environments using just-in-time provisioning, providing tremendous system flexibility and allowing consolidation of multiple physical adapters.
- Delivers uncompromising virtualization support, including hardware-based implementation of Cisco VN-Link technology and pass-through switching.
- Improves system security and manageability by providing visibility and portability of network policies and security all the way to the virtual machine.

The virtual interface card makes Cisco VN-Link connections to the parent fabric interconnects, which allows virtual links to connect virtual NICs in virtual machines to virtual interfaces in the interconnect. In a Cisco Unified Computing System environment, virtual links then can be managed, network profiles applied, and interfaces dynamically reprovisioned as virtual machines move between servers in the system.

Cisco UCS VIC1225 Virtual Interface Card

The Cisco UCS VIC1225 Virtual Interface Card is a high-performance, converged network adapter that provides acceleration for the various new operational modes introduced by server virtualization. It brings superior flexibility, performance, and bandwidth to the new generation of Cisco UCS C-Series Rack-Mount Servers.

The Cisco UCS VIC 1225 implements the Cisco Virtual Machine Fabric Extender (VM-FEX), which unifies virtual and physical networking into a single infrastructure. It provides virtual-machine visibility from the physical network and a consistent network operations model for physical and virtual servers. In virtualized environments, this highly configurable and self-virtualized adapter provides integrated, modular LAN interfaces on Cisco UCS C-Series Rack-Mount Servers. Additional features and capabilities include:

- Supports up to 256 PCIe virtual devices, either virtual network interface cards (vNICs) or virtual host bus adapters (vHBAs), with high I/O operations per second (IOPS), support for lossless Ethernet, and 20 Gbps to servers.
- PCIe Gen2 x16 helps assure optimal bandwidth to the host for network-intensive applications with a redundant path to the fabric interconnect.
- Half-height design reserves full-height slots in servers for Cisco certified third-party adapters.
- Centrally managed by Cisco UCS Manager with support for Microsoft Windows, Red Hat Enterprise Linux, SUSE Linux, VMware vSphere, and Citrix XenServer.

Viewing Network Adapter Properties

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # show adapter [<i>index</i>] [<i>detail</i>]	Displays adapter properties. To display the properties of a single adapter, specify the PCI slot number as the <i>index</i> argument.

This example displays the properties of adapter 2:

```

Server# scope chassis
Server /chassis # show adapter
PCI Slot Product Name Serial Number Product ID Vendor
-----
1 UCS VIC 1225 FCH1613796C UCSC-PCIE-C... Cisco Systems Inc

Server /chassis # show adapter 2 detail
PCI Slot 2:
  Product Name: UCS VIC 1225
  Serial Number: FCH1613796C
  Product ID: UCSC-PCIE-CSC-02
  Adapter Hardware Revision: 4
  Current FW Version: 2.1(0.291)
  NIV: Disabled
  FIP: Enabled
  Configuration Pending: no
  CIMC Management Enabled : no
  VID: V00
  Vendor: Cisco Systems Inc
  Description:
  Bootloader Version: 2.1(0.291)
  FW Image 1 Version: 2.1(0.291)
  FW Image 1 State: RUNNING ACTIVATED
  FW Image 2 Version: 1.6(0.547)
  FW Image 2 State: BACKUP INACTIVATED
  FW Update Status: Idle
  FW Update Error: No error
  FW Update Stage: No operation (0%)
  FW Update Overall Progress: 0%

Server /chassis #

```

Configuring Network Adapter Properties

Before You Begin

- You must log in with admin privileges to perform this task.
- A supported Virtual Interface Card (VIC) must be installed in the chassis and the server must be powered on.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # show adapter	(Optional) Displays the available adapter devices.
Step 3	Server /chassis # scope adapter <i>index</i>	Enters the command mode for the adapter card at the PCI slot number specified by <i>index</i> . Note The server must be powered on before you can view or change adapter settings.
Step 4	Server /chassis/adapter # set fip-mode {disable enable}	Enables or disables FCoE Initialization Protocol (FIP) on the adapter card. FIP is enabled by default. Note We recommend that you disable this option only when explicitly directed to do so by a technical support representative.
Step 5	Server /chassis/adapter # set niv-mode {disable enable}	Enables or disables Network Interface Virtualization (NIV) on the adapter card. NIV is disabled by default. If NIV mode is enabled, vNICs: <ul style="list-style-type: none"> • Can be assigned to a specific channel • Can be associated with a port profile • Can fail over to another vNIC if there are communication problems
Step 6	Server /chassis/adapter # configure-vmfex <i>port-count</i>	If NIV mode is enabled, <i>port-count</i> specifies the number of VM FEX interfaces you want CIMC to create, from 0 to 112.
Step 7	Server /chassis/adapter # commit	Commits the transaction to the system configuration.

This example configures the properties of adapter 1:

```
Server# scope chassis
Server /chassis # scope adapter 1
Server /chassis/adapter # set fip-mode enable
Server /chassis/adapter *# commit
Server /chassis/adapter #
```

Managing vHBAs

Guidelines for Managing vHBAs

When managing vHBAs, consider the following guidelines and restrictions:

- The Cisco UCS P81E Virtual Interface Card and Cisco UCS VIC1225 Virtual Interface Card provide two vHBAs (fc0 and fc1). You can create up to 16 additional vHBAs on these adapter cards.

**Note**

If Network Interface Virtualization (NIV) mode is enabled for the adapter, you must assign a channel number to a vHBA when you create it.

- When using the Cisco UCS P81E Virtual Interface Card or Cisco UCS VIC1225 Virtual Interface Card in an FCoE application, you must associate the vHBA with the FCoE VLAN. Follow the instructions in [Modifying vHBA Properties, on page 96](#) to assign the VLAN.
- After making configuration changes, you must reboot the host for settings to take effect.

Viewing vHBA Properties

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope adapter <i>index</i>	Enters the command mode for the adapter card at the PCI slot number specified by <i>index</i> . Note The server must be powered on before you can view or change adapter settings.
Step 3	Server /chassis/adapter # show host-fc-if [fc0 fc1 <i>name</i>] [detail]	Displays properties of a single vHBA, if specified, or all vHBAs.

This example displays all vHBAs on adapter card 1 and the detailed properties of fc0:

```

Server# scope chassis
Server /chassis # scope adapter 1
Server /chassis/adapter # show host-fc-if
Name      World Wide Port Name      FC SAN Boot Uplink Port
-----
fc0       20:00:00:22:BD:D6:5C:35      Disabled    0
fc1       20:00:00:22:BD:D6:5C:36      Disabled    1

Server /chassis/adapter # show host-fc-if fc0 detail
Name fc0:
World Wide Node Name: 10:00:00:22:BD:D6:5C:35
World Wide Port Name: 20:00:00:22:BD:D6:5C:35
FC SAN Boot: Disabled
Persistent LUN Binding: Disabled
Uplink Port: 0
MAC Address: 00:22:BD:D6:5C:35
CoS: 3
VLAN: NONE
Rate Limiting: OFF
PCIe Device Order: ANY
EDTOV: 2000
RATOV: 10000
Maximum Data Field Size: 2112
Channel Number: 3
Port Profile:

Server /chassis/adapter #

```

Modifying vHBA Properties

Before You Begin

You must log in with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # show adapter	(Optional) Displays the available adapter devices.
Step 3	Server /chassis # scope adapter <i>index</i>	Enters the command mode for the adapter card at the PCI slot number specified by <i>index</i> . Note The server must be powered on before you can view or change adapter settings.
Step 4	Server /chassis/adapter # scope host-fc-if { fc0 fc1 <i>name</i> }	Enters the host Fibre Channel interface command mode for the specified vHBA.
Step 5	Server /chassis/adapter/host-fc-if # set wwnn <i>wwnn</i>	Specifies a unique World Wide Node Name (WWNN) for the adapter in the form hh:hh:hh:hh:hh:hh:hh:hh. Unless specified by this command, the WWNN is generated automatically by the system.
Step 6	Server /chassis/adapter/host-fc-if # set wwpn <i>wwpn</i>	Specifies a unique World Wide Port Name (WWPN) for the adapter in the form hh:hh:hh:hh:hh:hh:hh:hh. Unless specified by this command, the WWPN is generated automatically by the system.
Step 7	Server /chassis/adapter/host-fc-if # set boot { disable enable }	Enables or disables FC SAN boot. The default is disable.
Step 8	Server /chassis/adapter/host-fc-if # set persistent-lun-binding { disable enable }	Enables or disables persistent LUN binding. The default is disable.
Step 9	Server /chassis/adapter/host-fc-if # set mac-addr <i>mac-addr</i>	Specifies a MAC address for the vHBA.
Step 10	Server /chassis/adapter/host-fc-if # set vlan { none <i>vlan-id</i> }	Specifies the default VLAN for this vHBA. Valid VLAN numbers are 1 to 4094; the default is none.
Step 11	Server /chassis/adapter/host-fc-if # set cos <i>cos-value</i>	Specifies the class of service (CoS) value to be marked on received packets unless the vHBA is configured to trust host CoS. Valid CoS values are 0 to 6; the default is 0. Higher values indicate more important traffic. This setting is not functional in NIV mode.

	Command or Action	Purpose
Step 12	Server /chassis/adapter/host-fc-if # set rate-limit { <i>off</i> <i>rate</i> }	Specifies a maximum data rate for the vHBA. The range is 1 to 10000 Mbps; the default is off. This setting is not functional in NIV mode.
Step 13	Server /chassis/adapter/host-fc-if # set order { <i>any</i> <i>0-99</i> }	Specifies the relative order of this device for PCIe bus device number assignment; the default is any.
Step 14	Server /chassis/adapter/host-fc-if # set error-detect-timeout <i>msec</i>	Specifies the error detect timeout value (EDTOV), the number of milliseconds to wait before the system assumes that an error has occurred. The range is 1000 to 100000; the default is 2000 milliseconds.
Step 15	Server /chassis/adapter/host-fc-if # set resource-allocation-timeout <i>msec</i>	Specifies the resource allocation timeout value (RATOV), the number of milliseconds to wait before the system assumes that a resource cannot be properly allocated. The range is 5000 to 100000; the default is 10000 milliseconds.
Step 16	Server /chassis/adapter/host-fc-if # set max-field-size <i>size</i>	Specifies the maximum size of the Fibre Channel frame payload (in bytes) that the vHBA supports. The range is 1 to 2112; the default is 2112 bytes.
Step 17	Server /chassis/adapter/host-fc-if # scope error-recovery	Enters the Fibre Channel error recovery command mode.
Step 18	Server /chassis/adapter/host-fc-if/error-recovery # set fcp-error-recovery { <i>disable</i> <i>enable</i> }	Enables or disables FCP Error Recovery. The default is disable.
Step 19	Server /chassis/adapter/host-fc-if/error-recovery # set link-down-timeout <i>msec</i>	Specifies the link down timeout value, the number of milliseconds the uplink port should be offline before it informs the system that the uplink port is down and fabric connectivity has been lost. The range is 0 to 240000; the default is 30000 milliseconds.
Step 20	Server /chassis/adapter/host-fc-if/error-recovery # set port-down-io-retry-count <i>count</i>	Specifies the port down I/O retries value, the number of times an I/O request to a port is returned because the port is busy before the system decides the port is unavailable. The range is 0 to 255; the default is 8 retries.
Step 21	Server /chassis/adapter/host-fc-if/error-recovery # set port-down-timeout <i>msec</i>	Specifies the port down timeout value, the number of milliseconds a remote Fibre Channel port should be offline before informing the SCSI upper layer that the port is unavailable. The range is 0 to 240000; the default is 10000 milliseconds.
Step 22	Server /chassis/adapter/host-fc-if/error-recovery # exit	Exits to the host Fibre Channel interface command mode.

	Command or Action	Purpose
Step 23	Server /chassis/adapter/host-fc-if # scope interrupt	Enters the interrupt command mode.
Step 24	Server /chassis/adapter/host-fc-if/interrupt # set interrupt-mode {intx msi msix}	Specifies the Fibre Channel interrupt mode. The modes are as follows: <ul style="list-style-type: none"> • intx —Line-based interrupt (INTx) • msi —Message-Signaled Interrupt (MSI) • msix —Message Signaled Interrupts with the optional extension (MSIx). This is the recommended and default option.
Step 25	Server /chassis/adapter/host-fc-if/interrupt # exit	Exits to the host Fibre Channel interface command mode.
Step 26	Server /chassis/adapter/host-fc-if # scope port	Enters the Fibre Channel port command mode.
Step 27	Server /chassis/adapter/host-fc-if/port # set outstanding-io-count count	Specifies the I/O throttle count, the number of I/O operations that can be pending in the vHBA at one time. The range is 1 to 1024; the default is 512 operations.
Step 28	Server /chassis/adapter/host-fc-if/port # set max-target-luns count	Specifies the maximum logical unit numbers (LUNs) per target, the maximum number of LUNs that the driver will discover. This is usually an operating system platform limitation. The range is 1 to 1024; the default is 256 LUNs.
Step 29	Server /chassis/adapter/host-fc-if/port # exit	Exits to the host Fibre Channel interface command mode.
Step 30	Server /chassis/adapter/host-fc-if # scope port-f-logs	Enters the Fibre Channel fabric login command mode.
Step 31	Server /chassis/adapter/host-fc-if/port-f-logs # set flogi-retries {infinite count}	Specifies the fabric login (FLOGI) retries value, the number of times that the system tries to log in to the fabric after the first failure. Enter a number between 0 and 4294967295 or enter infinite ; the default is infinite retries.
Step 32	Server /chassis/adapter/host-fc-if/port-f-logs # set flogi-timeout msec	Specifies the fabric login (FLOGI) timeout value, the number of milliseconds that the system waits before it tries to log in again. The range is 1 to 255000; the default is 2000 milliseconds.
Step 33	Server /chassis/adapter/host-fc-if/port-f-logs # exit	Exits to the host Fibre Channel interface command mode.

	Command or Action	Purpose
Step 34	Server /chassis/adapter/host-fc-if# scope port-p-logic	Enters the Fibre Channel port login command mode.
Step 35	Server /chassis/adapter/host-fc-if/port-p-logic # set plogi-retries <i>count</i>	Specifies the port login (PLOGI) retries value, the number of times that the system tries to log in to the fabric after the first failure. The range is 0 and 255; the default is 8 retries.
Step 36	Server /chassis/adapter/host-fc-if/port-p-logic # set plogi-timeout <i>msec</i>	Specifies the port login (PLOGI) timeout value, the number of milliseconds that the system waits before it tries to log in again. The range is 1 to 255000; the default is 2000 milliseconds.
Step 37	Server /chassis/adapter/host-fc-if/port-p-logic # exit	Exits to the host Fibre Channel interface command mode.
Step 38	Server /chassis/adapter/host-fc-if# scope scsi-io	Enters the SCSI I/O command mode.
Step 39	Server /chassis/adapter/host-fc-if/scsi-io # set cdb-wq-count <i>count</i>	The number of command descriptor block (CDB) transmit queue resources to allocate. The range is 1 to 8; the default is 1.
Step 40	Server /chassis/adapter/host-fc-if/scsi-io # set cdb-wq-ring-size <i>size</i>	The number of descriptors in the command descriptor block (CDB) transmit queue. The range is 64 to 512; the default is 512.
Step 41	Server /chassis/adapter/host-fc-if/scsi-io # exit	Exits to the host Fibre Channel interface command mode.
Step 42	Server /chassis/adapter/host-fc-if# scope trans-queue	Enters the Fibre Channel transmit queue command mode.
Step 43	Server /chassis/adapter/host-fc-if/trans-queue # set fc-wq-ring-size <i>size</i>	The number of descriptors in the Fibre Channel transmit queue. The range is 64 to 128; the default is 64.
Step 44	Server /chassis/adapter/host-fc-if/trans-queue # exit	Exits to the host Fibre Channel interface command mode.
Step 45	Server /chassis/adapter/host-fc-if# scope recv-queue	Enters the Fibre Channel receive queue command mode.
Step 46	Server /chassis/adapter/host-fc-if/recv-queue # set fc-rq-ring-size <i>size</i>	The number of descriptors in the Fibre Channel receive queue. The range is 64 to 128; the default is 64.
Step 47	Server /chassis/adapter/host-fc-if/recv-queue # exit	Exits to the host Fibre Channel interface command mode.

	Command or Action	Purpose
Step 48	Server /chassis/adapter/host-fc-if # commit	Commits the transaction to the system configuration. Note The changes will take effect upon the next server reboot.

This example configures the properties of a vHBA:

```
Server# scope chassis
Server /chassis # show adapter
PCI Slot Product Name Serial Number Product ID Vendor
-----
1 UCS VIC P81E QCI1417A0QK N2XX-ACPCI01 Cisco Systems Inc

Server /chassis # scope adapter 1
Server /chassis/adapter # scope host-fc-if fcl
Server /chassis/adapter/host-fc-if # set boot enable
Server /chassis/adapter/host-fc-if *# scope scsi-io
Server /chassis/adapter/host-fc-if/scsi-io *# set cdb-wq-count 2
Server /chassis/adapter/host-fc-if/scsi-io *# exit
Server /chassis/adapter/host-fc-if *# commit
Server /chassis/adapter/host-fc-if #
```

What to Do Next

Reboot the server to apply the changes.

Creating a vHBA

The adapter provides two permanent vHBAs. If NIV mode is enabled, you can create up to 16 additional vHBAs.

Before You Begin

You must log in with user or admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope adapter <i>index</i>	Enters the command mode for the adapter card at the PCI slot number specified by <i>index</i> . Note The server must be powered on before you can view or change adapter settings.
Step 3	Server /chassis/adapter # create host-fc-if <i>name</i>	Creates a vHBA and enters the host Fibre Channel interface command mode. The <i>name</i> argument can be up to 32 ASCII characters.

	Command or Action	Purpose
Step 4	Server /chassis/adapter/host-fc-if # set channel-number <i>number</i>	(Optional) If NIV mode is enabled for the adapter, you must assign a channel number to this vHBA. The range is 1 to 1000.
Step 5	Server /chassis/adapter/host-fc-if # commit	Commits the transaction to the system configuration. Note The changes will take effect upon the next server reboot.

This example creates a vHBA on adapter 1:

```
Server# scope chassis
Server /chassis # scope adapter 1
Server /chassis/adapter # create host-fc-if Vhba5
Server /chassis/adapter/host-fc-if *# commit
New host-fc-if settings will take effect upon the next server reset
Server /chassis/adapter/host-fc-if #
```

What to Do Next

- Reboot the server to create the vHBA.
- If configuration changes are required, configure the new vHBA as described in [Modifying vHBA Properties](#), on page 96.

Deleting a vHBA

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope adapter <i>index</i>	Enters the command mode for the adapter card at the PCI slot number specified by <i>index</i> . Note The server must be powered on before you can view or change adapter settings.
Step 3	Server /chassis/adapter # delete host-fc-if <i>name</i>	Deletes the specified vHBA. Note You cannot delete either of the two default vHBAs, fc0 or fc1.
Step 4	Server /chassis/adapter # commit	Commits the transaction to the system configuration. Note The changes will take effect upon the next server reboot.

This example deletes a vHBA on adapter 1:

```
Server# scope chassis
Server /chassis # scope adapter 1
Server /chassis/adapter # delete host-fc-if Vhba5
Server /chassis/adapter *# commit
Server /chassis/adapter #
```

vHBA Boot Table

In the vHBA boot table, you can specify up to four LUNs from which the server can boot.

Viewing the Boot Table

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope adapter <i>index</i>	Enters the command mode for the adapter card at the PCI slot number specified by <i>index</i> . Note The server must be powered on before you can view or change adapter settings.
Step 3	Server /chassis/adapter # scope host-fc-if { fc0 fc1 <i>name</i> }	Enters the host Fibre Channel interface command mode for the specified vHBA.
Step 4	Server /chassis/adapter/host-fc-if # show boot	Displays the boot table of the Fibre Channel interface.

This example displays the boot table for a vHBA:

```
Server# scope chassis
Server /chassis # scope adapter 1
Server /chassis/adapter # scope host-fc-if fc1
Server /chassis/adapter/host-fc-if # show boot
Boot Table Entry  Boot Target WWPN          Boot LUN ID
-----
0                 20:00:00:11:22:33:44:55          3
1                 20:00:00:11:22:33:44:56          5

Server /chassis/adapter/host-fc-if #
```

Creating a Boot Table Entry

You can create up to four boot table entries.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope adapter <i>index</i>	Enters the command mode for the adapter card at the PCI slot number specified by <i>index</i> . Note The server must be powered on before you can view or change adapter settings.
Step 3	Server /chassis/adapter # scope host-fc-if { fc0 fc1 <i>name</i> }	Enters the host Fibre Channel interface command mode for the specified vHBA.
Step 4	Server /chassis/adapter/host-fc-if # create-boot-entry <i>wwpn lun-id</i>	Creates a boot table entry. <ul style="list-style-type: none"> • <i>wwpn</i> — The World Wide Port Name (WWPN) for the boot target in the form hh:hh:hh:hh:hh:hh:hh:hh. • <i>lun-id</i> —The LUN ID of the boot LUN. The range is 0 to 255.
Step 5	Server /chassis/adapter/host-fc-if # commit	Commits the transaction to the system configuration. Note The changes will take effect upon the next server reboot.

This example creates a boot table entry for vHBA fc1:

```

Server# scope chassis
Server /chassis # scope adapter 1
Server /chassis/adapter # scope host-fc-if fc1
Server /chassis/adapter/host-fc-if # create-boot-entry 20:00:00:11:22:33:44:55 3
Server /chassis/adapter/host-fc-if *# commit
New boot table entry will take effect upon the next server reset
Server /chassis/adapter/host-fc-if #

```

Deleting a Boot Table Entry

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope adapter <i>index</i>	Enters the command mode for the adapter card at the PCI slot number specified by <i>index</i> . Note The server must be powered on before you can view or change adapter settings.

	Command or Action	Purpose
Step 3	Server /chassis/adapter # scope host-fc-if {fc0 fc1 name}	Enters the host Fibre Channel interface command mode for the specified vHBA.
Step 4	Server /chassis/adapter/host-fc-if # show boot	Displays the boot table. From the Boot Table Entry field, locate the number of the entry to be deleted.
Step 5	Server /chassis/adapter/host-fc-if # delete boot entry	Deletes the boot table entry at the specified position in the table. The range of <i>entry</i> is 0 to 3. The change will take effect upon the next server reset.
Step 6	Server /chassis/adapter/host-fc-if # commit	Commits the transaction to the system configuration. Note The changes will take effect upon the next server reboot.

This example deletes boot table entry number 1 for the vHBA fc1:

```
Server# scope chassis
Server /chassis # scope adapter 1
Server /chassis/adapter # scope host-fc-if fc1
Server /chassis/adapter/host-fc-if # show boot
Boot Table Entry  Boot Target WWPN          Boot LUN ID
-----
0                 20:00:00:11:22:33:44:55          3
1                 20:00:00:11:22:33:44:56          5

Server /chassis/adapter/host-fc-if # delete boot 1
Server /chassis/adapter/host-fc-if *# commit
New host-fc-if settings will take effect upon the next server reset
Server /chassis/adapter/host-fc-if # show boot
Boot Table Entry  Boot Target WWPN          Boot LUN ID
-----
0                 20:00:00:11:22:33:44:55          3

Server /chassis/adapter/host-fc-if #
```

What to Do Next

Reboot the server to apply the changes.

vHBA Persistent Binding

Persistent binding ensures that the system-assigned mapping of Fibre Channel targets is maintained after a reboot.

Enabling Persistent Binding

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope adapter <i>index</i>	Enters the command mode for the adapter card at the PCI slot number specified by <i>index</i> . Note The server must be powered on before you can view or change adapter settings.
Step 3	Server /chassis/adapter # scope host-fc-if { fc0 fc1 <i>name</i> }	Enters the host Fibre Channel interface command mode for the specified vHBA.
Step 4	Server /chassis/adapter/host-fc-if # scope perbi	Enters the persistent binding command mode for the vHBA.
Step 5	Server /chassis/adapter/host-fc-if/perbi # set persistent-lun-binding enable	Enables persistent binding for the vHBA.
Step 6	Server /chassis/adapter/host-fc-if/perbi # commit	Commits the transaction to the system configuration.

This example enables persistent binding for a vHBA:

```
Server# scope chassis
Server /chassis # scope adapter 4
Server /chassis/adapter # scope host-fc-if fc1
Server /chassis/adapter/host-fc-if # scope perbi
Server /chassis/adapter/host-fc-if/perbi # set persistent-lun-binding enable
Server /chassis/adapter/host-fc-if/perbi *# commit
Server /chassis/adapter/host-fc-if/perbi #
```

Disabling Persistent Binding

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope adapter <i>index</i>	Enters the command mode for the adapter card at the PCI slot number specified by <i>index</i> . Note The server must be powered on before you can view or change adapter settings.

	Command or Action	Purpose
Step 3	Server /chassis/adapter # scope host-fc-if {fc0 fc1 name}	Enters the host Fibre Channel interface command mode for the specified vHBA.
Step 4	Server /chassis/adapter/host-fc-if # scope perbi	Enters the persistent binding command mode for the vHBA.
Step 5	Server /chassis/adapter/host-fc-if/perbi # set persistent-lun-binding disable	Disables persistent binding for the vHBA.
Step 6	Server /chassis/adapter/host-fc-if/perbi # commit	Commits the transaction to the system configuration.

This example disables persistent binding for a vHBA:

```
Server# scope chassis
Server /chassis # scope adapter 4
Server /chassis/adapter # scope host-fc-if fc1
Server /chassis/adapter/host-fc-if # scope perbi
Server /chassis/adapter/host-fc-if/perbi # set persistent-lun-binding disable
Server /chassis/adapter/host-fc-if/perbi *# commit
Server /chassis/adapter/host-fc-if/perbi #
```

Rebuilding Persistent Binding

Before You Begin

Persistent binding must be enabled in the vHBA properties.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope adapter index	Enters the command mode for the adapter card at the PCI slot number specified by <i>index</i> . Note The server must be powered on before you can view or change adapter settings.
Step 3	Server /chassis/adapter # scope host-fc-if {fc0 fc1 name}	Enters the host Fibre Channel interface command mode for the specified vHBA.
Step 4	Server /chassis/adapter/host-fc-if # scope perbi	Enters the persistent binding command mode for the vHBA.
Step 5	Server /chassis/adapter/host-fc-if/perbi # rebuild	Rebuilds the persistent binding table for the vHBA.

This example rebuilds the persistent binding table for a vHBA:

```
Server# scope chassis
Server /chassis # scope adapter 4
Server /chassis/adapter # scope host-fc-if fc1
Server /chassis/adapter/host-fc-if # scope perbi
Server /chassis/adapter/host-fc-if/perbi # rebuild

Server /chassis/adapter/host-fc-if/perbi #
```

Managing vNICs

Guidelines for Managing vNICs

When managing vNICs, consider the following guidelines and restrictions:

- The Cisco UCS P81E Virtual Interface Card and Cisco UCS VIC1225 Virtual Interface Card provide two default vNICs (eth0 and eth1). You can create up to 16 additional vNICs on these adapter cards.



Note

If Network Interface Virtualization (NIV) mode is enabled for the adapter, you must assign a channel number to a vNIC when you create it.

- After making configuration changes, you must reboot the host for settings to take effect.

Viewing vNIC Properties

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope adapter <i>index</i>	Enters the command mode for the adapter card at the PCI slot number specified by <i>index</i> . Note The server must be powered on before you can view or change adapter settings.
Step 3	Server /chassis/adapter # show host-eth-if [eth0 eth1 <i>name</i>] [detail]	Displays properties of a single vNIC, if specified, or all vNICs.

This example displays the brief properties of all vNICs and the detailed properties of eth0:

```
Server# scope chassis
Server /chassis # scope adapter 1
Server /chassis/adapter # show host-eth-if
Name      MTU   Uplink Port  MAC Address      CoS  VLAN  PXE  Boot
-----
eth0      1500  0           00:22:BD:D6:5C:33  0    NONE  Enabled
eth1      1500  1           00:22:BD:D6:5C:34  0    NONE  Enabled
```

```

Server /chassis/adapter # show host-eth-if eth0 detail
Name eth0:
  MTU: 1500
  Uplink Port: 0
  MAC Address: 00:22:BD:D6:5C:33
  CoS: 0
  Trust Host CoS: disabled
  PCI Order: ANY
  VLAN: NONE
  VLAN Mode: TRUNK
  Rate Limiting: OFF
  PXE Boot: enabled
  Channel Number: N/A
  Port Profile: N/A
  Uplink Failover: N/A
  Uplink Failback Timeout: N/A

```

```

Server /chassis/adapter #

```

Modifying vNIC Properties

Before You Begin

You must log in with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # show adapter	(Optional) Displays the available adapter devices.
Step 3	Server /chassis # scope adapter <i>index</i>	Enters the command mode for the adapter card at the PCI slot number specified by <i>index</i> . Note The server must be powered on before you can view or change adapter settings.
Step 4	Server /chassis/adapter # scope host-eth-if { eth0 eth1 <i>name</i> }	Enters the host Ethernet interface command mode for the specified vNIC.
Step 5	Server /chassis/adapter/host-eth-if # set mtu <i>mtu-value</i>	Specifies the maximum transmission unit (MTU) or packet size that the vNIC accepts. Valid MTU values are 1500 to 9000 bytes; the default is 1500.
Step 6	Server /chassis/adapter/host-eth-if # set uplink { 0 1 }	Specifies the uplink port associated with this vNIC. All traffic for this vNIC goes through this uplink port.
Step 7	Server /chassis/adapter/host-eth-if # set mac-addr <i>mac-addr</i>	Specifies a MAC address for the vNIC in the form hh:hh:hh:hh:hh:hh or hhhh:hhhh:hhhh.
Step 8	Server /chassis/adapter/host-eth-if # set cos <i>cos-value</i>	Specifies the class of service (CoS) value to be marked on received packets unless the vNIC is configured to trust host CoS. Valid CoS values are 0 to 6; the default is 0. Higher values indicate more important traffic.

	Command or Action	Purpose
		Note If NIV is enabled, this setting is determined by the switch, and the command is ignored.
Step 9	Server /chassis/adapter/host-eth-if# set trust-host-cos {disable enable}	<p>Specifies whether the vNIC will trust host CoS or will remark packets. The behavior is as follows:</p> <ul style="list-style-type: none"> • disable —Received packets are remarked with the configured CoS. This is the default. • enable —The existing CoS value of received packets (host CoS) is preserved.
Step 10	Server /chassis/adapter/host-eth-if# set order {any 0-99}	Specifies the relative order of this device for PCI bus device number assignment; the default is any.
Step 11	Server /chassis/adapter/host-eth-if# set vlan {none vlan-id}	<p>Specifies the default VLAN for this vNIC. Valid VLAN numbers are 1 to 4094; the default is none.</p> <p>Note If NIV is enabled, this setting is determined by the switch, and the command is ignored.</p>
Step 12	Server /chassis/adapter/host-eth-if# set vlan-mode {access trunk}	<p>Specifies the VLAN mode for the vNIC. The modes are as follows:</p> <ul style="list-style-type: none"> • access —The vNIC belongs to only one VLAN. • trunk —The vNIC can belong to more than one VLAN. This is the default. <p>Note If NIV is enabled, this setting is determined by the switch, and the command is ignored.</p>
Step 13	Server /chassis/adapter/host-eth-if# set rate-limit {off rate}	<p>Specifies a maximum data rate for the vNIC. The range is 1 to 10000 Mbps; the default is off.</p> <p>Note If NIV is enabled, this setting is determined by the switch, and the command is ignored.</p>
Step 14	Server /chassis/adapter/host-eth-if# set boot {disable enable}	Specifies whether the vNIC can be used to perform a PXE boot. The default is enable for the two default vNICs, and disable for user-created vNICs.
Step 15	Server /chassis/adapter/host-eth-if# set channel-number <i>number</i>	If NIV mode is enabled for the adapter, select the channel number that will be assigned to this vNIC. The range is 1 to 1000.
Step 16	Server /chassis/adapter/host-eth-if# set port-profile <i>name</i>	<p>If NIV mode is enabled for the adapter, select the port profile that should be associated with the vNIC.</p> <p>Note The <i>name</i> must be a port profile defined on the switch to which this server is connected.</p>
Step 17	Server /chassis/adapter/host-eth-if# set uplink-failover {disable enable}	If NIV mode is enabled for the adapter, enable this setting if traffic on this vNIC should fail over to the

	Command or Action	Purpose
		secondary interface if there are communication problems.
Step 18	Server /chassis/adapter/host-eth-if # set uplink-failback-timeout <i>seconds</i>	After a vNIC has started using its secondary interface, this setting controls how long the primary interface must be available before the system resumes using the primary interface for the vNIC. Enter a number of <i>seconds</i> between 0 and 600.
Step 19	Server /chassis/adapter/host-eth-if # scope interrupt	Enters the interrupt command mode.
Step 20	Server /chassis/adapter/host-eth-if/interrupt # set interrupt-count <i>count</i>	Specifies the number of interrupt resources. The range is 1 to 514; the default is 8. In general, you should allocate one interrupt resource for each completion queue.
Step 21	Server /chassis/adapter/host-eth-if/interrupt # set coalescing-time <i>usec</i>	The time to wait between interrupts or the idle period that must be encountered before an interrupt is sent. The range is 1 to 65535 microseconds; the default is 125. To turn off coalescing, enter 0 (zero).
Step 22	Server /chassis/adapter/host-eth-if/interrupt # set coalescing-type { <i>idle</i> <i>min</i> }	The coalescing types are as follows: <ul style="list-style-type: none"> • idle —The system does not send an interrupt until there is a period of no activity lasting as long as the time specified in the coalescing time configuration. • min —The system waits for the time specified in the coalescing time configuration before sending another interrupt event. This is the default.
Step 23	Server /chassis/adapter/host-eth-if/interrupt # set interrupt-mode { <i>intx</i> <i>msi</i> <i>msix</i> }	Specifies the Ethernet interrupt mode. The modes are as follows: <ul style="list-style-type: none"> • intx —Line-based interrupt (PCI INTx) • msi —Message-Signaled Interrupt (MSI) • msix —Message Signaled Interrupts with the optional extension (MSI-X). This is the recommended and default option.
Step 24	Server /chassis/adapter/host-eth-if/interrupt # exit	Exits to the host Ethernet interface command mode.
Step 25	Server /chassis/adapter/host-eth-if # scope rcv-queue	Enters receive queue command mode.

