Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide, Release 3.0

First Published: 2016-12-13

Last Modified: 2017-04-27

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

CONTENTS

Preface

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 *this font*.
TUI elements	In a Text-based User Interface, text the system displays appears in `this font`.
System output	Terminal sessions and information that the system displays appear in `this font`.
CLI commands	CLI command keywords appear in **this font**. Variables in a CLI command appear in *this font*.

Text Type	Indication
[ ]	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.

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

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

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

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.

For information on supported firmware versions and supported UCS Manager versions for the rack servers that are integrated with the UCS Manager for management, refer to Release Bundle Contents for Cisco UCS Software.

Other Documentation Resources

Follow Cisco UCS Docs on Twitter to receive document update notifications.

CHAPTER 1

Overview

This chapter includes the following sections:

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

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

- Cisco UCS C22 M3 Rack-Mount Server
- Cisco UCS C24 M3 Rack-Mount Server
- Cisco UCS C220 M3 Rack-Mount Server
- Cisco UCS C240 M3 Rack-Mount Server
- Cisco UCS C3160 M3 Rack-Mount Server
- Cisco UCS C220 M4 Rack-Mount Server
- Cisco UCS C240 M4 Rack-Mount Server
- Cisco UCS C460 M4 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 Cisco IMC firmware.

Cisco IMC Firmware

Cisco IMC is a separate management module built into the motherboard. A dedicated ARM-based processor, separate from the main server CPU, runs the Cisco IMC firmware. The system ships with a running version of the Cisco IMC firmware. You can update the Cisco IMC 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 Cisco IMC to install an OS on the server using the KVM console and vMedia.

Cisco Integrated Management Controller

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

Note The Cisco IMC 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 or an XML-based API 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 Cisco IMC GUI to invoke Cisco IMC CLI
- View a command that has been invoked through Cisco IMC CLI in Cisco IMC GUI
- Generate Cisco IMC CLI output from Cisco IMC GUI

Tasks You Can Perform in Cisco IMC

You can use Cisco IMC to perform the following server management tasks:

- Power on, power off, power cycle, reset and shut down the server
- Toggle the locator LED
- Configuring BIOS settings
- 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, IPMI Over LAN, and SNMP.
- Manage certificates
- Configure platform event filters
- Update Cisco IMC firmware
- Monitor faults, alarms, and server status
- Set time zone and view local time
- Install and activate Cisco IMC firmware
- Install and activate BIOS firmware

No Operating System or Application Provisioning or Management

Cisco IMC 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-Cisco IMC user accounts
- Configure or manage external storage on the SAN or NAS storage

Cisco IMC CLI

The Cisco IMC CLI is a command-line management interface for Cisco UCS C-Series servers. You can launch the Cisco IMC 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 #
boot-device	**scope boot-device** command from bios mode	/bios/boot-device #
certificate	**scope certificate** command from EXEC mode	/certificate #
chassis	**scope chassis** command from EXEC mode	/chassis #
adapter	**scope adapter** *index* 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 #
dimm-summary	**scope dimm-summary** *index* command from chassis mode	/chassis/dimm-summary #
flexflash	**scope flexflash** *index* 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** *slot* 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** *index* 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** *user-number* command from EXEC mode	/user #
`user-session`	**scope user-session** *session-number* command from EXEC mode	/user-session #
`vmedia`	**scope vmedia** command from EXEC mode	/vmedia #
`xmlapi`	**scope xmlapi** command from EXEC mode	/xmlapi #
`dimm-blacklisting`	**scope dimm-blacklisting** command from EXEC mode	/dimm-blacklisting #
`reset-ecc`	**scope reset-ecc** command from EXEC mode	/ reset-ecc #

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.

Smart Access: Serial

The Smart Access: Serial allows offline configuration of C-series servers using the command line interface (CLI) through serial connection. With this setup, you are not required to connect the Cisco IMC to the network in order to access the command line interface.

The serial connection can be accessed using either the KVM dongle (DB9), or the serial port (RJ-45) at the rear of the chassis.

Once you have completed the setup and the BIOS and OS messages are visible on the console, you can view the Cisco IMC CLI by pressing Esc+9. You are required to authenticate the connection with Cisco IMC user credentials. The default user name is admin and default password is password. You can press Esc+8 to switch back to the BIOS or OS on the same console.

When the session is created, the session is visible on the Web UI sessions tab as a serial connection.

Note Note the following limitations while using the CLI through a serial connection:

- You cannot use the arrow keys to revert to previously executed commands.
- The CLI is not visible when the terminal type is set to either **VT100+** or **VTUFT8**.
- The smart access feature does not work as expected after an OS boot unless the "`console`" property in the grub configuration file of the OS is set to **ttyS0**. You must set the "`console`" property in the grub configuration file of the OS to **ttyS0** for it to work as expected.

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.

Logging In to Cisco IMC

Procedure

Step 1 Connect to the console port.

Step 2 When logging in to an unconfigured system for the first time, use **admin** as the username and **password** as the password.
The following situations occur when you login to the CLI for the first time:

- You cannot perform any operation until you change default admin credentials on the Cisco IMC web UI or CLI.

Note After an upgrade from Cisco IMC version 1.5(x) or 2.0(1) to the latest version, or when you do a factory reset, during first login Cisco IMC prompts for a password change. You cannot choose the word 'password' as your new password. If this creates problems for any scripts you may be running, you could change it to password by logging back into the user management options, but this is ENTIRELY at your own risk. It is not recommended by Cisco.

The following example shows how to login in to Cisco IMC first time:

```
Login as # admin
admin10.101.255.255's password # password

***********************WARNING*******************
Default credentials were used for login.
Administration passwords needs to be changed for security purpose.
********************************************************************

Enter current password # abcxyz
```

```
Re-enter new password # abcxyz
Updating password...
Password updated successfully.
Server #
```

CHAPTER 2

Installing the Server OS

This chapter includes the following sections:

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 Cisco IMC 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. Always follow your OS vendors recommended configuration, including software interoperability and driver compatibility. For more information on driver recommendations and installation, follow the Cisco UCS Hardware Compatibility list here:

https://ucshcltool.cloudapps.cisco.com/public/

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.

CHAPTER 3

Managing the Server

This chapter includes the following sections:

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 Front Locator LED for the Chassis

This option is available only on some UCS C-Series servers.

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 front-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 front-locator-led off
Server /chassis *# commit

Server /chassis #
```

Toggling the Locator LED for a Hard Drive

This action is available only on some UCS C-Series servers.

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** *drivenum* {**1** | **2**}	Where *drivenum* 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 #
```

Selecting a Time Zone

Selecting a Time Zone

Selecting a time zone helps you choose a local time zone so that you can view the local time rather than the default machine time. Cisco IMC Web UI and the CLI provide you options to choose and set a time zone of your choice.

Setting the time zone to your local time will apply the time zone variable to all the services that utilize the system timing. This impacts the logging information and is utilized in the following applications of the Cisco IMC:

- Fault summary and fault history logs
- Cisco IMC log
- rsyslog

When you set a local time, the timestamp on the applications that you can view are updated with the local time that you have chosen.

Selecting a Time Zone

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 CIMC**	Enters Cisco IMC command mode.
Step 2	Server /CIMC # **timezone-select**	Displays a list of continents and oceans.
Step 3	Enter the number corresponding to your continent or ocean.	A list of all the countries or regions of the chosen continent or ocean displays.
Step 4	Enter the number corresponding to the country or region that you want to set as your time zone.	If a country or a region has more than one time zones, a list of time zones in that country or region displays.
Step 5	Enter the number corresponding to time zone.	**Is the above information OK?** message appears.
Step 6	Enter **1**.	**Continue?[y|N]**: prompt appears.
Step 7	Enter **y** if you want to set the chosen time zone.	The chosen time zone is set as the time zone for your Cisco IMC server.

This example sets the time zone:

```
Server# scope CIMC
Server /CIMC # timezone-select

Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
1) Africa
2) Americas
3) Antarctica
4) Arctic Ocean
5) Asia
6) Atlantic Ocean
7) Australia
8) Europe
9) Indian Ocean
10) Pacific Ocean
#? 2
Please select a country whose clocks agree with yours.
1) Anguilla
2) Antigua & Barbuda
3) Argentina
4) Aruba
5) Bahamas
6) Barbados
7) Belize
8) Bolivia
9) Brazil
10) Canada
11) Caribbean Netherlands
12) Cayman Islands
13) Chile
```

```
14) Colombia
15) Costa Rica
16) Cuba
17) Curacao
18) Dominica
19) Dominican Republic
20) Ecuador
21) El Salvador
22) French Guiana
23) Greenland
24) Grenada
25) Guadeloupe
26) Guatemala
27) Guyana
28) Haiti
29) Honduras
30) Jamaica
31) Martinique
32) Mexico
33) Montserrat
34) Nicaragua
35) Panama
36) Paraguay
37) Peru
38) Puerto Rico
39) St Barthelemy
40) St Kitts & Nevis
41) St Lucia
42) St Maarten (Dutch part)
43) St Martin (French part)
44) St Pierre & Miquelon
45) St Vincent
46) Suriname
47) Trinidad & Tobago
48) Turks & Caicos Is
49) United States
50) Uruguay
51) Venezuela
52) Virgin Islands (UK)
53) Virgin Islands (US)
#? 49
Please select one of the following time zone regions.
1) Eastern Time
2) Eastern Time - Michigan - most locations
3) Eastern Time - Kentucky - Louisville area
4) Eastern Time - Kentucky - Wayne County
5) Eastern Time - Indiana - most locations
6) Eastern Time - Indiana - Daviess, Dubois, Knox & Martin Counties
7) Eastern Time - Indiana - Pulaski County
8) Eastern Time - Indiana - Crawford County
9) Eastern Time - Indiana - Pike County
10) Eastern Time - Indiana - Switzerland County
11) Central Time
12) Central Time - Indiana - Perry County
13) Central Time - Indiana - Starke County
14) Central Time - Michigan - Dickinson, Gogebic, Iron & Menominee Counties
15) Central Time - North Dakota - Oliver County
16) Central Time - North Dakota - Morton County (except Mandan area)
17) Central Time - North Dakota - Mercer County
18) Mountain Time
19) Mountain Time - south Idaho & east Oregon
20) Mountain Standard Time - Arizona (except Navajo)
21) Pacific Time
22) Alaska Time
23) Alaska Time - Alaska panhandle
24) Alaska Time - southeast Alaska panhandle
25) Alaska Time - Alaska panhandle neck
26) Alaska Time - west Alaska
27) Aleutian Islands
28) Metlakatla Time - Annette Island
29) Hawaii
#? 8
```

```
The following information has been given:

        United States
        Eastern Time - Indiana - Crawford County

Is the above information OK?
1) Yes
2) No
#? 1

You have chosen to set timezone settings to:

        America/Indiana/Marengo

Continue?[y|N]: y
Timezone has been updated.
The local time now is: Sun Jun 1 02:21:15 2014 EST

Server /CIMC #
```

Managing the Server Boot Order

Server Boot Order

Using Cisco IMC, you can configure the order in which the server attempts to boot from available boot device types. In the legacy boot order configuration, Cisco IMC allows you to reorder the device types but not the devices within the device types. With the precision boot order configuration, you can have a linear ordering of the devices. In the web UI or CLI you can change the boot order and boot mode, add multiple devices under each device types, rearrange the boot order, set parameters for each device type.