	Command or Action	Purpose
Step 26	Server /chassis/adapter/host-eth-if/recv-queue # set rq-count <i>count</i>	The number of receive queue resources to allocate. The range is 1 to 256; the default is 4.
Step 27	Server /chassis/adapter/host-eth-if/recv-queue # set rq-ring-size <i>size</i>	The number of descriptors in the receive queue. The range is 64 to 4094; the default is 512.
Step 28	Server /chassis/adapter/host-eth-if/recv-queue # exit	Exits to the host Ethernet interface command mode.
Step 29	Server /chassis/adapter/host-eth-if # scope trans-queue	Enters transmit queue command mode.
Step 30	Server /chassis/adapter/host-eth-if/trans-queue # set wq-count <i>count</i>	The number of transmit queue resources to allocate. The range is 1 to 256; the default is 1.
Step 31	Server /chassis/adapter/host-eth-if/trans-queue # set wq-ring-size <i>size</i>	The number of descriptors in the transmit queue. The range is 64 to 4094; the default is 256.
Step 32	Server /chassis/adapter/host-eth-if/trans-queue # exit	Exits to the host Ethernet interface command mode.
Step 33	Server /chassis/adapter/host-eth-if # scope comp-queue	Enters completion queue command mode.
Step 34	Server /chassis/adapter/host-eth-if/comp-queue # set cq-count <i>count</i>	The number of completion queue resources to allocate. The range is 1 to 512; the default is 5. In general, the number of completion queues equals the number of transmit queues plus the number of receive queues.
Step 35	Server /chassis/adapter/host-eth-if/comp-queue # exit	Exits to the host Ethernet interface command mode.
Step 36	Server /chassis/adapter/host-eth-if # scope offload	Enters TCP offload command mode.
Step 37	Server /chassis/adapter/host-eth-if/offload # set tcp-segment-offload { disable enable }	Enables or disables TCP Segmentation Offload as follows: <ul style="list-style-type: none"> • disable —The CPU segments large TCP packets. • enable —The CPU sends large TCP packets to the hardware to be segmented. This option may reduce CPU overhead and increase throughput rate. This is the default. <p>Note This option is also known as Large Send Offload (LSO).</p>

	Command or Action	Purpose
Step 38	Server /chassis/adapter/host-eth-if/offload # set tcp-rx-checksum-offload {disable enable}	Enables or disables TCP Receive Offload Checksum Validation as follows: <ul style="list-style-type: none"> • disable —The CPU validates all packet checksums. • enable —The CPU sends all packet checksums to the hardware for validation. This option may reduce CPU overhead. This is the default.
Step 39	Server /chassis/adapter/host-eth-if/offload # set tcp-tx-checksum-offload {disable enable}	Enables or disables TCP Transmit Offload Checksum Validation as follows: <ul style="list-style-type: none"> • disable —The CPU validates all packet checksums. • enable —The CPU sends all packet checksums to the hardware for validation. This option may reduce CPU overhead. This is the default.
Step 40	Server /chassis/adapter/host-eth-if/offload # set tcp-large-receive-offload {disable enable}	Enables or disables TCP Large Packet Receive Offload as follows: <ul style="list-style-type: none"> • disable —The CPU processes all large packets. • enable —The hardware reassembles all segmented packets before sending them to the CPU. This option may reduce CPU utilization and increase inbound throughput. This is the default.
Step 41	Server /chassis/adapter/host-eth-if/offload # exit	Exits to the host Ethernet interface command mode.
Step 42	Server /chassis/adapter/host-eth-if # scope rss	Enters Receive-side Scaling (RSS) command mode.
Step 43	Server /chassis/adapter/host-eth-if/rss # set rss {disable enable}	Enables or disables RSS, which allows the efficient distribution of network receive processing across multiple CPUs in multiprocessor systems. The default is enable for the two default vNICs, and disable for user-created vNICs.
Step 44	Server /chassis/adapter/host-eth-if/rss # set rss-hash-ipv4 {disable enable}	Enables or disables IPv4 RSS. The default is enable.
Step 45	Server /chassis/adapter/host-eth-if/rss # set rss-hash-tcp-ipv4 {disable enable}	Enables or disables TCP/IPv4 RSS. The default is enable.
Step 46	Server /chassis/adapter/host-eth-if/rss # set rss-hash-ipv6 {disable enable}	Enables or disables IPv6 RSS. The default is enable.

	Command or Action	Purpose
Step 47	Server /chassis/adapter/host-eth-if/rss # set rss-hash-tcp-ipv6 {disable enable}	Enables or disables TCP/IPv6 RSS. The default is enable.
Step 48	Server /chassis/adapter/host-eth-if/rss # set rss-hash-ipv6-ex {disable enable}	Enables or disables IPv6 Extension RSS. The default is disable.
Step 49	Server /chassis/adapter/host-eth-if/rss # set rss-hash-tcp-ipv6-ex {disable enable}	Enables or disables TCP/IPv6 Extension RSS. The default is disable.
Step 50	Server /chassis/adapter/host-eth-if/rss # exit	Exits to the host Ethernet interface command mode.
Step 51	Server /chassis/adapter/host-eth-if # commit	Commits the transaction to the system configuration. Note The changes will take effect upon the next server reboot.

This example configures the properties of a vNIC:

```

Server# scope chassis
Server /chassis # show adapter
PCI Slot Product Name Serial Number Product ID Vendor
-----
1 UCS VIC P81E QC11417A0QK N2XX-ACPCTI01 Cisco Systems Inc

Server /chassis # scope adapter 1
Server /chassis/adapter # scope host-eth-if Test1
Server /chassis/adapter/host-eth-if # set uplink 1
Server /chassis/adapter/host-eth-if *# scope offload
Server /chassis/adapter/host-eth-if/offload *# set tcp-segment-offload enable
Server /chassis/adapter/host-eth-if/offload *# exit
Server /chassis/adapter/host-eth-if *# commit
Server /chassis/adapter/host-eth-if #

```

What to Do Next

Reboot the server to apply the changes.

Creating a vNIC

The adapter provides two permanent vNICs. You can create up to 16 additional vNICs.

Before You Begin

You must log in with user or admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope adapter <i>index</i>	Enters the command mode for the adapter card at the PCI slot number specified by <i>index</i> . Note The server must be powered on before you can view or change adapter settings.
Step 3	Server /chassis/adapter # create host-eth-if <i>name</i>	Creates a vNIC and enters the host Ethernet interface command mode. The <i>name</i> argument can be up to 32 ASCII characters.
Step 4	Server /chassis/adapter/host-eth-if # set channel-number <i>number</i>	(Optional) If NIV mode is enabled for the adapter, you must assign a channel number to this vNIC. The range is 1 to 1000.
Step 5	Server /chassis/adapter/host-eth-if # commit	Commits the transaction to the system configuration. Note The changes will take effect upon the next server reboot.

This example creates a vNIC on adapter 1:

```
Server# scope chassis
Server /chassis # scope adapter 1
Server /chassis/adapter # create host-eth-if Vnic5
Server /chassis/adapter/host-eth-if *# commit
New host-eth-if settings will take effect upon the next server reset
Server /chassis/adapter/host-eth-if #
```

Deleting a vNIC

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope adapter <i>index</i>	Enters the command mode for the adapter card at the PCI slot number specified by <i>index</i> . Note The server must be powered on before you can view or change adapter settings.
Step 3	Server /chassis/adapter # delete host-eth-if <i>name</i>	Deletes the specified vNIC. Note You cannot delete either of the two default vNICs, eth0 or eth1.
Step 4	Server /chassis/adapter # commit	Commits the transaction to the system configuration.

	Command or Action	Purpose
		Note The changes will take effect upon the next server reboot.

This example deletes a vNIC on adapter 1:

```
Server# scope chassis
Server /chassis # scope adapter 1
Server /chassis/adapter # delete host-eth-if Vnic5
Server /chassis/adapter *# commit
Server /chassis/adapter #
```

Creating Cisco usNIC Using the CIMC CLI



Note

Even though several properties are listed for Cisco usNIC in the usNIC properties dialog box, you must configure only the following properties because the other properties are not currently being used.

- cq-count
- rq-count
- tq-count
- usnic-count

Before You Begin

You must log in to the CIMC CLI with administrator privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	server# scope chassis	Enters chassis command mode.
Step 2	server/chassis# scope adapter <i>index</i>	Enters the command mode for the adapter card at the PCI slot number specified by <i>index</i> . Note Make sure that the server is powered on before you attempt to view or change adapter settings. To view the index of the adapters configured on your server, use the show adapter command.
Step 3	server/chassis/adapter# scope host-eth-if { eth0 eth1 }	Enters the command mode for the vNIC. Specify the Ethernet ID based on the number of vNICs that you have configured in your environment. For example, specify eth0 if you configured only one vNIC.

	Command or Action	Purpose
Step 4	server/chassis/adapter/host-eth-if# create usnic-config 0	Creates a usNIC config and enters its command mode. Make sure that you always set the index value to 0. Note To create a Cisco usNIC for the first time for a given vNIC using the CIMC CLI, you must first create a usnic-config . Subsequently, you only need to scope into the usnic-config and modify the properties for Cisco usNIC. For more information about modifying Cisco usNIC properties, see Modifying a Cisco usNIC using the CIMC CLI , on page 118.
Step 5	server/chassis/adapter/host-eth-if/usnic-config# set cq-count count	Specifies the number of completion queue resources to allocate. We recommend that you set this value to 4. The number of completion queues equals the number of transmit queues plus the number of receive queues.
Step 6	server/chassis/adapter/host-eth-if/usnic-config# set rq-count count	Specifies the number of receive queue resources to allocate. MPI uses 2 receive queues per process. We recommend that you set this value to 2.
Step 7	server/chassis/adapter/host-eth-if/usnic-config# set tq-count count	Specifies the number of transmit queue resources to allocate. MPI uses 2 transmit queues per process. We recommend that you set this value to 2.
Step 8	server/chassis/adapter/host-eth-if/usnic-config# set usnic-count number of usNICs .	Specifies the number of Cisco usNICs to create. Each MPI process that is running on the server requires a dedicated Cisco usNIC. Therefore, you might need to create up to 64 Cisco usNICs to sustain 64 MPI processes running simultaneously. We recommend that you create at least as many Cisco usNICs, per Cisco usNIC-enabled vNIC, as the number of physical cores on your server. For example, if you have 8 physical cores on your server, create 8 Cisco usNICs.
Step 9	server/chassis/adapter/host-eth-if/usnic-config# commit	Commits the transaction to the system configuration. Note The changes take effect when the server is rebooted.
Step 10	server/chassis/adapter/host-eth-if/usnic-config# exit	Exits to host Ethernet interface command mode.

	Command or Action	Purpose
Step 11	server/chassis/adapter/host-eth-if# exit	Exits to adapter interface command mode.
Step 12	server/chassis/adapter# exit	Exits to chassis interface command mode.
Step 13	server/chassis# exit	Exits to server interface command mode.
Step 14	server# scope bios	Enters Bios command mode.
Step 15	server/bios# scope advanced	Enters the advanced settings of BIOS command mode.
Step 16	server/bios/advanced# set IntelVTD Enabled	Enables the Intel Virtualization Technology.
Step 17	server/bios/advanced# set ATS Enabled	Enables the Intel VT-d Address Translation Services (ATS) support for the processor.
Step 18	server/bios/advanced# set CoherencySupport Enabled	Enables Intel VT-d coherency support for the processor.
Step 19	server /bios/advanced# commit	Commits the transaction to the system configuration. Note The changes take effect when the server is rebooted.

This example shows how to configure Cisco usNIC properties:

```

Server # scope chassis
server /chassis # show adapter
server /chassis # scope adapter 2
server /chassis/adapter # scope host-eth-if eth0
server /chassis/adapter/host-eth-if # create usnic-config 0
server /chassis/adapter/host-eth-if/usnic-config *# set usnic-count 64
server /chassis/adapter/host-eth-if/usnic-config *# set cq-count 4
server /chassis/adapter/host-eth-if/usnic-config *# set rq-count 2
server /chassis/adapter/host-eth-if/usnic-config *# set tq-count 2
server /chassis/adapter/host-eth-if/usnic-config *# commit
Committed settings will take effect upon the next server reset
server /chassis/adapter/host-eth-if/usnic-config # exit
server /chassis/adapter/host-eth-if # exit
server /chassis/adapter # exit
server /chassis # exit
server # exit
server/bios # scope bios
server/bios/advanced # scope advanced
server/bios/advanced # set Intel VTD Enabled
server/bios/advanced # set ATS Enabled
server/bios/advanced # set CoherencySupport Enabled
server /chassis/adapter/host-eth-if/usnic-config # commit
Committed settings will take effect upon the next server reset

```

Modifying a Cisco usNIC using the CIMC CLI



Note

Even though several properties are listed for Cisco usNIC in the usNIC properties dialog box, you must configure only the following properties because the other properties are not currently being used.

- **cq-count**
- **rq-count**
- **tq-count**
- **usnic-count**

Before You Begin

You must log in to the CIMC GUI with administrator privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	server# scope chassis	Enters chassis command mode.
Step 2	server/chassis# scope adapter <i>index</i>	Enters the command mode for the adapter card at the PCI slot number specified by <i>index</i> . Note Make sure that the server is powered on before you attempt to view or change adapter settings. To view the index of the adapters configured on your server, use the show adapter command.
Step 3	server/chassis/adapter# scope host-eth-if { eth0 eth1 }	Enters the command mode for the vNIC. Specify the Ethernet ID based on the number of vNICs that you have configured in your environment. For example, specify eth0 if you configured only one vNIC.
Step 4	server/chassis/adapter/host-eth-if# scope usnic-config 0	Enters the command mode for the usNIC. Make sure that you always set the index value as 0 to configure a Cisco usNIC.
Step 5	server/chassis/adapter/host-eth-if/usnic-config# set cq-count <i>count</i>	The number of completion queue resources to allocate. We recommend that you set this value to 4. The number of completion queues equals the number of transmit queues plus the number of receive queues.
Step 6	server/chassis/adapter/host-eth-if/usnic-config# set rq-count <i>count</i>	Specifies the number of receive queue resources to allocate. MPI uses two receive queues per

	Command or Action	Purpose
		process. We recommend that you set this value to 2.
Step 7	server/chassis/adapter/host-eth-if/usnic-config# set tq-count <i>count</i>	Specifies the number of transmit queue resources to allocate. MPI uses two transmit queues per process. We recommend that you set this value to 2.
Step 8	server/chassis/adapter/host-eth-if/usnic-config# set usnic-count <i>number of usNICs</i> .	Specifies the number of Cisco usNICs to create. Each MPI process running on the server requires a dedicated Cisco usNIC. Therefore, you might need to create up to 64 Cisco usNIC to sustain 64 MPI processes running simultaneously. We recommend that you create at least as many Cisco usNIC, per Cisco usNIC-enabled vNIC, as the number of physical cores on your server. For example, if you have 8 physical cores on your server, create 8 usNICs.
Step 9	server /chassis/adapter/host-eth-if /usnic-config# commit	Commits the transaction to the system configuration. Note The changes take effect when the server is rebooted.
Step 10	server/chassis/adapter/host-eth-if/usnic-config# exit	Exits to host Ethernet interface command mode.
Step 11	server/chassis/adapter/host-eth-if# exit	Exits to adapter interface command mode.
Step 12	server/chassis/adapter# exit	Exits to chassis interface command mode.
Step 13	server/chassis# exit	Exits to server interface command mode.
Step 14	server# scope bios	Enters BIOS command mode.
Step 15	server/bios# scope advanced	Enters the advanced settings of BIOS command mode.
Step 16	server/bios/advanced# set IntelVTD Enabled	Enables the Intel Virtualization Technology.
Step 17	server/bios/advanced# set ATS Enabled	Enables the Intel VT-d Address Translation Services (ATS) support for the processor.
Step 18	server/bios/advanced# set CoherencySupport Enabled	Enables Intel VT-d coherency support for the processor.
Step 19	server/bios/advanced# commit	Commits the transaction to the system configuration. Note The changes take effect when the server is rebooted.

This example shows how to configure Cisco usNIC properties:

```
server # scope chassis
server /chassis # show adapter
server /chassis # scope adapter 2
server /chassis/adapter # scope host-eth-if eth0
server /chassis/adapter/host-eth-if # scope usnic-config 0
server /chassis/adapter/host-eth-if/usnic-config # set usnic-count 64
server /chassis/adapter/host-eth-if/usnic-config # set cq-count 4
server /chassis/adapter/host-eth-if/usnic-config # set rq-count 2
server /chassis/adapter/host-eth-if/usnic-config # set tq-count 2
server /chassis/adapter/host-eth-if/usnic-config # commit
Committed settings will take effect upon the next server reset
server /chassis/adapter/host-eth-if/usnic-config # exit
server /chassis/adapter/host-eth-if # exit
server /chassis/adapter # exit
server /chassis # exit
server # exit
server/bios # scope bios
server/bios/advanced # scope advanced
server/bios/advanced # set Intel VTD Enabled
server/bios/advanced # set ATS Enabled
server/bios/advanced # set CoherencySupport Enabled
server /chassis/adapter/host-eth-if/usnic-config # commit
Committed settings will take effect upon the next server reset
```

Viewing usNIC Properties

Before You Begin

You must log in with admin privileges to perform this task.

usNIC must be configured on a vNIC.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope adapter <i>index</i>	Enters the command mode for the adapter card at the PCI slot number specified by <i>index</i> . Note The server must be powered on before you can view or change adapter settings.
Step 3	Server /chassis/adapter # scope host-eth-if { <i>eth0</i> <i>eth1</i> <i>name</i> }	Enters the host Ethernet interface command mode for the specified vNIC.
Step 4	Server /chassis/adapter/host-eth-if # show usnic-config <i>index</i>	Displays the usNIC properties for a vNIC.

This example displays the usNIC properties for a vNIC:

```
Server # scope chassis
Server /chassis # scope adapter 1
Server /chassis/adapter # scope host-eth-if eth0
Server /chassis/adapter/host-eth-if # show usnic-config 0
Idx usNIC Count TQ Count RQ Count CQ Count TQ Ring Size RQ Ring Size Interrupt Count
```

```

-----
0    113          2          2          4          256          512          4
Server /chassis/adapter/host-eth-if #

```

Deleting Cisco usNIC from a vNIC

Before You Begin

You must log in to CIMC CLI with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	server# scope chassis	Enters chassis command mode.
Step 2	server/chassis# scope adapter <i>index</i>	Enters the command mode for the adapter card at the PCI slot number specified by <i>index</i> . Note Make sure that the server is powered on before you attempt to view or change adapter settings. To view the index of the adapters configured on your server, use the show adapter command.
Step 3	server/chassis/adapter# scope host-eth-if {eth0 eth1}	Enters the command mode for the vNIC. Specify the Ethernet ID based on the number of vNICs that you have configured in your environment. For example, specify eth0 if you configured only one vNIC.
Step 4	Server/chassis/adapter/host-eth-if# delete usnic-config 0	Deletes the Cisco usNIC configuration for the vNIC.
Step 5	Server/chassis/adapter/host-eth-if# commit	Commits the transaction to the system configuration Note The changes take effect when the server is rebooted.

This example shows how to delete the Cisco usNIC configuration for a vNIC:

```

server # scope chassis
server/chassis # show adapter
server/chassis # scope adapter 1
server/chassis/adapter # scope host-eth-if eth0
Server/chassis/adapter/host-eth-if # delete usnic-config 0
server/adapter/host-eth-if/iscsi-boot *# commit
New host-eth-if settings will take effect upon the next adapter reboot

server /adapter/host-eth-if/usnic-config #

```

Configuring iSCSI Boot Capability

Configuring iSCSI Boot Capability for vNICs

When the rack-servers are configured in a standalone mode, and when the VIC adapters are directly attached to the Nexus 5000 family of switches, you can configure these VIC adapters to boot the servers remotely from iSCSI storage targets. You can configure Ethernet vNICs to enable a rack server to load the host OS image from remote iSCSI target devices.

To configure the iSCSI boot capability on a vNIC:

- You must log in with admin privileges to perform this task.
- To configure a vNIC to boot a server remotely from an iSCSI storage target, you must enable the PXE boot option on the vNIC.



Note

You can configure a maximum of 2 iSCSI vNICs for each host.

Configuring iSCSI Boot Capability on a vNIC

You can configure a maximum of 2 iSCSI vNICs for each host.

Before You Begin

- To configure a vNIC to boot a server remotely from an iSCSI storage target, you must enable the PXE boot option on the vNIC.
- You must log in with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope adapter <i>index</i>	Enters the command mode for the adapter card at the PCI slot number specified by <i>index</i> . Note The server must be powered on before you can view or change adapter settings.
Step 3	Server /chassis/adapter # scope host-eth-if { eth0 eth1 <i>name</i> }	Enters the host Ethernet interface command mode for the specified vNIC.
Step 4	Server /chassis/adapter/host-eth-if # create iscsi-boot <i>index</i>	Creates the iSCSI boot index for the vNIC. At this moment, only 0 is allowed as the index.

	Command or Action	Purpose
Step 5	Server /chassis/adapter/host-eth-if/iscsi-boot* # create iscsi-target <i>index</i>	Creates an iSCSI target for the vNIC. The value can either be 0 or 1.
Step 6	Server /chassis/adapter/host-eth-if/iscsi-boot* # set dhcp-net-settings enabled	Enables the DHCP network settings for the iSCSI boot.
Step 7	Server /chassis/adapter/host-eth-if/iscsi-boot* # set initiator-name <i>string</i>	Sets the initiator name. It cannot be more than 223 characters.
Step 8	Server /chassis/adapter/host-eth-if/iscsi-boot* # set dhcp-iscsi-settings enabled	Enables the DHCP iSCSI settings.
Step 9	Server /chassis/adapter/host-eth-if/iscsi-boot* # commit	Commits the transaction to the system configuration. Note The changes will take effect upon the next server reboot.

This example shows how to configure the iSCSI boot capability for a vNIC:

```
Server # scope chassis
Server /chassis # scope adapter 1
Server /chassis/adapter # scope host-eth-if eth0
Server /chassis/adapter/host-eth-if # create iscsi-boot 0
Server /adapter/host-eth-if/iscsi-boot *# set dhcp-net-settings enabled
Server /adapter/host-eth-if/iscsi-boot *# set initiator-name ign.2012-01.com.adser:abcde
Server /adapter/host-eth-if/iscsi-boot *# set dhcp-iscsi-settings enabled
Server /adapter/host-eth-if/iscsi-boot *# commit
```

New host-eth-if settings will take effect upon the next server reset
Server /adapter/host-eth-if/iscsi-boot #

Deleting an iSCSI Boot Configuration for a vNIC

Before You Begin

You must log in with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope adapter <i>index</i>	Enters the command mode for the adapter card at the PCI slot number specified by <i>index</i> . Note The server must be powered on before you can view or change adapter settings.

	Command or Action	Purpose
Step 3	Server /chassis/adapter # scope host-eth-if {eth0 eth1 name}	Enters the host Ethernet interface command mode for the specified vNIC.
Step 4	Server /chassis/adapter/host-eth-if # delete iscsi-boot 0	Deletes the iSCSI boot capability for the vNIC.
Step 5	Server /chassis/adapter/host-eth-if* # commit	Commits the transaction to the system configuration Note The changes will take effect upon the next server reboot.

This example shows how to delete the iSCSI boot capability for a vNIC:

```
Server # scope chassis
Server /chassis # scope adapter 1
Server /chassis/adapter # scope host-eth-if eth0
Server /chassis/adapter/host-eth-if # delete iscsi-boot 0
Server /adapter/host-eth-if/iscsi-boot *# commit
New host-eth-if settings will take effect upon the next server reset

Server /adapter/host-eth-if/iscsi-boot #
```

Managing VM FEX

Virtual Machine Fabric Extender

Cisco Virtual Machine Fabric Extender (VM FEX) extends the (prestandard) IEEE 802.1Qbh port extender architecture to virtual machines. In this architecture, each VM interface is provided with a virtual Peripheral Component Interconnect Express (PCIe) device and a virtual port on a switch.

Viewing VM FEX Properties

Before You Begin

- The server must be powered on, or the properties will not display.
- A supported Virtual Interface Card (VIC) must be installed in the chassis and the server must be powered on.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope adapter index	Enters the command mode for the adapter card at the PCI slot number specified by <i>index</i> .

	Command or Action	Purpose
		Note The server must be powered on before you can view or change adapter settings.
Step 3	Server /chassis/adapter # show vmfex [detail]	Displays the general VM FEX properties. For field descriptions, see General Properties Settings , on page 126.
Step 4	Server /chassis/adapter # scope vmfex name	Enters the command mode for the specified VM FEX interface.
Step 5	Server /chassis/adapter/vmfex # show interrupt [detail]	Displays Ethernet interrupt settings. For field descriptions, see Ethernet Interrupt Settings , on page 127.
Step 6	Server /chassis/adapter/vmfex # show recv-queue [detail]	Displays Ethernet receive queue settings. For field descriptions, see Ethernet Receive Queue Settings , on page 128.
Step 7	Server /chassis/adapter/vmfex # show trans-queue [detail]	Displays Ethernet transmit queue settings. For field descriptions, see Ethernet Transmit Queue Settings , on page 128.
Step 8	Server /chassis/adapter/vmfex # show comp-queue [detail]	Displays completion queue settings. For field descriptions, see Completion Queue Settings , on page 128.
Step 9	Server /chassis/adapter/vmfex # show offload [detail]	Displays TCP offload settings. For field descriptions, see TCP Offload Settings , on page 128.
Step 10	Server /chassis/adapter/vmfex # show rss [detail]	Displays RSS settings. For field descriptions, see Receive Side Scaling Settings , on page 129.

This example displays the VM FEX properties:

```

Server /chassis/adapter # show vmfex detail
Name pts0:
  MTU: 1500
  Uplink Port: 0
  MAC Address: 00:00:00:00:00:00
  CoS: N/A
  Trust Host CoS:
  PCI Order:
  VLAN: N/A
  VLAN Mode: N/A
  Rate Limiting:
  PXE Boot: disabled
  Channel Number: 0
  Port Profile:
  Uplink Failover: Enabled
  Uplink Failback Timeout: 5

Server /chassis/adapter # scope vmfex pts0

Server /chassis/adapter/vmfex # show interrupt
Interrupt Count Coalescing Time (us) Coalescing Type Interrupt Mode
-----

```

```

6                               125                               MIN                               MSI

Server /chassis/adapter/vmfex # show recv-queue
Receive Queue Count Receive Queue Ring Size
-----
4                               512

Server /chassis/adapter/vmfex # show trans-queue
Transmit Queue Count Transmit Queue Ring Size
-----
1                               256

Server /chassis/adapter/vmfex # show comp-queue
Completion Queue Count Completion Queue Ring Size
-----
5                               1

Server /chassis/adapter/vmfex # show offload
TCP Segment Offload TCP Rx Checksum TCP Tx Checksum Large Receive
-----
enabled              enabled          enabled          enabled

Server /chassis/adapter/vmfex # show rss
TCP Rx Side Scaling
-----
enabled

Server /chassis/adapter/vmfex #

```

VM FEX Settings

The following tables describe the VM FEX settings that you can view.

General Properties Settings

Name	Description
Name	A user-defined name for the VM FEX.
MTU	The maximum transmission unit, or packet size, that this VM FEX accepts.
Uplink Port	The uplink port associated with this VM FEX. All traffic for this VM FEX goes through this uplink port.
MAC Address	The MAC address associated with the VM FEX.
Class of Service	The class of service to associate with traffic from this VM FEX.
Trust Host CoS	Whether the VM FEX can use the class of service provided by the host operating system.
PCI Order	The order in which this VM FEX will be used.
Default VLAN	The default VLAN for this VM FEX.
VLAN Mode	Whether VLAN trunking or access is configured.

Name	Description
Rate Limit	If rate limiting is configured, the maximum rate.
Enable PXE Boot	Whether the VM FEX can be used to perform a PXE boot.
Channel Number	If NIV mode is enabled for the adapter, the channel number assigned to this VM FEX.
Port Profile	<p>If NIV mode is enabled for the adapter, the port profile associated with the VM FEX.</p> <p>Note This field displays the port profiles defined on the switch to which this server is connected.</p>
Enable Uplink Failover	If NIV mode is enabled for the adapter, whether traffic on this VM FEX should fail over to the secondary interface if there are communication problems.
Failback Timeout	After a VM FEX has started using its secondary interface, this setting controls how long the primary interface must be available before the system resumes using the primary interface for the VM FEX.

Ethernet Interrupt Settings

Name	Description
Interrupt Count field	The number of interrupt resources allocated to this VM FEX.
Coalescing Time field	The time CIMC waits between interrupts or the idle period that must be encountered before an interrupt is sent.
Coalescing Type field	<p>This can be one of the following:</p> <ul style="list-style-type: none"> • MIN—The system waits for the time specified in the Coalescing Time field before sending another interrupt event. • IDLE—The system does not send an interrupt until there is a period of no activity lasting as long as the time specified in the Coalescing Time field.
Interrupt Mode field	<p>The preferred driver interrupt mode. This can be one of the following:</p> <ul style="list-style-type: none"> • MSIx—Message Signaled Interrupts (MSI) with the optional extension. • MSI—MSI only. • INTx—PCI INTx interrupts.

Ethernet Receive Queue Settings

Name	Description
Receive Queue Count field	The number of receive queue resources allocated to this VM FEX.
Receive Queue Ring Size field	The number of descriptors in each receive queue.

Ethernet Transmit Queue Settings

Name	Description
Transmit Queue Count field	The number of transmit queue resources allocated to this VM FEX.
Transmit Queue Ring Size field	The number of descriptors in each transmit queue.

Completion Queue Settings

Name	Description
Completion Queue Count field	The number of completion queue resources allocated to this VM FEX.
Completion Queue Ring Size field	The number of descriptors in each completion queue.

TCP Offload Settings

Name	Description
Enable TCP Segmentation Offload field	If enabled, the CPU sends large TCP packets to the hardware to be segmented. If disabled, the CPU segments large packets. Note This option is also known as Large Send Offload (LSO).
Enable TCP Rx Offload Checksum Validation field	If enabled, the CPU sends all packet checksums to the hardware for validation. If disabled, the CPU validates all packet checksums.
Enable TCP Tx Offload Checksum Generation field	If enabled, the CPU sends all packets to the hardware so that the checksum can be calculated. If disabled, the CPU calculates all packet checksums.
Enable Large Receive field	If enabled, the hardware reassembles all segmented packets before sending them to the CPU. If disabled, the CPU processes all large packets.

Receive Side Scaling Settings

Name	Description
Enable TCP Receive Side Scaling field	Receive Side Scaling (RSS) distributes network receive processing across multiple CPUs in multiprocessor systems. If enabled, network receive processing is shared across processors whenever possible. If disabled, network receive processing is always handled by a single processor even if additional processors are available.
Enable IPv4 RSS field	If enabled, RSS is enabled on IPv4 networks.
Enable TCP-IPv4 RSS field	If enabled, RSS is enabled for TCP transmissions across IPv4 networks.
Enable IPv6 RSS field	If enabled, RSS is enabled on IPv6 networks.
Enable TCP-IPv6 RSS field	If enabled, RSS is enabled for TCP transmissions across IPv6 networks.
Enable IPv6 Extension RSS field	If enabled, RSS is enabled for IPv6 extensions.
Enable TCP-IPv6 Extension RSS field	If enabled, RSS is enabled for TCP transmissions across IPv6 networks.

Managing Storage Adapters

Create Virtual Drive from Unused Physical Drives

Before You Begin

You must log in with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	<code>Server# scope chassis</code>	Enters the chassis command mode.
Step 2	<code>Server /chassis # scope storageadapter slot</code>	Enters command mode for an installed storage card.
Step 3	<code>Server /chassis/storageadapter # create virtual-drive</code>	At this point, you are prompted to enter information corresponding to the RAID level, the physical drives to be used, the size and the write policy for the new virtual drive. Enter the appropriate information at each prompt. When you have finished specifying the virtual drive information, you are prompted to confirm that the information is correct. Enter y (yes) to confirm, or n (no) to cancel the operation.

	Command or Action	Purpose
Step 4	Server /chassis/storageadapter # show virtual-drive	Displays the existing virtual drives.

This example shows how to create a new virtual drive that spans two unused physical drives.

```

Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter # create-virtual-drive
Please enter RAID level
(0, 1, 5, 6, 10, 50, 60) --> 1

Please choose from the following 2 unused physical drives:
  Slot 6: size 68664 MB
  Slot 7: size 68664 MB

Specify physical disks for span 0:
  Enter comma-separated PDs from above list--> 6,7
Please enter Virtual Drive name (15 characters maximum)--> test_v_drive
Please enter Virtual Drive size in MB, GB, or TB
Example format: '400 GB' --> 1000 MB

Optional attribute:
  Write Policy: defaults to Write Back
    OK? (y or n)--> n
    0: Write Through
    1: Write Back
    2: Write Back with Bad BBU
    3: Write Back Adaptive
  Choose number from above options--> 2

Write Policy will be set to Write Back with Bad BBU (2 and 'write-policy\2')

New virtual drive will have the following characteristics:
- Spans: '[6.7]'
- RAID level: '1'
- Name: 'test_v_drive'
- Size: 1000 MB
- Write Policy: Write Back with Bad BBU
OK? (y or n)--> y

```

```

Server /chassis/storageadapter # show virtual-drive
Virtual Drive Health      Status      Name              Size      RAID Level
Boot Drive
-----
0                          Good        Optimal           150528 MB RAID 0
false
1                          Good        Optimal           20480 MB  RAID 0
true
2                          Good        Optimal           114140 MB RAID 0
false
3                          Good        Optimal           test_v_drive 1000 MB  RAID 1
false
4                          Good        Optimal           new_from_test 500 MB    RAID 1
false

Server /chassis/storageadapter #

```

Create Virtual Drive from an Existing Drive Group

Before You Begin

You must log in with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope storageadapter slot	Enters command mode for an installed storage card.
Step 3	Server /chassis/storageadapter # carve-virtual-drive	At this point, you are prompted to enter information corresponding to the virtual drives to be used, and the size and the write policy for the new virtual drive. Enter the appropriate information at each prompt. When you have finished specifying the virtual drive information, you are prompted to confirm that the information is correct. Enter y (yes) to confirm, or n (no) to cancel the operation.
Step 4	Server /chassis/storageadapter # show virtual-drive	Displays the existing virtual drives.

This example shows how to carve a new virtual drive out of unused space in an existing RAID 1 drive group:

```

Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter # carve-virtual-drive
  < Fetching virtual drives...>

ID  Name                RL  VDSize      MaxPossibleSize PD(s)
-----
 3  test_v_drive          1   1000 MB      67664 MB        6,7

Please choose from the above list the virtual drive number
whose space the new virtual drive will share--> 3
New virtual drive will share space with VD 3

Please enter Virtual Drive name (15 characters maximum)--> new_from_test
Please enter Virtual Drive size in MB, GB, or TB (maximum: 67664 MB)
  Example format: '400 GB' --> 500 MB

Optional attribute:
  Write Policy: defaults to Write Back
  OK? (y or n)--> y

New virtual drive will have the following characteristics:
- It will share space with virtual drive 3
- Name: 'new_from_test'
- Size: 500 MB

OK? (y or n)--> y
Server /chassis/storageadapter # show virtual-drive
Virtual Drive Health      Status      Name      Size      RAID Level
Boot Drive

```

```

-----
-----
0          Good          Optimal          150528 MB  RAID 0
false
1          Good          Optimal          20480 MB  RAID 0
true
2          Good          Optimal          114140 MB RAID 0
false
3          Good          Optimal          test_v_drive 1000 MB  RAID 1
false
4          Good          Optimal          new_from_test 500 MB   RAID 1
false

Server /chassis/storageadapter #

```

Clearing Foreign Configuration



Important

This task clears all foreign configuration on the controller. Also, all configuration information from all physical drives hosting foreign configuration is deleted. This action cannot be reverted.