When you change the boot order configuration, Cisco IMC sends the configured boot order to BIOS the next time that server is rebooted. To implement the new boot order, reboot the server after you make the configuration change. The new boot order takes effect on any subsequent reboot. The configured boot order remains until the configuration is changed again in Cisco IMC or in the BIOS setup.

Note The actual boot order differs from the configured boot order if either of the following conditions occur:

- BIOS encounters issues while trying to boot using the configured boot order.
- A user changes the boot order directly through BIOS.
- BIOS appends devices that are seen by the host but are not configured from the user.

Note When you create a new policy using the configure boot order feature, BIOS tries to map this new policy to the devices in the system. It displays the actual device name and the policy name to which it is mapped in the **Actual Boot Order** area. If BIOS cannot map any device to a particular policy in Cisco IMC, the actual device name is stated as **NonPolicyTarget** in the **Actual Boot Order** area.

Note When you upgrade Cisco IMC to the latest version 2.0(x) for the first time, the legacy boot order is migrated to the precision boot order. During this process, previous boot order configuration is erased and all device types configured before updating to 2.0 version are converted to corresponding precision boot device types and some dummy devices are created for the same device types. you can view these devices in the **Configured Boot Order** area in the web UI. To view these devices in the CLI, enter **show boot-device** command. During this the server's actual boot order is retained and it can be viewed under actual boot order option in web UI and CLI.

When you downgrade Cisco IMC prior to 2.0(x) verison the server's last legacy boot order is retained, and the same can be viewed under **Actual Boot Order** area. For example:

- If you configured the server in a legacy boot order in 2.0(x) version, upon downgrade a legacy boot order configuration is retained.
- If you configured the server in a precision boot order in 2.0(x), upon downgrade the last configured legacy boot order is retained.

Important

- Boot order configuration prior to 2.0(x) is referred as legacy boot order. If your running version is 2.0(x), then you cannot configure legacy boot order through web UI, but you can configure through CLI and XML API. In the CLI, you can configure it by using **set boot-order HDD,PXE** command. Even though, you can configure legacy boot order through CLI or XML API, in the web UI this configured boot order is not displayed.
- Legacy and precision boot order features are mutually exclusive. You can configure either legacy or precision boot order. If you configure legacy boot order, it disables all the precision boot devices configured. If you configure precision boot order, then it erases legacy boot order configuration.

Viewing the Boot Device Detail

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 the BIOS command mode.
Step 2	Server /bios # **show boot-device [detail]**.	Displays the detailed information of the boot device.

This example displays the details of the created bootable device:

```
Server# scope bios
Server /bios # show boot-device
Boot Device          Device Type  Device State       Device Order
-------------------- ------------ ------------------ ----------------
TestUSB              USB          Enabled            1
TestPXE              PXE          Enabled            2
Server /bios # show boot-device detail
Boot Device TestSAN:
    Device Type: SAN
    Device State: Enabled
    Device Order: 1
    Slot Id:
    Lun Id:
Boot Device TestUSB:
    Device Type: USB
    Device State: Enabled
    Device Order: 2
    Sub Type: HDD
Boot Device TestPXE:
    Device Type: PXE
    Device State: Enabled
    Device Order: 3
    Slot Id: L
    Port Number: 1
```

Configuring the Precision 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 the BIOS command mode.
Step 2	Server /bios # **create-boot-device**[*device name*] [*device type*].	Creates a bootable device that BIOS chooses to boot. This can be one of the following: • **HDD—**Hard disk drive • **PXE—**PXE boot • **SAN** boot • **iSCSI** boot • **SD** Card **Note** SD card option is available only on some UCS C-Series servers. • **USB** • **Virtual Media**

	Command or Action	Purpose
		• **PCHStorage** • **UEFISHELL**
Step 3	Server /bios # **scope boot-device** *created boot device name*.	Enters the management of the created bootable devices.
Step 4	Server /bios /boot-device # **set** *values*	Specifies the property values for particular bootable device. You can set one or more of the following: • cli— CLI options • state— Whether the device will be visible by BIOS. By default the device is disabled. **Note** If enabled, the device will overwrite the legacy boot order configuration. • slot— Slot id where the device is plugged in. • port— Port of the slot in which the device is present. • LUN— Logical unit in a slot where the device is present. • sub-type—Sub device type under a certain device type. • order—The order of the device in the available list of devices.
Step 5	Server /bios /boot-device # **commit**	Commits the transaction to the system configuration.

This example configures the boot order, creates a boot device, set the attributes of the new device and commit the transaction:

```
Server# scope bios
Server /bios #  create boot-device TestPXE PXE
Server /bios #  scope boot-device TestPXE
Server /bios /boot-device #  set state Enabled
Server /bios /boot-device #  set slot L
Server /bios /boot-device #  set port 1
Server /bios /boot-device #  set order 1
Server /bios /boot-device #  commit
Enabling boot device will overwrite Legacy Boot Order configuration
Continue?[y|N]y
Server /bios /boot-device #  y
Commiting device configuration
Server /bios/boot-device # show detail
BIOS:
    BIOS Version: "C240M3.2.0.0.15 (Build Date: 03/16/2014)"
    Boot Order: (none)
    Boot Override Priority:
    FW Update/Recovery Status: None, OK
    UEFI Secure Boot: disabled
    Configured Boot Mode: None
    Actual Boot Mode: Legacy
    Last Configured Boot Order Source: CIMC
```

```
Server /bios/boot-device # show boot-device detail
Boot Device TestPXE:
    Device Type: PXE
    Device State: Enabled
    Device Order: 1
    Slot Id: L
    Port Number: 1
```

What to Do Next

Reboot the server to boot with your new boot order.

Modifying the Attributes of a Boot Device

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 the BIOS command mode.
Step 2	Server /bios # **scope boot-device** *created boot device name*.	Enters the management of the created bootable devices.
Step 3	Server /bios /boot-device # **set state** {*Enabled*|*Disabled*}.	Enables or disables the device. The default state is disabled. **Note** If enabled, the device will overwrite the legacy boot order configuration.
Step 4	Server /bios /boot-device* # **set order** {*Index* | *1-50*}.	Specifies the order of booting for particular device in the device list. Enter a number between 1 and 50 based on the total number of created device. **Note** When you set the boot device order individually, it is not assured that the order appears in the way it was set. So, it is recommended that to set the order for multiple devices in a single execution, use **re-arrange-boot-device** command.
Step 5	Server /bios /boot-device* # **set port** {*value* | *1-255* }.	Specifies the port of the slot in which the device is present. Enter a number between 1 and 255.
Step 6	Server /bios /boot-device* # **commit**	Commits the transaction to the system configuration.

This example modifies the attributes of an existing device:

```
Server# scope bios
Server /bios *# scope boot-device scu-device-hdd
```

```
Server /bios/boot-device # set status enabled
Server /bios/boot-device *# set order 2
Server /bios/boot-device *# set port 1
Server /bios/boot-device *# commit
Enabling boot device will overwrite boot order Level 1 configuration
Continue?[y|N]y
Server /bios/boot-device #
```

Rearranging Device 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 the BIOS command mode.
Step 2	Server /bios # **rearrange boot-device**[*device name*]:[*position*].	Rearranges the selected boot devices in a single execution.

This example rearranges the selected boot devices:

```
Server# scope bios
Server /bios # rearrange-boot-device  TestPXE:1,TestUSB:2
 Server /bios # show boot-device
Boot Device          Device Type  Device State       Device Order
-------------------- ------------ ------------------ ----------------
TestPXE              PXE          Disabled           1
TestUSB              USB          Disabled           2

Server /bios #
```

What to Do Next

Re-Applying the Boot Order Configuration

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 the BIOS command mode.
Step 2	Server /bios # **re-apply**.	Re-applies the boot order to BIOS, if the last configured boot order source is BIOS..

This example re-applies the boot order to BIOS:

```
Server# scope bios
Server /bios # re-apply
Server /bios #
```

What to Do Next

Reboot the host after reapplying the boot order to BIOS.

Deleting an Existing Boot Device

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 the BIOS command mode.
Step 2	Server /bios # **remove-boot-device** *device name*	Deletes the particular device from the boot order.

This example deletes the selected device from the device list:

```
Server# scope bios
Server /bios # remove-boot-device scu-device-hdd
Server /bios #
```

Overview to UEFI Secure Boot

You can use Unified Extensible Firmware Interface (UEFI) secure boot to ensure that all the EFI drivers, EFI applications, option ROM or operating systems prior to loading and execution are signed and verified for authenticity and integrity, before you load and execute the operating system. You can enable this option using either web UI or CLI. When you enable UEFI secure boot mode, the boot mode is set to UEFI mode and you cannot modify the configured boot mode until the UEFI boot mode is disabled.

Note If you enable UEFI secure boot on a nonsupported OS, on the next reboot, you cannot boot from that particular OS. If you try to boot from the previous OS, an error is reported and recorded the under system software event in the web UI. You must disable the UEFI secure boot option using Cisco IMC to boot from your previous OS.

Important Also, if you use an unsupported adapter, an error log event in Cisco IMC SEL is recorded. The error messages is displayed that says:

System Software event: Post sensor, System Firmware error. EFI Load Image Security Violation. [0x5302] was asserted .

UEFI secure boot is supported on the following components:

Components	Types
Supported OS	• Windows Server 2012 • Windows Server 2012 R2
Broadcom PCI adapters	• 5709 dual and quad port adapters • 57712 10GBASE-T adapter • 57810 CNA • 57712 SFP port
Intel PCI adapters	• i350 quad port adapter • X520 adapter • X540 adapter • LOM
QLogic PCI adapters	• 8362 dual port adapter • 2672 dual port adapter
Fusion-io	

Components	Types
LSI	• LSI MegaRAID SAS 9240-8i • LSI MegaRAID SAS 9220-8i • LSI MegaRAID SAS 9265CV-8i • LSI MegaRAID SAS 9285CV-8e • LSI MegaRAID SAS 9285CV-8e • LSI MegaRAID SAS 9266-8i • LSI SAS2008-8i mezz • LSI Nytro card

Enabling UEFI Secure Boot Mode

Before You Begin

Procedure

	Command or Action	Purpose
Step 1	Server# **scope bios**	Enters the BIOS command mode.
Step 2	Server/ BIOS # **set secure-boot enable | disable**	Enables or disables UEFI secure boot. **Note** If enabled, the boot mode is set to UEFI secure mode. You cannot modify configure boot mode until UEFI secure boot mode is disabled.

This example enables UEFI secure boot mode and commits the transaction

```
Server# scope bios
Server /bios # set secure-boot enable
Setting Value : enable
Commit Pending.
Server /bios *# commit
UEFI Secure boot state changed successfully. Execute 'show detail' command to check the
current status
Server /bios #
```

What to Do Next

Reboot the server to have your configuration boot mode settings take place.

Disabling UEFI Secure Boot

Procedure

	Command or Action	Purpose
Step 1	Server# **scope bios**	Enters the BIOS command mode.
Step 2	Server/ BIOS # **set secure-boot enable | disable**	Enables or disables UEFI secure boot.