Before You Begin

You must log in with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope storageadapter slot	Enters command mode for an installed storage card.
Step 3	Server /chassis/storageadapter # clear-foreign-config	You are prompted to confirm the action. Enter yes to confirm. Note If you do not enter yes , the action is aborted.

This example shows how to clear all foreign configurations on the MegaRAID controller in slot 3:

```

Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter # clear-foreign-config
Are you sure you want to clear all foreign configurations on this controller?
All data on the drive(s) will be lost.
Enter 'yes' to confirm -> yes
Server /chassis/storageadapter #

```

Deleting a Virtual Drive



Important

This task deletes a virtual drive, including the drives that run the booted operating system. So back up any data that you want to retain before you delete a virtual drive.

Before You Begin

You must log in with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope storageadapter slot	Enters command mode for an installed storage card.
Step 3	Server /chassis/storageadapter # scope virtual-drive drive-number	Enters command mode for the specified virtual drive.
Step 4	Server /chassis/storageadapter/virtual-drive # delete-virtual-drive	You are prompted to confirm the action. Enter yes to confirm. Note If you do not enter yes , the action is aborted.

This example shows how to delete virtual drive 3.

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter # scope virtual-drive 3
Server /chassis/storageadapter/virtual-drive # delete-virtual-drive
Are you sure you want to delete virtual drive 3?
All data on the drive will be lost. Enter 'yes' to confirm -> yes
Server /chassis/storageadapter/virtual-drive #
```

Initializing a Virtual Drive

All data on a virtual drive is lost when you initialize the drive. Before you run an initialization, back up any data on the virtual drive that you want to save.

Before You Begin

You must log in with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope storageadapter slot	Enters command mode for an installed storage card.
Step 3	Server /chassis/storageadapter # scope virtual-drive drive-number	Enters command mode for the specified virtual drive.
Step 4	Server /chassis/storageadapter/virtual-drive # start-initialization	Initializes the specified virtual drive.
Step 5	Server /chassis/storageadapter/virtual-drive # cancel-initialization	(Optional) Cancels the initialization of the specified virtual drive.
Step 6	Server /chassis/storageadapter/physical-drive # get-operation-status	Displays the status of the task that is in progress on the drive.

This example shows how to initialize virtual drive 3 using fast initialization:

```

Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter # scope virtual-drive 3
Server /chassis/storageadapter/virtual-drive # start-initialization
Are you sure you want to initialize virtual drive 3?
All data on the drive will be lost. Enter 'yes' to confirm -> yes
Fast (0) or full (1) initialization? -> 0
Server /chassis/storageadapter/virtual-drive # get-operation-status

progress-percent: 20%
elapsed -seconds: 30
operation-in-progress: initializing virtual drive

Server /chassis/storageadapter/virtual-drive #

```

Set as Boot Drive

Before You Begin

You must log in with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope storageadapter slot	Enters command mode for an installed storage card.

	Command or Action	Purpose
Step 3	Server /chassis/storageadapter # scope virtual-drive <i>drive-number</i>	Enters command mode for the specified virtual drive.
Step 4	Server /chassis/storageadapter # set-boot-drive	Specifies the controller to boot from this virtual drive.

This example shows how to specify the controller to boot from virtual drive 3:

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter # scope virtual-drive 3
Server /chassis/storageadapter/virtual-drive # set-boot-drive
Are you sure you want to set virtual drive 3 as the boot drive?
Enter 'yes' to confirm -> yes
Server /chassis/storageadapter/virtual-drive #
```

Modifying Attributes of a Virtual Drive

Before You Begin

You must log in with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope storageadapter <i>slot</i>	Enters command mode for an installed storage card.
Step 3	Server /chassis/storageadapter # scope virtual-drive <i>3</i>	Enters the command mode for the virtual drive.
Step 4	Server /chassis/storageadapter/virtual-drive # modify-attributes	Prompts you to select a different current policy.

This example shows how to carve a new virtual drive out of unused space in an existing RAID 1 drive group:

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter # scope virtual-drive
Server /chassis/storageadapter/virtual-drive # modify-attributes

Current write policy: Write Back

0: Write Through
1: Write Back
2: Write Back even if Bad BBU

Choose number from above options --> 0
```

```

The following attribute will be modified:
- Write policy: Write Through

OK? (y or n) --> y

operation in progress.

Server /chassis/storageadapter/virtual-drive #

```

Making a Dedicated Hot Spare

Before You Begin

You must log in with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope storageadapter slot	Enters command mode for an installed storage card.
Step 3	Server /chassis/storageadapter # scope physical-drive drive-number	Enters command mode for the specified physical drive.
Step 4	Server /chassis/storageadapter/physical-drive # make-dedicated-hot-spare	You are prompted to choose a virtual drive for which the dedicated hot spare is being created.

This example shows how to make physical drive 3 a dedicated hot spare for virtual drive 6:

```

Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter # scope physical-drive 3
Server /chassis/storageadapter/physical-drive # make-dedicated-hot-spare
  5: VD_OS_1, RAID 0, 102400 MB, physical disks: 1
  6: VD_OS_2, RAID 0, 12288 MB, physical disks: 1
  7: VD_OS_3, RAID 0, 12288 MB, physical disks: 1
  8: VD_DATA_1, RAID 0, 12512 MB, physical disks: 1
  9: RAID1_2358, RAID 1, 40000 MB, physical disks: 2,3,5,8
 11: JFB_RAID1_67, RAID 1, 20000 MB, physical disks: 6,7
 12: JFB_Crv_R1_40, RAID 1, 40000 MB, physical disks: 6,7
 13: JFB_R1_10GB, RAID 1, 10000 MB, physical disks: 6,7

Please choose from the above 8 virtual drives-->6

Server /chassis/storageadapter/physical-drive #

```

Making a Global Hot Spare

Before You Begin

You must log in with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope storageadapter slot	Enters command mode for an installed storage card.
Step 3	Server /chassis/storageadapter # scope physical-drive drive-number	Enters command mode for the specified physical drive.
Step 4	Server /chassis/storageadapter/physical-drive # make-global-hot-spare	
Step 5	Server /chassis/storageadapter/physical-drive # get-operation-status	Displays the status of the task that is in progress on the drive.

This example shows how to make physical drive 3 a global hot spare:

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter # scope physical-drive 3
Server /chassis/storageadapter/physical-drive # make-global-hot-spare
Server /chassis/storageadapter/physical-drive #
```

Preparing a Drive for Removal

You can confirm this task only on physical drives that display the **Unconfigured Good** status.

Before You Begin

You must log in with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope storageadapter slot	Enters command mode for an installed storage card.
Step 3	Server /chassis/storageadapter # scope physical-drive drive-number	Enters command mode for the specified physical drive.
Step 4	Server /chassis/storageadapter/physical-drive # prepare-for-removal	

This example shows how to prepare physical drive 3 for removal.

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
```

```

Server /chassis/storageadapter # scope physical-drive 3
Server /chassis/storageadapter/physical-drive # prepare-for-removal
Server /chassis/storageadapter/physical-drive #

```

Removing a Drive from Hot Spare Pools

Before You Begin

You must log in with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope storageadapter slot	Enters command mode for an installed storage card.
Step 3	Server /chassis/storageadapter # scope physical-drive drive-number	Enters command mode for the specified physical drive.
Step 4	Server /chassis/storageadapter/physical-drive # remove-hot-spare	Removes a drive from the host spare pool.

This example shows how to remove physical drive 3 from the hot spare pools:

```

Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter # scope physical-drive 3
Server /chassis/storageadapter/physical-drive # remove-hot-spare
Server /chassis/storageadapter/physical-drive #

```

Undo Preparing a Drive for Removal

Before You Begin

You must log in with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope storageadapter slot	Enters command mode for an installed storage card.
Step 3	Server /chassis/storageadapter # scope physical-drive drive-number	Enters command mode for the specified physical drive.

	Command or Action	Purpose
Step 4	Server /chassis/storageadapter/physical-drive # undo-prepare-for-removal	

This example shows how to respin physical drive 3 after preparing the drive for removal.

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter # scope physical-drive 3
Server /chassis/storageadapter/physical-drive # undo-prepare-for-removal
Server /chassis/storageadapter/physical-drive #
```

Enabling Auto Learn Cycles for the Battery Backup Unit

Before You Begin

You must log in with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope storageadapter slot	Enters command mode for an installed storage card.
Step 3	Server /chassis/storageadapter # scope bbu	Enter the battery backup unit command mode.
Step 4	Server /chassis/storageadapter # enable-auto-learn	Enables the battery auto-learn cycles

This example shows how to enable the battery auto-learn cycles:

```
Server # scope chassis
Server /chassis # scope storageadapter SLOT-2
Server /chassis/storageadapter # scope bbu
Server /chassis/storageadapter/bbu # enable-auto-learn
Automatic BBU learn cycles will occur without notice if enabled.
Are you sure? [y/n] --> y
enable-auto-learn initiated
Server /chassis/storageadapter/bbu #
```

Disabling Auto Learn Cycles for the Battery Backup Unit

Before You Begin

You must log in with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope storageadapter slot	Enters command mode for an installed storage card.
Step 3	Server /chassis/storageadapter # scope bbu	Enter the battery backup unit command mode.
Step 4	Server /chassis/storageadapter # disable-auto-learn	Disables the battery auto-learn cycles

This example shows how to disables the battery auto-learn cycles:

```
Server # scope chassis
Server /chassis # scope storageadapter SLOT-2
Server /chassis/storageadapter # scope bbu
Server /chassis/storageadapter/bbu # disable-auto-learn
Automatic BBU learn cycles will no longer occur if disabled.
Are you sure? [y/n] --> y
disable-auto-learn initiated

Server /chassis/storageadapter/bbu #
```

Starting a Learn Cycle for a Battery Backup Unit

Before You Begin

You must be logged in as an admin to use this command.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope storageadapter slot	Enters command mode for an installed storage card.
Step 3	Server /chassis/storageadapter # scope bbu	Enter the battery backup unit command mode.
Step 4	Server /chassis/storageadapter # start-learn-cycle	Starts the learn cycle for the battery.

This example shows how to initiate the learn cycles for a battery:

```
Server # scope chassis
Server /chassis # scope storageadapter SLOT-2
Server /chassis/storageadapter # scope bbu
Server /chassis/storageadapter/bbu # start-learn-cycle
Server /chassis/storageadapter/bbu #
```

Toggling the Locator LED for a Physical Drive

Before You Begin

You must be logged in as an admin to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope storageadapter slot	Enters command mode for an installed storage card.
Step 3	Server /chassis/storageadapter # scope physical-drive 3	Enters the physical drive command mode.
Step 4	Server /chassis/storageadapter/physical-drive # locator-led {on off}	Enables or disables the physical drive locator LED.

This example shows how to enable the locator LED for physical drive 3:

```
Server # scope chassis
Server /chassis # scope storageadapter SLOT-2
Server /chassis/storageadapter # scope physical-drive 3
Server /chassis/storageadapter/physical-drive # locator-led on
Server /chassis/storageadapter/physical-drive* # commit
Server /chassis/storageadapter/physical-drive #
```

Viewing Storage Controller Logs

Before You Begin

You must log in with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope storageadapter slot	Enters command mode for an installed storage card.
Step 3	Server /chassis/storageadapter # show log	Displays the storage controller logs.

This example shows how to display storage controller logs:

```
Server # scope chassis
Server /chassis # scope storageadapter SLOT-3
```

```
Server /chassis/storageadapter # show log
```

Time	Severity	Description
Fri March 1 09:52:19 2013	Warning	Predictive Failure
Fri March 1 07:50:19 2013	Info	Battery charge complete
Fri March 1 07:50:19 2013	Info	Battery charge started
Fri March 1 07:48:19 2013	Info	Battery relearn complete
Fri March 1 07:47:19 2013	Info	Battery is discharging
Fri March 1 07:45:19 2013	Info	Battery relearn started

```
Server /chassis/storageadapter #
```

Backing Up and Restoring the Adapter Configuration

Exporting the Adapter Configuration

The adapter configuration can be exported as an XML file to a TFTP server.



Important

If any firmware or BIOS updates are in progress, do not export the adapter configuration until those tasks are complete.

Before You Begin

A supported Virtual Interface Card (VIC) must be installed in the chassis and the server must be powered on. Obtain the TFTP server IP address.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope adapter <i>index</i>	Enters the command mode for the adapter card at the PCI slot number specified by <i>index</i> . Note The server must be powered on before you can view or change adapter settings.
Step 3	Server /chassis/adapter # export-vnic <i>protocol remote</i> <i>server IP address</i>	Starts the export operation. The adapter configuration file will be stored at the specified path and filename on the remote server at the specified IP address. The protocol can be one of the following: <ul style="list-style-type: none"> • TFTP • FTP • SFTP • SCP • HTTP

	Command or Action	Purpose
--	-------------------	---------

This example exports the configuration of adapter 1:

```
Server# scope chassis
Server /chassis # scope adapter 1
Server /chassis/adapter # export-vnic ftp 192.0.20.34 //test/dnld-ucs-k9-bundle.1.0.2h.bin
Server /chassis/adapter #
```

Importing the Adapter Configuration



Important

If any firmware or BIOS updates are in progress, do not import the adapter configuration until those tasks are complete.

Before You Begin

You must log in with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # scope adapter <i>index</i>	Enters the command mode for the adapter card at the PCI slot number specified by <i>index</i> . Note The server must be powered on before you can view or change adapter settings.
Step 3	Server /chassis/adapter # import-vnic <i>tftp-ip-address</i> <i>path-and-filename</i>	Starts the import operation. The adapter downloads the configuration file from the specified path on the TFTP server at the specified IP address. The configuration will be installed during the next server reboot.

This example imports a configuration for the adapter in PCI slot 1:

```
Server# scope chassis
Server /chassis # scope adapter 1
Server /chassis/adapter # import-vnic 192.0.2.34 /ucs/backups/adapter4.xml
Import succeeded.
New VNIC adapter settings will take effect upon the next server reset.
Server /chassis/adapter #
```

What to Do Next

Reboot the server to apply the imported configuration.

Restoring Adapter Defaults

Before You Begin

You must log in with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # adapter-reset-defaults index	Restores factory default settings for the adapter at the PCI slot number specified by the <i>index</i> argument.

This example restores the default configuration of the adapter in PCI slot 1:

```
Server# scope chassis
Server /chassis # adapter-reset-defaults 1
This operation will reset the adapter to factory default.
All your configuration will be lost.
Continue?[y|N] y
Server /chassis #
```

Managing Adapter Firmware

Adapter Firmware

A Cisco UCS C-Series network adapter contains the following firmware components:

- Adapter firmware—The main operating firmware, consisting of an active and a backup image, can be installed from the CIMC GUI or CLI interface or from the Host Upgrade Utility (HUU). You can upload a firmware image from either a local file system or a TFTP server.
- Bootloader firmware—The bootloader firmware cannot be installed from the CIMC GUI or CLI. You can install this firmware using the Host Upgrade Utility.

Installing Adapter Firmware



Important

If any firmware or BIOS updates are in progress, do not install the adapter firmware until those tasks are complete.

Before You Begin

You must log in with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server /chassis # update-adapter-fw <i>tftp-ip-address path-and-filename</i> { activate no-activate } [<i>pci-slot</i>] [<i>pci-slot</i>]	Downloads the specified adapter firmware file from the TFTP server, then installs the firmware as the backup image on one or two specified adapters or, if no adapter is specified, on all adapters. If the activate keyword is specified, the new firmware is activated after installation.
Step 3	Server /chassis # recover-adapter-update [<i>pci-slot</i>] [<i>pci-slot</i>]	(Optional) Clears an incomplete firmware update condition on one or two specified adapters or, if no adapter is specified, on all adapters.

This example begins an adapter firmware upgrade on the adapter in PCI slot 1:

```
Server# scope chassis
Server /chassis # update-adapter-fw 192.0.2.34 /ucs/adapters/adapter4.bin activate 1
Server /chassis #
```

What to Do Next

To activate the new firmware, see [Activating Adapter Firmware, on page 145](#).

Activating Adapter Firmware

**Important**

While the activation is in progress, do not:

- Reset, power off, or shut down the server.
- Reboot or reset CIMC.
- Activate any other firmware.
- Export technical support or configuration data.

Before You Begin

You must log in with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.

	Command or Action	Purpose
Step 2	Server /chassis # activate-adapter-fw <i>pci-slot</i> { 1 2 }	Activates adapter firmware image 1 or 2 on the adapter in the specified PCI slot. Note The changes will take effect upon the next server reboot.

This example activates adapter firmware image 2 on the adapter in PCI slot 1:

```
Server# scope chassis
Server /chassis # activate-adapter-fw 1 2
Firmware image activation succeeded
Please reset the server to run the activated image
Server /chassis #
```

What to Do Next

Reboot the server to apply the changes.

Resetting the Adapter

Before You Begin

You must log in with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters the chassis command mode.
Step 2	Server/chassis # adapter-reset <i>index</i>	Resets the adapter at the PCI slot number specified by the <i>index</i> argument. Note Resetting the adapter also resets the host.

This example resets the adapter in PCI slot 1:

```
Server# scope chassis
Server /chassis # adapter-reset 1
This operation will reset the adapter and the host if it is on.
You may lose connectivity to the CIMC and may have to log in again.
Continue?[y|N] y
Server /chassis #
```



Configuring Communication Services

This chapter includes the following sections:

- [Configuring HTTP, page 147](#)
- [Configuring SSH, page 148](#)
- [Configuring XML API, page 149](#)
- [Configuring IPMI, page 150](#)
- [Configuring SNMP, page 151](#)

Configuring HTTP

Before You Begin

You must log in as a user with admin privileges to configure HTTP.

Procedure

	Command or Action	Purpose
Step 1	Server# scope http	Enters the HTTP command mode.
Step 2	Server /http # set enabled {yes no}	Enables or disables HTTP and HTTPS service on the CIMC.
Step 3	Server /http # set http-port number	Sets the port to use for HTTP communication. The default is 80.
Step 4	Server /http # set https-port number	Sets the port to use for HTTPS communication. The default is 443.
Step 5	Server /http # set http-redirect {yes no}	Enables or disables the redirection of an HTTP request to HTTPS.

	Command or Action	Purpose
Step 6	Server /http # set timeout <i>seconds</i>	Sets the number of seconds to wait between HTTP requests before the CIMC times out and terminates the session. Enter an integer between 60 and 10,800. The default is 1,800 seconds.
Step 7	Server /http # commit	Commits the transaction to the system configuration.

This example configures HTTP for the CIMC:

```
Server# scope http
Server /http # set enabled yes
Server /http *# set http-port 80
Server /http *# set https-port 443
Server /http *# set http-redirect yes
Server /http *# set timeout 1800
Server /http *# commit
Server /http # show
HTTP Port  HTTPS Port  Timeout  Active Sessions  Enabled  HTTP Redirected
-----
80          443          1800    0                 yes     yes
Server /http #
```

Configuring SSH

Before You Begin

You must log in as a user with admin privileges to configure SSH.

Procedure

	Command or Action	Purpose
Step 1	Server# scope ssh	Enters the SSH command mode.
Step 2	Server /ssh # set enabled {yes no}	Enables or disables SSH on the CIMC.
Step 3	Server /ssh # set ssh-port <i>number</i>	Sets the port to use for secure shell access. The default is 22.
Step 4	Server /ssh # set timeout <i>seconds</i>	Sets the number of seconds to wait before the system considers an SSH request to have timed out. Enter an integer between 60 and 10,800. The default is 300 seconds.
Step 5	Server /ssh # commit	Commits the transaction to the system configuration.
Step 6	Server /ssh # show [detail]	(Optional) Displays the SSH configuration.

This example configures SSH for the CIMC:

```
Server# scope ssh
Server /ssh # set enabled yes
Server /ssh *# set ssh-port 22
Server /ssh *# set timeout 600
Server /ssh *# commit
Server /ssh # show
SSH Port      Timeout    Active Sessions Enabled
-----
22            600        1                yes
Server /ssh #
```

Configuring XML API

XML API for CIMC

The Cisco CIMC XML application programming interface (API) is a programmatic interface to CIMC for a C-Series Rack-Mount Server. The API accepts XML documents through HTTP or HTTPS.

For detailed information about the XML API, see *Cisco UCS Rack-Mount Servers CIMC XML API Programmer's Guide*.

Enabling XML API

Before You Begin

You must log in as a user with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope xmlapi	Enters XML API command mode.
Step 2	Server /xmlapi # set enabled {yes no}	Enables or disables XML API control of CIMC.
Step 3	Server /xmlapi # commit	Commits the transaction to the system configuration.

This example enables XML API control of CIMC and commits the transaction:

```
Server# scope xmlapi
Server /xmlapi # set enabled yes
Server /xmlapi *# commit
Server /xmlapi # show detail
XMLAPI Settings:
  Enabled: yes
  Active Sessions: 0
  Max Sessions: 4
Server /xmlapi #
```

Configuring IPMI

IPMI Over LAN

Intelligent Platform Management Interface (IPMI) defines the protocols for interfacing with a service processor embedded in a server platform. This service processor is called a Baseboard Management Controller (BMC) and resides on the server motherboard. The BMC links to a main processor and other on-board elements using a simple serial bus.

During normal operations, IPMI lets a server operating system obtain information about system health and control system hardware. For example, IPMI enables the monitoring of sensors, such as temperature, fan speeds and voltages, for proactive problem detection. If server temperature rises above specified levels, the server operating system can direct the BMC to increase fan speed or reduce processor speed to address the problem.

Configuring IPMI over LAN

Configure IPMI over LAN when you want to manage the CIMC with IPMI messages.

Before You Begin

You must log in with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope ipmi	Enters the IPMI command mode.
Step 2	Server /ipmi # set enabled {yes no}	Enables or disables IPMI access on this server.
Step 3	Server /ipmi # set privilege-level {readonly user admin}	Specifies the highest privilege level that can be assigned to an IPMI session on this server. This can be: <ul style="list-style-type: none"> • readonly — IPMI users can view information but cannot make any changes. If you select this option, IPMI users with the "Administrator", "Operator", or "User" user roles can only create read-only IPMI sessions, regardless of their other IPMI privileges. • user — IPMI users can perform some functions but cannot perform administrative tasks. If you select this option, IPMI users with the "Administrator" or "Operator" user role can create user and read-only sessions on this server. • admin — IPMI users can perform all available actions. If you select this option, IPMI users with the "Administrator" user role can create admin, user, and read-only sessions on this server.

	Command or Action	Purpose
Step 4	Server /ipmi # set encryption-key <i>key</i>	Sets the IPMI encryption key to use for IPMI communications. The key value must be 40 hexadecimal numbers.
Step 5	Server /ipmi # commit	Commits the transaction to the system configuration.

This example configures IPMI over LAN for the CIMC:

```

Server# scope ipmi
Server /ipmi # set enabled yes
Server /ipmi *# set privilege-level admin
Server /ipmi *# set encryption-key abcdef01234567890abcdef01234567890abcdef
Server /ipmi *# commit
Server /ipmi # show
Enabled Encryption Key                               Privilege Level Limit
-----
yes      abcdef01234567890abcdef01234567890abcdef admin
Server /ipmi #

```

Configuring SNMP

SNMP

The Cisco UCS C-Series Rack-Mount Servers support the Simple Network Management Protocol (SNMP) for viewing server configuration and status and for sending fault and alert information by SNMP traps. For information on Management Information Base (MIB) files supported by CIMC, see the *MIB Quick Reference for Cisco UCS* at this URL: http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/mib/reference/UCS_MIBRef.html.

Configuring SNMP Properties

Before You Begin

You must log in as a user with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope snmp	Enters SNMP command mode.
Step 2	Server /snmp # set enabled { yes no }	Enables or disables SNMP. Note SNMP must be enabled and saved before additional SNMP configuration commands are accepted.
Step 3	Server /snmp # commit	Commits the transaction to the system configuration.

	Command or Action	Purpose
Step 4	Server /snmp # set community-str <i>community</i>	Specifies the default SNMP v1 or v2c community name that CIMC includes on any trap messages it sends to the SNMP host. The name can be up to 18 characters.
Step 5	Server /snmp # setcommunity-access	This can be one of the following : Disabled, Limited, or Full.
Step 6	Server /snmp # settrap-community-str	Specifies the SNMP community group to which trap information should be sent. The name can be up to 18 characters
Step 7	Server /snmp # set sys-contact <i>contact</i>	Specifies the system contact person responsible for the SNMP implementation. The contact information can be up to 254 characters, such as an email address or a name and telephone number. To enter a value that contains spaces, you must enclose the entry with quotation marks.
Step 8	Server /snmp # set sys-location <i>location</i>	Specifies the location of the host on which the SNMP agent (server) runs. The location information can be up to 254 characters. To enter a value that contains spaces, you must enclose the entry with quotation marks.
Step 9	Server /snmp # commit	Commits the transaction to the system configuration.

This example configures the SNMP properties and commits the transaction:

```

Server# scope snmp
Server /snmp # set enabled yes
Server /snmp *# commit
Server /snmp # set community-str cimcpublish
Server /snmp # set community-access Full
Server /snmp # set trap-community-str public
Server /snmp *# set sys-contact "User Name <username@example.com> +1-408-555-1212"
Server /snmp *# set sys-location "San Jose, California"
Server /snmp *# commit
Server /snmp # show detail
SNMP Settings:
  SNMP Port: 161
  System Contact: User Name <username@example.com> +1-408-555-1212
  System Location: San Jose, California
  SNMP Community: cimcpublish
  SNMP Trap community: public
  SNMP Community access: Full
  Enabled: yes

Server /snmp #

```

What to Do Next

Configure SNMP trap settings as described in [Configuring SNMP Trap Settings](#), on page 153.

Configuring SNMP Trap Settings

Before You Begin

- You must log in with admin privileges to perform this task.
- SNMP must be enabled and saved before trap settings can be configured.

Procedure

	Command or Action	Purpose
Step 1	Server# scope snmp	Enters the SNMP command mode.
Step 2	Server /snmp # scope trap-destinations <i>number</i>	Enters the SNMP trap destination command mode for the specified destination. Four SNMP trap destinations are available. The destination <i>number</i> is an integer between 1 and 15.
Step 3	Server /snmp/trap-destinations # set enabled {yes no}	Enables or disables the SNMP trap destination.
Step 4	Server /snmp/trap-destinations # set version {1 2 3}	Specify the desired SNMP version of the trap message. Note SNMPv3 traps will be delivered only to locations where the SNMPv3 user and key values are configured correctly.
Step 5	Server /snmp/trap-destinations # set type {trap inform}	Specifies whether SNMP notification messages are sent as simple traps or as inform requests requiring acknowledgment by the receiver. Note The inform option can be chosen only for V2 users.
Step 6	Server /snmp/trap-destinations # set user <i>user</i>	
Step 7	Server /snmp/trap-destination # set v4-addr <i>ip-address</i>	Specifies the destination IP address to which SNMP trap information is sent.
Step 8	Server /snmp/trap-destination # commit	Commits the transaction to the system configuration.

This example configures general SNMP trap settings and trap destination number 1 and commits the transaction:

```

Server# scope snmp
Server /snmp # Scope trap-destinations 1
Server /snmp/trap-destination *# set enabled yes
Server /snmp/trap-destination *# set version 2
Server /snmp/trap-destination *# set type inform
Server /snmp/trap-destination *# set user user1
Server /snmp/trap-destination *# set v4-addr 192.2.3.4
Server /snmp/trap-destination *# commit
Server /snmp/trap-destination # show detail
Trap Destination 1:

```

```

Enabled: yes
SNMP version: 2
Trap type: inform
SNMP user: user1
IPv4 Address: 192.2.3.4
Delete Trap: no
Server /snmp/trap-destination #

```

Sending a Test SNMP Trap Message

Before You Begin

You must log in with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope snmp	Enters the SNMP command mode.
Step 2	Server /snmp # sendSNMPtrap	Sends an SNMP test trap to the configured SNMP trap destination that are enabled. Note The trap must be configured and enabled in order to send a test message.

This example sends a test message to all the enabled SNMP trap destinations:

```

Server# scope snmp
Server /snmp # sendSNMPtrap
SNMP Test Trap sent to the destination.
Server /snmp #

```

Configuring SNMPv3 Users

Before You Begin

- You must log in as a user with admin privileges to perform this task.
- SNMP must be enabled and saved before these configuration commands are accepted.

Procedure

	Command or Action	Purpose
Step 1	Server# scope snmp	Enters the SNMP command mode.
Step 2	Server /snmp # scope v3users <i>number</i>	Enters the SNMPv3 users command mode for the specified user number.
Step 3	Server /snmp/v3users # set v3add {yes no}	Adds or deletes an SNMPv3 user. This can be one of the following:

	Command or Action	Purpose
		<ul style="list-style-type: none"> • yes—This user is enabled as an SNMPv3 user and is allowed to access the SNMP OID tree. <p>Note The security name and security level must also be configured at this time or the user addition will fail.</p> <ul style="list-style-type: none"> • no—This user configuration is deleted.
Step 4	Server /snmp/v3users # set v3security-name <i>security-name</i>	Enter an SNMP username for this user.
Step 5	Server /snmp/v3users # set v3security-level { noauthnopriv authnopriv authpriv }	<p>Select a security level for this user. This can be one of the following:</p> <ul style="list-style-type: none"> • noauthnopriv—The user does not require an authorization or privacy password. • authnopriv—The user requires an authorization password but not a privacy password. If you select this option, you must configure an authentication key. • authpriv—The user requires both an authorization password and a privacy password. If you select this option, you must configure an authentication key and a private encryption key.
Step 6	Server /snmp/v3users # set v3proto { MD5 SHA }	Select an authentication protocol for this user.
Step 7	Server /snmp/v3users # set v3auth-key <i>auth-key</i>	Enter an authorization password for this user.
Step 8	Server /snmp/v3users # set v3priv-proto { DES AES }	Select an encryption protocol for this user.
Step 9	Server /snmp/v3users # set v3priv-auth-key <i>priv-auth-key</i>	Enter a private encryption key (privacy password) for this user.
Step 10	Server /snmp/v3users # commit	Commits the transaction to the system configuration.

This example configures SNMPv3 user number 2 and commits the transaction:

```

Server# scope snmp
Server /snmp # scope v3users 2
Server /snmp/v3users # set v3add yes
Server /snmp/v3users *# set v3security-name ucsSNMPV3user
Server /snmp/v3users *# set v3security-level authpriv
Server /snmp/v3users *# set v3proto SHA
Server /snmp/v3users *# set v3auth-key
Please enter v3auth-key:ex4mplek3y
Please confirm v3auth-key:ex4mplek3y
Server /snmp/v3users *# set v3priv-proto AES
Server /snmp/v3users *# set v3priv-auth-key

```

```
Please enter v3priv-auth-key:!1@2#3$4%5^6&7*8
Please confirm v3priv-auth-key:!1@2#3$4%5^6&7*8
Server /snmp/v3users *# commit
Settings are being applied ... allow a few minutes for the process to complete
Server /snmp/v3users # show detail
User 2:
  Add User: yes
  Security Name: ucsSNMPV3user
  Security Level: authpriv
  Auth Type: SHA
  Auth Key: *****
  Encryption: AES
  Private Key: *****

Server /snmp/v3users #
```



Managing Certificates

This chapter includes the following sections:

- [Managing the Server Certificate, page 157](#)
- [Generating a Certificate Signing Request, page 157](#)
- [Creating a Self-Signed Certificate, page 159](#)
- [Uploading a Server Certificate, page 161](#)

Managing the Server Certificate

You can generate a certificate signing request (CSR) to obtain a new certificate, and you can upload the new certificate to the CIMC to replace the current server certificate. The server certificate may be signed either by a public Certificate Authority (CA), such as Verisign, or by your own certificate authority.

Procedure

- Step 1** Generate the CSR from the CIMC.
 - Step 2** Submit the CSR file to a certificate authority that will issue and sign your certificate. If your organization generates its own self-signed certificates, you can use the CSR file to generate a self-signed certificate.
 - Step 3** Upload the new certificate to the CIMC.
- Note** The uploaded certificate must be created from a CSR generated by the CIMC. Do not upload a certificate that was not created by this method.

Generating a Certificate Signing Request

You can either generate a self-signed certificate manually using the **generate-csr** command, or automatically when you change the hostname. For information on changing the hostname and auto generation of the self-signed certificate, see [Configuring Common Properties, on page 81](#).

To manually generate a certificate signing request, follow these steps:

Before You Begin

You must log in as a user with admin privileges to configure certificates.

Procedure

	Command or Action	Purpose
Step 1	Server# scope certificate	Enters the certificate command mode.
Step 2	Server /certificate # generate-csr	Launches a dialog for the generation of a certificate signing request (CSR).

You will be prompted to enter the following information for the certificate signing request:

Common Name (CN)	The fully qualified hostname of the CIMC.
Organization Name (O)	The organization requesting the certificate.
Organization Unit (OU)	The organizational unit.
Locality (L)	The city or town in which the company requesting the certificate is headquartered.
StateName (S)	The state or province in which the company requesting the certificate is headquartered.
Country Code (CC)	The two-letter ISO country code for the country in which the company is headquartered.
Email	The administrative email contact at the company.

After you have entered the requested information, the system will generate and display a certificate signing request in the console output. A CSR file will not be created, but you can copy the CSR information from the console output and paste the information into a text file.

This example generates a certificate signing request:

```

Server# scope certificate
Server /certificate # generate-csr
Common Name (CN): test.example.com
Organization Name (O): Example, Inc.
Organization Unit (OU): Test Department
Locality (L): San Jose
StateName (S): CA
Country Code (CC): US
Email: user@example.com
Continue to generate CSR?[y|N]y

-----BEGIN CERTIFICATE REQUEST-----
MIIB/zCQAwgCAQAwgZkxCzAJBgNVBAYTA1VTMQswCQYDVQQIEwJDQTEVMBMGA1UE
BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBASt
ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG

```



```

9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCCyU
ZgAmivyCsKgb/6CjQtsofvzxmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBKOND1
GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAGMBAAGgJTAjBgkq
hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
gYEAG61CaJoJaVMhzC1903O6Mg51zq1zXcz75+VFj2I6rH9asckClD3mkOVx5gJU
Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtv1WvfhevskV0j6
mK3Ku+YiORnv6DhxrOoqau8r/hyI/L43l7IPN1HhOi3oha4=
-----END CERTIFICATE REQUEST-----

```

Copy everything from "-----BEGIN ..." to "END CERTIFICATE REQUEST-----", paste to a file, send to your chosen CA for signing, and finally upload the signed certificate via upload command.

---OR---

Continue to self sign CSR and overwrite the current certificate?
All HTTPS and SSH sessions will be disconnected. [y|N]**N**

What to Do Next

Perform one of the following tasks:

- If you do not want to obtain a certificate from a public certificate authority, and if your organization does not operate its own certificate authority, you can allow CIMC to internally generate a self-signed certificate from the CSR and upload it immediately to the server. Type **y** after the final prompt in the example to perform this action.
- If your organization operates its own certificate server for generating self-signed certificates, copy the command output from "-----BEGIN ..." to "END CERTIFICATE REQUEST-----" and paste to a file named `csr.txt`. Input the CSR file to your certificate server to generate a self-signed certificate.
- If you will obtain a certificate from a public certificate authority, copy the command output from "-----BEGIN ..." to "END CERTIFICATE REQUEST-----" and paste to a file named `csr.txt`. Submit the CSR file to the certificate authority to obtain a signed certificate.