This example disables UEFI secure boot mode and commits the transaction

```
Server# scope bios
Server /bios # set secure-boot disable
Setting Value : enable
Commit Pending.
Server /bios *# commit
UEFI Secure boot state changed successfully. Execute 'show detail' command to check the
current status
Server /bios #
```

What to Do Next

Reboot the server to have your configuration boot mode settings take place.

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 Cisco IMC.

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 of the legacy 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 #
```

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

```
Server /bios # show actual-boot-order
Boot Order   Boot Device                         Device Type     Boot Policy
------------ ----------------------------------- --------------- --------------------
1            IBA GE Slot 0201 v1398              PXE             TestPXE
2            IBA GE Slot 0200 v1398              PXE             NonPolicyTarget
3            IBA GE Slot 0202 v1398              PXE             NonPolicyTarget
4            IBA GE Slot 0203 v1398              PXE             NonPolicyTarget
5            "UEFI: Built-in EFI Shell "         EFI             NonPolicyTarget
Server  /bios #
```

Configuring a Server to Boot With a One-Time Boot Device

You can configure a server to boot from a particular device only for the next server boot, without disrupting the currently configured boot order. Once the server boots from the one time boot device, all its future reboots occur from the previously configured boot order.

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 the BIOS command mode.
Step 2	Server# /bios **show boot-device**	Displays the list of available boot drives.
Step 3	Server# /bios **set one-time-boot-device** *device-order*	Sets the boot order. **Note** The host boots to the one time boot device even when configured with a disabled advanced boot device.
Step 4	Server# /bios * **commit**	Commits the transaction.
Step 5	Server# /bios **show detail**	(Optional) Displays the BIOS details.

This example shows how to configure a server to boot with a one-time boot device:

```
Server scope bios
Server /bios # show boot-device
Boot Device                    Device Type  Device State       Device Order
------------------------------ ------------ ------------------ ----------------
KVMDVD                         VMEDIA       Enabled            1
vkvm                           VMEDIA       Enabled            2

Server /bios # set one-time-boot-device KVMDVD
Server /bios *# 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 # show detail
BIOS:
    BIOS Version: "C240M3.3.0.0.9 (Build Date: 10/02/16)"
    Boot Order: (none)
    FW Update/Recovery Status: None, OK
    UEFI Secure Boot: disabled
    Configured Boot Mode: Legacy
    Actual Boot Mode: Legacy
    Last Configured Boot Order Source: CIMC
    One time boot device: KVMDVD
Server /bios #
```

Assigning User-defined Server Description and Asset Tag

Procedure

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **set description** <*Server Description*>	Enters the server description.
Step 3	Server /chassis* # **set asset-tag** <*Asset Tag*>	Enters the asset tag.
Step 4	Server /chassis* # **commit**	Commits the transaction.
Step 5	Server /chassis # **show detail**	(Optional) Displays the server details.

This example shows how to assign user-defined server description and asset tag:

```
Server# scope chassis
Server/chassis # set description DN1-server
Server/chassis* # set asset-tag powerpolicy
Server /chassis* # commit
Server /chassis # show detail
Chassis:
    Power: on
    Serial Number: FCH1834V23X
    Product Name: UCS C220 M4S
    PID : UCSC-C220-M4S
    UUID: 414949AC-22D6-4D0D-B0C0-F7950E9217C1
    Locator LED: off
    Description: DN1-server
    Asset Tag: powerpolicy
Server /chassis #
```

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 Cisco IMC, the server will not become active immediately when powered on. In this case, the server will enter standby mode until the Cisco IMC 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 the chassis command mode.
Step 2	Server /chassis # **power on**	Turns on the server.
Step 3	At the prompt, enter y to confirm.	Turns on the server.

This example shows how to turn on the server:

```
Server# scope chassis
Server /chassis # power on
Warning: System is already powered ON, this action is ineffective.
Do you want to continue?[y|N]y
```

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

Power Capping

Important This section is valid only for some UCS C-Series servers.

Power capping determines how server power consumption is actively managed. When you enable power capping option, the system monitors power consumption and maintains the power below the allocated power limit. If the server cannot maintain the power limit or cannot bring the platform power back to the specified power limit within the correction time, power capping performs actions that you specify in the **Action** field under the **Power Profile** area.

Once power capping is enabled, you can configure multiple power profiles to either have standard or advanced power profiles with defined attributes. If you choose a standard power profile, you can set the power limit, correction time, corrective-action, suspend period, hard capping, and policy state (if enabled). If you choose an advanced power profile, in addition to the attributes of the standard power profile, you can also set the domain specific power limits, safe throttle level, and ambient temperature based power capping attributes.

Note The following changes are applicable for Cisco UCS C-Series release 2.0(13) and later:

- After upgrading to the 2.0(13) release, power characterization automatically runs during the first host power on. Subsequent characterization runs only if initiated as described in section **Run Power Characterization** section.
- Also, when a server is power cycled and there is a change to the CPU or DIMM configurations, power characterization automatically runs on first host boot. For any other hardware change like PCIe adapters, GPU or HDDs, power characterization does not run. The characterized power range is modified depending on the components present after the host power cycle.

The **Run Power Characterization** option in the **Power Cap Configuration** Tab of the Web UI power cycles the host and starts power characterization.

Enabling Power Characterization

This option is available only on some Cisco UCS C-Series servers.

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 chassis command mode.
Step 2	Server /chassis # **scope power-cap-config**	Enters power cap command mode.
Step 3	Server /chassis # **set run-pow-char-at-boot**	Runs the power characterization at boot.
Step 4	Server /chassis # **commit**	Commits the transaction to the system.

This example shows how to automatically invoke power characterization during a host reboot:

```
Server# scope chassis
Server /chassis# scope power-cap-config
Server /chassis /power-cap-config # set run-pow-char-at-boot
Server /chassis /power-cap-config* # commit
Server /chassis/power-cap-config #
```

Configuring the Power Cap Policy

This option is available only on some Cisco UCS C-Series servers.

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 chassis command mode.
Step 2	Server /chassis # **scope power-cap-config**	Enters power cap command mode.
Step 3	Server /chassis /power-cap-config# **set pow-cap-enable** {**yes** | **no**}	Enables or disables the capping of power to the server.
Step 4	Server /chassis /power-cap-config# **commit**	Commits the transaction to the system configuration.

This example shows how to enable the power capping policy:

```
Server# scope chassis
Server /chassis# scope power-cap-config
Server /chassis /power-cap-config # set pow-cap-enable yes
Server /chassis /power-cap-config* # commit
Server /chassis/power-cap-config #
```

Configuring Standard Power Profile

This option is available only on some Cisco UCS C-Series servers.

Before You Begin

- Power capping must be enabled.
- You must log in 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 power-cap-config**	Enters power cap command mode.
Step 3	Server /chassis /power-cap-config# **set pow-cap-enable** {**yes** | **no**}	Enables or disables the power capping capability of the system.
Step 4	Server /chassis /power-cap-config# **scope power-profile standard**	Enters the standard command mode of a power profile
Step 5	Server /chassis /power-cap-config# **set allow-throttle yes** | **no**	Enables or disables the system to maintain the power limit by forcing the processor to use the throttling state (T-state) and memory throttle.
Step 6	Server /chassis /power-cap-config# **set corr-time** *value*	Sets the correction time in which the platform power should be brought back to the specified power limit before taking the action specified in the **Action** mode. The range is from 3 and 600 seconds. The default is 3 seconds.
Step 7	Server /chassis /power-cap-config# **set except-action alert** | **shutdown**	Specifies the action to be performed if the specified power limit is not maintained within the correction time. This can be one of the following: • **Alert**—Logs the event to the Cisco IMC SEL. • **Shutdown**—Gracefully shuts down the host. • **None**—No actions are taken.
Step 8	Server /chassis /power-cap-config# **set hard-cap yes** | **no**	Enables or disables the system to maintain the power consumption below the specified power limit.
Step 9	Server /chassis /power-cap-config# **set pow-limit** *value*	Specifies the power limit. Enter a value within the specified range.

	Command or Action	Purpose
Step 10	Server /chassis /power-cap-config# **set susp-pd** {*h:m-h:m* | |*ll,Mo,Tu,We,Th,Fr,Sa,Su.*}	Specifies the time period that the power capping profile is not active.
Step 11	Server /chassis /power-cap-config# **commit**	Commits the transaction to the system.

This example shows how to configure standard power profile:

```
Server# scope chassis
Server /chassis# scope power-cap-config
Server /chassis /power-cap-config # set pow-cap-enable yes
Server /chassis /power-cap-config* # commit
Server /chassis/power-cap-config # scope power-profile advance
Server /chassis/power-cap-config # set allow-throttle yes
Server /chassis/power-cap-config* # set corr-time 6
Server /chassis/power-cap-config* # set except-action alert
Server /chassis/power-cap-config* # set hard-cap yes
Server /chassis/power-cap-config* # set pow-limit 360
Server /chassis/power-cap-config* # set susp-pd 1:30-2:30|All
Server /chassis/power-cap-config* # commit
Server /chassis/power-cap-config # show detail
Power Cap Config:
    Power Characterization Enabled: yes
    Power Capping: no
    Power Characterization Status: Completed
    Platform Min (Allow-Throttle)(W): 164
    Platform Min (Efficient)(W): 290
    Platform Max (W): 581
    Memory Min (W): 2
    Memory Max (W): 5
    CPU Min (Allow-Throttle)(W): 64
    CPU Min (Efficient)(W): 177
    CPU Max (W): 330
```

Configuring Advanced Power Profile Settings

You can configure these settings only on some UCS C-Series servers.

Before You Begin

- You must enable power capping.
- You must log in 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 power-cap-config**	Enters power cap command mode.

	Command or Action	Purpose
Step 3	Server /chassis /power-cap-config # **set pow-cap-enable** {**yes** | **no**}	Enables or disables the power capping capability of the server.
Step 4	Server /chassis /power-cap-config # **commit**	Commits the transaction to the system.
Step 5	Server /chassis /power-cap-config # **scope power-profile advanced**	Enters the advance command mode of a power profile.
Step 6	Server /chassis /power-cap-config/power-profile # **set allow-throttle** {**yes** | **no**}	Enables or disables the system to maintain the power limit by forcing the processor to use the throttling state (T-state) and memory throttle.
Step 7	Server /chassis /power-cap-config/power-profile # **set corr-time** *value*	Sets the maximum time to take corrective actions in order to bring the platform back to the specified power limit before taking the actions specified in the **Action** mode. The range is from 3 and 600 seconds. The default is 3 seconds.
Step 8	Server /chassis /power-cap-config/power-profile # **set cpu-power-limit** *value*	Specifies the power limit for the CPU. Enter power in watts within the range specified.
Step 9	Server /chassis /power-cap-config/power-profile # **set cpu-safe-Tlvl** *value*	Specifies the throttling level for the CPU. The range is from 0 and 100 percentage.
Step 10	Server /chassis /power-cap-config/power-profile # **set except-action** {**alert** | **shutdown**}	Specifies the action to be performed if the specified power limit is not maintained within the correction time. This can be one of the following: • **Alert**—Reports the event to the Cisco IMC SEL. • **Shutdown**—Gracefully shuts down the host. • **None**—No actions are taken.
Step 11	Server /chassis /power-cap-config/power-profile # **set hard-cap** {**yes** | **no**}	Enables or disables the system to maintain the power consumption below the specified power limit.
Step 12	Server /chassis /power-cap-config/power-profile # **set mem-pow-limit** *value*	Specifies the power limit for the memory. Enter power in watts within the range specified.
Step 13	Server /chassis /power-cap-config/power-profile # **set mem-safe-Tlvl** *value*	Specifies the throttling level for the memory. The range is from 0 and 100 percentage.

	Command or Action	Purpose
Step 14	Server /chassis /power-cap-config/power-profile # **set fail-safe-timeout** *value*	Specifies a safe throttle policy when the power capping functionality is impacted internal faults such as missing power readings for platforms or CPUs. The range is from 1 and 10 seconds.
Step 15	Server /chassis /power-cap-config/power-profile # **set plat-safe-Tlvl** *value*	Specifies the throttling level for the platform in percentage. The range is from 0 and 100.
Step 16	Server /chassis /power-cap-config/power-profile # **set plat-temp** *value*	Specifies the inlet temperature sensor. Enter value in Celsius.
Step 17	Server /chassis /power-cap-config/power-profile # **set pow-limit** *value*	Specifies the power limit. Enter power in watts within the range specified.
Step 18	Server /chassis /power-cap-config/power-profile # **set susp-pd** {*h:m-h:m* | |*ll,Mo,Tu,We,Th,Fr,Sa,Su.*}	Specifies the time period that the power capping profile will not be active.
Step 19	Server /chassis/power-cap-config/power-profile # **set thermal-power-limit** *value*	Specifies the power limit to be maintained. Enter power in watts within the range specified.
Step 20	Server /power-cap-config/power-profile # **commit**	Commits the transaction to the system configuration.

This example shows how to configure the advance power profile setting:

```
Server# scope chassis
Server /chassis# scope power-cap-config
Server /chassis /power-cap-config # set pow-cap-enable yes
Server /chassis /power-cap-config* # commit
Server /chassis/power-cap-config # scope power-profile advanced
Server /chassis/power-cap-config/power-profile # set allow-throttle yes
Server /chassis/power-cap-config/power-profile* # set corr-time 6
Server /chassis/power-cap-config/power-profile*# set cpu-power-limit 259
Server /chassis/power-cap-config/power-profile* # set cpu-safe-Tlvl 50
Server /chassis/power-cap-config/power-profile* # set except-action alert
Server /chassis/power-cap-config/power-profile* # set hard-cap yes
Server /chassis/power-cap-config/power-profile* # set mem-pow-limit 259
Server /chassis/power-cap-config/power-profile* # set mem-safe-Tlvl 50
Server /chassis/power-cap-config/power-profile* # set fail-safe-timeout 10
Server /chassis/power-cap-config/power-profile* # set plat-safe-Tlvl 50
Server /chassis/power-cap-config/power-profile* # set plat-temp 35
Server /chassis/power-cap-config/power-profile* # set pow-limit 360
Server /chassis/power-cap-config/power-profile* # set susp-pd 1:30-2:30|All
Server /chassis/power-cap-config/power-profile* # set thermal-power-limit 354
Server /chassis/power-cap-config/power-profile* # commit
Server /chassis/power-cap-config/power-profile #
```

Resetting the Power Profiles to Defaults

This option is available only on some Cisco UCS C-Series servers.

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 chassis command mode.
Step 2	Server /chassis # **scope power-cap-config**	Enters power cap command mode.
Step 3	Server /chassis # **set reset-power-profile-to-defaults**	Resets the power profile settings to factory-default values and disables power capping.
Step 4	Server /chassis # **commit**	Commits the transaction to the system.

This example shows how to reset the power profile to the default settings:

```
Server# scope chassis
Server /chassis# scope power-cap-config
Server /chassis /power-cap-config # reset-power-profile-to-defaults
Server /chassis /power-cap-config* # commit
Server /chassis/power-cap-config #
```

Viewing the Power Capping Configuration

This option is available only on some Cisco UCS C-Series servers.

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 chassis command mode.
Step 2	Server /chassis # **scope power-cap-config**	Enters power cap configuration command mode.
Step 3	Server /chassis/power-cap-config # **show detail**	Displays information about the power characterization.

This example shows how to view information about the power cap configuration:

```
Server #scope chassis
Server/chassis # scope power-cap-config
Server /chassis/power-cap-config # show detail
Power Cap Config:
    Power Characterization Enabled: yes
    Power Capping: no
    Power Characterization Status: Completed
    Platform Min (Allow-Throttle)(W): 164
    Platform Min (Efficient)(W): 290
    Platform Max (W): 581
    Memory Min (W): 2
    Memory Max (W): 5
    CPU Min (Allow-Throttle)(W): 64
    CPU Min (Efficient)(W): 177
    CPU Max (W): 330
Server /chassis/power-cap-config #
```

Viewing the Power Statistics

This option is available only on some UCS C-Series servers.

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 chassis command mode.
Step 2	Server /chassis # **show power-monitoring**	Displays the power used by the server, CPU, and memory since the last time it was rebooted.

This example shows how to view the power statistics of an individual domain:

```
Server #scope chassis
Server /chassis # show power-monitoring
Domain     Current (W)  Minimum (W)  Maximum (W)  Average (W)
---------- ------------ ------------ ------------ ------------
Platform   180          160          504          180
CPU        53           33           275          53
Memory     2            2            6            2
Server /chassis #
```

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 CIMC**	Enters the Cisco IMC command mode.
Step 2	Server /CIMC # **Scope power-restore-policy**	Enters the power restore policy command mode.
Step 3	Server /CIMC/power-restore-policy # **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: • **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 4	Server /CIMC/power-restore-policy # **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 5	Server /CIMC/power-restore-policy # **set delay-value** *delay*	(Optional) Specifies the delay time in seconds. The range is 0 to 240; the default is 0.
Step 6	Server /CIMC/power-restore-policy # **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 CIMC
Server /CIMC # Scope  power-restore-policy
Server /CIMC/power-restore-policy # set policy power-on
Server /CIMC/power-restore-policy *# commit
Server /CIMC/power-restore-policy # set delay fixed
Server /CIMC/power-restore-policy *# set delay-value 180
Server /CIMC/power-restore-policy *# commit
Server /CIMC/power-restore-policy #  show detail
Power Restore Policy:
    Power Restore Policy: power-on
    Power Delay Type: fixed
    Power Delay Value(sec): 180

Server /CIMC/power-restore-policy #
```

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 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 is the default policy. 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 Cisco IMC, 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 to the required minimum fan speed to prevent the overheating. If you have set a fan speed configuration higher than required, the system retains the selected fan speed. The **Applied Fan Policy** displays the actual fan speed that runs on the server.

The **Configuration Status** displays the status of the configured fan policy. This can be one of the following:

- SUCCESS —The selected fan policy matches the actual fan speed that runs on the server.
- PENDING —The configured fan policy is not in effect yet. This can be due to one of the following:
    - The server is powered off
    - The BIOS POST is not complete
- FAN POLICY OVERRIDE—Overrides the specified fan speed with the actual speed determined by the configuration requirements of the server.

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**	Sets the fan policy for the server. It can be one of the following: • **balanced** 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

	Command or Action	Purpose
		speeds will run at the same speed or higher speed than that of the **balanced** fan policy. • **low-power** This is the default policy. 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%.
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
  Applied Fan Policy: Max Power
  Configuration Status: SUCCESS
server /chassis/fan-policy #
```

Configuring DIMM Black Listing

DIMM Black Listing

In Cisco IMC, the state of the Dual In-line Memory Module (DIMM) is based on SEL event records. A DIMM is marked bad if the BIOS encounters a non-correctable memory error or correctable memory error with 16000 error counts during memory test execution during BIOS post. If a DIMM is marked bad, it is considered a non-functional device.

If you enable DIMM blacklisting, Cisco IMC monitors the memory test execution messages and blacklists any DIMM that encounters memory errors at any given point of time in the DIMM SPD data. This allows the host to map out those DIMMs.

DIMMs are mapped out or blacklisted only when Uncorrectable errors occur. When a DIMM gets blacklisted, other DIMMs in the same channel are ignored or disabled, which means that the DIMM is no longer considered bad.

Note DIMMs do not get mapped out or blacklisted for 16000 Correctable errors.

Enabling DIMM Black Listing

Before You Begin

You must be logged in as an administrator.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope dimm-blacklisting** /	Enters the DIMM blacklisting mode.
Step 2	Server /dimm-blacklisting # **set enabled** {**yes** | **no**}	Enables or disables DIMM blacklisting.
Step 3	Server /dimm-blacklisting* # **commit**	Commits the transaction to the system configuration.

The following example shows how to enable DIMM blacklisting:

```
Server# scope dimm-blacklisting
Server /dimm-blacklisting # set enabled yes
Server /dimm-blacklisting* # commit
Server /dimm-blacklisting #
Server /dimm-blacklisting # show detail

DIMM Blacklisting:
      Enabled: yes
```

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 legacy boot order of bootable target types that the server will attempt to use.
Boot Override Priority	This can be None, or HV.
FW Update/Recovery Status	The status of any pending firmware update or recovery action.
UEFI Secure Boot	Enables or Disables UEFI secure boot.
Configured Boot Mode	The boot mode in which h BIOS will try to boot the devices.
Actual Boot Mode	The actual boot mode in which BIOS booted the devices.
Last Configured Boot Order Source	The last configured boot order source by BIOS.

This example displays the BIOS status:

```
Server# scope bios
Server /bios # show detail
Server /bios # show detail
BIOS Version: "CxxxM1.1.2.2a.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 #
```

```
 Server# scope bios
Server /bios # show detail
BIOS:
    BIOS Version: "Cxxx3.2.0.0.15 (Build Date: 03/xx/201x)"
    Boot Order: (none)
    Boot Override Priority:
    FW Update/Recovery Status: None, OK
    UEFI Secure Boot: disabled
    Configured Boot Mode: Legacy
    Actual Boot Mode: Legacy
    Last Configured Boot Order Source: CIMC
    One time boot device: (none)
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: • Main BIOS Parameters for C22 and C24 Servers , on page 329 • Main BIOS Parameters for C220 and C240 Servers , on page 350 • Main Tab for C460 M4 Servers, on page 370 • Main Tab for C220M4 and C240M4 Servers, on page 394 • Main BIOS Parameters for C3160 Servers , on page 419
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.	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: • Advanced BIOS Parameters for C22 and C24 Servers , on page 330 • Advanced BIOS Parameters for C220 and C240 Servers , on page 350 • Advanced Tab for C460 M4 Servers, on page 371 • Advanced Tab for C220M4 and C240M4 Servers, on page 395 • Advanced BIOS Parameters for C3160 Servers , on page 420
Step 4	Server /bios/advanced # **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 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.	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: • Server Management BIOS Parameters for C22 and C24 Servers , on page 348 • Server Management BIOS Parameters for C220 and C240 Servers , on page 369 • Server Management Tab for C460 M4 Servers, on page 392 • Server Management Tab for C220M4 and C240M4 Servers, on page 417 • Server Management Tab for C3160 Servers, on page 437
Step 4	Server /bios/server-management # **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 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
```

Entering BIOS Setup

Before You Begin

- The server must be powered on.
- 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 # **enter-bios-setup**	Enters BIOS setup on reboot.

This example enables you to enter BIOS setup:

```
Server# scope bios
Server /bios # enter-bios-setup
This operation will enable Enter BIOS Setup option.
Host must be rebooted for this option to be enabled.
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 #
```

BIOS Profiles

On the Cisco UCS server, default token files are available for every server platform, and you can configure the value of these tokens using the Graphic User Interface (GUI), CLI interface, and the XML API interface. To optimize server performance, these token values must be configured in a specific combination.

Configuring a BIOS profile helps you to utilize pre-configured token files with the right combination of the token values. Some of the pre-configured profiles that are available are virtualization, high-performance, low power, and so on. You can download the various options of these pre-configured token files from the Cisco website and apply it on the servers through the BMC.

You can edit the downloaded profile to change the value of the tokens or add new tokens. This allows you to customize the profile to your requirements without having to wait for turnaround time.

Activating a BIOS Profile

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 the BIOS command mode.
Step 2	Server# /bios **scope bios-profile**	Enters the BIOS profile command mode.
Step 3	Server# /bios/bios-profile **activate** *virtualization*	You are prompted to back up the BIOS configuration. Enter y.
Step 4	You are prompted to reboot the system to apply the changes to the BIOS set-up parameters. Enter y.	Initiates the system reboot.

This example activates the specified BIOS profile:

```
Server # scope bios
Server /bios # scope bios-profile
Server /bios/bios-profile # activate virtualization
It is recommended to take a backup before activating a profile.
Do you want to take backup of BIOS configuration?[y/n] y
backup-bios-profile succeeded.
bios profile “virtualization” deleted
Changes to BIOS set-up parameters will require a reboot.
Do you want to reboot the system?[y|N]y
A system reboot has been initiated.
Server /bios/bios-profile #
```

Taking a Back-Up of a BIOS Profile

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 the BIOS command mode.
Step 2	Server# /bios **scope bios-profile**	Enters the BIOS profile command mode.
Step 3	Server# /bios/bios-profile **backup**	Displays a message that the backup of the BIOS profile was successful.

This example backs up a BIOS profile:

```
Server # scope bios
Server /bios # scope bios-profile
Server /bios/bios-profile # backup
backup-bios-profile succeeded.
Server /bios #
```

Deleting a BIOS Profile

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 the BIOS command mode.
Step 2	Server# /bios **scope bios-profile**	Enters the BIOS profile command mode.
Step 3	Server# /bios/bios-profile **delete** *BIOS profile*	Deletes the specified BIOS profile.

This example deletes the specified BIOS profile:

```
Server # scope bios
Server /bios # scope bios-profile
Server /bios/bios-profile # delete performance
Server /bios/bios-profile #
```

Displaying BIOS Profiles

Procedure

	Command or Action	Purpose
Step 1	Server# **scope bios**	Enters the BIOS command mode.
Step 2	Server# /bios **show bios-profile**	Displays all the BIOS profiles.

This example displays all the BIOS profiles:

```
Server # scope bios
Server /bios # show bios-profile
ID     Name             Active
------ ---------------- -------- --------
1      performance      yes
2      virtualization   no
3      none             no
4      cisco_backup     no
Server /bios #scope bios-profile
Server /bios #
```

Displaying Information of a BIOS Profile

Procedure

	Command or Action	Purpose
Step 1	Server# **scope bios**	Enters the BIOS command mode.
Step 2	Server# /bios **scope bios-profile**	Displays all the BIOS profiles.
Step 3	Server# /bios/bios-profile **info** *performance*	Displays information of the BIOS profile such as token name, profile value, and active value.

This example displays information of the specified BIOS profile:

```
Server # scope bios
Server /bios # scope bios-profile
Server /bios/bios-profile # info performance

TOKEN NAME                    PROFILE VALUE        ACTUAL VALUE
====================================================================
 TPMAdminCtrl                  Enabled              Enabled
 ASPMSupport                   Disabled             Disabled
Server /bios/bios-profile #
```

Displaying details of the BIOS Profile

Procedure

	Command or Action	Purpose
Step 1	Server# **scope bios**	Enters the BIOS command mode.
Step 2	Server# /bios **scope bios-profile**	Enters the BIOS profile command mode.
Step 3	Server# /bios/bios-profile **show detail**	Displays the details of BIOS profile.

This example displays the details of the BIOS profile:

```
Server # scope bios
Server /bios # scope bios-profile
Server /bios/bios-profile # show detail
Active Profile: Virtualization
Install Status: bios profile install done
Server /bios/bios-profile #
```

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.

Server must be powered off.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **scope firmware**	Enters firmware 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 Product ID (PID) Catalog Details

Procedure

	Command or Action	Purpose
Step 1	Server # **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **show cpu-pid**	Displays the CPU PID details.
Step 3	Server /chassis # **show dimm-pid**	Displays the memory PID details.
Step 4	Server /chassis # **show pciadapter-pid**	Displays the PCI adapters PID details.

	Command or Action	Purpose
Step 5	Server /chassis # **show hdd-pid**	Displays the HDD PID details.

This example shows how to create view PID details

```
Server # scope chassis
Viewing CPU PID details
Server /chassis # show cpu-pid
Socket Product ID           Model
------ -------------------- ----------------------------------------
CPU1   UCS-CPU-E52660B      Intel(R) Xeon(R) CPU E5-2660 v2 @ 2.2...
CPU2   UCS-CPU-E52660B      Intel(R) Xeon(R) CPU E5-2660 v2 @ 2.2...
Viewing memory PID details
Server /chassis # show dimm-pid
Name               Product ID           Vendor ID  Capacity  Speed
------------------ -------------------- ---------- --------- ------
DIMM_A1            UNKNOWN              NA         Failed    NA
DIMM_A2            UNKNOWN              NA         Ignore... NA
DIMM_B1            UCS-MR-1X162RZ-A     0xCE00     16384 MB  1866
DIMM_B2            UCS-MR-1X162RZ-A     0xCE00     16384 MB  1866
DIMM_C1            UCS-MR-1X162RZ-A     0xCE00     16384 MB  1866
DIMM_C2            UCS-MR-1X162RZ-A     0xCE00     16384 MB  1866
DIMM_D1            UCS-MR-1X162RZ-A     0xCE00     16384 MB  1866
DIMM_D2            UCS-MR-1X162RZ-A     0xCE00     16384 MB  1866
DIMM_E1            UCS-MR-1X162RZ-A     0xCE00     16384 MB  1866
DIMM_E2            UCS-MR-1X162RZ-A     0xCE00     16384 MB  1866
DIMM_F1            UCS-MR-1X162RZ-A     0xCE00     16384 MB  1866
DIMM_F2            UCS-MR-1X162RZ-A     0xCE00     16384 MB  1866
DIMM_G1            UCS-MR-1X162RZ-A     0xCE00     16384 MB  1866
DIMM_G2            UCS-MR-1X162RZ-A     0xCE00     16384 MB  1866
DIMM_H1            UCS-MR-1X162RZ-A     0xCE00     16384 MB  1866
DIMM_H2            UCS-MR-1X162RZ-A     0xCE00     16384 MB  1866
Viewing PCI adapters PID details
Server /chassis # show pciadapter-pid
Slot   Product ID           Vendor ID  Device ID   SubVendor ID  SubDevice ID
------ -------------------- ---------- ----------- ------------- -------------
1      UCSC-MLOM-CSC-02     0x1137     0x0042      0x1137        0x012e
Viewing HDD PID details
Server /chassis # show hdd-pid
Disk Controller  Product ID           Vendor     Model
---- ----------- -------------------- ---------- ------------
1    SLOT-MEZZ   UCSC-C3X60-HD4TB     TOSHIBA    MG03SCA400
2    SLOT-MEZZ   UCS-C3X60-HD4TB      SEAGATE    ST4000NM0023
3    SLOT-MEZZ   UCSC-C3X60-HD4TB     TOSHIBA    MG03SCA400
4    SLOT-MEZZ   UCSC-C3X60-HD4TB     TOSHIBA    MG03SCA400
5    SLOT-MEZZ   UCSC-C3X60-HD4TB     TOSHIBA    MG03SCA400
6    SLOT-MEZZ   UCSC-C3X60-HD4TB     TOSHIBA    MG03SCA400
7    SLOT-MEZZ   UCSC-C3X60-HD4TB     TOSHIBA    MG03SCA400
8    SLOT-MEZZ   UCSC-C3X60-HD4TB     TOSHIBA    MG03SCA400
9    SLOT-MEZZ   UCSC-C3X60-HD4TB     TOSHIBA    MG03SCA400
10   SLOT-MEZZ   UCSC-C3X60-HD4TB     TOSHIBA    MG03SCA400
11   SLOT-MEZZ   UCSC-C3X60-HD4TB     TOSHIBA    MG03SCA400
12   SLOT-MEZZ   UCSC-C3X60-HD4TB     TOSHIBA    MG03SCA400
13   SLOT-MEZZ   UCSC-C3X60-HD4TB     TOSHIBA    MG03SCA400
14   SLOT-MEZZ   UCSC-C3X60-HD4TB     TOSHIBA    MG03SCA400
15   SLOT-MEZZ   UCS-C3X60-HD4TB      SEAGATE    ST4000NM0023
16   SLOT-MEZZ   UCS-C3X60-HD4TB      SEAGATE    ST4000NM0023
19   SLOT-MEZZ   UCSC-C3X60-HD4TB     TOSHIBA    MG03SCA400
28   SLOT-MEZZ   UCSC-C3X60-HD4TB     TOSHIBA    MG03SCA400
54   SLOT-MEZZ   UCSC-C3X60-HD6TB     SEAGATE    ST6000NM0014
55   SLOT-MEZZ   UCSC-C3X60-HD6TB     SEAGATE    ST6000NM0014
56   SLOT-MEZZ   UCSC-C3X60-HD4TB     TOSHIBA    MG03SCA400
57   SLOT-MEZZ   UCS-HD4T7KS3-E       WD         WD4001FYY...
58   SLOT-MEZZ   UCS-HD4T7KS3-E       WD         WD4001FYY...
59   SLOT-MEZZ   UCS-HD4T7KS3-E       WD         WD4001FYY...
60   SLOT-MEZZ   UCS-HD4T7KS3-E       WD         WD4001FYY...
```

```
Server /chassis #
```

Uploading and Activating PID Catalog

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 chassis**	Enters the chassis command mode.
Step 2	Server# /chassis **scope pid-catalog**	Enters the PID catalog command mode.
Step 3	Server /chassis/pid-catalog # **upload-pid-catalog** *remote-protocol IP Address PID Catalog file*	Specifies the protocol to connect to the remote server. It can be one of the following types: • TFTP • FTP • SFTP • SCP • HTTP **Note** The Cisco UCS C-Series server now supports fingerprint confirmation of the server when you update firmware through a remote server. This option is available only if you choose SCP or SFTP as the remote server type. If you chose SCP or SFTP as the remote server type while performing this action, a prompt with the message Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue? Click y or n depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.
Step 4	Server# /chassis/pid-catalog **show detail**	(Optional) Displays the status of the upload.
Step 5	Server# /chassis/pid-catalog **activate**	Activates the uploaded PID catalog.
Step 6	Server# /chassis/pid-catalog **show detail**	Displays the status of the activation.

This example uploads and activates the PID catalog:

```
Server # scope chassis
Server /chassis # scope pid-catalog
Uploading PID Catalog
Server /chassis/pid-catalog # upload-pid-catalog tftp 172.22.141.66
pid-ctlg-2_0_12_78_01.tar.gz
upload-pid-catalog initialized.
Please check the status using "show detail".
Server /chassis/pid-catalog #
Server /chassis/pid-catalog # show detail
    Upload Status: Upload Successful
    Activation Status: Please Activate Catalog
    Current Activated Version: N/A
Activating the uploaded PID catalog
Server /chassis/pid-catalog # activate
Successfully activated PID catalog
Server /chassis/pid-catalog # show detail
    Upload Status:
    Activation Status: Activation Successful
    Current Activated Version: 2.0(12.78).01
Server /chassis/pid-catalog #
```

CHAPTER 4

Viewing Server Properties

This chapter includes the following sections:

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-FFFFFFFFFFFF
    Locator LED: off
    Description: This shows the chassis details.

Server#
```

This example displays server properties for C3160 servers:

```
Server# show chassis detail
Chassis:
    Power: on
    Serial Number: FCH1821JAVL
    Product Name: UCS C3160
    PID : UCSC-C3X60-SVRNB
    UUID: 84312F76-75F0-4BD1-9167-28B74EBB444C
    Locator LED: off
    Front Panel Locator LED: off
    Description: This shows the chassis details
Server#
```

Viewing System Information

Before You Begin

Procedure

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters the chassis command mode.
Step 2	Server /chassis # **show sku-details**	Displays the system information.

This example shows how to view system details:

```
Server# scope chassis
Server /chassis # show sku-details
    SAS Expander: Not-Present
    HDD: 10-SFF_drive_back_plane
    Riser1: (1 Slot x16)
    Riser2: (1 Slot x16)
    M.2 SATA/NVMe: Not-Present
    M.2 SD Card Controller: Not-Present
    CPU1 PKG-ID: Non-MCP
    CPU2 PKG-ID: Non-MCP
    Intrusion Sensor: Not-Equipped
Server /chassis #
```

Viewing a Server Utilization

You can view a server utilization only on some UCS C-Series servers.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters the chassis command mode.
Step 2	Server /chassis # **show cups-utilization**	Displays the server utilization value on all the available CPUs. **Note** These utilization values are reported as a percentage of the total hardware bandwidth. These values may not match with the values being displayed by the host based resource monitoring software.

This example shows how to view the server utilization value:

```
Server# scope chassis
Server /chassis # show cups-utilization

CPU Utilization (%)  Memory Utilization (%)  I/O Utilization (%)  Overall Utilization (%)
-------------------- ----------------------- -------------------- ------------------------
100                  69                      0                    86

Server /chassis #
```

Viewing Cisco IMC Properties

Note Cisco IMC 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 Cisco IMC properties.

This example displays Cisco IMC properties:

```
Server# show cimc detail
Cisco IMC:
    Firmware Version: 2.0(8.122)
    Current Time: Wed Dec  9 23:14:28 2015
    Boot-loader Version: 2.0(8.122).36
    Local Time: Wed Dec  9 23:14:28 2015 UTC +0000
    Timezone: UTC
    Reset Reason: graceful-reboot (This provides the last Cisco IMC reboot reason.)

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 #
```

Note **Input Power** and **Maximum Output Power** options are available only for some C-Series servers.

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 Cisco IMC. If an installed controller or storage device is not displayed, then it cannot be managed through Cisco IMC.
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.

	Command or Action	Purpose
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 *index* 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** [*drive-number*] [**detail**]	Displays physical drive information for the storage card.
Step 4	Server /chassis/storageadapter # **show physical-drive-count** [**detail**]	Displays the number of physical drives on the storage card.
Step 5	Server /chassis/storageadapter # **scope physical-drive** *drive-number*	Enters command mode for the specified physical drive.

	Command or Action	Purpose
Step 6	Server /chassis/storageadapter/physical-drive # **show general** [**detail**]	Displays general information about the specified physical drive.
Step 7	Server /chassis/storageadapter/physical-drive # **show inquiry-data** [**detail**]	Displays inquiry data about the specified physical drive.
Step 8	Server /chassis/storageadapter/physical-drive # **show status** [**detail**]	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** *slot-number*	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
Slot Vendor ID Device ID  SubVendor ID SubDevice ID  Firmware Version Product Name
---- --------- ---------- ------------ ------------- ---------------- -------------------
L    0x8086    0x1521     0x1137        0x008b        0x80000AA5... Intel(R) I350 1 Gbps N...
1    0x19a2    0x0710     0x10df        0xe702        4.6.142.10    Emulex OCe11102-FX 2 p...
3    0x10de    0x118f     0x10de        0x097f        N/A           Nvidia TESLA K10 P2055...
4    0x14e4    0x1639     0x14e4        0x1639        N/A           Broadcom 5709 1 Gbps 2...
5    0x10de    0x0ff2     0x10de        0x1012        N/A           Nvidia GRID K1 P2401-502
M    0x1000    0x0073     0x1137        0x00b1        N/A           Cisco UCSC RAID SAS 20…

Option ROM Status
----------
Loaded
Not-Loaded
Not-Loaded
Loaded

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 L
Server /chassis/network-adapter # show mac-list
Interface ID       MAC Address
-------------  --------------------
```

```
eth0            010000002000
eth1            010000002000

Server /chassis/network-adapter #
```

Viewing TPM 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 tpm-inventory**	Displays the TPM properties.

This example displays the TPM properties:

```
Server# scope chassis
Server /chassis # show tpm-inventory

Version Presence  Enabled-Status  Active-Status  Ownership  Revision     Model
Vendor      Serial
------- --------  --------------  -------------- ---------- ---------  -------------
--------   -----------
 A      equipped    disabled       deactivated    unowned      1       UCSX-TPMX-00X   ABC
 Inc    FCHXXXXXXXX

Server /chassis #
```

Enabling 6G or 12G Mixed Mode Speed on SAS Expanders

Cisco IMC supports mixed mode speeds of 6 gigabytes or 12 gigabytes for SAS expanders. This support is added because 6 gigabyte solid state drives (SSDs) are now giving way to 12 gigabyte SSDs. Using this feature you can select a SAS expander in the Dynamic Storage tab and enable either modes based on your requirements.

Enabling 6G or 12G Mixed Mode on a SAS Expander

This action is available only 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 chassis**	Enters the chassis command mode.
Step 2	Server /chassis # **scope sas-expander sas-expander ID**	Enters the SAS expander command mode.
Step 3	Server /chassis/sas-expander # **scope 6G-12G-Mixed-Mode-status**	Enters the 6G or 12G mixed mode command mode.
Step 4	Server /chassis/sas-expander/6G-12G-Mixed-Mode-status # **set set-6G-12G-mixed-mode Enabled**	Enables the 6G or 12G mixed mode on the SAS expander.
Step 5	Server /chassis/sas-expander/6G-12G-Mixed-Mode-status * # **commit**	Enter y at the confirmation prompt. Commits the transaction to the system configuration.
Step 6	Server /chassis/sas-expander/6G-12G-Mixed-Mode-status # **show detail**	(Optional) Displays the 6G or 12G mixed mode status.

This example shows how to enable the 6G or 12G mixed mode on the SAS expander:

```
Server# scope chassis
Server /chassis # scope sas-expander 1
Server /chassis/sas-expander # scope 6G-12G-Mixed-Mode-status
Server /chassis/sas-expander/6G-12G-Mixed-Mode-status # set set-6G-12G-mixed-mode Enabled
Server /chassis/sas-expander/6G-12G-Mixed-Mode-status *# commit
Are you sure you want to change the enable-mixed-mode setting to Enable mode?[y|N]y
Setting enable-mixed-mode setting to Enable ..
Successfully set enable-6G-12G-mixed-mode to Enable..
Server /chassis/sas-expander/6G-12G-Mixed-Mode-status # show detail
6G/12G Mixed Mode Settings:
    Mixed 6G/12G Drive Support: Enabled
Server /chassis/sas-expander/6G-12G-Mixed-Mode-status #
```

CHAPTER 5

Viewing Sensors

This chapter includes the following sections:

Viewing Power Supply Sensors

Procedure

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

```
SU1_PIN       Normal        102      Watts      N/A        882              N/A
 1098
PSU2_PIN       Normal        96       Watts      N/A       882              N/A
 1098
PSU3_PIN       Normal        102      Watts      N/A       882              N/A
 1098
PSU4_PIN       Normal        96       Watts      N/A       882              N/A
 1098
PSU1_POUT      Normal        78       Watts      N/A       798              N/A
 996
PSU2_POUT      Normal        78       Watts      N/A       798              N/A
 996
PSU3_POUT      Normal        84       Watts      N/A       798              N/A
 996
PSU4_POUT      Normal        84       Watts      N/A       798              N/A
 996
POWER_USAGE    Normal        406      Watts      N/A       N/A              N/A
 2674
PSU1_DC_OK     Normal        good

PSU2_DC_OK     Normal        good

PSU3_DC_OK     Normal        good

PSU4_DC_OK     Normal        good

PSU1_AC_OK     Normal        good

PSU2_AC_OK     Normal        good

PSU3_AC_OK     Normal        good

PSU4_AC_OK     Normal        good

PSU1_STATUS    Normal        present

PSU2_STATUS    Normal        present

PSU3_STATUS    Normal        present

PSU4_STATUS    Normal        present

Server /sensor # show psu-redundancy
Name                 Reading         Sensor Status
-------------------- --------------- --------------------
PS_RDNDNT_MODE       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
---------------- -------------   ---------- ------ ------------- ------------ -------------
------------
PSU1_FAN_SPEED    Normal          5160       RPM    1118            N/A            946
  N/A
PSU2_FAN_SPEED    Normal          6106       RPM    1118            N/A            946
  N/A
PSU3_FAN_SPEED    Normal          5762       RPM    1118            N/A            946
  N/A
PSU4_FAN_SPEED    Normal          4988       RPM    1118            N/A            946
  N/A
FAN1_SPEED        Normal          6600       RPM    2040            N/A            1800
  N/A
FAN2_SPEED        Normal          6660       RPM    2040            N/A            1800
  N/A
FAN3_SPEED        Normal          6600       RPM    2040            N/A            1800
  N/A
FAN4_SPEED        Normal          6660       RPM    2040            N/A            1800
  N/A
FAN5_SPEED        Normal          6660       RPM    2040            N/A            1800
  N/A
FAN6_SPEED        Normal          6660       RPM    2040            N/A            1800
  N/A
FAN7_SPEED        Normal          6660       RPM    2040            N/A            1800
  N/A
FAN8_SPEED        Normal          6660       RPM    2040            N/A            1800
  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.
LED Status column	The current LED color, if any. 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**. **Note** This information is only available for some C-Series servers.