If you did not use the first option, in which CIMC internally generates and uploads a self-signed certificate, you must upload the new certificate using the **upload** command in certificate command mode.

Creating a Self-Signed Certificate

As an alternative to using a public Certificate Authority (CA) to generate and sign a server certificate, you can operate your own CA and sign your own certificates. This section shows commands for creating a CA and generating a server certificate using the OpenSSL certificate server running on Linux. For detailed information about OpenSSL, see <http://www.openssl.org>.



Note

These commands are to be entered on a Linux server with the OpenSSL package, not in the CIMC CLI.

Before You Begin

Obtain and install a certificate server software package on a server within your organization.

Procedure

	Command or Action	Purpose
Step 1	openssl genrsa -out <i>CA_keyfilename</i> <i>keysize</i> Example: # openssl genrsa -out ca.key 1024	This command generates an RSA private key that will be used by the CA. Note To allow the CA to access the key without user input, do not use the -des3 option for this command. The specified file name contains an RSA key of the specified key size.
Step 2	openssl req -new -x509 -days <i>numdays</i> -key <i>CA_keyfilename</i> -out <i>CA_certfilename</i> Example: # openssl req -new -x509 -days 365 -key ca.key -out ca.crt	This command generates a new self-signed certificate for the CA using the specified key. The certificate is valid for the specified period. The command prompts the user for additional certificate information. The certificate server is an active CA.
Step 3	echo "nsCertType = server" > openssl.conf Example: # echo "nsCertType = server" > openssl.conf	This command adds a line to the OpenSSL configuration file to designate the certificate as a server-only certificate. This designation is a defense against a man-in-the-middle attack, in which an authorized client attempts to impersonate the server. The OpenSSL configuration file openssl.conf contains the statement "nsCertType = server".
Step 4	openssl x509 -req -days <i>numdays</i> -in <i>CSR_filename</i> -CA <i>CA_certfilename</i> -set_serial 04 -CAkey <i>CA_keyfilename</i> -out <i>server_certfilename</i> -extfile openssl.conf Example: # openssl x509 -req -days 365 -in csr.txt -CA ca.crt -set_serial 04 -CAkey ca.key -out myserver05.crt -extfile openssl.conf	This command directs the CA to use your CSR file to generate a server certificate. Your server certificate is contained in the output file.

This example shows how to create a CA and to generate a server certificate signed by the new CA. These commands are entered on a Linux server running OpenSSL.

```
# /usr/bin/openssl genrsa -out ca.key 1024
Generating RSA private key, 1024 bit long modulus
.....++++++
.....++++++
e is 65537 (0x10001)
# /usr/bin/openssl req -new -x509 -days 365 -key ca.key -out ca.crt
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
```

```

If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:US
State or Province Name (full name) [Berkshire]:California
Locality Name (eg, city) [Newbury]:San Jose
Organization Name (eg, company) [My Company Ltd]:Example Incorporated
Organizational Unit Name (eg, section) []:Unit A
Common Name (eg, your name or your server's hostname) []:example.com
Email Address []:admin@example.com
# echo "nsCertType = server" > openssl.conf
# /usr/bin/openssl x509 -req -days 365 -in csr.txt -CA ca.crt -set_serial 01 -CAkey ca.key -out server.crt
-extfile openssl.conf
Signature ok
subject=/C=US/ST=California/L=San Jose/O=Example Inc./OU=Unit
A/CN=example.com/emailAddress=john@example.com
Getting CA Private Key
#

```

What to Do Next

Upload the new certificate to the CIMC.

Uploading a Server Certificate

Before You Begin

You must log in as a user with admin privileges to upload a certificate.

The certificate to be uploaded must be available as readable text. During the upload procedure, you will copy the certificate text and paste it into the CLI.



Note

You must first generate a CSR using the CIMC certificate management CSR generation procedure, and you must use that CSR to obtain the certificate for uploading. Do not upload a certificate that was not obtained by this method.



Note

All current HTTPS and SSH sessions are disconnected when the new server certificate is uploaded.

Procedure

	Command or Action	Purpose
Step 1	Server# scope certificate	Enters the certificate command mode.
Step 2	Server /certificate # upload	Launches a dialog for entering and uploading the new server certificate.

Copy the certificate text, paste it into the console when prompted, and type CTRL+D to upload the certificate.

This example uploads a new certificate to the server:

```
Server# scope certificate
Server /certificate # upload
Please paste your certificate here, when finished, press CTRL+D.
-----BEGIN CERTIFICATE-----
MIIB/zCCAwgCAQAwgZkxCzAJBgNVBAYTA1VTMQswCQYDVQQIEwJDQTEVMBMGA1UE
BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGx1IEluYy4xEzARBgNVBASt
C1Rlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
ZgAMivYCsKgb/6CjQtsofvzxmc/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBKOND1
GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bf5wZVNAGMBAAGgJTAjBgkq
hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
gYEAG61CaJoJaVMhzC190306Mg51zq1zXcz75+VFj2I6rH9asckCl3mkOVx5gJU
Ptt5CVQpNgNldvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvLWvfhevskV0j6
mK3Ku+YiORnv6DhxrOoqau8r/hyI/L4317IPN1HhOi3oha4=
-----END CERTIFICATE-----
<CTRL+D>
```



Configuring Platform Event Filters

This chapter includes the following sections:

- [Platform Event Filters, page 163](#)
- [Enabling Platform Event Alerts, page 163](#)
- [Disabling Platform Event Alerts, page 164](#)
- [Configuring Platform Event Filters, page 164](#)
- [Configuring Platform Event Trap Settings, page 166](#)
- [Interpreting Platform Event Traps, page 167](#)

Platform Event Filters

A platform event filter (PEF) can trigger an action and generate an alert when a critical hardware-related event occurs. For each PEF, you can choose the action to be taken (or take no action) when a platform event occurs. You can also choose to generate and send an alert when a platform event occurs. Alerts are sent as an SNMP trap, so you must configure an SNMP trap destination before the alerts can be sent.

You can globally enable or disable the generation of platform event alerts. When disabled, alerts are not sent even if PEFs are configured to send them.

Enabling Platform Event Alerts

Procedure

	Command or Action	Purpose
Step 1	Server# scope fault	Enters the fault command mode.
Step 2	Server /fault # set platform-event-enabled yes	Enables platform event alerts.

	Command or Action	Purpose
Step 3	Server /fault # commit	Commits the transaction to the system configuration.
Step 4	Server /fault # show [detail]	(Optional) Displays the platform event alert configuration.

The following example enables platform event alerts:

```
Server# scope fault
Server /fault # set platform-event-enabled yes
Server /fault *# commit
Server /fault # show
SNMP Community String Platform Event Enabled
-----
public                               yes
Server /fault #
```

Disabling Platform Event Alerts

Procedure

	Command or Action	Purpose
Step 1	Server# scope fault	Enters the fault command mode.
Step 2	Server /fault # set platform-event-enabled no	Disables platform event alerts.
Step 3	Server /fault # commit	Commits the transaction to the system configuration.
Step 4	Server /fault # show [detail]	(Optional) Displays the platform event alert configuration.

The following example disables platform event alerts:

```
Server# scope fault
Server /fault # set platform-event-enabled no
Server /fault *# commit
Server /fault # show
SNMP Community String Platform Event Enabled
-----
public                               no
Server /fault #
```

Configuring Platform Event Filters

You can configure actions and alerts for the following platform event filters:

ID	Platform Event Filter
1	Temperature Critical Assert Filter
2	Temperature Warning Assert Filter
3	Voltage Critical Assert Filter
4	Current Assert Filter
5	Fan Critical Assert Filter
6	Processor Assert Filter
7	Power Supply Critical Assert Filter
8	Power Supply Warning Assert Filter
9	Power Supply Redundancy Lost Filter
10	Discrete Power Supply Assert Filter
11	Memory Assert Filter
12	Drive Slot Assert Filter

Procedure

	Command or Action	Purpose
Step 1	Server# scope fault	Enters the fault command mode.
Step 2	Server /fault # scope pef id	Enters the platform event filter command mode for the specified event. See the Platform Event Filter table for event ID numbers.
Step 3	Server /fault/pef# set action { none reboot power-cycle power-off }	Selects the desired system action when this event occurs. The action can be one of the following: <ul style="list-style-type: none"> • none —No system action is taken. • reboot —The server is rebooted. • power-cycle —The server is power cycled. • power-off —The server is powered off.
Step 4	Server /fault/pef# set send-alert { yes no }	Enables or disables the sending of a platform event alert for this event.

	Command or Action	Purpose
		Note For an alert to be sent, the filter trap settings must be configured properly and platform event alerts must be enabled.
Step 5	Server /fault/pef # commit	Commits the transaction to the system configuration.

This example configures the platform event alert for an event:

```

Server# scope fault
Server /fault # scope pef 11
Server /fault/pef # set action reboot
Server /fault/pef *# set send-alert yes
Server /fault/pef *# commit
Server /fault/pef # show
Platform Event Filter Event          Action      Send Alert
-----
11          Memory Assert Filter    reboot      yes
Server /fault/pef #

```

What to Do Next

If you configure any PEFs to send an alert, enable platform event alerts.

Configuring Platform Event Trap Settings

Before You Begin

You must log in with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope fault	Enters the fault command mode.
Step 2	Server /fault # scope pef-destinations	Enters the platform event filter destinations command mode.
Step 3	Server /fault /pef-destinations # set enabled yes	Enables the platform event trap destination.
Step 4	Server /fault /pef-destinations # set addr <i>IP Address</i>	Specifies the destination IP address to which platform event trap information is sent.
Step 5	Server /fault /pef-destinations # commit	Commits the transaction to the system configuration.

This example configures general platform event trap settings and trap destination number 1 and commits the transaction:

```
Server# scope fault
Server /fault # scope pef-destination 1
Server /fault /pef-destinations *# set enabled yes
Server /fault /pef-destinations *# set addr 1.2.3.4
Server /fault /pef-destinations *# commit
Server /fault /pef-destinations # show

Trap Destination 1:
  IP Address: 1.2.3.4
  Enabled: yes

Server /fault /pef-destinations #
```

Interpreting Platform Event Traps

A CIMC platform event alert contains an enterprise object identifier (OID) in the form 1.3.6.1.4.1.3183.1.1.0.event. The first ten fields of the OID represent the following information: iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).wired_for_management(3183).PET(1).version(1).version(0), indicating an IPMI platform event trap (PET) version 1.0 message. The last field is an event number, indicating the specific condition or alert being notified.

Platform Event Trap Descriptions

The following table provides a description of the event being notified in a platform event trap message, based on the event number in the trap OID.

Event Number [Note 1]		Platform Event Description
0	0h	Test Trap
65799	010107h	Temperature Warning
65801	010109h	Temperature Critical
131330	020102h	Under Voltage, Critical
131337	020109h	Voltage Critical
196871	030107h	Current Warning
262402	040102h	Fan Critical
459776	070400h	Processor related (IOH-Thermalert/Caterr sensor) – predictive failure deasserted
459777	070401h	Processor related (IOH-Thermalert/Caterr sensor) – predictive failure asserted
460032	070500h	Processor Power Warning – limit not exceeded
460033	070501h	Processor Power Warning – limit exceeded
524533	0800F5h	Power Supply Critical
524551	080107h	Power Supply Warning

Event Number [Note 1]		Platform Event Description
525313	080401h	Discrete Power Supply Warning
527105	080B01h	Power Supply Redundancy Lost
527106	080B02h	Power Supply Redundancy Restored
552704	086F00h	Power Supply Inserted
552705	086F01h	Power Supply Failure
552707	086F03h	Power Supply AC Lost
786433	0C0001h	Correctable ECC Memory Errors, Release 1.3(1) and later releases, filter set to accept all reading types [Note 4]
786439	0C0007h	DDR3_INFO sensor LED - RED bit asserted (Probable ECC error on a DIMM), Generic Sensor [Notes 2,3]
786689	0C0101h	Correctable ECC Memory Errors, Release 1.3(1) and later releases
818945	0C7F01h	Correctable ECC Memory Errors, Release 1.2(x) and earlier releases
818951	0C7F07h	DDR3_INFO sensor LED - RED bit asserted (Probable ECC error on a DIMM), 1.2(x) and earlier releases [Note 3]
851968	0D0000h	HDD sensor indicates no fault, Generic Sensor [Note 2]
851972	0D0004h	HDD sensor indicates a fault, Generic Sensor [Note 2]
854016	0D0800h	HDD Absent, Generic Sensor [Note 2]
854017	0D0801h	HDD Present, Generic Sensor [Note 2]
880384	0D6F00h	HDD Present, no fault indicated
880385	0D6F01h	HDD Fault
880512	0D6F80h	HDD Not Present
880513	0D6F81h	HDD is deasserted but not in a fault state
884480	0D7F00h	Drive Slot LED Off
884481	0D7F01h	Drive Slot LED On
884482	0D7F02h	Drive Slot LED fast blink
884483	0D7F03h	Drive Slot LED slow blink
884484	0D7F04h	Drive Slot LED green
884485	0D7F05h	Drive Slot LED amber
884486	0D7F01h	Drive Slot LED blue
884487	0D7F01h	Drive Slot LED read
884488	0D7F08h	Drive Slot Online
884489	0D7F09h	Drive Slot Degraded

Event Number [Note 1]	Platform Event Description
Note 1: Basic information about the event number format can be found in the <i>IPMI Platform Event Trap Format Specification v1.0</i> at this URL: ftp://download.intel.com/design/servers/ipmi/pet100.pdf .	
Note 2: Some platforms and releases use generic sensor implementations, while some use Cisco proprietary sensor implementations.	
Note 3: In Release 1.3(1) and later releases, the ECC sensor no longer activates the LED.	
Note 4: When the event filter is set to accept all reading types, bits 15:8 of the hex event number are masked to 0. For example, event number 786689 (0C0101h) becomes 786433 (0C0001h).	



CIMC Firmware Management

This chapter includes the following sections:

- [Overview of Firmware, page 171](#)
- [Obtaining Firmware from Cisco, page 172](#)
- [Installing CIMC Firmware from a Remote Server, page 173](#)
- [Activating Installed CIMC Firmware, page 174](#)
- [Installing BIOS Firmware from a Remote Server, page 176](#)

Overview of Firmware

C-Series servers use Cisco-certified firmware specific to the C-Series server model that you are using. You can download new releases of the firmware for all supported server models from Cisco.com.



Caution

When you install new BIOS firmware, it must be from the same software release as the CIMC firmware running on the server. Do not install new BIOS firmware until after you have activated the matching CIMC firmware or the server will not boot.

To avoid potential problems, we strongly recommend that you use the Cisco Host Upgrade Utility (HUU), which upgrades the BIOS, CIMC, and other firmware to compatible levels. For detailed information about this utility, see the *Cisco Host Upgrade Utility Guide* for the version of the HUU that goes with the CIMC software release that you want to install. The HUU guides are available at the following URL: http://www.cisco.com/en/US/products/ps10493/products_user_guide_list.html.

If you elect to update the firmware manually, you must update the CIMC firmware first. The CIMC firmware update process is divided into the following stages to minimize the amount of time the server will be offline:

- **Installation.** During this stage, CIMC installs the selected CIMC firmware in the non-active, or backup, slot on the server.
- **Activation.** During this stage, CIMC sets the non-active firmware version as active and reboots the server, causing a disruption in service. When the server reboots, the firmware in the new active slot becomes the running version.

After you activate the CIMC firmware, you can update the BIOS firmware. The server must be powered off during the entire BIOS update process, so the process is not divided into stages. Instead, you only need to issue a single command and CIMC installs and updates the BIOS firmware as quickly as possible. Once the CIMC finishes rebooting, the server can be powered on and returned to service.



Note You can either upgrade an older firmware version to a newer one, or downgrade a newer firmware version to an older one.

Obtaining Firmware from Cisco

Procedure

- Step 1** Navigate to <http://www.cisco.com/>.
- Step 2** If you are not already logged in, click **Log In** at the top right-hand edge of the page and log in using your Cisco.com credentials.
- Step 3** In the menu bar at the top, click **Support**.
- Step 4** Click **All Downloads** in the roll down menu.
- Step 5** If your server model is listed in the **Recently Used Products** list, click the server name. Otherwise, do the following:
 - a) In the left-hand box, click **Products**.
 - b) In the center box, click **Unified Computing and Servers**.
 - c) In the right-hand box, click **Cisco UCS C-Series Rack-Mount Standalone Server Software**.
 - d) In the right-hand box, click the server model whose software you want to download.
- Step 6** Click the **Unified Computing System (UCS) Server Firmware** link.
- Step 7** (Optional) Select a prior release from the menu bar on the left-hand side of the page.
- Step 8** Click the **Download** button associated with the Cisco Host Upgrade Utility ISO for the selected release.
- Step 9** Click **Accept License Agreement**.
- Step 10** Save the ISO file to a local drive.
We recommend you upgrade the CIMC and BIOS firmware on your server using this ISO file, which contains the Cisco Host Upgrade Utility. For detailed information about this utility, see the *Cisco Host Upgrade Utility Guide* for the version of the HUU that goes with the CIMC software release that you want to install. The HUU guides are available at the following URL: http://www.cisco.com/en/US/products/ps10493/products_user_guide_list.html.
- Step 11** (Optional) If you plan to upgrade the CIMC and BIOS firmware manually, do the following:
 - a) From the ISO file, open the ZIP file containing the firmware installation files.
The ZIP file is on the top-level of the ISO file, and its name follows the format `ServerModel_ReleaseNumber.ZIP`.
For example, `C240M3_1.4.4A.ZIP`.
You do not need to extract all of the files contained in this ZIP file. Instead, you only need to open it so that you can access the BIOS firmware installation CAP file and the ZIP file containing the CIMC firmware installation BIN file.

- b) From the *ServerModel_ReleaseNumber*.ZIP file, extract the BIOS firmware installation CAP file and save it to your local drive.
The CAP file is in the *ReleaseNumber/bios/cimc* folder, and its name follows the format *Server-BIOS-Release-Number.CAP*.
For example, *1.4.4a/bios/cimc/C240-BIOS-1-4-4c-0.CAP*.
- c) From the *ServerModel_ReleaseNumber*.ZIP file, open the ZIP file containing the CIMC firmware installation files.
The ZIP file is in the *ReleaseNumber/cimc* folder and its name follows the format *server-model-cimc-release.zip*.
For example, *1.4.4a/cimc/c240-m3-cimc.1.4.4a.zip*.
You do not need to extract all of the files contained in this zip file. Instead, you only need to open it so that you can access the CIMC firmware installation BIN file.
- d) From the *server-model-cimc-release.zip* file, extract the full CIMC firmware installation BIN file and save it to your local drive.
The BIN file is in the *server-model-cimc-release* folder and its name follows the format *upd-pkg-server-model-cimc.full.release.bin*.
For example, *c240-m3-cimc.1.4.4a/upd-pkg-c240-m3-cimc.full.1.4.4a.bin*.

Step 12 (Optional) If you plan to install the firmware from a remote server, copy the BIOS installation CAP file and the CIMC installation BIN file to the remote server you want to use.
The remote server can be one of the following:

- TFTP
- FTP
- SFTP
- SCP
- HTTP

The server must have read permission for the destination folder on the remote server.

What to Do Next

Use the Cisco Host Upgrade Utility to upgrade all firmware on the server or manually install the CIMC firmware on the server.

Installing CIMC Firmware from a Remote Server

Before You Begin

- Log in to the CIMC CLI as a user with admin privileges.
- Obtain the Cisco Host Upgrade Utility ISO file from Cisco.com and extract the firmware installation files as described in [Obtaining Firmware from Cisco, on page 172](#).

**Note**

If you start an update while an update is already in process, both updates will fail.

Procedure

	Command or Action	Purpose
Step 1	Server# scope cimc	Enters the CIMC command mode.
Step 2	Server /cimc # scope firmware	Enters the CIMC firmware command mode.
Step 3	Server /cimc/firmware # update <i>protocol IP Address path</i>	Specifies the protocol, IP address of the remote server and the file path to the firmware file on the server. The protocol can be one of the following: <ul style="list-style-type: none"> • TFTP • FTP • SFTP • SCP • HTTP
Step 4	Server /cimc/firmware # show detail	(Optional) Displays the progress of the firmware update.

This example updates the CIMC firmware:

```
Server# scope cimc
Server /cimc # scope firmware
Server /cimc/firmware # update ftp 192.0.20.34 //test/dnld-ucs-k9-bundle.1.0.2h.bin
<CR> Press Enter key
Firmware update has started.
Please check the status using "show detail"
Server /cimc/firmware #
```

What to Do Next

Activate the new firmware.

Activating Installed CIMC Firmware

Before You Begin

Install the CIMC firmware on the server.

**Important**

While the activation is in progress, do not:

- Reset, power off, or shut down the server.
- Reboot or reset CIMC.
- Activate any other firmware.
- Export technical support or configuration data.

Procedure

	Command or Action	Purpose
Step 1	Server# scope cimc	Enters the CIMC command mode.
Step 2	Server /cimc # scope firmware	Enters the firmware command mode.
Step 3	Server /cimc/firmware # show detail	Displays the available firmware images and status.
Step 4	Server /cimc/firmware # activate [1 2]	Activates the selected image. If no image number is specified, the server activates the currently inactive image.
Step 5	At the prompt, enter y to activate the selected firmware image.	The BMC reboots, terminating all CLI and GUI sessions until the reboot completes.
Step 6	Log back into the CLI and repeat steps 1–3 to verify the activation.	(Optional)

This example activates firmware image 1 and then verifies the activation after the BMC reboots:

```

Server# scope cimc
Server /cimc # scope firmware
Server /cimc/firmware # show detail
Firmware Image Information:
  Update Stage: NONE
  Update Progress: 100
  Current FW Version: 1.3(3a)
  FW Image 1 Version: 1.4(3j)
  FW Image 1 State: BACKUP INACTIVATED
  FW Image 2 Version: 1.3(3a)
  FW Image 2 State: RUNNING ACTIVATED
  Boot-loader Version: 1.4(3.21).18

Server /cimc/firmware # activate 1
This operation will activate firmware 1 and reboot the BMC.
Continue?[y|N]y
.
.
-- BMC reboot --
.
.
-- Log into CLI as Admin --

Server# scope cimc

```

```

Server /cimc # scope firmware
Server /cimc/firmware # show detail
Firmware Image Information:
  Update Stage: NONE
  Update Progress: 100
  Current FW Version: 1.4(3j)
  FW Image 1 Version: 1.4(3j)
  FW Image 1 State: RUNNING ACTIVATED
  FW Image 2 Version: 1.3(3a)
  FW Image 2 State: BACKUP INACTIVATED
  Boot-loader Version: 1.4(3.21).18

```

Installing BIOS Firmware from a Remote Server



Note

This procedure is not available on some servers. For other BIOS installation methods, see the *Cisco UCS C-Series Rack-Mount Server BIOS Upgrade Guide* available at the following URL: http://www.cisco.com/en/US/docs/unified_computing/ucs/c/sw/bios/b_Upgrading_BIOS_Firmware.html.

Before You Begin

- Log in to the CIMC CLI as a user with admin privileges.
- Activate the CIMC firmware that goes with the BIOS version you want to install, as described in [Activating Installed CIMC Firmware](#), on page 174.
- Power off the server.



Note

If you start an update while an update is already in process, both updates will fail.

Procedure

	Command or Action	Purpose
Step 1	Server# scope cimc	Enters the CIMC command mode.
Step 2	Server /cimc # scope firmware	Enters the firmware command mode.
Step 3	Server /cimc/firmware # show detail	Displays the available firmware images and status.
Step 4	Make sure the firmware version shown in the Current FW Version field matches the BIOS firmware version you are installing.	Important If the CIMC firmware version does not match, activate the CIMC firmware before continuing with this procedure or the server will not boot. For details, see Activating Installed CIMC Firmware , on page 174.
Step 5	Server /cimc/firmware # top	Returns to the server root level.
Step 6	Server# scope bios	Enters the BIOS command mode.

	Command or Action	Purpose
Step 7	Server /bios # update protocol	Specifies the protocol to be used. It can be TFTP, FTP, SFTP, SCP or HTTP.
Step 8	Server /bios # update IP Address	Specifies the IP address or the host name of the remote server.
Step 9	Server /bios # update path	Specifies the file path to the BIOS firmware file on the remote server.

This example updates the BIOS firmware to CIMC software release 1.4(3j):

```

Server# scope cimc
Server /cimc # scope firmware
Server /cimc/firmware # show detail
Firmware Image Information:
  Update Stage: NONE
  Update Progress: 100
  Current FW Version: 1.4(3j)
  FW Image 1 Version: 1.4(3j)
  FW Image 1 State: RUNNING ACTIVATED
  FW Image 2 Version: 1.3(3a)
  FW Image 2 State: BACKUP INACTIVATED
  Boot-loader Version: 1.4(3.21).18
Server /cimc/firmware # top
Server # scope bios
Server /bios # update ftp 192.0.20.34 //upgrade_bios_files/C260-BIOS-1-4-3j-0.CAP
<CR> Press Enter key
Firmware update has started.
Please check the status using "show detail"
Server /bios #

```




Viewing Faults and Logs

This chapter includes the following sections:

- [Viewing the Faults and Logs Summary, page 179](#)
- [CIMC Log, page 180](#)
- [System Event Log, page 184](#)

Viewing the Faults and Logs Summary

Procedure

	Command or Action	Purpose
Step 1	Server # scope fault	Enters fault command mode.
Step 2	Server # show fault-entries	Displays a log of all the faults.

This example displays a summary of faults:

```
Server # scope fault
Server /fault # show fault-entries
Time                Severity      Description
-----
Sun Jun 27 04:00:52 2013  info      Storage Local disk 12 missing
Sat Jun 26 05:00:22 2013  warning   Power Supply redundancy is lost

Server /fault #
```

CIMC Log

Viewing the CIMC Log

Procedure

	Command or Action	Purpose
Step 1	Server# scope cimc	Enters the CIMC command mode.
Step 2	Server /cimc # scope log	Enters the CIMC log command mode.
Step 3	Server /cimc/log # show entries [detail]	Displays CIMC events, including timestamp, the software module that logged the event, and a description of the event.

This example displays the log of CIMC events:

```

Server# scope cimc
Server /cimc # scope log
Server /cimc/log # show entries
Time                Severity      Source                Description
-----
2012 Jan 30 05:20:45 Informational BMC:ciscoNET:961 " rpc_aim_callback_function_1_svc() -
result == SUCCESS, callbackData size: 600 "
2012 Jan 30 05:20:45 Informational BMC:ciscoNET:961 rpc_aim_callback_function_1_svc() -
returned from pFunctionCallback result:0
2012 Jan 30 05:20:45 Informational BMC:ciscoNET:961 " rpc_aim_callback_function_1_svc() -
szFunctionName:netGetCurrentIfConfig nSize:0 nMaxSize: 600 "
--More--

Server /cimc/log # show entries detail
Trace Log:
  Time: 2012 Jan 30 05:20:45
  Severity: Informational
  Source: BMC:ciscoNET:961
  Description: " rpc_aim_callback_function_1_svc() - result == SUCCESS, callbackData size:
600 "
  Order: 0
Trace Log:
  Time: 2012 Jan 30 05:20:45
  Severity: Informational
  Source: BMC:ciscoNET:961
  Description: rpc_aim_callback_function_1_svc() - returned from pFunctionCallback result:0
  Order: 1
Trace Log:
  Time: 2012 Jan 30 05:20:45
  Severity: Informational
  Source: BMC:ciscoNET:961
  Description: " rpc_aim_callback_function_1_svc() - szFunctionName:netGetCurrentIfConfig
nSize:0 nMaxSize: 600 "
  Order: 2
--More--

Server /cimc/log #

```

Clearing the CIMC Log

Procedure

	Command or Action	Purpose
Step 1	Server# scope cimc	Enters the CIMC command mode.
Step 2	Server /cimc # scope log	Enters the CIMC log command mode.
Step 3	Server /cimc/log # clear	Clears the CIMC log.

The following example clears the log of CIMC events:

```
Server# scope cimc
Server /cimc # scope log
Server /cimc/log # clear
```

Configuring the CIMC Log Threshold

You can specify the lowest level of messages that will be included in the CIMC log.

Procedure

	Command or Action	Purpose
Step 1	Server# scope cimc	Enters the CIMC command mode.
Step 2	Server /cimc # scope log	Enters the CIMC log command mode.
Step 3	Server /cimc/log # set local-syslog-severity level	<p>The severity <i>level</i> can be one of the following, in decreasing order of severity:</p> <ul style="list-style-type: none"> • emergency • alert • critical • error • warning • notice • informational • debug

	Command or Action	Purpose
		Note CIMC does not log any messages with a severity below the selected severity. For example, if you select error , then the CIMC log will contain all messages with the severity Emergency, Alert, Critical, or Error. It will not show Warning, Notice, Informational, or Debug messages.
Step 4	Server /cimc/log # commit	Commits the transaction to the system configuration.
Step 5	Server /cimc/log # show local-syslog-severity	(Optional) Displays the configured severity level.

This example shows how to configure the logging of messages with a minimum severity of Warning:

```
Server# scope cimc
Server /cimc # scope log
Server /cimc/log # set local-syslog-severity warning
Server /cimc/log *# commit
Server /cimc/log # show local-syslog-severity
Local Syslog Severity: warning

Server /cimc/log #
```

Sending the CIMC Log to a Remote Server

You can configure profiles for one or two remote syslog servers to receive CIMC log entries.

Before You Begin

- The remote syslog server must be configured to receive logs from a remote host.
- The remote syslog server must be configured to receive all types of logs, including authentication-related logs.
- The remote syslog server's firewall must be configured to allow syslog messages to reach the syslog server.

Procedure

	Command or Action	Purpose
Step 1	Server# scope cimc	Enters the CIMC command mode.
Step 2	Server /cimc # scope log	Enters the CIMC log command mode.
Step 3	Server /cimc/log # set remote-syslog-severity level	(Optional) The severity <i>level</i> can be one of the following, in decreasing order of severity: <ul style="list-style-type: none"> • emergency • alert

	Command or Action	Purpose
		<ul style="list-style-type: none"> • critical • error • warning • notice • informational • debug <p>Note CIMC does not remotely log any messages with a severity below the selected severity. For example, if you select error, then the remote syslog server will receive all CIMC log messages with the severity Emergency, Alert, Critical, or Error. It will not show Warning, Notice, Informational, or Debug messages.</p>
Step 4	Server /cimc/log # scope server {1 2}	Selects one of the two remote syslog server profiles and enters the command mode for configuring the profile.
Step 5	Server /cimc/log/server # set server-ip ip-address	Specifies the remote syslog server IP address.
Step 6	Server /cimc/log/server # set enabled {yes no}	Enables the sending of CIMC log entries to this syslog server.
Step 7	Server /cimc/log/server # commit	Commits the transaction to the system configuration.

This example shows how to configure a remote syslog server profile and enable the sending of CIMC log entries with a minimum severity level of Warning:

```

Server# scope cimc
Server /cimc # scope log
Server /cimc/log # set remote-syslog-severity warning
Server /cimc/log *# scope server 2
Server /cimc/log/server *# set server-ip 192.0.2.34
Server /cimc/log/server *# set enabled yes
Server /cimc/log/server *# commit
Server /cimc/log/server # exit
Server /cimc/log # show server
Syslog Server      IP Address      Enabled
-----
1                  0.0.0.0        no
2                  192.0.2.34     yes

Server /cimc/log # show remote-syslog-severity
Remote Syslog Severity: warning

Server /cimc/log #

```

System Event Log

Viewing the System Event Log

Procedure

	Command or Action	Purpose
Step 1	Server# scope sel	Enters the system event log (SEL) command mode.
Step 2	Server /sel # show entries [detail]	For system events, displays timestamp, the severity of the event, and a description of the event. The detail keyword displays the information in a list format instead of a table format.

This example displays the system event log:

```

Server# scope sel
Server /sel # show entries
Time                Severity      Description
-----
[System Boot]       Informational " LED_PSU_STATUS: Platform sensor, OFF event was asserted"

[System Boot]       Informational " LED_HLTH_STATUS: Platform sensor, GREEN was asserted"
[System Boot]       Normal      " PSU_REDUNDANCY: PS Redundancy sensor, Fully Redundant
was asserted"
[System Boot]       Normal      " PSU2 PSU2_STATUS: Power Supply sensor for PSU2, Power
Supply input lost (AC/DC) was deasserted"
[System Boot]       Informational " LED_PSU_STATUS: Platform sensor, ON event was asserted"

[System Boot]       Informational " LED_HLTH_STATUS: Platform sensor, AMBER was asserted"
[System Boot]       Critical    " PSU_REDUNDANCY: PS Redundancy sensor, Redundancy Lost
was asserted"
[System Boot]       Critical    " PSU2 PSU2_STATUS: Power Supply sensor for PSU2, Power
Supply input lost (AC/DC) was asserted"
[System Boot]       Normal      " HDD_01_STATUS: Drive Slot sensor, Drive Presence was
asserted"
[System Boot]       Critical    " HDD_01_STATUS: Drive Slot sensor, Drive Presence was
deasserted"
[System Boot]       Informational " DDR3_P2_D1_INFO: Memory sensor, OFF event was asserted"

2001-01-01 08:30:16 Warning      " PSU2 PSU2_VOUT: Voltage sensor for PSU2, failure event
was deasserted"
2001-01-01 08:30:16 Critical      " PSU2 PSU2_VOUT: Voltage sensor for PSU2, non-recoverable
event was deasserted"
2001-01-01 08:30:15 Informational " LED_PSU_STATUS: Platform sensor, ON event was asserted"

2001-01-01 08:30:15 Informational " LED_HLTH_STATUS: Platform sensor, AMBER was asserted"
2001-01-01 08:30:15 Informational " LED_HLTH_STATUS: Platform sensor, FAST BLINK event was
asserted"
2001-01-01 08:30:14 Non-Recoverable " PSU2 PSU2_VOUT: Voltage sensor for PSU2, non-recoverable
event was asserted"
2001-01-01 08:30:14 Critical      " PSU2 PSU2_VOUT: Voltage sensor for PSU2, failure event
was asserted"
--More--

```

Clearing the System Event Log

Procedure

	Command or Action	Purpose
Step 1	Server# scope sel	Enters the system event log command mode.
Step 2	Server /sel # clear	You are prompted to confirm the action. If you enter y at the prompt, the system event log is cleared.

This example clears the system event log:

```
Server# scope sel
Server /sel # clear
This operation will clear the whole sel.
Continue?[y|N]y
```




Server Utilities

This chapter includes the following sections:

- [Exporting Technical Support Data, page 187](#)
- [Rebooting the CIMC, page 189](#)
- [Clearing the BIOS CMOS, page 189](#)
- [Recovering from a Corrupted BIOS, page 190](#)
- [Resetting the CIMC to Factory Defaults, page 191](#)
- [Exporting and Importing the CIMC Configuration, page 192](#)
- [Generating Non maskable Interrupts to the Host, page 194](#)

Exporting Technical Support Data

Perform this task when requested by the Cisco Technical Assistance Center (TAC). This utility creates a summary report containing configuration information, logs and diagnostic data that will help TAC in troubleshooting and resolving a technical issue.



Important

If any firmware or BIOS updates are in progress, do not export the technical support data until those tasks are complete.

Procedure

	Command or Action	Purpose
Step 1	Server# scope cimc	Enters the CIMC command mode.
Step 2	Server /cimc # scope tech-support	Enters the tech-support command mode.
Step 3	Server /cimc/tech-support # set remote-ip ip-address	Specifies the IP address of the remote server on which the technical support data file should be stored.

	Command or Action	Purpose
Step 4	Server /cimc/tech-support # set remote-path <i>path/filename</i>	Specifies the file name in which the support data should be stored on the remote server. When you enter this name, include the relative path for the file from the top of the server tree to the desired location. Tip To have the system auto-generate the file name, enter the file name as default.tar.gz.
Step 5	Server /cimc/tech-support # set remote-protocol <i>protocol</i>	Specifies the protocol to connect to the remote server. It can be of the following types: <ul style="list-style-type: none"> • tftp • ftp • sftp • scp • http
Step 6	Server /cimc/tech-support # set remote-username <i>name</i>	Specifies the user name on the remote server on which the technical support data file should be stored. This field does not apply if the protocol is TFTP or HTTP.
Step 7	Server /cimc/tech-support # set remote-password <i>password</i>	Specifies the password on the remote server on which the technical support data file should be stored. This field does not apply if the protocol is TFTP or HTTP.
Step 8	Server /cimc/tech-support # commit	Commits the transaction to the system configuration.
Step 9	Server /cimc/tech-support # start	Begins the transfer of the data file to the remote server.
Step 10	Server /cimc/tech-support # show detail	(Optional) Displays the progress of the transfer of the data file to the remote server.
Step 11	Server /cimc/tech-support # cancel	(Optional) Cancels the transfer of the data file to the remote server.

This example creates a technical support data file and transfers the file to a TFTP server:

```

Server# scope cimc
Server /cimc # scope tech-support
Server /cimc/tech-support # set remote-ip 192.0.20.41
Server /cimc/tech-support* # set remote-protocol tftp
Server /cimc/tech-support* # set remote-path /user/user1/default.tar.gz
Server /cimc/tech-support* # commit
Server /cimc/tech-support # start
Tech Support upload started.

Server /cimc/tech-support # show detail

Tech Support:
  Server Address: 192.0.20.41
  Path: default.tar.gz

```

```

Protocol: tftp
Username:
Password: *****
Progress (%): 5
Status: Collecting

```

```
Server /cimc/tech-support #
```

What to Do Next

Provide the generated report file to Cisco TAC.

Rebooting the CIMC

On rare occasions, such as an issue with the current running firmware, troubleshooting a server may require you to reboot the CIMC. This procedure is not part of the normal maintenance of a server. After you reboot the CIMC, you are logged off and the CIMC will be unavailable for a few minutes.



Note

If you reboot the CIMC while the server is performing power-on self test (POST) or is operating in the Extensible Firmware Interface (EFI) shell, the server will be powered down until the CIMC reboot is complete.

Procedure

	Command or Action	Purpose
Step 1	Server# scope cimc	Enters the CIMC command mode.
Step 2	Server /cimc # reboot	The CIMC reboots.

This example reboots the CIMC:

```

Server# scope cimc
Server /cimc # reboot

```

Clearing the BIOS CMOS

On rare occasions, troubleshooting a server may require you to clear the server's BIOS CMOS memory. This procedure is not part of the normal maintenance of a server.

Procedure

	Command or Action	Purpose
Step 1	Server# scope bios	Enters the bios command mode.

	Command or Action	Purpose
Step 2	Server /bios # clear-cmos	After a prompt to confirm, clears the CMOS memory.

This example clears the BIOS CMOS memory:

```
Server# scope bios
Server /bios # clear-cmos

This operation will clear the BIOS CMOS.
Note: Server should be in powered off state to clear CMOS.
Continue?[y|n] y

Server /bios #
```

Recovering from a Corrupted BIOS



Note

This procedure is not available in some server models.

In addition to this procedure, there are three other methods for recovering from a corrupted BIOS:

- Use the Cisco Host Upgrade Utility (HUU). This is the recommended method.
- Use the CIMC GUI interface.
- If your server model supports it, use the BIOS recovery function of the hardware jumper on the server motherboard. For instructions, see the Cisco UCS Server Installation and Service Guide for your server model.

Before You Begin

- You must be logged in as admin to recover from a corrupted BIOS.
- Have the BIOS recovery ISO image ready. You will find the BIOS recovery ISO image under the Recovery folder of the firmware distribution package.
- Schedule some down time for the server because it will be power cycled at the end of the recovery procedure.

Procedure

	Command or Action	Purpose
Step 1	Server# scope bios	Enters the bios command mode.
Step 2	Server# recover	Launches a dialog for loading the BIOS recovery image.

This example shows how to recover from a corrupted BIOS:

```
Server# scope bios
Server /bios # recover
This operation will automatically power on the server to perform BIOS FW recovery.
Continue?[y|N]y
```

What to Do Next

Power cycle or reset the server.

Resetting the CIMC to Factory Defaults

On rare occasions, such as an issue with the current running firmware, troubleshooting a server may require you to reset the CIMC to the factory default. When this happens, all user-configurable settings are reset.

This procedure is not part of the normal server maintenance. After you reset the CIMC, you are logged off and must log in again. You may also lose connectivity and may need to reconfigure the network settings.

When you upgrade from version 1.5(1) to version 1.5(2), the hostname in the CIMC interface is retained as is. However, after upgrading to version 1.5(2), if you do a factory reset, the hostname changes to CXXX-YYYYYY format, where XXX is the model number and YYYYYY is the serial number of the server.

When you downgrade from version 1.5(2) to version 1.5(1), the hostname is retained as is. However, if you do a factory reset, the hostname changes to ucs-cxx-mx format.

Procedure

	Command or Action	Purpose
Step 1	Server# scope cimc	Enters the CIMC command mode.
Step 2	Server /cimc # factory-default	After a prompt to confirm, the CIMC resets to factory defaults.

The CIMC factory defaults include the following conditions:

- SSH is enabled for access to the CIMC CLI. Telnet is disabled.
- HTTPS is enabled for access to the CIMC GUI.
- A single user account exists (user name is **admin** , password is **password**).
- DHCP is enabled on the management port.
- The boot order is EFI, CDROM, PXE (using LoM), FDD, HDD.
- KVM and vMedia are enabled.
- USB is enabled.
- SoL is disabled.

This example resets the CIMC to factory defaults:

```
Server# scope cimc
Server /cimc # factory-default
This operation will reset the CIMC configuration to factory default.
```

```
All your configuration will be lost.
Continue?[y|N]
```

Exporting and Importing the CIMC Configuration

Exporting and Importing the CIMC Configuration

To perform a backup of the CIMC configuration, you take a snapshot of the system configuration and export the resulting CIMC configuration file to a location on your network. The export operation saves information from the management plane only; it does not back up data on the servers. Sensitive configuration information such as user accounts and the server certificate are not exported.

You can restore an exported CIMC configuration file to the same system or you can import it to another CIMC system, provided that the software version of the importing system is the same as or is configuration-compatible with the software version of the exporting system. When you import a configuration file to another system as a configuration template, you must modify system-specific settings such as IP addresses and host names. An import operation modifies information on the management plane only.

The CIMC configuration file is an XML text file whose structure and elements correspond to the CIMC command modes.

When performing an export or import operation, consider these guidelines:

- You can perform an export or an import while the system is up and running. While an export operation has no impact on the server or network traffic, some modifications caused by an import operation, such as IP address changes, can disrupt traffic or cause a server reboot.
- You cannot execute an export and an import simultaneously.

Exporting the CIMC Configuration



Note

For security reasons, this operation does not export user accounts or the server certificate.



Important

If any firmware or BIOS updates are in progress, do not export the CIMC configuration until those tasks are complete.

Before You Begin

Obtain the backup remote server IP address.

Procedure

	Command or Action	Purpose
Step 1	Server# scope cimc	Enters the CIMC command mode.

	Command or Action	Purpose
Step 2	Server /cimc # scope import-export	Enters the import-export command mode.
Step 3	Server /cimc/import-export # export-config <i>protocol ip-address path-and-filename</i>	Starts the backup operation. The configuration file will be stored at the specified path and file name on a remote server at the specified IP address. The remote server could be one of the following types: <ul style="list-style-type: none"> • TFTP • FTP • SFTP • SCP • HTTP

To determine whether the export operation has completed successfully, use the **show detail** command. To abort the operation, type CTRL+C.

This example shows how to back up the CIMC configuration:

```
Server# scope cimc
Server /cimc # scope import-export
Server /cimc/import-export # export-config tftp 192.0.2.34 /ucs/backups/cimc5.xml
Export config started. Please check the status using "show detail".
Server /cimc/import-export # show detail
Import Export:
  Operation: EXPORT
  Status: COMPLETED
  Error Code: 100 (No Error)
  Diagnostic Message: NONE

Server /cimc/import-export #
```

Importing a CIMC Configuration



Important

If any firmware or BIOS updates are in progress, do not import the CIMC configuration until those tasks are complete.

Before You Begin

If you want to restore the SNMP configuration information when you import the configuration file, make sure that SNMP is disabled on this server before you do the import. If SNMP is enabled when you perform the import, CIMC does not overwrite the current values with those saved in the configuration file.

Procedure

	Command or Action	Purpose
Step 1	Server# scope cimc	Enters the CIMC command mode.
Step 2	Server /cimc # scope import-export	Enters the import-export command mode.
Step 3	Server /cimc/import-export # import-config <i>protocol ip-address</i> <i>path-and-filename</i>	Starts the import operation. The configuration file at the specified path and file name on the remote server at the specified IP address will be imported. The remote server can be one of the following: <ul style="list-style-type: none"> • TFTP • FTP • SFTP • SCP • HTTP

To determine whether the import operation has completed successfully, use the **show detail** command. To abort the operation, type CTRL+C.

This example shows how to import a CIMC configuration:

```
Server# scope cimc
Server /cimc # scope import-export
Server /cimc/import-export # import-config tftp 192.0.2.34 /ucs/backups/cimc5.xml
Import config started. Please check the status using "show detail".
Server /cimc/import-export #
```

Generating Non maskable Interrupts to the Host

In some situations, the server might hang and not respond to traditional debug mechanisms. By generating a non maskable interrupt (NMI) to the host, you can create and send a crash dump file of the server and use it to debug the server.

Depending on the type of operating system associated with the server, this task might restart the OS.

Procedure

	Command or Action	Purpose
Step 1	Server # scope chassis	Enters chassis command mode.
Step 2	Server /chassis # generate-nmi	Generates the crash dump file for the server. To use this command, the server must be powered on, and you must be logged in as an administrator.

This example shows how to generate NMI signals to the host:

```
Server # scope chassis
Server /chassis # generate-nmi
This operation will send NMI to the host and may cause reboot of the OS.
OS reboot depends on it's NMI configuration.
Do you want to continue? [y|N] y
Server /chassis #
```




BIOS Parameters by Server Model

This appendix contains the following sections:

- [C22 and C24 Servers, page 197](#)
- [C220 and C240 Servers, page 217](#)
- [C260 Servers, page 237](#)
- [C420 Servers, page 250](#)
- [C460 Servers, page 270](#)

C22 and C24 Servers

Main BIOS Parameters for C22 and C24 Servers

Name	Description
TPM Support set TPMAdminCtrl	<p>TPM (Trusted Platform Module) is a microchip designed to provide basic security-related functions primarily involving encryption keys. This option allows you to control the TPM Security Device support for the system. It can be one of the following:</p> <ul style="list-style-type: none">• Disabled—The server does not use the TPM.• Enabled—The server uses the TPM. <p>Note We recommend that you contact your operating system vendor to make sure the operating system supports this feature.</p>

Advanced BIOS Parameters for C22 and C24 Servers

Processor Configuration Parameters

Name	Description
Intel Hyper-Threading Technology set IntelHyperThread	<p>Whether the processor uses Intel Hyper-Threading Technology, which allows multithreaded software applications to execute threads in parallel within each processor. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The processor does not permit hyperthreading. • Enabled—The processor allows for the parallel execution of multiple threads. <p>We recommend that you contact your operating system vendor to make sure the operating system supports this feature.</p>
Number of Enabled Cores set CoreMultiProcessing	<p>Allows you to disable one or more of the physical cores on the server. This can be one of the following:</p> <ul style="list-style-type: none"> • All—Enables all physical cores. This also enables Hyper Threading on the associated logical processor cores. • 1 through n—Specifies the number of physical processor cores that can run on the server. Each physical core has an associated logical core. <p>We recommend that you contact your operating system vendor to make sure the operating system supports this feature.</p>
Execute Disable set ExecuteDisable	<p>Classifies memory areas on the server to specify where application code can execute. As a result of this classification, the processor disables code execution if a malicious worm attempts to insert code in the buffer. This setting helps to prevent damage, worm propagation, and certain classes of malicious buffer overflow attacks. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The processor does not classify memory areas. • Enabled—The processor classifies memory areas. <p>We recommend that you contact your operating system vendor to make sure the operating system supports this feature.</p>

Name	Description
Intel VT set IntelVT	<p>Whether the processor uses Intel Virtualization Technology (VT), which allows a platform to run multiple operating systems and applications in independent partitions. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The processor does not permit virtualization. • Enabled—The processor allows multiple operating systems in independent partitions. <p>Note If you change this option, you must power cycle the server before the setting takes effect.</p>
Intel VT-d set IntelVTD	<p>Whether the processor uses Intel Virtualization Technology for Directed I/O (VT-d). This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The processor does not use virtualization technology. • Enabled—The processor uses virtualization technology.
Intel VT-d Coherency Support set CoherencySupport	<p>Whether the processor supports Intel VT-d Coherency. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The processor does not support coherency. • Enabled—The processor uses VT-d Coherency as required.
Intel VT-d ATS Support set ATS	<p>Whether the processor supports Intel VT-d Address Translation Services (ATS). This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The processor does not support ATS. • Enabled—The processor uses VT-d ATS as required.

Name	Description
CPU Performance set CPUPerformance	<p>Sets the CPU performance profile for the server. The performance profile consists of the following options:</p> <ul style="list-style-type: none"> • DCU Streamer Prefetcher • DCU IP Prefetcher • Hardware Prefetcher • Adjacent Cache-Line Prefetch <p>This can be one of the following:</p> <ul style="list-style-type: none"> • Enterprise—All options are enabled. • High_Throughput—Only the DCU IP Prefetcher is enabled. The rest of the options are disabled. • HPC—All options are enabled. This setting is also known as high performance computing. • Custom—All performance profile options can be configured from the BIOS setup on the server. In addition, the Hardware Prefetcher and Adjacent Cache-Line Prefetch options can be configured in the fields below.
Hardware Prefetcher set HardwarePrefetch	<p>Whether the processor allows the Intel hardware prefetcher to fetch streams of data and instruction from memory into the unified second-level cache when necessary. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The hardware prefetcher is not used. • Enabled—The processor uses the hardware prefetcher when cache issues are detected.
Adjacent Cache Line Prefetcher set AdjacentCacheLinePrefetch	<p>Whether the processor fetches cache lines in even/odd pairs instead of fetching just the required line. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The processor only fetches the required line. • Enabled—The processor fetches both the required line and its paired line.

Name	Description
DCU Streamer Prefetch set DcuStreamerPrefetch	<p>Whether the processor uses the DCU IP Prefetch mechanism to analyze historical cache access patterns and preload the most relevant lines in the L1 cache. This can be one of the following:</p> <ul style="list-style-type: none">• Disabled—The processor does not try to anticipate cache read requirements and only fetches explicitly requested lines.• Enabled—The DCU prefetcher analyzes the cache read pattern and prefetches the next line in the cache if it determines that it may be needed.
DCU IP Prefetcher set DcuIpPrefetch	<p>Whether the processor uses the DCU IP Prefetch mechanism to analyze historical cache access patterns and preload the most relevant lines in the L1 cache. This can be one of the following:</p> <ul style="list-style-type: none">• Disabled—The processor does not preload any cache data.• Enabled—The DCU IP prefetcher preloads the L1 cache with the data it determines to be the most relevant.
Direct Cache Access Support set DirectCacheAccess	<p>Allows processors to increase I/O performance by placing data from I/O devices directly into the processor cache. This setting helps to reduce cache misses. This can be one of the following:</p> <ul style="list-style-type: none">• Disabled—Data from I/O devices is not placed directly into the processor cache.• Enabled—Data from I/O devices is placed directly into the processor cache.

Name	Description
Power Technology set CPUPowerManagement	<p>Enables you to configure the CPU power management settings for the following options:</p> <ul style="list-style-type: none"> • Enhanced Intel Speedstep Technology • Intel Turbo Boost Technology • Processor Power State C6 <p>Power Technology can be one of the following:</p> <ul style="list-style-type: none"> • Custom—The server uses the individual settings for the BIOS parameters mentioned above. You must select this option if you want to change any of these BIOS parameters. • Disabled—The server does not perform any CPU power management and any settings for the BIOS parameters mentioned above are ignored. • Energy_Efficient—The server determines the best settings for the BIOS parameters mentioned above and ignores the individual settings for these parameters.
Enhanced Intel Speedstep Technology set EnhancedIntelSpeedStep	<p>Whether the processor uses Enhanced Intel SpeedStep Technology, which allows the system to dynamically adjust processor voltage and core frequency. This technology can result in decreased average power consumption and decreased average heat production. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The processor never dynamically adjusts its voltage or frequency. • Enabled—The processor utilizes Enhanced Intel SpeedStep Technology and enables all supported processor sleep states to further conserve power. <p>We recommend that you contact your operating system vendor to make sure the operating system supports this feature.</p> <p>Note CPUPowerManagement must be set to Custom or the server ignores the setting for this parameter.</p>

Name	Description
Intel Turbo Boost Technology set IntelTurboBoostTech	<p>Whether the processor uses Intel Turbo Boost Technology, which allows the processor to automatically increase its frequency if it is running below power, temperature, or voltage specifications. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The processor does not increase its frequency automatically. • Enabled—The processor utilizes Turbo Boost Technology if required. <p>Note CPUPowerManagement must be set to Custom or the server ignores the setting for this parameter.</p>
Processor Power State C6 set ProcessorC6Report	<p>Whether the BIOS sends the C6 report to the operating system. When the OS receives the report, it can transition the processor into the lower C6 power state to decrease energy usage while maintaining optimal processor performance. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The BIOS does not send the C6 report. • Enabled—The BIOS sends the C6 report, allowing the OS to transition the processor to the C6 low power state. <p>Note CPUPowerManagement must be set to Custom or the server ignores the setting for this parameter.</p>
Processor Power State C1 Enhanced set ProcessorC1EReport	<p>Whether the CPU transitions to its minimum frequency when entering the C1 state. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The CPU continues to run at its maximum frequency in C1 state. • Enabled—The CPU transitions to its minimum frequency. This option saves the maximum amount of power in C1 state.
Frequency Floor Override set CpuFreqFloor	<p>Whether the CPU is allowed to drop below the maximum non-turbo frequency when idle. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled— The CPU can drop below the maximum non-turbo frequency when idle. This option decreases power consumption but may reduce system performance. • Enabled— The CPU cannot drop below the maximum non-turbo frequency when idle. This option improves system performance but may increase power consumption.

Name	Description
P-STATE Coordination set PsdCoordType	<p>Allows you to define how BIOS communicates the P-state support model to the operating system. There are 3 models as defined by the Advanced Configuration and Power Interface (ACPI) specification.</p> <ul style="list-style-type: none"> • HW_ALL—The processor hardware is responsible for coordinating the P-state among logical processors with dependencies (all logical processors in a package). • SW_ALL—The OS Power Manager (OSPM) is responsible for coordinating the P-state among logical processors with dependencies (all logical processors in a physical package), and must initiate the transition on all of the logical processors. • SW_ANY—The OS Power Manager (OSPM) is responsible for coordinating the P-state among logical processors with dependencies (all logical processors in a package), and may initiate the transition on any of the logical processors in the domain. <p>Note CPUPowerManagement must be set to Custom or the server ignores the setting for this parameter.</p>
Energy Performance set CpuEngPerfBias	<p>Allows you to determine whether system performance or energy efficiency is more important on this server. This can be one of the following:</p> <ul style="list-style-type: none"> • Balanced_Energy • Balanced_Performance • Energy_Efficient • Performance

Memory Configuration Parameters

Name	Description
Select Memory RAS set SelectMemoryRAS	<p>How the memory reliability, availability, and serviceability (RAS) is configured for the server. This can be one of the following:</p> <ul style="list-style-type: none"> • Maximum_Performance—System performance is optimized. • Mirroring—System reliability is optimized by using half the system memory as backup. • Lockstep—If the DIMM pairs in the server have an identical type, size, and organization and are populated across the SMI channels, you can enable lockstep mode to minimize memory access latency and provide better performance. This option offers better system performance than Mirroring and better reliability than Maximum Performance but lower reliability than Mirroring and lower system performance than Maximum Performance.
DRAM Clock Throttling set DRAMClockThrottling	<p>Allows you to tune the system settings between the memory bandwidth and power consumption. This can be one of the following:</p> <ul style="list-style-type: none"> • Balanced—DRAM clock throttling is reduced, providing a balance between performance and power. • Performance—DRAM clock throttling is disabled, providing increased memory bandwidth at the cost of additional power. • Energy_Efficient—DRAM clock throttling is increased to improve energy efficiency.
NUMA set NUMAOptimize	<p>Whether the BIOS supports NUMA. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The BIOS does not support NUMA. • Enabled—The BIOS includes the ACPI tables that are required for NUMA-aware operating systems. If you enable this option, the system must disable Inter-Socket Memory interleaving on some platforms.

Name	Description
Low Voltage DDR Mode set LvDDRMode	<p>Whether the system prioritizes low voltage or high frequency memory operations. This can be one of the following:</p> <ul style="list-style-type: none"> • Power_Saving_Mode—The system prioritizes low voltage memory operations over high frequency memory operations. This mode may lower memory frequency in order to keep the voltage low. • Performance_Mode—The system prioritizes high frequency operations over low voltage operations.
DRAM Refresh rate set DramRefreshRate	<p>Allows you to set the rate at which the DRAM cells are refreshed. This can be one of the following:</p> <ul style="list-style-type: none"> • 1x—DRAM cells are refreshed every 64ms. • 2x—DRAM cells are refreshed every 32ms. • 3x—DRAM cells are refreshed every 21ms. • 4x—DRAM cells are refreshed every 16ms. • Auto—DRAM cells refresh rate is automatically chosen by the BIOS based on the system configuration. This is the recommended setting for this parameter.
Channel Interleaving set ChannelInterLeave	<p>Whether the CPU divides memory blocks and spreads contiguous portions of data across interleaved channels to enable simultaneous read operations. This can be one of the following:</p> <ul style="list-style-type: none"> • Auto—The CPU determines what interleaving is done. • 1_Way—Some channel interleaving is used. • 2_Way • 3_Way • 4_Way—The maximum amount of channel interleaving is used.

Name	Description
Rank Interleaving set RankInterLeave	<p>Whether the CPU interleaves physical ranks of memory so that one rank can be accessed while another is being refreshed. This can be one of the following:</p> <ul style="list-style-type: none"> • Auto—The CPU determines what interleaving is done. • 1_Way—Some rank interleaving is used. • 2_Way • 4_Way • 8_Way—The maximum amount of rank interleaving is used.
Patrol Scrub set PatrolScrub	<p>Whether the system actively searches for, and corrects, single bit memory errors even in unused portions of the memory on the server. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The system checks for memory ECC errors only when the CPU reads or writes a memory address. • Enabled—The system periodically reads and writes memory searching for ECC errors. If any errors are found, the system attempts to fix them. This option may correct single bit errors before they become multi-bit errors, but it may adversely affect performance when the patrol scrub is running.
Demand Scrub set DemandScrub	<p>Whether the system corrects single bit memory errors encountered when the CPU or I/O makes a demand read. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled— Single bit memory errors are not corrected. • Enabled— Single bit memory errors are corrected in memory and the corrected data is set in response to the demand read.

Name	Description
Altitude set Altitude	<p>The approximate number of meters above sea level at which the physical server is installed. This can be one of the following:</p> <ul style="list-style-type: none"> • Auto—The CPU determines the physical elevation. • 300_M—The server is approximately 300 meters above sea level. • 900_M—The server is approximately 900 meters above sea level. • 1500_M—The server is approximately 1500 meters above sea level. • 3000_M—The server is approximately 3000 meters above sea level.

QPI Configuration Parameters

Name	Description
QPI Link Frequency set QPILinkFrequency	<p>The Intel QuickPath Interconnect (QPI) link frequency, in gigatransfers per second (GT/s). This can be one of the following:</p> <ul style="list-style-type: none"> • Auto—The CPU determines the QPI link frequency. • 6.4_GT/s • 7.2_GT/s • 8.0_GT/s

Onboard Storage Parameters

Name	Description
Onboard SCU Storage Support set DisableSCU	<p>Whether the onboard software RAID controller is available to the server. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The software RAID controller is not available. • Enabled—The software RAID controller is available.

USB Configuration Parameters

Name	Description
Legacy USB Support set LegacyUSBSupport	<p>Whether the system supports legacy USB devices. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—USB devices are only available to EFI applications. • Enabled—Legacy USB support is always available. • Auto—Disables legacy USB support if no USB devices are connected.
Port 60/64 Emulation set UsbEmul6064	<p>Whether the system supports 60h/64h emulation for complete USB keyboard legacy support. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—60h/64 emulation is not supported. • Enabled—60h/64 emulation is supported. <p>You should select this option if you are using a non-USB aware operating system on the server.</p>
All USB Devices set AllUsbDevices	<p>Whether all physical and virtual USB devices are enabled or disabled. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—All USB devices are disabled. • Enabled—All USB devices are enabled.
USB Port: Rear set UsbPortRear	<p>Whether the rear panel USB devices are enabled or disabled. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—Disables the rear panel USB ports. Devices connected to these ports are not detected by the BIOS and operating system. • Enabled—Enables the rear panel USB ports. Devices connected to these ports are detected by the BIOS and operating system.
USB Port: Front set UsbPortFront	<p>Whether the front panel USB devices are enabled or disabled. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—Disables the front panel USB ports. Devices connected to these ports are not detected by the BIOS and operating system. • Enabled—Enables the front panel USB ports. Devices connected to these ports are detected by the BIOS and operating system.

Name	Description
USB Port: Internal set UsbPortInt	Whether the internal USB devices are enabled or disabled. This can be one of the following: <ul style="list-style-type: none"> • Disabled—Disables the internal USB ports. Devices connected to these ports are not detected by the BIOS and operating system. • Enabled—Enables the internal USB ports. Devices connected to these ports are detected by the BIOS and operating system.
USB Port: KVM set UsbPortKVM	Whether the KVM ports are enabled or disabled. This can be one of the following: <ul style="list-style-type: none"> • Disabled—Disables the KVM keyboard and/or mouse devices. Keyboard and/or mouse will not work in the KVM window. • Enabled—Enables the KVM keyboard and/or mouse devices.
USB Port: VMedia set UsbPortVMedia	Whether the virtual media devices are enabled or disabled. This can be one of the following: <ul style="list-style-type: none"> • Disabled—Disables the vMedia devices. • Enabled—Enables the vMedia devices.

PCI Configuration Parameters

Name	Description
MMIO Above 4GB set MemoryMappedIOAbove4GB	Whether to enable or disable memory mapped I/O of 64-bit PCI devices to 4GB or greater address space. Legacy option ROMs are not able to access addresses above 4GB. PCI devices that are 64-bit compliant but use a legacy option ROM may not function correctly with this setting enabled. This can be one of the following: <ul style="list-style-type: none"> • Disabled—The server does not map I/O of 64-bit PCI devices to 4GB or greater address space. • Enabled—The server maps I/O of 64-bit PCI devices to 4GB or greater address space.
ASPM Support set ASPMsSupport	Allows you to set the level of ASPM (Active Power State Management) support in the BIOS. This can be one of the following: <ul style="list-style-type: none"> • Disabled—ASPM support is disabled in the BIOS. • Force L0s—Force all links to L0 standby (L0s) state. • Auto—The CPU determines the power state.

Name	Description
VGA Priority set VgaPriority	<p>Allows you to set the priority for VGA graphics devices if multiple VGA devices are found in the system. This can be one of the following:</p> <ul style="list-style-type: none"> • Onboard—Priority is given to the onboard VGA device. BIOS post screen and OS boot are driven through the onboard VGA port. • Offboard—Priority is given to the PCIE Graphics adapter. BIOS post screen and OS boot are driven through the external graphics adapter port. • Onboard_VGA_Disabled—Priority is given to the PCIE Graphics adapter, and the onboard VGA device is disabled. <p>Note The vKVM does not function when the onboard VGA is disabled.</p>

Serial Configuration Parameters

Name	Description
Console Redirection set ConsoleRedir	<p>Allows a serial port to be used for console redirection during POST and BIOS booting. After the BIOS has booted and the operating system is responsible for the server, console redirection is irrelevant and has no effect. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—No console redirection occurs during POST. • Enabled—Enables console redirection on serial port A during POST.
Terminal Type set TerminalType	<p>What type of character formatting is used for console redirection. This can be one of the following:</p> <ul style="list-style-type: none"> • PC-ANSI—The PC-ANSI terminal font is used. • VT100—A supported vt100 video terminal and its character set are used. • VT100+—A supported vt100-plus video terminal and its character set are used. • VT-UTF8—A video terminal with the UTF-8 character set is used. <p>Note This setting must match the setting on the remote terminal application.</p>

Name	Description
Bits per second set BaudRate	<p>What BAUD rate is used for the serial port transmission speed. If you disable Console Redirection, this option is not available. This can be one of the following:</p> <ul style="list-style-type: none"> • 9600—A 9,600 BAUD rate is used. • 19200—A 19,200 BAUD rate is used. • 38400—A 38,400 BAUD rate is used. • 57600—A 57,600 BAUD rate is used. • 115200—A 115,200 BAUD rate is used. <p>Note This setting must match the setting on the remote terminal application.</p>
Flow Control set FlowCtrl	<p>Whether a handshake protocol is used for flow control. Request to Send / Clear to Send (RTS/CTS) helps to reduce frame collisions that can be introduced by a hidden terminal problem. This can be one of the following:</p> <ul style="list-style-type: none"> • None—No flow control is used. • Hardware_RTS/CTS—RTS/CTS is used for flow control. <p>Note This setting must match the setting on the remote terminal application.</p>
Putty KeyPad set PuttyFunctionKeyPad	<p>Allows you to change the action of the PuTTY function keys and the top row of the numeric keypad. This can be one of the following:</p> <ul style="list-style-type: none"> • VT100—The function keys generate ESC OP through ESC O[. • LINUX—Mimics the Linux virtual console. Function keys F6 to F12 behave like the default mode, but F1 to F5 generate ESC [[A through ESC [[E. • XTERMR6—Function keys F5 to F12 behave like the default mode. Function keys F1 to F4 generate ESC OP through ESC OS, which are the sequences produced by the top row of the keypad on Digital terminals. • SCO—The function keys F1 to F12 generate ESC [M through ESC [X. The function and shift keys generate ESC [Y through ESC [j. The control and function keys generate ESC [k through ESC [v. The shift, control and function keys generate ESC [w through ESC [{. • ESCN—The default mode. The function keys match the general behavior of Digital terminals. The function keys generate sequences such as ESC [11~ and ESC [12~. • VT400—The function keys behave like the default mode. The top row of the numeric keypad generates ESC OP through ESC OS.

Name	Description
Redirection After BIOS POST set RedirectionAfterPOST	Whether BIOS console redirection should be active after BIOS POST is complete and control given to the OS bootloader. This can be one of the following: <ul style="list-style-type: none"> • Always_Enable—BIOS Legacy console redirection is active during the OS boot and run time. • Bootloader—BIOS Legacy console redirection is disabled before giving control to the OS boot loader.
Out-of-Band Mgmt Port set comSpcrEnable	Allows you to configure the COM port 0 that can be used for Windows Emergency Management services. ACPI SPCR table is reported based on this setup option. This can be one of the following: <ul style="list-style-type: none"> • Disabled—Configures the COM port 0 as a general purpose port for use with the Windows Operating System. • Enabled—Configures the COM port 0 as a remote management port for Windows Emergency Management services.

LOM and PCIe Slots Configuration Parameters

Name	Description
All Onboard LOM Ports set AllLomPortControl	Whether all LOM ports are enabled or disabled. This can be one of the following: <ul style="list-style-type: none"> • Disabled—All LOM ports are disabled. • Enabled—All LOM ports are enabled.
LOM Port <i>n</i> OptionROM set LomOpromControlPort<i>n</i>	Whether Option ROM is available on the LOM port designated by <i>n</i> . This can be one of the following: <ul style="list-style-type: none"> • Disabled—Option ROM is not available on LOM port <i>n</i>. • Enabled—Option ROM is available on LOM port <i>n</i>. • UEFI_Only—The expansion slot <i>n</i> is available for UEFI only. • Legacy_Only—The expansion slot <i>n</i> is available for legacy only.

Name	Description
All PCIe Slots OptionROM set PcieOptionROMs	Whether the server can use the PCIe Option ROM expansion slots. This can be one of the following: <ul style="list-style-type: none"> • Disabled—PCIe Option ROMs are not available. • Enabled—PCIe Option ROMs are available. • UEFI_Only—The expansion slot <i>n</i> is available for UEFI only. • Legacy_Only—The expansion slot <i>n</i> is available for legacy only.
PCIe Slot:<i>n</i> OptionROM set Slot-<i>n</i>-ROM	Whether PCIe expansion slot <i>n</i> is available to the server. This can be one of the following: <ul style="list-style-type: none"> • Disabled—The expansion slot <i>n</i> is not available. • Enabled—The expansion slot <i>n</i> is available. • UEFI_Only—The expansion slot <i>n</i> is available for UEFI only. • Legacy_Only—The expansion slot <i>n</i> is available for legacy only.
PCIe Slot:<i>n</i> Link Speed PCIe Slot:<i>n</i>LinkSpeed	This option allows you to restrict the maximum speed of an adapter card installed in PCIe slot <i>n</i> . This can be one of the following: <ul style="list-style-type: none"> • GEN1—2.5GT/s (gigatransfers per second) is the maximum speed allowed. • GEN2—5GT/s is the maximum speed allowed. • GEN3—8GT/s is the maximum speed allowed. • Disabled—The maximum speed is not restricted. <p>For example, if you have a 3rd generation adapter card in PCIe slot 2 that you want to run at a maximum of 5GT/s instead of the 8GT/s that card supports, set the PCIe Slot 2 Link Speed to GEN2. The system then ignores the card's supported maximum speed of 8GT/s and forces it to run at a maximum of 5 GT/s.</p>

Server Management BIOS Parameters for C22 and C24 Servers

Name	Description
FRB-2 Timer set FRB-2	Whether the FRB2 timer is used by CIMC to recover the system if it hangs during POST. This can be one of the following: <ul style="list-style-type: none"> • Disabled—The FRB2 timer is not used. • Enabled—The FRB2 timer is started during POST and used to recover the system if necessary.