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 #
```

Setting Dynamic Front Panel Temperature Threshold

Before You Begin

Log in as a user with admin privileges.

Procedure

	Command or Action	Purpose
Step 1	server # **scope sensor**	Enters sensor command mode
Step 2	server /sensor # **set fp-critical-temp** *upper critical temperature threshold value*	Sets the upper critical temperature threshold. The valid range is between 8 and 50.
Step 3	server /sensor * # **commit**	Commits the change in temperature threshold value.

This example shows how to set the dynamic front panel temperature threshold:

```
Server # scope sensor
Valid value for "fp-critical-temp" is from 8 to 50
Server /sensor # set fp-critical-temp 44
Server /sensor *# commit
Server /sensor # show temperature
Name                      Sensor Status  Reading    Units   Critical Min  Critical Max
Non-Recoverable Min   Non-Recoverable Max
-------------------       -------------  --------   ------   ------------  ------------
--------------------  -------------------
VIC_SLOT1_TEMP            Normal         58.0       C          N/A           90.0
N/A                  95.0
TEMP_SENS_FRONT           Normal         27.0       C          N/A           40.0
N/A                  50.0
DDR4_P1_A1_TMP            Normal         29.0       C          N/A           85.0
N/A                  90.0
DDR4_P2_G1_TMP            Normal         28.0       C          N/A           85.0
N/A                  90.0
P1_TEMP_SENS              Normal         39.5       C          N/A           103.0
N/A                  113.0
P2_TEMP_SENS              Normal         39.5       C          N/A           103.0
N/A                  113.0
PSU1_TEMP                 Normal         27.0       C          N/A           65.0
N/A                  70.0
PSU2_TEMP                 Normal         26.0       C          N/A           65.0
N/A                  70.0
PCH_TEMP_SENS             Normal         36.0       C          N/A           85.0
N/A                  90.0
RISER2_INLET_TMP          Normal         37.0       C          N/A           70.0
N/A                  80.0
RISER1_INLET_TMP          Normal         36.0       C          N/A           70.0
N/A                  80.0
```

CHAPTER 6

Managing Remote Presence

This chapter includes the following sections:

Managing the Virtual KVM

KVM Console

The KVM console is an interface accessible from Cisco IMC 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.

	Command or Action	Purpose
		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.
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 *sessions* 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: • 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 Cisco IMC, the virtual drivers appear on the boot selection menu as expected.

	Command or Action	Purpose
Step 5	Server /vmedia # **commit**	Commits the transaction to the system configuration.
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 Cisco IMC-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** [*mount options*]	Maps a CIFS file for vMedia. You must specify the following: • 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

	Command or Action	Purpose
Step 3	Server /vmedia # **map-nfs** {**volume-name** | **remote-share** | **remote-file-path**} [*mount options*]	Maps an NFS file for vMedia. You must specify the following: • 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
Step 4	Server /vmedia # **map-www** {**volume-name** | **remote-share** | **remote-file-path** [*mount options*]	Maps an HTTPS file for vMedia. You must specify the following: • 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 Cisco IMC-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 Cisco IMC-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
```

Remapping an Existing Cisco IMC vMedia Image

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 vmedia**	Enters the vMedia command mode.
Step 2	Server /vmedia # **show saved-mappings**	Displays the available saved mappings.
Step 3	Server /vmedia # **remap** *mapping volume*	Remaps the vMedia. **Note** You must use the volume name of the saved mapping as the variable for this command.
Step 4	Server /vmedia # **show mappings**	(Optional) Displays the mapped vMedia details.

This example shows how to remap a vMedia image to a saved mapping:

```
Server # scope vmedia
Server/vmedia # remap huu
Server/vmedia # show mappings
Volume           Map-Status               Drive-Type Remote-Share             Remote-File
             Mount-Type
---------------- ------------------------ ---------- ------------------------
------------------------ --------
huu              OK                       CD         https://10.104.236.99...
ucs-c240-huu-3.0.0.33... www
Server/vmedia # show saved-mappings
Volume           Drive-Type Remote-Share             Remote-File              Mount-Type
---------------- ---------- ------------------------ ------------------------ --------
huu              CD         https://10.104.236.99... ucs-c240-huu-3.0.0.33... www
Server/vmedia #
```

Deleting a Cisco IMC vMedia Image

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 vmedia**	Enters the vMedia command mode.
Step 2	Server /vmedia # **delete-saved-mappings**	Enter yes in the confirmation prompt. Deletes the saved mapping.
Step 3	Server /vmedia # **show saved-mappings**	Does not display any saved mapping as it is deleted.

This example shows how to delete a saved mapping:

```
Server # scope vmedia
Server/vmedia # show saved-mappings
Volume           Drive-Type Remote-Share             Remote-File              Mount-Type
---------------- ---------- ------------------------ ------------------------ --------
huu              CD         https://10.104.236.99... ucs-c240-huu-3.0.0.33... www
Server/vmedia # delete-saved-mappings
Purge saved mappings? Enter 'yes' to confirm -> yes
Server/vmedia # show saved-mappings
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 Cisco IMC.

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.
Step 4	Server /sol # **set comport** {**com0** | **com1**	(Optional) Sets the serial port through which the system routes SoL communications. **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. You can specify: • **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. 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. • **com1—**SoL communication is routed through COM port 1, an internal port accessible only through SoL. If you select this option, you can use SoL on COM port 1 and the physical RJ45 connection on COM port 0. **Note** Changing the comport setting disconnects any existing SoL sessions.

	Command or Action	Purpose
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.

CHAPTER 7

Managing User Accounts

This chapter includes the following sections:

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** *usernumber*	Enters user command mode for user number *usernumber*.

	Command or Action	Purpose
Step 2	Server /user # **set enabled** {**yes** | **no**}	Enables or disables the user account on the Cisco IMC.
Step 3	Server /user # **set name** *username*	Specifies the username for the user.
Step 4	Server /user # **set password**	You are prompted to enter the password twice. **Note** When strong password is enabled, you must follow these guidelines while setting a password: • The password must have a minimum of 8 and a maximum of 14 characters. • The password must not contain the User's Name. • The password must contain characters from three of the following four categories: ◦ English uppercase characters (A through Z) ◦ English lowercase characters (a through z) ◦ Base 10 digits (0 through 9) ◦ Non-alphabetic characters (!, @, #, $, %, ^, &, *, -, _, +, =) when strong password is disabled, you can set a password using characters of your choice (alphanumeric, special characters, or integers) within the range 1-20.
Step 5	Server /user # **set role** {**readonly** | **user** | **admin**}	Specifies the role assigned to the user. The roles are as follows: • readonly—This user can view information but cannot make any changes. • user—This user can do the following: • 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 • Set the time zone • Ping an IP address • admin—This user can perform all actions available through the GUI, CLI, and IPMI.

	Command or Action	Purpose
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
Warning:
Strong Password Policy is enabled!

For CIMC protection your password must meet the following requirements:
        The password must have a minimum of 8 and a maximum of 14 characters.
        The password must not contain the User's Name.
        The password must contain characters from three of the following four categories.
            English uppercase characters (A through Z)
            English lowercase characters (a through z)
            Base 10 digits (0 through 9)
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
```

Disabling Strong Password

The Cisco IMC now implements a strong password policy wherein you are required to follow guidelines and set a strong password when you first log on to the server for the first time. The Cisco IMC CLI provides you option which allows you to disable the strong password policy and set a password of your choice by ignoring the guidelines. Once you disable the strong password, an Enable Strong Password button is displayed. By default, the strong password policy is enabled.

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# **scope user-policy**	Enters user policy command mode.
Step 2	Server /user-policy # **set password-policy** {**enabled** | **disabled**}	At the confirmation prompt, enter y to complete the action or n to cancel the action. Enables or disables the strong password.
Step 3	Server /user-policy # **commit**	Commits the transaction to the system configuration.

This example shows how to disable strong password:

```
Server# scope user-policy
Server /user-policy # set password-policy disabled
Warning: Strong password policy is being disabled.
Do you wish to continue? [y/N] y
Server /user-policy *# commit
Server /user-policy #
```

Password Expiry

You can set a shelf life for a password, after which it expires. As an administrator, you can set this time in days. This configuration would be common to all users. Upon password expiry, the user is notified on login and would not be allowed to login unless the password is reset.

Note When you downgrade to an older database, existing users are deleted. The database returns to default settings. Previously configured users are cleared and the database is empty, that is, the database has the default username - 'admin' and password - 'password'. Since the server is left with the default user database, the change default credential feature is enabled. This means that when the 'admin' user logs on to the database for the first time after a downgrade, the user must mandatorily change the default credential.

Password Set Time

A 'Password set time' is configured for every existing user, to the time when the migration or upgrade occurred. For new users (users created after an upgrade), the Password Set time is configured to the time when the user was created, and the password is set. For users in general (new and existing), the Password Set Time is updated whenever the password is changed.

Configuring Password Expiry for Users

Procedure

	Command or Action	Purpose
Step 1	Server # **scope user-policy**	Enters the user policy command mode.
Step 2	Server /user-policy # **scope password-expiration**	Enters the password expiration command mode.
Step 3	Server /user-policy/password-expiration # **set password-expiry-duration** *integer in the range 0-3650*	The time period that you can set for the existing password to expire (from the time you set a new password or modify an existing one). The range is between 0 to 3650 days. Entering 0 disables this option.
Step 4	Server /user-policy/password-expiration * # **set notification-period** *integer in the range 0-15*	Notifies the time by when the password expires. Enter a value between 0 to 15 days. Entering 0 disables this option.

	Command or Action	Purpose
Step 5	Server /user-policy/password-expiration * # **set grace-period** *integer in the range 0-5*	Time period till when the existing password can still be used, after it expires. Enter a value between 0 to 5 days. Entering 0 disables this option.
Step 6	Server /user-policy/password-expiration * # **set password-history** *integer in the range 0-5*	The number of occurrences when a password was entered. When this is enabled, you cannot repeat a password. Enter a value between 0 to 5. Entering 0 disables this option.
Step 7	Server /user-policy/password-expiration *# **commit**	Commits the transactions.
Step 8	Server /user-policy/password-expiration # **show detail**	(Optional) Shows the password expiration details.
Step 9	Server /user-policy/password-expiration # **restore**	(Optional) At the confirmation prompt, enter yes to restore the password expiry settings to default values.

This example sets the password expiration and restore the settings to default vales:

```
Server # scope user-policy
Server /user-policy # scope password-expiration
Server /user-policy/password-expiration # set password-expiry-duration 5
Server /user-policy/password-expiration * # set notification-period 2
Server /user-policy/password-expiration *# set grace-period 1
Server /user-policy/password-expiration *# set password-history 4
Server /user-policy/password-expiration *# commit
Server /user-policy/password-expiration # show detail
Password expiration parameters:
 Valid password duration: 5
 Number of stored old passwords: 4
 Notification period: 2
 Grace period: 1
Server /user-policy/password-expiration #
Restoring the password expiry parameters to default values:
Server /user-policy/password-expiration # restoreAre you sure you want to restore
User password expiration parameters to defaults?
Please enter 'yes' to confirm:yes
Server /user-policy/password-expiration #
```

LDAP Servers

Cisco IMC supports directory services that organize information in a directory, and manage access to this information. Cisco IMC supports Lightweight Directory Access Protocol (LDAP), which stores and maintains directory information in a network. In addition, Cisco IMC 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 Cisco IMC utilizes the Kerberos-based authentication service of LDAP.

When LDAP is enabled in the Cisco IMC, 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 Cisco IMC 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 Cisco IMC. You can use an existing LDAP attribute that is mapped to the Cisco IMC 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 Cisco IMC user roles and locales.

If you are using Group Authorization on the Cisco IMC LDAP configuration, then you can skip Steps 1-4 and perform the steps listed in the *Configuring LDAP Settings and Group Authorization in Cisco IMC* section.

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:

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

d) Click **OK**.

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

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 Cisco IMC to configure the LDAP server.