Name	Description
OS Watchdog Timer set OSBootWatchdogTimer	<p>Whether the BIOS programs the watchdog timer with a specified timeout value. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The watchdog timer is not used to track how long the server takes to boot. • Enabled—The watchdog timer tracks how long the server takes to boot. If the server does not boot within the length of time specified by the set OSBootWatchdogTimerTimeout command, the CIMC logs an error and takes the action specified by the set OSBootWatchdogTimerPolicy command.
OS Watchdog Timer Timeout set OSBootWatchdogTimerTimeOut	<p>What timeout value the BIOS uses to configure the watchdog timer. This can be one of the following:</p> <ul style="list-style-type: none"> • 5_Minutes—The watchdog timer expires 5 minutes after the OS begins to boot. • 10_Minutes—The watchdog timer expires 10 minutes after the OS begins to boot. • 15_Minutes—The watchdog timer expires 15 minutes after the OS begins to boot. • 20_Minutes—The watchdog timer expires 20 minutes after the OS begins to boot. <p>Note This option is only applicable if you enable the OS Boot Watchdog Timer.</p>
OS Watchdog Timer Policy set OSBootWatchdogTimerPolicy	<p>What action the system takes if the watchdog timer expires. This can be one of the following:</p> <ul style="list-style-type: none"> • Do_Nothing—The server takes no action if the watchdog timer expires during OS boot. • Power_Down—The server is powered off if the watchdog timer expires during OS boot. • Reset—The server is reset if the watchdog timer expires during OS boot. <p>Note This option is only applicable if you enable the OS Boot Watchdog Timer.</p>

Name	Description
Boot Order Rules set ManagedBootRule	<p>How the server changes the boot order list defined through the CIMC GUI or CLI when there are no devices of a particular device type available or when the user defines a different boot order using the server's BIOS Setup Utility.</p> <p>The supported device types are:</p> <ul style="list-style-type: none"> • HDD—Hard disk drive • FDD—Floppy disk drive • CDROM—Bootable CD-ROM or DVD • PXE—PXE boot • EFI—Extensible Firmware Interface <p>The Boot Order Rules option can be one of the following:</p> <ul style="list-style-type: none"> • Strict—When no devices of a particular type are available, the system creates a placeholder for that device type in the boot order list. When a device of that type becomes available, it is added to the boot order in the previously defined position. <p>If the user defines a boot order through the server's BIOS Setup Utility, that boot order is given priority over the boot order configured through the CIMC GUI or CLI. All device types defined through CIMC that are not present in the boot order defined through the BIOS Setup Utility are removed from the boot order list.</p> <ul style="list-style-type: none"> • Loose—When no devices of a particular type are available, the system removes that device type from the boot order. When a device of that type becomes available, the system adds it to the end of the boot order list. <p>If the boot order is configured through the server's BIOS Setup Utility, that boot order is given priority over the boot order configured through the CIMC GUI or CLI. All device types defined through CIMC that are not present in the boot order defined through the BIOS Setup Utility are moved to the end of the boot order list.</p>

C220 and C240 Servers

Main BIOS Parameters for C220 and C240 Servers

Name	Description
TPM Support set TPMAdminCtrl	<p>TPM (Trusted Platform Module) is a microchip designed to provide basic security-related functions primarily involving encryption keys. This option allows you to control the TPM Security Device support for the system. It can be one of the following:</p> <ul style="list-style-type: none">• Disabled—The server does not use the TPM.• Enabled—The server uses the TPM. <p>Note We recommend that you contact your operating system vendor to make sure the operating system supports this feature.</p>

Advanced BIOS Parameters for C220 and C240 Servers

Processor Configuration Parameters

Name	Description
Intel Hyper-Threading Technology set IntelHyperThread	<p>Whether the processor uses Intel Hyper-Threading Technology, which allows multithreaded software applications to execute threads in parallel within each processor. This can be one of the following:</p> <ul style="list-style-type: none">• Disabled—The processor does not permit hyperthreading.• Enabled—The processor allows for the parallel execution of multiple threads. <p>We recommend that you contact your operating system vendor to make sure the operating system supports this feature.</p>

Name	Description
Number of Enabled Cores set CoreMultiProcessing	<p>Allows you to disable one or more of the physical cores on the server. This can be one of the following:</p> <ul style="list-style-type: none"> • All—Enables all physical cores. This also enables Hyper Threading on the associated logical processor cores. • 1 through <i>n</i>—Specifies the number of physical processor cores that can run on the server. Each physical core has an associated logical core. <p>We recommend that you contact your operating system vendor to make sure the operating system supports this feature.</p>
Execute Disable set ExecuteDisable	<p>Classifies memory areas on the server to specify where application code can execute. As a result of this classification, the processor disables code execution if a malicious worm attempts to insert code in the buffer. This setting helps to prevent damage, worm propagation, and certain classes of malicious buffer overflow attacks. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The processor does not classify memory areas. • Enabled—The processor classifies memory areas. <p>We recommend that you contact your operating system vendor to make sure the operating system supports this feature.</p>
Intel VT set IntelVT	<p>Whether the processor uses Intel Virtualization Technology (VT), which allows a platform to run multiple operating systems and applications in independent partitions. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The processor does not permit virtualization. • Enabled—The processor allows multiple operating systems in independent partitions. <p>Note If you change this option, you must power cycle the server before the setting takes effect.</p>
Intel VT-d set IntelVTD	<p>Whether the processor uses Intel Virtualization Technology for Directed I/O (VT-d). This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The processor does not use virtualization technology. • Enabled—The processor uses virtualization technology.

Name	Description
Intel VT-d Coherency Support set CoherencySupport	<p>Whether the processor supports Intel VT-d Coherency. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The processor does not support coherency. • Enabled—The processor uses VT-d Coherency as required.
Intel VT-d ATS Support set ATS	<p>Whether the processor supports Intel VT-d Address Translation Services (ATS). This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The processor does not support ATS. • Enabled—The processor uses VT-d ATS as required.
CPU Performance set CPUPerformance	<p>Sets the CPU performance profile for the server. The performance profile consists of the following options:</p> <ul style="list-style-type: none"> • DCU Streamer Prefetcher • DCU IP Prefetcher • Hardware Prefetcher • Adjacent Cache-Line Prefetch <p>This can be one of the following:</p> <ul style="list-style-type: none"> • Enterprise—All options are enabled. • High_Throughput—Only the DCU IP Prefetcher is enabled. The rest of the options are disabled. • HPC—All options are enabled. This setting is also known as high performance computing. • Custom—All performance profile options can be configured from the BIOS setup on the server. In addition, the Hardware Prefetcher and Adjacent Cache-Line Prefetch options can be configured in the fields below.
Hardware Prefetcher set HardwarePrefetch	<p>Whether the processor allows the Intel hardware prefetcher to fetch streams of data and instruction from memory into the unified second-level cache when necessary. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The hardware prefetcher is not used. • Enabled—The processor uses the hardware prefetcher when cache issues are detected.

Name	Description
Adjacent Cache Line Prefetcher set AdjacentCacheLinePrefetch	<p>Whether the processor fetches cache lines in even/odd pairs instead of fetching just the required line. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The processor only fetches the required line. • Enabled— The processor fetches both the required line and its paired line.
DCU Streamer Prefetch set DcuStreamerPrefetch	<p>Whether the processor uses the DCU IP Prefetch mechanism to analyze historical cache access patterns and preload the most relevant lines in the L1 cache. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The processor does not try to anticipate cache read requirements and only fetches explicitly requested lines. • Enabled—The DCU prefetcher analyzes the cache read pattern and prefetches the next line in the cache if it determines that it may be needed.
DCU IP Prefetcher set DculpPrefetch	<p>Whether the processor uses the DCU IP Prefetch mechanism to analyze historical cache access patterns and preload the most relevant lines in the L1 cache. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The processor does not preload any cache data. • Enabled—The DCU IP prefetcher preloads the L1 cache with the data it determines to be the most relevant.
Direct Cache Access Support set DirectCacheAccess	<p>Allows processors to increase I/O performance by placing data from I/O devices directly into the processor cache. This setting helps to reduce cache misses. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—Data from I/O devices is not placed directly into the processor cache. • Enabled—Data from I/O devices is placed directly into the processor cache.

Name	Description
Power Technology set CPUPowerManagement	<p>Enables you to configure the CPU power management settings for the following options:</p> <ul style="list-style-type: none"> • Enhanced Intel Speedstep Technology • Intel Turbo Boost Technology • Processor Power State C6 <p>Power Technology can be one of the following:</p> <ul style="list-style-type: none"> • Custom—The server uses the individual settings for the BIOS parameters mentioned above. You must select this option if you want to change any of these BIOS parameters. • Disabled—The server does not perform any CPU power management and any settings for the BIOS parameters mentioned above are ignored. • Energy_Efficient—The server determines the best settings for the BIOS parameters mentioned above and ignores the individual settings for these parameters.
Enhanced Intel Speedstep Technology set EnhancedIntelSpeedStep	<p>Whether the processor uses Enhanced Intel SpeedStep Technology, which allows the system to dynamically adjust processor voltage and core frequency. This technology can result in decreased average power consumption and decreased average heat production. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The processor never dynamically adjusts its voltage or frequency. • Enabled—The processor utilizes Enhanced Intel SpeedStep Technology and enables all supported processor sleep states to further conserve power. <p>We recommend that you contact your operating system vendor to make sure the operating system supports this feature.</p> <p>Note CPUPowerManagement must be set to Custom or the server ignores the setting for this parameter.</p>

Name	Description
Intel Turbo Boost Technology set IntelTurboBoostTech	<p>Whether the processor uses Intel Turbo Boost Technology, which allows the processor to automatically increase its frequency if it is running below power, temperature, or voltage specifications. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The processor does not increase its frequency automatically. • Enabled—The processor utilizes Turbo Boost Technology if required. <p>Note CPUPowerManagement must be set to Custom or the server ignores the setting for this parameter.</p>
Processor Power State C6 set ProcessorC6Report	<p>Whether the BIOS sends the C6 report to the operating system. When the OS receives the report, it can transition the processor into the lower C6 power state to decrease energy usage while maintaining optimal processor performance. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The BIOS does not send the C6 report. • Enabled—The BIOS sends the C6 report, allowing the OS to transition the processor to the C6 low power state. <p>Note CPUPowerManagement must be set to Custom or the server ignores the setting for this parameter.</p>
Processor Power State C1 Enhanced set ProcessorC1EReport	<p>Whether the CPU transitions to its minimum frequency when entering the C1 state. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The CPU continues to run at its maximum frequency in C1 state. • Enabled—The CPU transitions to its minimum frequency. This option saves the maximum amount of power in C1 state.
Frequency Floor Override set CpuFreqFloor	<p>Whether the CPU is allowed to drop below the maximum non-turbo frequency when idle. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled— The CPU can drop below the maximum non-turbo frequency when idle. This option decreases power consumption but may reduce system performance. • Enabled— The CPU cannot drop below the maximum non-turbo frequency when idle. This option improves system performance but may increase power consumption.

Name	Description
P-STATE Coordination set PsdCoordType	<p>Allows you to define how BIOS communicates the P-state support model to the operating system. There are 3 models as defined by the Advanced Configuration and Power Interface (ACPI) specification.</p> <ul style="list-style-type: none"> • HW_ALL—The processor hardware is responsible for coordinating the P-state among logical processors with dependencies (all logical processors in a package). • SW_ALL—The OS Power Manager (OSPM) is responsible for coordinating the P-state among logical processors with dependencies (all logical processors in a physical package), and must initiate the transition on all of the logical processors. • SW_ANY—The OS Power Manager (OSPM) is responsible for coordinating the P-state among logical processors with dependencies (all logical processors in a package), and may initiate the transition on any of the logical processors in the domain. <p>Note CPUPowerManagement must be set to Custom or the server ignores the setting for this parameter.</p>
Energy Performance set CpuEngPerfBias	<p>Allows you to determine whether system performance or energy efficiency is more important on this server. This can be one of the following:</p> <ul style="list-style-type: none"> • Balanced_Energy • Balanced_Performance • Energy_Efficient • Performance

Memory Configuration Parameters

Name	Description
Select Memory RAS set SelectMemoryRAS	<p>How the memory reliability, availability, and serviceability (RAS) is configured for the server. This can be one of the following:</p> <ul style="list-style-type: none"> • Maximum_Performance—System performance is optimized. • Mirroring—System reliability is optimized by using half the system memory as backup. • Lockstep—If the DIMM pairs in the server have an identical type, size, and organization and are populated across the SMI channels, you can enable lockstep mode to minimize memory access latency and provide better performance. This option offers better system performance than Mirroring and better reliability than Maximum Performance but lower reliability than Mirroring and lower system performance than Maximum Performance.
DRAM Clock Throttling set DRAMClockThrottling	<p>Allows you to tune the system settings between the memory bandwidth and power consumption. This can be one of the following:</p> <ul style="list-style-type: none"> • Balanced—DRAM clock throttling is reduced, providing a balance between performance and power. • Performance—DRAM clock throttling is disabled, providing increased memory bandwidth at the cost of additional power. • Energy_Efficient—DRAM clock throttling is increased to improve energy efficiency.
NUMA set NUMAOptimize	<p>Whether the BIOS supports NUMA. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The BIOS does not support NUMA. • Enabled—The BIOS includes the ACPI tables that are required for NUMA-aware operating systems. If you enable this option, the system must disable Inter-Socket Memory interleaving on some platforms.

Name	Description
Low Voltage DDR Mode set LvDDRMode	<p>Whether the system prioritizes low voltage or high frequency memory operations. This can be one of the following:</p> <ul style="list-style-type: none"> • Power_Saving_Mode—The system prioritizes low voltage memory operations over high frequency memory operations. This mode may lower memory frequency in order to keep the voltage low. • Performance_Mode—The system prioritizes high frequency operations over low voltage operations.
DRAM Refresh rate set DramRefreshRate	<p>Allows you to set the rate at which the DRAM cells are refreshed. This can be one of the following:</p> <ul style="list-style-type: none"> • 1x—DRAM cells are refreshed every 64ms. • 2x—DRAM cells are refreshed every 32ms. • 3x—DRAM cells are refreshed every 21ms. • 4x—DRAM cells are refreshed every 16ms. • Auto—DRAM cells refresh rate is automatically chosen by the BIOS based on the system configuration. This is the recommended setting for this parameter.
Channel Interleaving set ChannelInterLeave	<p>Whether the CPU divides memory blocks and spreads contiguous portions of data across interleaved channels to enable simultaneous read operations. This can be one of the following:</p> <ul style="list-style-type: none"> • Auto—The CPU determines what interleaving is done. • 1_Way—Some channel interleaving is used. • 2_Way • 3_Way • 4_Way—The maximum amount of channel interleaving is used.

Name	Description
Rank Interleaving set RankInterLeave	<p>Whether the CPU interleaves physical ranks of memory so that one rank can be accessed while another is being refreshed. This can be one of the following:</p> <ul style="list-style-type: none"> • Auto—The CPU determines what interleaving is done. • 1_Way—Some rank interleaving is used. • 2_Way • 4_Way • 8_Way—The maximum amount of rank interleaving is used.
Patrol Scrub set PatrolScrub	<p>Whether the system actively searches for, and corrects, single bit memory errors even in unused portions of the memory on the server. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The system checks for memory ECC errors only when the CPU reads or writes a memory address. • Enabled—The system periodically reads and writes memory searching for ECC errors. If any errors are found, the system attempts to fix them. This option may correct single bit errors before they become multi-bit errors, but it may adversely affect performance when the patrol scrub is running.
Demand Scrub set DemandScrub	<p>Whether the system corrects single bit memory errors encountered when the CPU or I/O makes a demand read. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—Single bit memory errors are not corrected. • Enabled—Single bit memory errors are corrected in memory and the corrected data is set in response to the demand read.

Name	Description
Altitude set Altitude	<p>The approximate number of meters above sea level at which the physical server is installed. This can be one of the following:</p> <ul style="list-style-type: none"> • Auto—The CPU determines the physical elevation. • 300_M—The server is approximately 300 meters above sea level. • 900_M—The server is approximately 900 meters above sea level. • 1500_M—The server is approximately 1500 meters above sea level. • 3000_M—The server is approximately 3000 meters above sea level.

QPI Configuration Parameters

Name	Description
QPI Link Frequency set QPILinkFrequency	<p>The Intel QuickPath Interconnect (QPI) link frequency, in gigatransfers per second (GT/s). This can be one of the following:</p> <ul style="list-style-type: none"> • Auto—The CPU determines the QPI link frequency. • 6.4_GT/s • 7.2_GT/s • 8.0_GT/s

Onboard Storage Parameters

Name	Description
Onboard SCU Storage Support set DisableSCU	<p>Whether the onboard software RAID controller is available to the server. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The software RAID controller is not available. • Enabled—The software RAID controller is available.

Name	Description
Onboard SCU Storage SW Stack set PchScuOromSelect	<p>Allows you to choose a pre-boot software stack for an onboard SCU storage controller. This can be one of the following:</p> <ul style="list-style-type: none"> • Intel RSTe(1) • LSI SW RAID (0) <p>Note This configuration parameter is valid only for the C220 servers.</p>

USB Configuration Parameters

Name	Description
Legacy USB Support set LegacyUSBSupport	<p>Whether the system supports legacy USB devices. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—USB devices are only available to EFI applications. • Enabled—Legacy USB support is always available. • Auto—Disables legacy USB support if no USB devices are connected.
Port 60/64 Emulation set UsbEmul6064	<p>Whether the system supports 60h/64h emulation for complete USB keyboard legacy support. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—60h/64 emulation is not supported. • Enabled—60h/64 emulation is supported. <p>You should select this option if you are using a non-USB aware operating system on the server.</p>
All USB Devices set AllUsbDevices	<p>Whether all physical and virtual USB devices are enabled or disabled. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—All USB devices are disabled. • Enabled—All USB devices are enabled.
USB Port: Rear set UsbPortRear	<p>Whether the rear panel USB devices are enabled or disabled. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—Disables the rear panel USB ports. Devices connected to these ports are not detected by the BIOS and operating system. • Enabled—Enables the rear panel USB ports. Devices connected to these ports are detected by the BIOS and operating system.

Name	Description
USB Port: Front set UsbPortFront	<p>Whether the front panel USB devices are enabled or disabled. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—Disables the front panel USB ports. Devices connected to these ports are not detected by the BIOS and operating system. • Enabled—Enables the front panel USB ports. Devices connected to these ports are detected by the BIOS and operating system.
USB Port: Internal set UsbPortInt	<p>Whether the internal USB devices are enabled or disabled. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—Disables the internal USB ports. Devices connected to these ports are not detected by the BIOS and operating system. • Enabled—Enables the internal USB ports. Devices connected to these ports are detected by the BIOS and operating system.
USB Port: KVM set UsbPortKVM	<p>Whether the KVM ports are enabled or disabled. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—Disables the KVM keyboard and/or mouse devices. Keyboard and/or mouse will not work in the KVM window. • Enabled—Enables the KVM keyboard and/or mouse devices.
USB Port: VMedia set UsbPortVMedia	<p>Whether the virtual media devices are enabled or disabled. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—Disables the vMedia devices. • Enabled—Enables the vMedia devices.
USB Port: SD Card set UsbPortSdCard	<p>Whether the SD card drives are enabled or disabled. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—Disables the SD card drives. The SD card drives are not detected by the BIOS and operating system. • Enabled—Enables the SD card drives.

PCI Configuration Parameters

Name	Description
Memory Mapped I/O Above 4GB set MemoryMappedIOAbove4GB	<p>Whether to enable or disable memory mapped I/O of 64-bit PCI devices to 4GB or greater address space. Legacy option ROMs are not able to access addresses above 4GB. PCI devices that are 64-bit compliant but use a legacy option ROM may not function correctly with this setting enabled. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The server does not map I/O of 64-bit PCI devices to 4GB or greater address space. • Enabled—The server maps I/O of 64-bit PCI devices to 4GB or greater address space.
ASPM Support set ASPMSupport	<p>Allows you to set the level of ASPM (Active Power State Management) support in the BIOS. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—ASPM support is disabled in the BIOS. • Force L0s—Force all links to L0 standby (L0s) state. • Auto—The CPU determines the power state.
VGA Priority set VgaPriority	<p>Allows you to set the priority for VGA graphics devices if multiple VGA devices are found in the system. This can be one of the following:</p> <ul style="list-style-type: none"> • Onboard—Priority is given to the onboard VGA device. BIOS post screen and OS boot are driven through the onboard VGA port. • Offboard—Priority is given to the PCIe Graphics adapter. BIOS post screen and OS boot are driven through the external graphics adapter port. • Onboard_VGA_Disabled—Priority is given to the PCIe Graphics adapter, and the onboard VGA device is disabled. <p>Note The vKVM does not function when the onboard VGA is disabled.</p>

Serial Configuration Parameters

Name	Description
Console Redirection set ConsoleRedir	<p>Allows a serial port to be used for console redirection during POST and BIOS booting. After the BIOS has booted and the operating system is responsible for the server, console redirection is irrelevant and has no effect. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—No console redirection occurs during POST. • COM_0—Enables console redirection on COM port 0 during POST. • COM_1—Enables console redirection on COM port 1 during POST.
Terminal Type set TerminalType	<p>What type of character formatting is used for console redirection. This can be one of the following:</p> <ul style="list-style-type: none"> • PC-ANSI—The PC-ANSI terminal font is used. • VT100—A supported vt100 video terminal and its character set are used. • VT100+—A supported vt100-plus video terminal and its character set are used. • VT-UTF8—A video terminal with the UTF-8 character set is used. <p>Note This setting must match the setting on the remote terminal application.</p>
Bits per second set BaudRate	<p>What BAUD rate is used for the serial port transmission speed. If you disable Console Redirection, this option is not available. This can be one of the following:</p> <ul style="list-style-type: none"> • 9600—A 9,600 BAUD rate is used. • 19200—A 19,200 BAUD rate is used. • 38400—A 38,400 BAUD rate is used. • 57600—A 57,600 BAUD rate is used. • 115200—A 115,200 BAUD rate is used. <p>Note This setting must match the setting on the remote terminal application.</p>

Name	Description
Flow Control set FlowCtrl	<p>Whether a handshake protocol is used for flow control. Request to Send / Clear to Send (RTS/CTS) helps to reduce frame collisions that can be introduced by a hidden terminal problem. This can be one of the following:</p> <ul style="list-style-type: none"> • None—No flow control is used. • Hardware_RTS/CTS—RTS/CTS is used for flow control. <p>Note This setting must match the setting on the remote terminal application.</p>
Putty KeyPad set PuttyFunctionKeyPad	<p>Allows you to change the action of the PuTTY function keys and the top row of the numeric keypad. This can be one of the following:</p> <ul style="list-style-type: none"> • VT100—The function keys generate ESC OP through ESC O[. • LINUX—Mimics the Linux virtual console. Function keys F6 to F12 behave like the default mode, but F1 to F5 generate ESC [[A through ESC [[E. • XTERMR6—Function keys F5 to F12 behave like the default mode. Function keys F1 to F4 generate ESC OP through ESC OS, which are the sequences produced by the top row of the keypad on Digital terminals. • SCO—The function keys F1 to F12 generate ESC [M through ESC [X. The function and shift keys generate ESC [Y through ESC [j. The control and function keys generate ESC [k through ESC [v. The shift, control and function keys generate ESC [w through ESC [{. • ESCN—The default mode. The function keys match the general behavior of Digital terminals. The function keys generate sequences such as ESC [11~ and ESC [12~. • VT400—The function keys behave like the default mode. The top row of the numeric keypad generates ESC OP through ESC OS.
Redirection After BIOS POST set RedirectionAfterPOST	<p>Whether BIOS console redirection should be active after BIOS POST is complete and control given to the OS bootloader. This can be one of the following:</p> <ul style="list-style-type: none"> • Always_Enable—BIOS Legacy console redirection is active during the OS boot and run time. • Bootloader—BIOS Legacy console redirection is disabled before giving control to the OS boot loader.

Name	Description
Out-of-Band Mgmt Port set comSpcrEnable	<p>Allows you to configure the COM port 0 that can be used for Windows Emergency Management services. ACPI SPCR table is reported based on this setup option. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—Configures the COM port 0 as a general purpose port for use with the Windows Operating System. • Enabled—Configures the COM port 0 as a remote management port for Windows Emergency Management services.

LOM and PCIe Slots Configuration Parameters

Name	Description
All Onboard LOM Ports set AllLomPortControl	<p>Whether all LOM ports are enabled or disabled. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—All LOM ports are disabled. • Enabled—All LOM ports are enabled.
LOM Port <i>n</i> OptionROM set LomOpromControlPort <i>n</i>	<p>Whether Option ROM is available on the LOM port designated by <i>n</i>. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The expansion slot <i>n</i> is not available. • Enabled—The expansion slot <i>n</i> is available. • UEFI_Only—The expansion slot <i>n</i> is available for UEFI only. • Legacy_Only—The expansion slot <i>n</i> is available for legacy only.
All PCIe Slots OptionROM set PcieOptionROMs	<p>Whether the server can use the PCIe Option ROM expansion slots. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The expansion slot <i>n</i> is not available. • Enabled—The expansion slot <i>n</i> is available. • UEFI_Only—The expansion slot <i>n</i> is available for UEFI only. • Legacy_Only—The expansion slot <i>n</i> is available for legacy only.

Name	Description
PCIe Slot:<i>n</i> OptionROM set PcieSlot<i>n</i>OptionROM	Whether PCIe expansion slot <i>n</i> is available to the server. This can be one of the following: <ul style="list-style-type: none"> • Disabled—The expansion slot <i>n</i> is not available. • Enabled—The expansion slot <i>n</i> is available. • UEFI_Only—The expansion slot <i>n</i> is available for UEFI only. • Legacy_Only—The expansion slot <i>n</i> is available for legacy only.
PCIe Mezzanine OptionROM set PcieMezzOptionROM	Whether the PCIe mezzanine slot expansion ROM is available to the server. This can be one of the following: <ul style="list-style-type: none"> • Disabled—The expansion slot <i>n</i> is not available. • Enabled—The expansion slot <i>n</i> is available. • UEFI_Only—The expansion slot <i>n</i> is available for UEFI only. • Legacy_Only—The expansion slot <i>n</i> is available for legacy only.
PCIe Slot:<i>n</i> Link Speed PCIe Slot:<i>n</i>LinkSpeed	This option allows you to restrict the maximum speed of an adapter card installed in PCIe slot <i>n</i> . This can be one of the following: <ul style="list-style-type: none"> • GEN1—2.5GT/s (gigatransfers per second) is the maximum speed allowed. • GEN2—5GT/s is the maximum speed allowed. • GEN3—8GT/s is the maximum speed allowed. • Disabled—The maximum speed is not restricted. <p>For example, if you have a 3rd generation adapter card in PCIe slot 2 that you want to run at a maximum of 5GT/s instead of the 8GT/s that card supports, set the PCIe Slot 2 Link Speed to GEN2. The system then ignores the card's supported maximum speed of 8GT/s and forces it to run at a maximum of 5 GT/s.</p>

Server Management BIOS Parameters for C220 and C240 Servers

Name	Description
FRB-2 Timer set FRB-2	Whether the FRB2 timer is used by CIMC to recover the system if it hangs during POST. This can be one of the following: <ul style="list-style-type: none"> • Disabled—The FRB2 timer is not used. • Enabled—The FRB2 timer is started during POST and used to recover the system if necessary.

Name	Description
OS Watchdog Timer set OSBootWatchdogTimer	<p>Whether the BIOS programs the watchdog timer with a specified timeout value. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The watchdog timer is not used to track how long the server takes to boot. • Enabled—The watchdog timer tracks how long the server takes to boot. If the server does not boot within the length of time specified by the set OSBootWatchdogTimerTimeout command, the CIMC logs an error and takes the action specified by the set OSBootWatchdogTimerPolicy command.
OS Watchdog Timer Timeout set OSBootWatchdogTimerTimeOut	<p>What timeout value the BIOS uses to configure the watchdog timer. This can be one of the following:</p> <ul style="list-style-type: none"> • 5_Minutes—The watchdog timer expires 5 minutes after the OS begins to boot. • 10_Minutes—The watchdog timer expires 10 minutes after the OS begins to boot. • 15_Minutes—The watchdog timer expires 15 minutes after the OS begins to boot. • 20_Minutes—The watchdog timer expires 20 minutes after the OS begins to boot. <p>Note This option is only applicable if you enable the OS Boot Watchdog Timer.</p>
OS Watchdog Timer Policy set OSBootWatchdogTimerPolicy	<p>What action the system takes if the watchdog timer expires. This can be one of the following:</p> <ul style="list-style-type: none"> • Do_Nothing—The server takes no action if the watchdog timer expires during OS boot. • Power_Down—The server is powered off if the watchdog timer expires during OS boot. • Reset—The server is reset if the watchdog timer expires during OS boot. <p>Note This option is only applicable if you enable the OS Boot Watchdog Timer.</p>

Name	Description
Boot Order Rules set ManagedBootRule	<p>How the server changes the boot order list defined through the CIMC GUI or CLI when there are no devices of a particular device type available or when the user defines a different boot order using the server's BIOS Setup Utility.</p> <p>The supported device types are:</p> <ul style="list-style-type: none"> • HDD—Hard disk drive • FDD—Floppy disk drive • CDROM—Bootable CD-ROM or DVD • PXE—PXE boot • EFI—Extensible Firmware Interface <p>The Boot Order Rules option can be one of the following:</p> <ul style="list-style-type: none"> • Strict—When no devices of a particular type are available, the system creates a placeholder for that device type in the boot order list. When a device of that type becomes available, it is added to the boot order in the previously defined position. <p>If the user defines a boot order through the server's BIOS Setup Utility, that boot order is given priority over the boot order configured through the CIMC GUI or CLI. All device types defined through CIMC that are not present in the boot order defined through the BIOS Setup Utility are removed from the boot order list.</p> <ul style="list-style-type: none"> • Loose—When no devices of a particular type are available, the system removes that device type from the boot order. When a device of that type becomes available, the system adds it to the end of the boot order list. <p>If the boot order is configured through the server's BIOS Setup Utility, that boot order is given priority over the boot order configured through the CIMC GUI or CLI. All device types defined through CIMC that are not present in the boot order defined through the BIOS Setup Utility are moved to the end of the boot order list.</p>

C260 Servers

Main BIOS Parameters for C260 Servers

Name	Description
POST Error Pause set POSTErrorPause	What happens when the server encounters a critical error during POST. This can be one of the following: <ul style="list-style-type: none">• Enabled—The BIOS pauses the attempt to boot the server and opens the Error Manager when a critical error occurs during POST.• Disabled—The BIOS continues to attempt to boot the server.
Boot Option Retry set BootOptionRetry	Whether the BIOS retries NON-EFI based boot options without waiting for user input. This can be one of the following: <ul style="list-style-type: none">• Enabled—Continually retries NON-EFI based boot options without waiting for user input.• Disabled—Waits for user input before retrying NON-EFI based boot options.

Advanced BIOS Parameters for C260 Servers

Processor Configuration Parameters

Name	Description
Intel Turbo Boost Technology set IntelTurboBoostTech	Whether the processor uses Intel Turbo Boost Technology, which allows the processor to automatically increase its frequency if it is running below power, temperature, or voltage specifications. This can be one of the following: <ul style="list-style-type: none">• Disabled—The processor does not increase its frequency automatically.• Enabled—The processor utilizes Turbo Boost Technology if required.

Name	Description
Enhanced Intel Speedstep Technology set EnhancedIntelSpeedStep	<p>Whether the processor uses Enhanced Intel SpeedStep Technology, which allows the system to dynamically adjust processor voltage and core frequency. This technology can result in decreased average power consumption and decreased average heat production. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The processor never dynamically adjusts its voltage or frequency. • Enabled—The processor utilizes Enhanced Intel SpeedStep Technology and enables all supported processor sleep states to further conserve power. <p>We recommend that you contact your operating system vendor to make sure the operating system supports this feature.</p>
Intel Hyper-Threading Technology set IntelHyperThread	<p>Whether the processor uses Intel Hyper-Threading Technology, which allows multithreaded software applications to execute threads in parallel within each processor. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The processor does not permit hyperthreading. • Enabled—The processor allows for the parallel execution of multiple threads. <p>We recommend that you contact your operating system vendor to make sure the operating system supports this feature.</p>
Number of Enabled Cores set CoreMultiProcessing	<p>Allows you to disable one or more of the physical cores on the server. This can be one of the following:</p> <ul style="list-style-type: none"> • All—Enables all physical cores. This also enables Hyper Threading on the associated logical processor cores. • 1 through <i>n</i>—Specifies the number of physical processor cores that can run on the server. Each physical core has an associated logical core. <p>We recommend that you contact your operating system vendor to make sure the operating system supports this feature.</p>

Name	Description
Execute Disable set ExecuteDisable	<p>Classifies memory areas on the server to specify where application code can execute. As a result of this classification, the processor disables code execution if a malicious worm attempts to insert code in the buffer. This setting helps to prevent damage, worm propagation, and certain classes of malicious buffer overflow attacks. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The processor does not classify memory areas. • Enabled—The processor classifies memory areas. <p>We recommend that you contact your operating system vendor to make sure the operating system supports this feature.</p>
Intel Virtualization Technology set IntelVT	<p>Whether the processor uses Intel Virtualization Technology (VT), which allows a platform to run multiple operating systems and applications in independent partitions. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The processor does not permit virtualization. • Enabled—The processor allows multiple operating systems in independent partitions. <p>Note If you change this option, you must power cycle the server before the setting takes effect.</p>
Intel VT for Directed IO set IntelVTD	<p>Whether the processor uses Intel Virtualization Technology for Directed I/O (VT-d). This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The processor does not use virtualization technology. • Enabled—The processor uses virtualization technology.
Intel VT-d Interrupt Remapping set InterruptRemap	<p>Whether the processor supports Intel VT-d Interrupt Remapping. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The processor does not support remapping. • Enabled—The processor uses VT-d Interrupt Remapping as required.
Intel VT-d Coherency Support set CoherencySupport	<p>Whether the processor supports Intel VT-d Coherency. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The processor does not support coherency. • Enabled—The processor uses VT-d Coherency as required.

Name	Description
Intel VT-d Address Translation Services set ATS	Whether the processor supports Intel VT-d Address Translation Services (ATS). This can be one of the following: <ul style="list-style-type: none"> • Disabled—The processor does not support ATS. • Enabled—The processor uses VT-d ATS as required.
Intel VT-d PassThrough DMA set PassThroughDMA	Whether the processor supports Intel VT-d Pass-through DMA. This can be one of the following: <ul style="list-style-type: none"> • Disabled—The processor does not support pass-through DMA. • Enabled—The processor uses VT-d Pass-through DMA as required.
Direct Cache Access set DirectCacheAccess	Allows processors to increase I/O performance by placing data from I/O devices directly into the processor cache. This setting helps to reduce cache misses. This can be one of the following: <ul style="list-style-type: none"> • Disabled—Data from I/O devices is not placed directly into the processor cache. • Enabled—Data from I/O devices is placed directly into the processor cache.
Processor C3 Report set ProcessorC3Report	Whether the BIOS sends the C3 report to the operating system. When the OS receives the report, it can transition the processor into the lower C3 power state to decrease energy usage while maintaining optimal processor performance. This can be one of the following: <ul style="list-style-type: none"> • Disabled—The BIOS does not send the C3 report. • ACPI_C2—The BIOS sends the C3 report using the ACPI C2 format, allowing the OS to transition the processor to the C3 low power state. • ACPI_C3—The BIOS sends the C3 report using the ACPI C3 format, allowing the OS to transition the processor to the C3 low power state.

Name	Description
Processor C6 Report set ProcessorC6Report	<p>Whether the BIOS sends the C6 report to the operating system. When the OS receives the report, it can transition the processor into the lower C6 power state to decrease energy usage while maintaining optimal processor performance. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The BIOS does not send the C6 report. • Enabled—The BIOS sends the C6 report, allowing the OS to transition the processor to the C6 low power state.
Package C State Limit set PackageCStateLimit	<p>The amount of power available to the server components when they are idle. This can be one of the following:</p> <ul style="list-style-type: none"> • C0_state—The server provides all server components with full power at all times. This option maintains the highest level of performance and requires the greatest amount of power. • C1_state—When the CPU is idle, the system slightly reduces the power consumption. This option requires less power than C0 and allows the server to return quickly to high performance mode. • C3_state—When the CPU is idle, the system reduces the power consumption further than with the C1 option. This requires less power than C1 or C0, but it takes the server slightly longer to return to high performance mode. • C6_state—When the CPU is idle, the system reduces the power consumption further than with the C3 option. This option saves more power than C0, C1, or C3, but there may be performance issues until the server returns to full power. • C7_state—When the CPU is idle, the server makes a minimal amount of power available to the components. This option saves the maximum amount of power but it also requires the longest time for the server to return to high performance mode. • No_Limit—The server may enter any available C state. <p>Note This option is used only if CPU C State is enabled.</p>

Name	Description
CPU C State set ProcessorCcxEnable	<p>Whether the system can enter a power savings mode during idle periods. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The system remains in high performance state even when idle. • Enabled—The system can reduce power to system components such as the DIMMs and CPUs. The amount of power reduction is specified by the set PackageCStateLimit command.
C1E set ProcessorC1eEnable	<p>Whether the CPU transitions to its minimum frequency when entering the C1 state. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The CPU continues to run at its maximum frequency in C1 state. • Enabled—The CPU transitions to its minimum frequency. This option saves the maximum amount of power in C1 state. <p>Note This option is used only if ProcessorCcxEnable is enabled.</p>

Memory Configuration Parameters

Name	Description
Select Memory RAS set SelectMemoryRAS	<p>How the memory reliability, availability, and serviceability (RAS) is configured for the server. This can be one of the following:</p> <ul style="list-style-type: none"> • Maximum_Performance—System performance is optimized. • Mirroring—System reliability is optimized by using half the system memory as backup. • Sparing—The system reserves some memory for use in the event a DIMM fails. If that happens, the server takes the DIMM offline and replaces it with the reserved memory. This option provides less redundancy than mirroring, but it leaves more of the memory available for programs running on the server.

Name	Description
NUMA Optimized set NUMAOptimize	<p>Whether the BIOS supports NUMA. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The BIOS does not support NUMA. • Enabled—The BIOS includes the ACPI tables that are required for NUMA-aware operating systems. If you enable this option, the system must disable Inter-Socket Memory interleaving on some platforms.
Sparing Mode set SparingMode	<p>The sparing mode used by the CIMC. This can be one of the following:</p> <ul style="list-style-type: none"> • Rank_Sparing—The spared memory is allocated at the rank level. • DIMM Sparing—The spared memory is allocated at the DIMM level. <p>Note This option is used only if set SelectMemoryRAS is set to Sparing.</p>
Mirroring Mode set MirroringMode	<p>Mirroring is supported across Integrated Memory Controllers (IMCs) where one memory riser is mirrored with another. This can be one of the following:</p> <ul style="list-style-type: none"> • Intersocket—Each IMC is mirrored across two sockets. • Intrasocket—One IMC is mirrored with another IMC in the same socket. <p>Note This option is used only if SelectMemoryRAS is set to Mirroring.</p>
DRAM Refresh rate set DramRefreshRate	<p>Allows you to set the rate at which the DRAM cells are refreshed. This can be one of the following:</p> <ul style="list-style-type: none"> • 1x—DRAM cells are refreshed every 64ms. • 2x—DRAM cells are refreshed every 32ms. • 3x—DRAM cells are refreshed every 21ms. • 4x—DRAM cells are refreshed every 16ms. • Auto—DRAM cells refresh rate is automatically chosen by the BIOS based on the system configuration. This is the recommended setting for this parameter.

Name	Description
Patrol Scrub set PatrolScrub	<p>Whether the system actively searches for, and corrects, single bit memory errors even in unused portions of the memory on the server. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The system checks for memory ECC errors only when the CPU reads or writes a memory address. • Enabled—The system periodically reads and writes memory searching for ECC errors. If any errors are found, the system attempts to fix them. This option may correct single bit errors before they become multi-bit errors, but it may adversely affect performance when the patrol scrub is running.
Patrol Scrub Interval set PatrolScrubDuration	<p>Controls the time interval between each patrol scrub memory access. A lower interval scrubs the memory more often but requires more memory bandwidth.</p> <p>Select a value between 5 and 23. The default value is 8.</p> <p>Note This option is used only if Patrol Scrub is enabled.</p>
CKE Low Policy set CkeLowPolicy	<p>Controls the DIMM power savings mode policy. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—DIMMs do not enter power saving mode. • Slow—DIMMs can enter power saving mode, but the requirements are higher. Therefore, DIMMs enter power saving mode less frequently. • Fast—DIMMs enter power saving mode as often as possible. • Auto—The BIOS controls when a DIMM enters power saving mode based on the DIMM configuration.

Serial Port Configuration Parameters

Name	Description
Serial A Enable set Serial-PortA	<p>Whether serial port A is enabled or disabled. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The serial port is disabled. • Enabled—The serial port is enabled.

USB Configuration Parameters

Name	Description
Make Device Non-Bootable set MakeUSBDeviceNonBootable	Whether the server can boot from a USB device. This can be one of the following: <ul style="list-style-type: none"> • Disabled—The server can boot from a USB device. • Enabled—The server cannot boot from a USB device.

PCI Configuration Parameters

Name	Description
Memory Mapped I/O Above 4GB set MemoryMappedIOAbove4GB	Whether to enable or disable memory mapped I/O of 64-bit PCI devices to 4GB or greater address space. Legacy option ROMs are not able to access addresses above 4GB. PCI devices that are 64-bit compliant but use a legacy option ROM may not function correctly with this setting enabled. This can be one of the following: <ul style="list-style-type: none"> • Disabled—The server does not map I/O of 64-bit PCI devices to 4GB or greater address space. • Enabled—The server maps I/O of 64-bit PCI devices to 4GB or greater address space.
Onboard NIC <i>n</i> ROM set NIC- <i>n</i> -ROM	Whether the system loads the embedded PXE option ROM for the onboard NIC designated by <i>n</i> . This can be one of the following: <ul style="list-style-type: none"> • Disabled—PXE option ROM is not available for NIC <i>n</i>. • Enabled—PXE option ROM is available for NIC <i>n</i>.
PCIe OptionROMs set PciOptionRomsDisable	Whether the server can use the PCIe Option ROM expansion slots. This can be one of the following: <ul style="list-style-type: none"> • Disabled—PCIe Option ROMs are not available. • Enabled—PCIe Option ROMs are available. • UEFI_Only—The expansion slot <i>n</i> is available for UEFI only. • Legacy_Only—The expansion slot <i>n</i> is available for legacy only.

Name	Description
PCIe Slot <i>n</i> ROM set Slot-<i>n</i>-ROM	<p>Whether PCIe expansion slot <i>n</i> is available to the server. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The expansion slot <i>n</i> is not available. • Enabled—The expansion slot <i>n</i> is available. • UEFI_Only—The expansion slot <i>n</i> is available for UEFI only. • Legacy_Only—The expansion slot <i>n</i> is available for legacy only.
Onboard Gbit LOM set OnboardNic1	<p>Whether Gbit LOM is enabled or disabled on the server. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—Gbit LOM is not available. • Enabled—10Git LOM is available.
Onboard 10Gbit LOM set OnboardNic2	<p>Whether 10Gbit LOM is enabled or disabled on the server. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—10GBit LOM is not available. • Enabled—10GBit LOM is available.
Srlov set Srlov	<p>Whether SR-IOV (Single Root I/O Virtualization) is enabled or disabled on the server. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—SR-IOV is disabled. • Enabled—SR-IOV is enabled.

Name	Description
IOH Resource Allocation set IOHResource	<p>Enables you to distribute 64KB of 16-bit IO resources between IOH0 and IOH1 as per system requirement. This can be one of the following:</p> <ul style="list-style-type: none"> • IOH0 24k IOH1 40k— Allocates 24KB of 16-bit IO resources to IOH0 and 40KB of 16-bit IO resources to IOH1. • IOH0 32k IOH1 32k— Allocates 32KB of 16-bit IO resources to IOH0 and 32KB of 16-bit IO resources to IOH1. • IOH0 40k IOH1 24k— Allocates 40KB of 16-bit IO resources to IOH0 and 24KB of 16-bit IO resources to IOH1. • IOH0 48k IOH1 16k— Allocates 48KB of 16-bit IO resources to IOH0 and 16KB of 16-bit IO resources to IOH1. • IOH0 56k IOH1 8k— Allocates 56KB of 16-bit IO resources to IOH0 and 8KB of 16-bit IO resources to IOH1.

Server Management BIOS Parameters for C260 Servers

Name	Description
Assert NMI on SERR set AssertNMIONSERR	<p>Whether the BIOS generates a non-maskable interrupt (NMI) and logs an error when a system error (SERR) occurs. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The BIOS does not generate an NMI or log an error when a SERR occurs. • Enabled—The BIOS generates an NMI and logs an error when a SERR occurs. You must enable this setting if you want to enable Assert_NMI_on_PERR.
Assert NMI on PERR set AssertNMIONPERR	<p>Whether the BIOS generates a non-maskable interrupt (NMI) and logs an error when a processor bus parity error (PERR) occurs. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The BIOS does not generate an NMI or log an error when a PERR occurs. • Enabled—The BIOS generates an NMI and logs an error when a PERR occurs. You must enable Assert_NMI_on_SERR to use this setting.

Name	Description
Console Redirection set ConsoleRedir	<p>Allows a serial port to be used for console redirection during POST and BIOS booting. After the BIOS has booted and the operating system is responsible for the server, console redirection is irrelevant and has no effect. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—No console redirection occurs during POST. • Serial_Port_A—Enables console redirection on serial port A during POST. <p>Note If you enable this option, you also disable the display of the Quiet Boot logo screen during POST.</p>
Flow Control set FlowCtrl	<p>Whether a handshake protocol is used for flow control. Request to Send / Clear to Send (RTS/CTS) helps to reduce frame collisions that can be introduced by a hidden terminal problem. This can be one of the following:</p> <ul style="list-style-type: none"> • None—No flow control is used. • RTS-CTS—RTS/CTS is used for flow control. <p>Note This setting must match the setting on the remote terminal application.</p>
Baud Rate set BaudRate	<p>What BAUD rate is used for the serial port transmission speed. If you disable Console Redirection, this option is not available. This can be one of the following:</p> <ul style="list-style-type: none"> • 9.6k—A 9600 BAUD rate is used. • 19.2k—A 19200 BAUD rate is used. • 38.4k—A 38400 BAUD rate is used. • 57.6k—A 57600 BAUD rate is used. • 115.2k—A 115200 BAUD rate is used. <p>Note This setting must match the setting on the remote terminal application.</p>

Name	Description
Terminal Type set TerminalType	<p>What type of character formatting is used for console redirection. This can be one of the following:</p> <ul style="list-style-type: none"> • PC-ANSI—The PC-ANSI terminal font is used. • VT100—A supported vt100 video terminal and its character set are used. • VT100-PLUS—A supported vt100-plus video terminal and its character set are used. • VT-UTF8—A video terminal with the UTF-8 character set is used. <p>Note This setting must match the setting on the remote terminal application.</p>
OS Boot Watchdog Timer Timeout set OSBootWatchdogTimerTimeOut	<p>What timeout value the BIOS uses to configure the watchdog timer. This can be one of the following:</p> <ul style="list-style-type: none"> • 5_Minutes—The watchdog timer expires 5 minutes after the OS begins to boot. • 10_Minutes—The watchdog timer expires 10 minutes after the OS begins to boot. • 15_Minutes—The watchdog timer expires 15 minutes after the OS begins to boot. • 20_Minutes—The watchdog timer expires 20 minutes after the OS begins to boot. <p>Note This option is only applicable if you enable the OS Boot Watchdog Timer.</p>
OS Boot Watchdog Policy set OSBootWatchdogTimerPolicy	<p>What action the system takes if the watchdog timer expires. This can be one of the following:</p> <ul style="list-style-type: none"> • Power_Off—The server is powered off if the watchdog timer expires during OS boot. • Reset—The server is reset if the watchdog timer expires during OS boot. <p>Note This option is only applicable if you enable the OS Boot Watchdog Timer.</p>

Name	Description
Legacy OS Redirection set LegacyOSRedir	<p>Whether redirection from a legacy operating system, such as DOS, is enabled on the serial port. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The serial port enabled for console redirection is hidden from the legacy operating system. • Enabled—The serial port enabled for console redirection is visible to the legacy operating system.
OS Boot Watchdog Timer set OSBootWatchdogTimer	<p>Whether the BIOS programs the watchdog timer with a specified timeout value. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The watchdog timer is not used to track how long the server takes to boot. • Enabled—The watchdog timer tracks how long the server takes to boot. If the server does not boot within the length of time specified by the set OSBootWatchdogTimerTimeout command, the CIMC logs an error and takes the action specified by the set OSBootWatchdogTimerPolicy command.

C420 Servers

Main BIOS Parameters for C420 Servers

Name	Description
TPM Support set TPMAdminCtrl	<p>TPM (Trusted Platform Module) is a microchip designed to provide basic security-related functions primarily involving encryption keys. This option allows you to control the TPM Security Device support for the system. It can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The server does not use the TPM. • Enabled—The server uses the TPM. <p>Note We recommend that you contact your operating system vendor to make sure the operating system supports this feature.</p>

Advanced BIOS Parameters for C420 Servers

Processor Configuration Parameters

Name	Description
Intel Hyper-Threading Technology set IntelHyperThread	<p>Whether the processor uses Intel Hyper-Threading Technology, which allows multithreaded software applications to execute threads in parallel within each processor. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The processor does not permit hyperthreading. • Enabled—The processor allows for the parallel execution of multiple threads. <p>We recommend that you contact your operating system vendor to make sure the operating system supports this feature.</p>
Number of Enabled Cores set CoreMultiProcessing	<p>Allows you to disable one or more of the physical cores on the server. This can be one of the following:</p> <ul style="list-style-type: none"> • All—Enables all physical cores. This also enables Hyper Threading on the associated logical processor cores. • 1 through <i>n</i>—Specifies the number of physical processor cores that can run on the server. Each physical core has an associated logical core. <p>We recommend that you contact your operating system vendor to make sure the operating system supports this feature.</p>
Execute Disable set ExecuteDisable	<p>Classifies memory areas on the server to specify where application code can execute. As a result of this classification, the processor disables code execution if a malicious worm attempts to insert code in the buffer. This setting helps to prevent damage, worm propagation, and certain classes of malicious buffer overflow attacks. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The processor does not classify memory areas. • Enabled—The processor classifies memory areas. <p>We recommend that you contact your operating system vendor to make sure the operating system supports this feature.</p>

Name	Description
Intel VT set IntelVT	<p>Whether the processor uses Intel Virtualization Technology (VT), which allows a platform to run multiple operating systems and applications in independent partitions. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The processor does not permit virtualization. • Enabled—The processor allows multiple operating systems in independent partitions. <p>Note If you change this option, you must power cycle the server before the setting takes effect.</p>
Intel VT-d set IntelVTD	<p>Whether the processor uses Intel Virtualization Technology for Directed I/O (VT-d). This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The processor does not use virtualization technology. • Enabled—The processor uses virtualization technology.
Intel VT-d Coherency Support set CoherencySupport	<p>Whether the processor supports Intel VT-d Coherency. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The processor does not support coherency. • Enabled—The processor uses VT-d Coherency as required.
Intel VT-d ATS Support set ATS	<p>Whether the processor supports Intel VT-d Address Translation Services (ATS). This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The processor does not support ATS. • Enabled—The processor uses VT-d ATS as required.

Name	Description
CPU Performance set CPUPerformance	<p>Sets the CPU performance profile for the server. The performance profile consists of the following options:</p> <ul style="list-style-type: none"> • DCU Streamer Prefetcher • DCU IP Prefetcher • Hardware Prefetcher • Adjacent Cache-Line Prefetch <p>This can be one of the following:</p> <ul style="list-style-type: none"> • Enterprise—All options are enabled. • High_Throughput—Only the DCU IP Prefetcher is enabled. The rest of the options are disabled. • HPC—All options are enabled. This setting is also known as high performance computing. • Custom—All performance profile options can be configured from the BIOS setup on the server. In addition, the Hardware Prefetcher and Adjacent Cache-Line Prefetch options can be configured in the fields below.
Hardware Prefetcher set HardwarePrefetch	<p>Whether the processor allows the Intel hardware prefetcher to fetch streams of data and instruction from memory into the unified second-level cache when necessary. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The hardware prefetcher is not used. • Enabled—The processor uses the hardware prefetcher when cache issues are detected.
Adjacent Cache Line Prefetcher set AdjacentCacheLinePrefetch	<p>Whether the processor fetches cache lines in even/odd pairs instead of fetching just the required line. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The processor only fetches the required line. • Enabled—The processor fetches both the required line and its paired line.

Name	Description
DCU Streamer Prefetch set DcuStreamerPrefetch	<p>Whether the processor uses the DCU IP Prefetch mechanism to analyze historical cache access patterns and preload the most relevant lines in the L1 cache. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The processor does not try to anticipate cache read requirements and only fetches explicitly requested lines. • Enabled—The DCU prefetcher analyzes the cache read pattern and prefetches the next line in the cache if it determines that it may be needed.
DCU IP Prefetcher set DcuIpPrefetch	<p>Whether the processor uses the DCU IP Prefetch mechanism to analyze historical cache access patterns and preload the most relevant lines in the L1 cache. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The processor does not preload any cache data. • Enabled—The DCU IP prefetcher preloads the L1 cache with the data it determines to be the most relevant.
Direct Cache Access Support set DirectCacheAccess	<p>Allows processors to increase I/O performance by placing data from I/O devices directly into the processor cache. This setting helps to reduce cache misses. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—Data from I/O devices is not placed directly into the processor cache. • Enabled—Data from I/O devices is placed directly into the processor cache.

Name	Description
Power Technology set CPUPowerManagement	<p>Enables you to configure the CPU power management settings for the following options:</p> <ul style="list-style-type: none"> • Enhanced Intel Speedstep Technology • Intel Turbo Boost Technology • Processor Power State C6 <p>Power Technology can be one of the following:</p> <ul style="list-style-type: none"> • Custom—The server uses the individual settings for the BIOS parameters mentioned above. You must select this option if you want to change any of these BIOS parameters. • Disabled—The server does not perform any CPU power management and any settings for the BIOS parameters mentioned above are ignored. • Energy_Efficient—The server determines the best settings for the BIOS parameters mentioned above and ignores the individual settings for these parameters.
Enhanced Intel Speedstep Technology set EnhancedIntelSpeedStep	<p>Whether the processor uses Enhanced Intel SpeedStep Technology, which allows the system to dynamically adjust processor voltage and core frequency. This technology can result in decreased average power consumption and decreased average heat production. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The processor never dynamically adjusts its voltage or frequency. • Enabled—The processor utilizes Enhanced Intel SpeedStep Technology and enables all supported processor sleep states to further conserve power. <p>We recommend that you contact your operating system vendor to make sure the operating system supports this feature.</p> <p>Note CPUPowerManagement must be set to Custom or the server ignores the setting for this parameter.</p>

Name	Description
Intel Turbo Boost Technology set IntelTurboBoostTech	<p>Whether the processor uses Intel Turbo Boost Technology, which allows the processor to automatically increase its frequency if it is running below power, temperature, or voltage specifications. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The processor does not increase its frequency automatically. • Enabled—The processor utilizes Turbo Boost Technology if required. <p>Note CPUPowerManagement must be set to Custom or the server ignores the setting for this parameter.</p>
Processor Power State C6 set ProcessorC6Report	<p>Whether the BIOS sends the C6 report to the operating system. When the OS receives the report, it can transition the processor into the lower C6 power state to decrease energy usage while maintaining optimal processor performance. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The BIOS does not send the C6 report. • Enabled—The BIOS sends the C6 report, allowing the OS to transition the processor to the C6 low power state. <p>Note CPUPowerManagement must be set to Custom or the server ignores the setting for this parameter.</p>
Processor Power State C1 Enhanced set ProcessorC1EReport	<p>Whether the CPU transitions to its minimum frequency when entering the C1 state. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The CPU continues to run at its maximum frequency in C1 state. • Enabled—The CPU transitions to its minimum frequency. This option saves the maximum amount of power in C1 state.
Frequency Floor Override set CpuFreqFloor	<p>Whether the CPU is allowed to drop below the maximum non-turbo frequency when idle. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled— The CPU can drop below the maximum non-turbo frequency when idle. This option decreases power consumption but may reduce system performance. • Enabled— The CPU cannot drop below the maximum non-turbo frequency when idle. This option improves system performance but may increase power consumption.

Name	Description
P-STATE Coordination set PsdCoordType	<p>Allows you to define how BIOS communicates the P-state support model to the operating system. There are 3 models as defined by the Advanced Configuration and Power Interface (ACPI) specification.</p> <ul style="list-style-type: none"> • HW_ALL—The processor hardware is responsible for coordinating the P-state among logical processors with dependencies (all logical processors in a package). • SW_ALL—The OS Power Manager (OSPM) is responsible for coordinating the P-state among logical processors with dependencies (all logical processors in a physical package), and must initiate the transition on all of the logical processors. • SW_ANY—The OS Power Manager (OSPM) is responsible for coordinating the P-state among logical processors with dependencies (all logical processors in a package), and may initiate the transition on any of the logical processors in the domain. <p>Note CPUPowerManagement must be set to Custom or the server ignores the setting for this parameter.</p>
Energy Performance set CpuEngPerfBias	<p>Allows you to determine whether system performance or energy efficiency is more important on this server. This can be one of the following:</p> <ul style="list-style-type: none"> • Balanced_Energy • Balanced_Performance • Energy_Efficient • Performance

Memory Configuration Parameters

Name	Description
Select Memory RAS set SelectMemoryRAS	<p>How the memory reliability, availability, and serviceability (RAS) is configured for the server. This can be one of the following:</p> <ul style="list-style-type: none"> • Maximum_Performance—System performance is optimized. • Mirroring—System reliability is optimized by using half the system memory as backup. • Lockstep—If the DIMM pairs in the server have an identical type, size, and organization and are populated across the SMI channels, you can enable lockstep mode to minimize memory access latency and provide better performance. This option offers better system performance than Mirroring and better reliability than Maximum Performance but lower reliability than Mirroring and lower system performance than Maximum Performance.
DRAM Clock Throttling set DRAMClockThrottling	<p>Allows you to tune the system settings between the memory bandwidth and power consumption. This can be one of the following:</p> <ul style="list-style-type: none"> • Balanced—DRAM clock throttling is reduced, providing a balance between performance and power. • Performance—DRAM clock throttling is disabled, providing increased memory bandwidth at the cost of additional power. • Energy_Efficient—DRAM clock throttling is increased to improve energy efficiency.
NUMA set NUMAOptimize	<p>Whether the BIOS supports NUMA. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The BIOS does not support NUMA. • Enabled—The BIOS includes the ACPI tables that are required for NUMA-aware operating systems. If you enable this option, the system must disable Inter-Socket Memory interleaving on some platforms.

Name	Description
Low Voltage DDR Mode set LvDDRMode	<p>Whether the system prioritizes low voltage or high frequency memory operations. This can be one of the following:</p> <ul style="list-style-type: none"> • Power_Saving_Mode—The system prioritizes low voltage memory operations over high frequency memory operations. This mode may lower memory frequency in order to keep the voltage low. • Performance_Mode—The system prioritizes high frequency operations over low voltage operations.
DRAM Refresh rate set DramRefreshRate	<p>Allows you to set the rate at which the DRAM cells are refreshed. This can be one of the following:</p> <ul style="list-style-type: none"> • 1x—DRAM cells are refreshed every 64ms. • 2x—DRAM cells are refreshed every 32ms. • 3x—DRAM cells are refreshed every 21ms. • 4x—DRAM cells are refreshed every 16ms. • Auto—DRAM cells refresh rate is automatically chosen by the BIOS based on the system configuration. This is the recommended setting for this parameter.
Channel Interleaving set ChannelInterLeave	<p>Whether the CPU divides memory blocks and spreads contiguous portions of data across interleaved channels to enable simultaneous read operations. This can be one of the following:</p> <ul style="list-style-type: none"> • Auto—The CPU determines what interleaving is done. • 1_Way—Some channel interleaving is used. • 2_Way • 3_Way • 4_Way—The maximum amount of channel interleaving is used.

Name	Description
Rank Interleaving set RankInterLeave	<p>Whether the CPU interleaves physical ranks of memory so that one rank can be accessed while another is being refreshed. This can be one of the following:</p> <ul style="list-style-type: none"> • Auto—The CPU determines what interleaving is done. • 1_Way—Some rank interleaving is used. • 2_Way • 4_Way • 8_Way—The maximum amount of rank interleaving is used.
Patrol Scrub set PatrolScrub	<p>Whether the system actively searches for, and corrects, single bit memory errors even in unused portions of the memory on the server. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The system checks for memory ECC errors only when the CPU reads or writes a memory address. • Enabled—The system periodically reads and writes memory searching for ECC errors. If any errors are found, the system attempts to fix them. This option may correct single bit errors before they become multi-bit errors, but it may adversely affect performance when the patrol scrub is running.
Demand Scrub set DemandScrub	<p>Whether the system corrects single bit memory errors encountered when the CPU or I/O makes a demand read. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—Single bit memory errors are not corrected. • Enabled—Single bit memory errors are corrected in memory and the corrected data is set in response to the demand read.

Name	Description
Altitude set Altitude	<p>The approximate number of meters above sea level at which the physical server is installed. This can be one of the following:</p> <ul style="list-style-type: none"> • Auto—The CPU determines the physical elevation. • 300_M—The server is approximately 300 meters above sea level. • 900_M—The server is approximately 900 meters above sea level. • 1500_M—The server is approximately 1500 meters above sea level. • 3000_M—The server is approximately 3000 meters above sea level.

QPI Configuration Parameters

Name	Description
QPI Link Frequency set QPILinkFrequency	<p>The Intel QuickPath Interconnect (QPI) link frequency, in gigatransfers per second (GT/s). This can be one of the following:</p> <ul style="list-style-type: none"> • Auto—The CPU determines the QPI link frequency. • 6.4_GT/s • 7.2_GT/s • 8.0_GT/s

USB Configuration Parameters

Name	Description
Legacy USB Support set LegacyUSBSupport	<p>Whether the system supports legacy USB devices. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—USB devices are only available to EFI applications. • Enabled—Legacy USB support is always available. • Auto—Disables legacy USB support if no USB devices are connected.

Name	Description
All USB Devices set AllUsbDevices	Whether all physical and virtual USB devices are enabled or disabled. This can be one of the following: <ul style="list-style-type: none"> • Disabled—All USB devices are disabled. • Enabled—All USB devices are enabled.
USB Port: Rear set UsbPortRear	Whether the rear panel USB devices are enabled or disabled. This can be one of the following: <ul style="list-style-type: none"> • Disabled—Disables the rear panel USB ports. Devices connected to these ports are not detected by the BIOS and operating system. • Enabled—Enables the rear panel USB ports. Devices connected to these ports are detected by the BIOS and operating system.
USB Port: Front set UsbPortFront	Whether the front panel USB devices are enabled or disabled. This can be one of the following: <ul style="list-style-type: none"> • Disabled—Disables the front panel USB ports. Devices connected to these ports are not detected by the BIOS and operating system. • Enabled—Enables the front panel USB ports. Devices connected to these ports are detected by the BIOS and operating system.
USB Port: Internal set UsbPortInt	Whether the internal USB devices are enabled or disabled. This can be one of the following: <ul style="list-style-type: none"> • Disabled—Disables the internal USB ports. Devices connected to these ports are not detected by the BIOS and operating system. • Enabled—Enables the internal USB ports. Devices connected to these ports are detected by the BIOS and operating system.
USB Port: KVM set UsbPortKVM	Whether the KVM ports are enabled or disabled. This can be one of the following: <ul style="list-style-type: none"> • Disabled—Disables the KVM keyboard and/or mouse devices. Keyboard and/or mouse will not work in the KVM window. • Enabled—Enables the KVM keyboard and/or mouse devices.
USB Port: VMedia set UsbPortVMedia	Whether the virtual media devices are enabled or disabled. This can be one of the following: <ul style="list-style-type: none"> • Disabled—Disables the vMedia devices. • Enabled—Enables the vMedia devices.

Name	Description
USB Port: SD Card set UsbPortSdCard	<p>Whether the SD card drives are enabled or disabled. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—Disables the SD card drives. The SD card drives are not detected by the BIOS and operating system. • Enabled—Enables the SD card drives.

PCI Configuration Parameters

Name	Description
MMIO Above 4GB set MemoryMappedIOAbove4GB	<p>Whether to enable or disable memory mapped I/O of 64-bit PCI devices to 4GB or greater address space. Legacy option ROMs are not able to access addresses above 4GB. PCI devices that are 64-bit compliant but use a legacy option ROM may not function correctly with this setting enabled. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The server does not map I/O of 64-bit PCI devices to 4GB or greater address space. • Enabled—The server maps I/O of 64-bit PCI devices to 4GB or greater address space.
ASPM Support set ASPMSupport	<p>Allows you to set the level of ASPM (Active Power State Management) support in the BIOS. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—ASPM support is disabled in the BIOS. • Force L0s—Force all links to L0 standby (L0s) state. • Auto—The CPU determines the power state.

Name	Description
VGA Priority set VgaPriority	<p>Allows you to set the priority for VGA graphics devices if multiple VGA devices are found in the system. This can be one of the following:</p> <ul style="list-style-type: none"> • Onboard—Priority is given to the onboard VGA device. BIOS post screen and OS boot are driven through the onboard VGA port. • Offboard—Priority is given to the PCIE Graphics adapter. BIOS post screen and OS boot are driven through the external graphics adapter port. • Onboard_VGA_Disabled—Priority is given to the PCIE Graphics adapter, and the onboard VGA device is disabled. <p>Note The vKVM does not function when the onboard VGA is disabled.</p>

Serial Configuration Parameters

Name	Description
Console Redirection set ConsoleRedir	<p>Allows a serial port to be used for console redirection during POST and BIOS booting. After the BIOS has booted and the operating system is responsible for the server, console redirection is irrelevant and has no effect. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—No console redirection occurs during POST. • Enabled—Enables console redirection on serial port A during POST.
Terminal Type set TerminalType	<p>What type of character formatting is used for console redirection. This can be one of the following:</p> <ul style="list-style-type: none"> • PC-ANSI—The PC-ANSI terminal font is used. • VT100—A supported vt100 video terminal and its character set are used. • VT100+—A supported vt100-plus video terminal and its character set are used. • VT-UTF8—A video terminal with the UTF-8 character set is used. <p>Note This setting must match the setting on the remote terminal application.</p>

Name	Description
Bits per second set BaudRate	<p>What BAUD rate is used for the serial port transmission speed. If you disable Console Redirection, this option is not available. This can be one of the following:</p> <ul style="list-style-type: none"> • 9600—A 9,600 BAUD rate is used. • 19200—A 19,200 BAUD rate is used. • 38400—A 38,400 BAUD rate is used. • 57600—A 57,600 BAUD rate is used. • 115200—A 115,200 BAUD rate is used. <p>Note This setting must match the setting on the remote terminal application.</p>
Flow Control set FlowCtrl	<p>Whether a handshake protocol is used for flow control. Request to Send / Clear to Send (RTS/CTS) helps to reduce frame collisions that can be introduced by a hidden terminal problem. This can be one of the following:</p> <ul style="list-style-type: none"> • None—No flow control is used. • Hardware_RTS/CTS—RTS/CTS is used for flow control. <p>Note This setting must match the setting on the remote terminal application.</p>
Putty KeyPad set PuttyFunctionKeyPad	<p>Allows you to change the action of the PuTTY function keys and the top row of the numeric keypad. This can be one of the following:</p> <ul style="list-style-type: none"> • VT100—The function keys generate ESC OP through ESC O[. • LINUX—Mimics the Linux virtual console. Function keys F6 to F12 behave like the default mode, but F1 to F5 generate ESC [[A through ESC [[E. • XTERMR6—Function keys F5 to F12 behave like the default mode. Function keys F1 to F4 generate ESC OP through ESC OS, which are the sequences produced by the top row of the keypad on Digital terminals. • SCO—The function keys F1 to F12 generate ESC [M through ESC [X. The function and shift keys generate ESC [Y through ESC [j. The control and function keys generate ESC [k through ESC [v. The shift, control and function keys generate ESC [w through ESC [{. • ESCN—The default mode. The function keys match the general behavior of Digital terminals. The function keys generate sequences such as ESC [11~ and ESC [12~. • VT400—The function keys behave like the default mode. The top row of the numeric keypad generates ESC OP through ESC OS.

Name	Description
Redirection After BIOS POST set <code>RedirectionAfterPOST</code>	<p>Whether BIOS console redirection should be active after BIOS POST is complete and control given to the OS bootloader. This can be one of the following:</p> <ul style="list-style-type: none"> • Always_Enable—BIOS Legacy console redirection is active during the OS boot and run time. • Bootloader—BIOS Legacy console redirection is disabled before giving control to the OS boot loader.

LOM and PCIe Slots Configuration Parameters

Name	Description
All Onboard LOM Ports set <code>AllLomPortControl</code>	<p>Whether all LOM ports are enabled or disabled. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—All LOM ports are disabled. • Enabled—All LOM ports are enabled.
LOM Port <i>n</i> OptionROM set <code>LomOpromControlPort<i>n</i></code>	<p>Whether Option ROM is available on the LOM port designated by <i>n</i>. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—Option ROM is not available on LOM port <i>n</i>. • Enabled—Option ROM is available on LOM port <i>n</i>. • UEFI_Only—The expansion slot <i>n</i> is available for UEFI only. • Legacy_Only—The expansion slot <i>n</i> is available for legacy only.
All PCIe Slots OptionROM set <code>PcieOptionROMs</code>	<p>Whether the server can use the PCIe Option ROM expansion slots. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—PCIe Option ROMs are not available. • Enabled—PCIe Option ROMs are available. • UEFI_Only—The expansion slot <i>n</i> is available for UEFI only. • Legacy_Only—The expansion slot <i>n</i> is available for legacy only.

Name	Description
PCIe Slot:<i>n</i> OptionROM set <code>PcieSlot<i>n</i>OptionROM</code>	Whether PCIe expansion slot <i>n</i> is available to the server. This can be one of the following: <ul style="list-style-type: none"> • Disabled—The expansion slot <i>n</i> is not available. • Enabled—The expansion slot <i>n</i> is available. • UEFI_Only—The expansion slot <i>n</i> is available for UEFI only. • Legacy_Only—The expansion slot <i>n</i> is available for legacy only.
PCIe Slot:<i>n</i> Link Speed PCIe Slot:<i>n</i>LinkSpeed	This option allows you to restrict the maximum speed of an adapter card installed in PCIe slot <i>n</i> . This can be one of the following: <ul style="list-style-type: none"> • GEN1—2.5GT/s (gigatransfers per second) is the maximum speed allowed. • GEN2—5GT/s is the maximum speed allowed. • GEN3—8GT/s is the maximum speed allowed. • Disabled—The maximum speed is not restricted. <p>For example, if you have a 3rd generation adapter card in PCIe slot 2 that you want to run at a maximum of 5GT/s instead of the 8GT/s that card supports, set the PCIe Slot 2 Link Speed to GEN2. The system then ignores the card's supported maximum speed of 8GT/s and forces it to run at a maximum of 5 GT/s.</p>

Server Management BIOS Parameters for C420 Servers

Name	Description
FRB-2 Timer set <code>FRB-2</code>	Whether the FRB2 timer is used by CIMC to recover the system if it hangs during POST. This can be one of the following: <ul style="list-style-type: none"> • Disabled—The FRB2 timer is not used. • Enabled—The FRB2 timer is started during POST and used to recover the system if necessary.

Name	Description
OS Watchdog Timer set OSBootWatchdogTimer	<p>Whether the BIOS programs the watchdog timer with a specified timeout value. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The watchdog timer is not used to track how long the server takes to boot. • Enabled—The watchdog timer tracks how long the server takes to boot. If the server does not boot within the length of time specified by the set OSBootWatchdogTimerTimeout command, the CIMC logs an error and takes the action specified by the set OSBootWatchdogTimerPolicy command.
OS Watchdog Timer Timeout set OSBootWatchdogTimerTimeOut	<p>What timeout value the BIOS uses to configure the watchdog timer. This can be one of the following:</p> <ul style="list-style-type: none"> • 5_Minutes—The watchdog timer expires 5 minutes after the OS begins to boot. • 10_Minutes—The watchdog timer expires 10 minutes after the OS begins to boot. • 15_Minutes—The watchdog timer expires 15 minutes after the OS begins to boot. • 20_Minutes—The watchdog timer expires 20 minutes after the OS begins to boot. <p>Note This option is only applicable if you enable the OS Boot Watchdog Timer.</p>
OS Watchdog Timer Policy set OSBootWatchdogTimerPolicy	<p>What action the system takes if the watchdog timer expires. This can be one of the following:</p> <ul style="list-style-type: none"> • Do_Nothing—The server takes no action if the watchdog timer expires during OS boot. • Power_Down—The server is powered off if the watchdog timer expires during OS boot. • Reset—The server is reset if the watchdog timer expires during OS boot. <p>Note This option is only applicable if you enable the OS Boot Watchdog Timer.</p>

Name	Description
Boot Order Rules set ManagedBootRule	<p>How the server changes the boot order list defined through the CIMC GUI or CLI when there are no devices of a particular device type available or when the user defines a different boot order using the server's BIOS Setup Utility.</p> <p>The supported device types are:</p> <ul style="list-style-type: none"> • HDD—Hard disk drive • FDD—Floppy disk drive • CDROM—Bootable CD-ROM or DVD • PXE—PXE boot • EFI—Extensible Firmware Interface <p>The Boot Order Rules option can be one of the following:</p> <ul style="list-style-type: none"> • Strict—When no devices of a particular type are available, the system creates a placeholder for that device type in the boot order list. When a device of that type becomes available, it is added to the boot order in the previously defined position. <p>If the user defines a boot order through the server's BIOS Setup Utility, that boot order is given priority over the boot order configured through the CIMC GUI or CLI. All device types defined through CIMC that are not present in the boot order defined through the BIOS Setup Utility are removed from the boot order list.</p> <ul style="list-style-type: none"> • Loose—When no devices of a particular type are available, the system removes that device type from the boot order. When a device of that type becomes available, the system adds it to the end of the boot order list. <p>If the boot order is configured through the server's BIOS Setup Utility, that boot order is given priority over the boot order configured through the CIMC GUI or CLI. All device types defined through CIMC that are not present in the boot order defined through the BIOS Setup Utility are moved to the end of the boot order list.</p>

C460 Servers

Main BIOS Parameters for C460 Servers

Name	Description
POST Error Pause set POSTErrorPause	What happens when the server encounters a critical error during POST. This can be one of the following: <ul style="list-style-type: none"> • Enabled—The BIOS pauses the attempt to boot the server and opens the Error Manager when a critical error occurs during POST. • Disabled—The BIOS continues to attempt to boot the server.
Boot Option Retry set BootOptionRetry	Whether the BIOS retries NON-EFI based boot options without waiting for user input. This can be one of the following: <ul style="list-style-type: none"> • Enabled—Continually retries NON-EFI based boot options without waiting for user input. • Disabled—Waits for user input before retrying NON-EFI based boot options.

Advanced BIOS Parameters for C460 Servers

Processor Configuration Parameters

Name	Description
Intel Turbo Boost Technology set IntelTurboBoostTech	Whether the processor uses Intel Turbo Boost Technology, which allows the processor to automatically increase its frequency if it is running below power, temperature, or voltage specifications. This can be one of the following: <ul style="list-style-type: none"> • Disabled—The processor does not increase its frequency automatically. • Enabled—The processor utilizes Turbo Boost Technology if required.

Name	Description
Enhanced Intel Speedstep Technology set EnhancedIntelSpeedStep	<p>Whether the processor uses Enhanced Intel SpeedStep Technology, which allows the system to dynamically adjust processor voltage and core frequency. This technology can result in decreased average power consumption and decreased average heat production. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The processor never dynamically adjusts its voltage or frequency. • Enabled—The processor utilizes Enhanced Intel SpeedStep Technology and enables all supported processor sleep states to further conserve power. <p>We recommend that you contact your operating system vendor to make sure the operating system supports this feature.</p>
Intel Hyper-Threading Technology set IntelHyperThread	<p>Whether the processor uses Intel Hyper-Threading Technology, which allows multithreaded software applications to execute threads in parallel within each processor. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The processor does not permit hyperthreading. • Enabled—The processor allows for the parallel execution of multiple threads. <p>We recommend that you contact your operating system vendor to make sure the operating system supports this feature.</p>
Number of Enabled Cores set CoreMultiProcessing	<p>Allows you to disable one or more of the physical cores on the server. This can be one of the following:</p> <ul style="list-style-type: none"> • All—Enables all physical cores. This also enables Hyper Threading on the associated logical processor cores. • 1 through <i>n</i>—Specifies the number of physical processor cores that can run on the server. Each physical core has an associated logical core. <p>We recommend that you contact your operating system vendor to make sure the operating system supports this feature.</p>

Name	Description
Execute Disable set ExecuteDisable	<p>Classifies memory areas on the server to specify where application code can execute. As a result of this classification, the processor disables code execution if a malicious worm attempts to insert code in the buffer. This setting helps to prevent damage, worm propagation, and certain classes of malicious buffer overflow attacks. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The processor does not classify memory areas. • Enabled—The processor classifies memory areas. <p>We recommend that you contact your operating system vendor to make sure the operating system supports this feature.</p>
Intel Virtualization Technology set IntelVT	<p>Whether the processor uses Intel Virtualization Technology (VT), which allows a platform to run multiple operating systems and applications in independent partitions. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The processor does not permit virtualization. • Enabled—The processor allows multiple operating systems in independent partitions. <p>Note If you change this option, you must power cycle the server before the setting takes effect.</p>
Intel VT for Directed IO set IntelVTD	<p>Whether the processor uses Intel Virtualization Technology for Directed I/O (VT-d). This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The processor does not use virtualization technology. • Enabled—The processor uses virtualization technology.
Intel VT-d Interrupt Remapping set InterruptRemap	<p>Whether the processor supports Intel VT-d Interrupt Remapping. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The processor does not support remapping. • Enabled—The processor uses VT-d Interrupt Remapping as required.
Intel VT-d Coherency Support set CoherencySupport	<p>Whether the processor supports Intel VT-d Coherency. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The processor does not support coherency. • Enabled—The processor uses VT-d Coherency as required.

Name	Description
Intel VT-d Address Translation Services set ATS	Whether the processor supports Intel VT-d Address Translation Services (ATS). This can be one of the following: <ul style="list-style-type: none"> • Disabled—The processor does not support ATS. • Enabled—The processor uses VT-d ATS as required.
Intel VT-d PassThrough DMA set PassThroughDMA	Whether the processor supports Intel VT-d Pass-through DMA. This can be one of the following: <ul style="list-style-type: none"> • Disabled—The processor does not support pass-through DMA. • Enabled—The processor uses VT-d Pass-through DMA as required.
Direct Cache Access set DirectCacheAccess	Allows processors to increase I/O performance by placing data from I/O devices directly into the processor cache. This setting helps to reduce cache misses. This can be one of the following: <ul style="list-style-type: none"> • Disabled—Data from I/O devices is not placed directly into the processor cache. • Enabled—Data from I/O devices is placed directly into the processor cache.
Processor C3 Report set ProcessorC3Report	Whether the BIOS sends the C3 report to the operating system. When the OS receives the report, it can transition the processor into the lower C3 power state to decrease energy usage while maintaining optimal processor performance. This can be one of the following: <ul style="list-style-type: none"> • Disabled—The BIOS does not send the C3 report. • ACPI_C2—The BIOS sends the C3 report using the ACPI C2 format, allowing the OS to transition the processor to the C3 low power state. • ACPI_C3—The BIOS sends the C3 report using the ACPI C3 format, allowing the OS to transition the processor to the C3 low power state.

Name	Description
Processor C6 Report set ProcessorC6Report	<p>Whether the BIOS sends the C6 report to the operating system. When the OS receives the report, it can transition the processor into the lower C6 power state to decrease energy usage while maintaining optimal processor performance. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The BIOS does not send the C6 report. • Enabled—The BIOS sends the C6 report, allowing the OS to transition the processor to the C6 low power state.
Package C State Limit set PackageCStateLimit	<p>The amount of power available to the server components when they are idle. This can be one of the following:</p> <ul style="list-style-type: none"> • C0_state—The server provides all server components with full power at all times. This option maintains the highest level of performance and requires the greatest amount of power. • C1_state—When the CPU is idle, the system slightly reduces the power consumption. This option requires less power than C0 and allows the server to return quickly to high performance mode. • C3_state—When the CPU is idle, the system reduces the power consumption further than with the C1 option. This requires less power than C1 or C0, but it takes the server slightly longer to return to high performance mode. • C6_state—When the CPU is idle, the system reduces the power consumption further than with the C3 option. This option saves more power than C0, C1, or C3, but there may be performance issues until the server returns to full power. • C7_state—When the CPU is idle, the server makes a minimal amount of power available to the components. This option saves the maximum amount of power but it also requires the longest time for the server to return to high performance mode. • No_Limit—The server may enter any available C state. <p>Note This option is used only if CPU C State is enabled.</p>

Name	Description
CPU C State set ProcessorCcxEnable	<p>Whether the system can enter a power savings mode during idle periods. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The system remains in high performance state even when idle. • Enabled—The system can reduce power to system components such as the DIMMs and CPUs. The amount of power reduction is specified by the set PackageCStateLimit command.
C1E set ProcessorC1eEnable	<p>Whether the CPU transitions to its minimum frequency when entering the C1 state. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The CPU continues to run at its maximum frequency in C1 state. • Enabled—The CPU transitions to its minimum frequency. This option saves the maximum amount of power in C1 state. <p>Note This option is used only if ProcessorCcxEnable is enabled.</p>

Memory Configuration Parameters

Name	Description
Select Memory RAS set SelectMemoryRAS	<p>How the memory reliability, availability, and serviceability (RAS) is configured for the server. This can be one of the following:</p> <ul style="list-style-type: none"> • Maximum_Performance—System performance is optimized. • Mirroring—System reliability is optimized by using half the system memory as backup. • Sparing—The system reserves some memory for use in the event a DIMM fails. If that happens, the server takes the DIMM offline and replaces it with the reserved memory. This option provides less redundancy than mirroring, but it leaves more of the memory available for programs running on the server.

Name	Description
NUMA Optimized set NUMAOptimize	<p>Whether the BIOS supports NUMA. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The BIOS does not support NUMA. • Enabled—The BIOS includes the ACPI tables that are required for NUMA-aware operating systems. If you enable this option, the system must disable Inter-Socket Memory interleaving on some platforms.
Sparing Mode set SparingMode	<p>The sparing mode used by the CIMC. This can be one of the following:</p> <ul style="list-style-type: none"> • Rank_Sparing—The spared memory is allocated at the rank level. • DIMM Sparing—The spared memory is allocated at the DIMM level. <p>Note This option is used only if set SelectMemoryRAS is set to Sparing.</p>
Mirroring Mode set MirroringMode	<p>Mirroring is supported across Integrated Memory Controllers (IMCs) where one memory riser is mirrored with another. This can be one of the following:</p> <ul style="list-style-type: none"> • Intersocket—Each IMC is mirrored across two sockets. • Intrasocket—One IMC is mirrored with another IMC in the same socket. <p>Note This option is used only if SelectMemoryRAS is set to Mirroring.</p>
Patrol Scrub set PatrolScrub	<p>Whether the system actively searches for, and corrects, single bit memory errors even in unused portions of the memory on the server. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The system checks for memory ECC errors only when the CPU reads or writes a memory address. • Enabled—The system periodically reads and writes memory searching for ECC errors. If any errors are found, the system attempts to fix them. This option may correct single bit errors before they become multi-bit errors, but it may adversely affect performance when the patrol scrub is running.

Name	Description
Patrol Scrub Interval set PatrolScrubDuration	<p>Controls the time interval between each patrol scrub memory access. A lower interval scrubs the memory more often but requires more memory bandwidth.</p> <p>Select a value between 5 and 23. The default value is 8.</p> <p>Note This option is used only if Patrol Scrub is enabled.</p>
CKE Low Policy set CkeLowPolicy	<p>Controls the DIMM power savings mode policy. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—DIMMs do not enter power saving mode. • Slow—DIMMs can enter power saving mode, but the requirements are higher. Therefore, DIMMs enter power saving mode less frequently. • Fast—DIMMs enter power saving mode as often as possible. • Auto—The BIOS controls when a DIMM enters power saving mode based on the DIMM configuration.

Serial Port Configuration Parameters

Name	Description
Serial A Enable set Serial-PortA	<p>Whether serial port A is enabled or disabled. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The serial port is disabled. • Enabled—The serial port is enabled.

USB Configuration Parameters

Name	Description
Make Device Non-Bootable set MakeUSBDeviceNonBootable	<p>Whether the server can boot from a USB device. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The server can boot from a USB device. • Enabled—The server cannot boot from a USB device.

PCI Configuration Parameters

Name	Description
Memory Mapped I/O Above 4GB set MemoryMappedIOAbove4GB	<p>Whether to enable or disable memory mapped I/O of 64-bit PCI devices to 4GB or greater address space. Legacy option ROMs are not able to access addresses above 4GB. PCI devices that are 64-bit compliant but use a legacy option ROM may not function correctly with this setting enabled. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The server does not map I/O of 64-bit PCI devices to 4GB or greater address space. • Enabled—The server maps I/O of 64-bit PCI devices to 4GB or greater address space.
Onboard NIC <i>n</i> ROM set NIC-<i>n</i>-ROM	<p>Whether the system loads the embedded PXE option ROM for the onboard NIC designated by <i>n</i>. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—PXE option ROM is not available for NIC <i>n</i>. • Enabled—PXE option ROM is available for NIC <i>n</i>.
PCIe OptionROMs set PciOptRomsDisable	<p>Whether the server can use the PCIe Option ROM expansion slots. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—PCIe Option ROMs are not available. • Enabled—PCIe Option ROMs are available. • UEFI_Only—The expansion slot <i>n</i> is available for UEFI only. • Legacy_Only—The expansion slot <i>n</i> is available for legacy only.
PCIe Slot <i>n</i> ROM set Slot-<i>n</i>-ROM	<p>Whether PCIe expansion slot <i>n</i> is available to the server. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The expansion slot <i>n</i> is not available. • Enabled—The expansion slot <i>n</i> is available. • UEFI_Only—The expansion slot <i>n</i> is available for UEFI only. • Legacy_Only—The expansion slot <i>n</i> is available for legacy only.

Name	Description
Onboard Gbit LOM set OnboardNic1	<p>Whether Gbit LOM is enabled or disabled on the server. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—Gbit LOM is not available. • Enabled—10Git LOM is available.
Onboard 10Gbit LOM set OnboardNic2	<p>Whether 10Gbit LOM is enabled or disabled on the server. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—10GBit LOM is not available. • Enabled—10GBit LOM is available.
SrIov set SrIov	<p>Whether SR-IOV (Single Root I/O Virtualization) is enabled or disabled on the server. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—SR-IOV is disabled. • Enabled—SR-IOV is enabled.
IOH Resource Allocation set IOHResource	<p>Enables you to distribute 64KB of 16-bit IO resources between IOH0 and IOH1 as per system requirement. This can be one of the following:</p> <ul style="list-style-type: none"> • IOH0 24k IOH1 40k— Allocates 24KB of 16-bit IO resources to IOH0 and 40KB of 16-bit IO resources to IOH1. • IOH0 32k IOH1 32k— Allocates 32KB of 16-bit IO resources to IOH0 and 32KB of 16-bit IO resources to IOH1. • IOH0 40k IOH1 24k— Allocates 40KB of 16-bit IO resources to IOH0 and 24KB of 16-bit IO resources to IOH1. • IOH0 48k IOH1 16k— Allocates 48KB of 16-bit IO resources to IOH0 and 16KB of 16-bit IO resources to IOH1. • IOH0 56k IOH1 8k— Allocates 56KB of 16-bit IO resources to IOH0 and 8KB of 16-bit IO resources to IOH1.

Server Management BIOS Parameters for C460 Servers

Name	Description
Assert NMI on SERR set AssertNMIONSERR	<p>Whether the BIOS generates a non-maskable interrupt (NMI) and logs an error when a system error (SERR) occurs. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The BIOS does not generate an NMI or log an error when a SERR occurs. • Enabled—The BIOS generates an NMI and logs an error when a SERR occurs. You must enable this setting if you want to enable Assert_NMI_on_PERR.
Assert NMI on PERR set AssertNMIONPERR	<p>Whether the BIOS generates a non-maskable interrupt (NMI) and logs an error when a processor bus parity error (PERR) occurs. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The BIOS does not generate an NMI or log an error when a PERR occurs. • Enabled—The BIOS generates an NMI and logs an error when a PERR occurs. You must enable Assert_NMI_on_SERR to use this setting.
Console Redirection set ConsoleRedir	<p>Allows a serial port to be used for console redirection during POST and BIOS booting. After the BIOS has booted and the operating system is responsible for the server, console redirection is irrelevant and has no effect. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—No console redirection occurs during POST. • Serial_Port_A—Enables console redirection on serial port A during POST. <p>Note If you enable this option, you also disable the display of the Quiet Boot logo screen during POST.</p>
Flow Control set FlowCtrl	<p>Whether a handshake protocol is used for flow control. Request to Send / Clear to Send (RTS/CTS) helps to reduce frame collisions that can be introduced by a hidden terminal problem. This can be one of the following:</p> <ul style="list-style-type: none"> • None—No flow control is used. • RTS-CTS—RTS/CTS is used for flow control. <p>Note This setting must match the setting on the remote terminal application.</p>

Name	Description
Baud Rate set BaudRate	<p>What BAUD rate is used for the serial port transmission speed. If you disable Console Redirection, this option is not available. This can be one of the following:</p> <ul style="list-style-type: none"> • 9.6k—A 9600 BAUD rate is used. • 19.2k—A 19200 BAUD rate is used. • 38.4k—A 38400 BAUD rate is used. • 57.6k—A 57600 BAUD rate is used. • 115.2k—A 115200 BAUD rate is used. <p>Note This setting must match the setting on the remote terminal application.</p>
Terminal Type set TerminalType	<p>What type of character formatting is used for console redirection. This can be one of the following:</p> <ul style="list-style-type: none"> • PC-ANSI—The PC-ANSI terminal font is used. • VT100—A supported vt100 video terminal and its character set are used. • VT100-PLUS—A supported vt100-plus video terminal and its character set are used. • VT-UTF8—A video terminal with the UTF-8 character set is used. <p>Note This setting must match the setting on the remote terminal application.</p>
OS Boot Watchdog Timer Timeout set OSBootWatchdogTimerTimeOut	<p>What timeout value the BIOS uses to configure the watchdog timer. This can be one of the following:</p> <ul style="list-style-type: none"> • 5_Minutes—The watchdog timer expires 5 minutes after the OS begins to boot. • 10_Minutes—The watchdog timer expires 10 minutes after the OS begins to boot. • 15_Minutes—The watchdog timer expires 15 minutes after the OS begins to boot. • 20_Minutes—The watchdog timer expires 20 minutes after the OS begins to boot. <p>Note This option is only applicable if you enable the OS Boot Watchdog Timer.</p>

Name	Description
OS Boot Watchdog Policy set OSBootWatchdogTimerPolicy	<p>What action the system takes if the watchdog timer expires. This can be one of the following:</p> <ul style="list-style-type: none"> • Power_Off—The server is powered off if the watchdog timer expires during OS boot. • Reset—The server is reset if the watchdog timer expires during OS boot. <p>Note This option is only applicable if you enable the OS Boot Watchdog Timer.</p>
Legacy OS Redirection set LegacyOSRedir	<p>Whether redirection from a legacy operating system, such as DOS, is enabled on the serial port. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The serial port enabled for console redirection is hidden from the legacy operating system. • Enabled—The serial port enabled for console redirection is visible to the legacy operating system.
OS Boot Watchdog Timer set OSBootWatchdogTimer	<p>Whether the BIOS programs the watchdog timer with a specified timeout value. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The watchdog timer is not used to track how long the server takes to boot. • Enabled—The watchdog timer tracks how long the server takes to boot. If the server does not boot within the length of time specified by the set OSBootWatchdogTimerTimeout command, the CIMC logs an error and takes the action specified by the set OSBootWatchdogTimerPolicy command.



INDEX

A

- Active Directory [75](#)
 - configuring groups [75](#)
- adapter [52, 93, 142, 143, 144, 145, 146](#)
 - activating firmware [145](#)
 - configuring properties [93](#)
 - exporting the configuration [142](#)
 - firmware [144](#)
 - importing the configuration [143](#)
 - installing firmware [144](#)
 - network [93](#)
 - PCI [52](#)
 - resetting [146](#)
 - restoring default configuration [144](#)
 - viewing properties [93](#)
- adapters [91](#)
 - overview [91](#)
- advanced BIOS parameters [198, 217, 237, 251, 270](#)
 - C22 and C24 servers [198](#)
 - C220 and C240 servers [217](#)
 - C260 server [237](#)
 - C420 servers [251](#)
 - C460 server [270](#)

B

- backing up [192](#)
 - CIMC configuration [192](#)
- bios [190](#)
 - recovering corrupt [190](#)
- BIOS [172, 176](#)
 - installing from remote server [176](#)
 - obtaining firmware from Cisco [172](#)
- BIOS parameters [197, 198, 214, 217, 234, 237, 247, 250, 251, 267, 270, 280](#)
 - advanced parameters for C22 and C24 [198](#)
 - advanced parameters for C220 and C240 [217](#)
 - advanced parameters for C260 [237](#)
 - advanced parameters for C420 [251](#)
 - advanced parameters for C460 [270](#)

BIOS parameters (*continued*)

- main parameters for C22 and C24 [197](#)
 - main parameters for C220 and C240 [217](#)
 - main parameters for C260 [237](#)
 - main parameters for C420 [250](#)
 - main parameters for C460 [270](#)
 - server management parameters for C22 and C24 [214](#)
 - server management parameters for C220 and C240 [234](#)
 - server management parameters for C260 [247](#)
 - server management parameters for C420 [267](#)
 - server management parameters for C460 [280](#)
- #### BIOS settings [17, 37, 38, 39](#)
- advanced [38](#)
 - main [37](#)
 - restoring defaults [39](#)
 - server boot order [17](#)
 - server management [39](#)
- #### BIOS status [36](#)
- viewing [36](#)
- #### boot order [17, 18](#)
- about [17](#)
 - configuring [17](#)
 - viewing [18](#)
- #### boot table [102, 103](#)
- creating entry [102](#)
 - deleting entry [102, 103](#)
 - description [102](#)

C

- C22 and C24 servers [197, 198, 214](#)
 - advanced BIOS parameters [198](#)
 - main BIOS parameters [197](#)
 - server management BIOS parameters [214](#)
- C220 and C240 servers [217, 234](#)
 - advanced BIOS parameters [217](#)
 - main BIOS parameters [217](#)
 - server management BIOS parameters [234](#)
- C260 server [237, 247](#)
 - advanced BIOS parameters [237](#)
 - main BIOS parameters [237](#)

- C260 server *(continued)*
 - server management BIOS parameters [247](#)
- C420 server [250, 267](#)
 - main BIOS parameters [250](#)
 - server management BIOS parameters [267](#)
- C420 servers [251](#)
 - advanced BIOS parameters [251](#)
- C460 server [270, 280](#)
 - advanced BIOS parameters [270](#)
 - main BIOS parameters [270](#)
 - server management BIOS parameters [280](#)
- certificate management [161](#)
 - uploading a certificate [161](#)
- CIMC [44, 171, 172, 173, 174, 180, 181, 182, 191](#)
 - activating firmware [174](#)
 - clearing log [181](#)
 - configuring log threshold [181](#)
 - firmware overview [171](#)
 - installing firmware from remote server [173](#)
 - obtaining firmware from Cisco [172](#)
 - resetting to factory defaults [191](#)
 - sending log [182](#)
 - viewing log [180](#)
 - viewing properties [44](#)
- CIMC CLI [3](#)
- CIMC overview [2](#)
- CIMC-mapped vmedia volume [65, 66, 67](#)
 - cifs [65](#)
 - nfs [65](#)
 - removing [67](#)
 - viewing properties [66](#)
 - www [65](#)
- clearing foreign configuration [132](#)
- common properties [81](#)
- communication services properties [147, 148, 150](#)
 - HTTP properties [147](#)
 - IPMI over LAN properties [150](#)
 - SSH properties [148](#)
- configuration [192, 193](#)
 - backing up [192](#)
 - exporting [192](#)
 - importing [193](#)
- configuring [27](#)
 - fan policy [27](#)
- CPU properties [44](#)
- create virtual drive [129](#)
- Create Virtual Drive [131](#)
- current sensors [58](#)

D

- date [44](#)
 - setting [44](#)
- delete virtual drive [133](#)
- disabling KVM [62](#)
- disabling-auto-learn [139](#)

E

- enabling KVM [62, 63](#)
- enabling-auto-learn [139](#)
- encrypting virtual media [64](#)
- event filters, platform [163, 164](#)
 - about [163](#)
 - configuring [164](#)
- event log, system [184, 185](#)
 - clearing [185](#)
 - viewing [184](#)
- events [163, 164](#)
 - platform [163, 164](#)
 - disabling alerts [164](#)
 - enabling alerts [163](#)
- exporting [192](#)
 - CIMC configuration [192](#)

F

- fan policy [26](#)
 - balanced [26](#)
 - high power [26](#)
 - low power [26](#)
 - maximum power [26](#)
 - performance [26](#)
- fan sensors [56](#)
- fault summary [179](#)
 - viewing [179](#)
- faults, logs [179](#)
 - viewing summary [179](#)
- FEX [124](#)
 - description [124](#)
 - viewing properties [124](#)
- FIP mode [93](#)
 - enabling [93](#)
- firmware [171, 172, 173, 174](#)
 - about [171](#)
 - activating [174](#)
 - installing from remote server [173](#)
 - obtaining from Cisco [172](#)
- Flexible Flash [28, 31, 32, 33, 48](#)
 - booting from [32](#)

Flexible Flash (*continued*)
 configuring properties [31](#)
 description [28](#)
 resetting [33](#)
 viewing properties [48](#)
 floppy disk emulation [64](#)

G

generate NMI [194](#)

H

hard drive locator LED [16](#)
 hot spare [136, 138](#)
 dedicated [136](#)
 global [136, 138](#)
 HTTP properties [147](#)

I

importing [193](#)
 CIMC configuration [193](#)
 initializing virtual drive [133](#)
 IP blocking [87](#)
 IPMI over LAN [150](#)
 description [150](#)
 IPMI over LAN properties [150](#)
 IPv4 properties [82](#)
 iscsi-boot [122](#)
 vNIC [122](#)

K

KVM [62, 63](#)
 configuring [63](#)
 disabling [62](#)
 enabling [62, 63](#)
 KVM console [11, 61](#)

L

LDAP [72, 74](#)
 See also [Active Directory](#)
 configuring in CIMC [74](#)
 See also [Active Directory](#)
 LDAP Server [73](#)
 local users [71](#)

locator LED [16](#)
 hard drive [16](#)
 server [16](#)
 locator-led [141](#)
 bbu [141](#)
 LOM ports [52](#)
 viewing properties [52](#)

M

MAC address [52](#)
 LOM ports [52](#)
 main BIOS parameters [197, 217, 237, 250, 270](#)
 C22 and C24 servers [197](#)
 C220 and C240 servers [217](#)
 C260 server [237](#)
 C420 server [250](#)
 C460 server [270](#)
 making a dedicated hot spare [136](#)
 making a global hot spare [136, 138](#)
 memory properties [45](#)

N

network adapter [93](#)
 viewing properties [93](#)
 network properties [80, 81, 82, 84, 85](#)
 common properties [81](#)
 IPv4 properties [82](#)
 NIC properties [80](#)
 port profile properties [85](#)
 VLAN properties [84](#)
 network security [87](#)
 NIC properties [80](#)
 NIV mode [93](#)
 enabling [93](#)
 NTP settings [88](#)
 Nvidia GPU card information [51](#)
 temperature [51](#)

O

OS boot [13](#)
 USB port [13](#)
 OS installation [11, 12](#)
 methods [11](#)
 PXE [12](#)

P

- PCI adapter [52](#)
 - viewing properties [52](#)
- persistent binding [104, 105, 106](#)
 - description [104](#)
 - disabling [105](#)
 - enabling [105](#)
 - rebuilding [106](#)
- platform event filters [163, 164](#)
 - about [163](#)
 - configuring [164](#)
- platform events [167](#)
 - interpreting traps [167](#)
- Platform events [163, 164](#)
 - disabling alerts [164](#)
 - enabling alerts [163](#)
- port profile properties [85](#)
- power cap policy [23](#)
 - configuring [23](#)
- power capping policy [23](#)
 - about [23](#)
- power cycling the server [21](#)
- power restore policy [25](#)
- power statistics [22](#)
 - viewing [22](#)
- power supply properties [46](#)
- power supply sensors [55](#)
- powering off the server [20](#)
- powering on the server [20](#)
- prepare for removal [137](#)
- PXE installation [12](#)

R

- recovering from a corrupted bios [190](#)
- remote presence [62, 63, 64, 68, 70](#)
 - configuring serial over LAN [68](#)
 - launching serial over LAN [70](#)
 - virtual KVM [62, 63](#)
 - virtual media [64](#)
- reset configuration of cards, Cisco FlexFlash Controller [34](#)
- resetting the server [19](#)
- restore BIOS manufacturing custom defaults [40](#)

S

- SD cards [30](#)
 - single to dual card mirroring [30](#)
- self-signed certificate [159](#)

- sensors [55, 56, 57, 58](#)
 - current [58](#)
 - fan [56](#)
 - power supply [55](#)
 - temperature [56](#)
 - voltage [57](#)
- serial over LAN [68, 70](#)
 - configuring [68](#)
 - launching [70](#)
- server [43](#)
 - viewing properties [43](#)
- server management [16, 17, 19, 20, 21](#)
 - hard drive locator LED [16](#)
 - power cycling the server [21](#)
 - powering off the server [20](#)
 - powering on the server [20](#)
 - resetting the server [19](#)
 - server boot order [17](#)
 - server locator LED [16](#)
 - shutting down the server [19](#)
- server management BIOS parameters [214, 234, 247, 267, 280](#)
 - C22 and C24 servers [214](#)
 - C220 and C240 servers [234](#)
 - C260 server [247](#)
 - C420 server [267](#)
 - C460 server [280](#)
- server NICs [79](#)
- server overview [1](#)
- server software [1](#)
- set as boot drive [134](#)
- shutting down the server [19](#)
- SNMP [151, 153, 154](#)
 - configuring properties [151](#)
 - configuring SNMPv3 users [154](#)
 - configuring trap settings [153](#)
 - sending test message [154](#)
- SSH properties [148](#)
- start-learn-cycle [140](#)
- storage properties [46, 49, 50](#)
 - viewing adapter properties [46](#)
 - viewing physical drive properties [49](#)
 - viewing virtual drive properties [50](#)
- storage sensors [58](#)
 - viewing [58](#)
- synchronize card configuration, FlexFlash Controller [35](#)
- syslog [182](#)
 - sending CIMC log [182](#)
- system event log [184, 185](#)
 - clearing [185](#)
 - viewing [184](#)

T

technical support data [187](#)
 exporting [187](#)
 Telnet [3](#)
 temperature sensors [56](#)
 time [44](#)
 setting [44](#)

U

undo prepare for removal [138](#)
 Updating Firmware on Server Components [41](#)
 uploading a server certificate [161](#)
 user management [71, 74, 77](#)
 LDAP [74](#)
 local users [71](#)
 terminating user sessions [77](#)
 viewing user sessions [77](#)
 user sessions [77](#)
 terminating [77](#)
 viewing [77](#)
 usNIC [120](#)
 viewing properties [120](#)

V

vHBA [94, 95, 96, 100, 101, 102, 103, 104, 105, 106](#)
 boot table [102](#)
 creating [100](#)
 creating boot table entry [102](#)
 deleting [101](#)
 deleting boot table entry [102, 103](#)
 disabling persistent binding [105](#)
 enabling persistent binding [105](#)
 guidelines for managing [94](#)
 modifying properties [96](#)

vHBA (*continued*)
 persistent binding [104](#)
 rebuilding persistent binding [106](#)
 viewing properties [95](#)
 viewing storage controller logs [141](#)
 virtual drive [133, 134, 135](#)
 initializing [133](#)
 modifying attributes [135](#)
 set as boot drive [134](#)
 virtual KVM [62, 63](#)
 virtual media [64](#)
 VLAN properties [84](#)
 VM FEX [124](#)
 description [124](#)
 viewing properties [124](#)
 vNIC [107, 108, 113, 114, 121, 122, 123](#)
 creating [113](#)
 deleting [114](#)
 guidelines for managing [107](#)
 iscsi-boot [122](#)
 iscsi-boot deletion [123](#)
 modifying properties [108](#)
 usnic deletion [121](#)
 viewing properties [107](#)
 vNICs [122](#)
 iSCSI-boot guidelines [122](#)
 voltage sensors [57](#)

X

XML API [149](#)
 description [149](#)
 enabling [149](#)

Y

YAML [8](#)