Configuring LDAP in Cisco IMC

Configure LDAP in Cisco IMC 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***LDAP domain name*	Specifies an LDAP domain name.
Step 4	Server /ldap # **set timeout** *seconds*	Specifies the number of seconds the Cisco IMC 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** *domain-name*	Specifies the Base DN that is searched on the LDAP server.

	Command or Action	Purpose
Step 7	Server /ldap # **set attribute** *name*	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. You can use an existing LDAP attribute that is mapped to the Cisco IMC user roles and locales or you can create a custom attribute, such as the CiscoAVPair attribute, which has the following attribute ID: `1.3.6.1.4.1.9.287247.1` **Note** If you do not specify this property, user access is denied.
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 Cisco IMC*.

Configuring LDAP Groups in Cisco IMC

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 Cisco IMC 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 *index* 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: • **admin—**The user can perform all actions available. • **user—**The user can perform the following tasks: ◦ 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.

	Command or Action	Purpose
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 #
```

Configuring Nested Group Search Depth in LDAP Groups

You can search for an LDAP group nested within another defined group in an LDAP group map.

- 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-search-depth** *value*	Enables search for a nested LDAP group.
Step 4	Server /ldap/role-group-rule # **commit**	Commits the transaction to the system configuration.

This example shows how to search for run a search for an LDAP group nested within another defined group.

```
Server# scope ldap
Server /ldap # scope ldap-group-rule
Server /ldap/ldap-group-rule # set group-search-depth 10
```

```
Server /ldap/role-group-rule* # commit
Server /ldap/role-group-rule # show detail
Group rules for LDAP:
    Group search attribute: memberOf
    Enable Group Authorization: yes
    Nested group search depth: 10
Server/ldap/ldap-group-rule #
```

LDAP Certificates Overview

Cisco C-series servers allow an LDAP client to validate a directory server certificate against an installed CA certificate or chained CA certificate during an LDAP binding step. This feature is introduced in the event where anyone can duplicate a directory server for user authentication and cause a security breach due to the inability to enter a trusted point or chained certificate into the Cisco IMC for remote user authentication.

An LDAP client needs a new configuration option to validate the directory server certificate during the encrypted TLS/SSL communication.

Exporting LDAP CA Certificate

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 **scope binding-certificate**	Enters the LDAP CA certificate binding command mode.
Step 3	Server /ldap/binding-certificate # **export-ca-certificate** *remote-protocol IP Adderss LDAP CA Certificate file*	Specifies the protocol to connect to the remote server. It can be of the following types: • TFTP • FTP • SFTP • SCP • HTTP

	Command or Action	Purpose
		Note The Cisco UCS C-Series server now supports fingerprint confirmation of the server when you update firmware through a remote server. This option is available only if you choose SCP or SFTP as the remote server type. If you chose SCP or SFTP as the remote server type while performing this action, a prompt with the message Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue? Click y or n depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to. Initiates the export of the certificate.

This example exports the LDAP certificate:

```
Server # scope ldap
Server /ldap # scope binding-certificate
Server /ldap/binding-certificate #  export-ca-certificate tftp 172.22.141.66 test.csv
 Initiating Export
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  1262    0     0  100  1262      0   1244  0:00:01  0:00:01 --:--:--  1653
100  1262    0     0  100  1262      0   1237  0:00:01  0:00:01 --:--:--  1237
LDAP CA Certificate is exported successfully
Server /ldap/binding-certificate #
```

Downloading LDAP CA Certificate Content by Copying Content

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 **scope binding-certificate**	Enters the LDAP CA certificate binding command mode.
Step 3	Server# /ldap/binding-certificate **set enabled** {**yes** | **no**}	Enables or disables LDAP CA certificate binding.
Step 4	Server /ldap/binding-certificate* # **commit**	Commits the transaction to the system configuration.
Step 5	Server /ldap/binding-certificate # **paste-ca-certificate**	Prompts you to paste the certificate content.

	Command or Action	Purpose
Step 6	Paste the certificate content and press **CTRL+D**.	Confirmation prompt appears.
Step 7	At the confirmation prompt, enter **y**.	This begins the download of the LDAP CA certificate.

This example downloads the LDAP certificate:

```
Server # scope ldap
Server /ldap # scope binding-certificate
Server /ldap/binding-certificate # set enabled yes
Server /ldap/binding-certificate *# commit
Server /ldap/binding-certificate # show detail
LDAP binding with Certificate:
    Enabled: yes
Server /ldap/binding-certificate # paste-ca-certificate
 Please paste your certificate here, when finished, press CTRL+D.
-----BEGIN CERTIFICATE-----
MIIDdzCCAl+gAwIBAgIQV06yJcJPAYNO8Cp+FYQttjANBgkqhkiG9w0BAQsFADBO
MRIwEAYKCZImiZPyLGQBGRYCaW4xGzAZBgoJkiaJk/IsZAEZFgs0T0JKUkEySkhC
UTEbMBkGA1UEAxMSV0lOLTRPQkpSQTJKSEJRLUNBMB4XDTE2MDIyNTE3MDczNloX
DTIxMDIyNTE3MTczM1owTjESMBAGCgmSJomT8ixkARkWAmluMRswGQYKCZImiZPy
LGQBGRYLNE9CSlJBMkpIQlExGzAZBgNVBAMTEldJTi00T0JKUkEySkhCUS1DQTCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMM2cdgmrPTkZe4K2zI+EbeZ
mfQnjfiUz8OIY97w8lC/2S4qK46T+fnX13rXe8vvVHAO5wgPDVQTGS4nlF46A6Ba
FK+krKcIgFrQB1gnF74qs/ln1YtKHNBjrvg5KyeWFrA7So6Mi2XEw8w/zMPL0d8T
b+LM1YnhnuXA9G8gVCJ/iUhXfMpB20L8sv30Mek7bw8x2cxJYTuJAviVIrjSwU5j
fO3WKttRuyFpeOIi00weklpF0+8D3Z9mBinoTbL2pl0U32am6wTI+8WmtJ+8W68v
jH4Y8YBY/kzMHdpwjpdZkC5pE9BcM0rL9xKoIu6X0kSNEssoGnepFyNaH3t8vnMC
AwEAAaNRME8wCwYDVR0PBAQDAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYE
FBAUulHTAWBT1OBz8IgAEzXsfcCsMBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSIb3
DQEBCwUAA4IBAQAzUMZr+0r1dWkVfFNBd7lu8tQbAEJf/A7PIKnJGNoUq8moAGs4
pMndoxdpNGZhYCWDWX3GWdeF1HqZHhb38gGQ9ylu0pIK7tgQufZmeCBH6T7Tzq/w
Dq+TMFGIjXF84xW3N665y4ePgUcUI7e/6aBGcGkGeUYodBPtExe28tQyeuYwD4Zj
nLuZKkT+I4PAYygVCqxDGsvfRHDpGneb3R+GeonOf4ED/0tn5PLSL9khb9qkHu/V
dO3/HmKVzUhloTDBuAMq/wES2WZAWhGr3hBc4nWQNjZWEMOKDpYZVK/GhBmNF+xi
eRcFqgh64oEmH9qAp0caGS1e7UyYaN+LtPRe
-----END CERTIFICATE-----
CTRL+D
  You are going to overwrite the LDAP CA Certificate.
  Are you sure you want to proceed and overwrite the LDAP CA Certificate? [y|N]
y
Server /ldap/binding-certificate #
```

Downloading LDAP CA Certificate Using Remote Server

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.

<table>
<tr><th></th><th>Command or Action</th><th>Purpose</th></tr>
<tr><td>Step 2</td><td>Server# /ldap scope binding-certificate</td><td>Enters the LDAP CA certificate binding command mode.</td></tr>
<tr><td>Step 3</td><td>Server# /ldap/binding-certificate set enabled {yes | no}</td><td>Enables or disables LDAP CA certificate binding.</td></tr>
<tr><td>Step 4</td><td>Server /ldap/binding-certificate* # commit</td><td>Commits the transaction to the system configuration.</td></tr>
<tr><td>Step 5</td><td>Server /ldap/binding-certificate # download-ca-certificate remote-protocol IP Address LDAP CA Certificate file</td><td>Specifies the protocol to connect to the remote server. It can be of the following types:
• TFTP
• FTP
• SFTP
• SCP
• HTTP

Note The Cisco UCS C-Series server now supports fingerprint confirmation of the server when you update firmware through a remote server. This option is available only if you choose SCP or SFTP as the remote server type.

If you chose SCP or SFTP as the remote server type while performing this action, a prompt with the message Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue? Click y or n depending on the authenticity of the server fingerprint.

The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.</td></tr>
<tr><td>Step 6</td><td>At the confirmation prompt, enter y.</td><td>This begins the download of the LDAP CA certificate.</td></tr>
</table>

This example downloads the LDAP certificate:

```
Server # scope ldap
Server /ldap # scope binding-certificate
Server /ldap/binding-certificate # set enabled yes
Server /ldap/binding-certificate *# commit
Server /ldap/binding-certificate # show detail
LDAP binding with Certificate:
    Enabled: yes
Server /ldap/binding-certificate #  download-ca-certificate tftp 172.22.141.66
new_com_chain.cer
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  1282  100  1282    0     0   1247      0  0:00:01  0:00:01 --:--:--  1635
100  1282  100  1282    0     0   1239      0  0:00:01  0:00:01 --:--:--  1239
```

```
  You are going to overwrite the LDAP CA Certificate.
  Are you sure you want to proceed and overwrite the LDAP CA Certificate? [y|N]y
LDAP CA Certificate is downloaded successfully
Server /ldap/binding-certificate #
```

Testing LDAP Binding

Before You Begin

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

Note If you checked the **Enable Encryption** and the **Enable Binding CA Certificate** check boxes, enter the fully qualified domain name (FQDN) of the LDAP server in the LDAP Server field. To resolve the FQDN of the LDAP server, configure the preferred DNS of Cisco IMC network with the appropriate DNS IP address.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope ldap**	Enters the LDAP command mode.
Step 2	Server# /ldap **scope binding-certificate**	Enters the LDAP CA certificate binding command mode.
Step 3	Server /ldap/binding-certificate # **test-ldap-binding** *username*	Password prompt appears.
Step 4	Enter the corresponding password.	Authenticates the user.

This example tests the LDAP user binding:

```
Server # scope ldap
Server /ldap # scope binding-certificate
Server /ldap/binding-certificate # test-ldap-binding user
Password:
diagldapbinding: Authenticated by LDAP
User user authenticated successfully.
Server /ldap/binding-certificate #
```

Deleting LDAP CA Certificate

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 **scope binding-certificate**	Enters the LDAP CA certificate binding command mode.
Step 3	Server /ldap/binding-certificate # **delete-ca-certificate**	Confirmation prompt appears.
Step 4	At the confirmation prompt, enter **y**.	This deletes the LDAP CA certificate.

This example deletes the LDAP certificate:

```
Server # scope ldap
Server /ldap # scope binding-certificate
Server /ldap/binding-certificate # delete-ca-certificate
You are going to delete the LDAP CA Certificate.
 Are you sure you want to proceed and delete the LDAP CA Certificate? [y|N]y
LDAP CA Certificate is deleted successfully
Server /ldap/binding-certificate #
```

Setting User Search Precedence

Procedure

	Command or Action	Purpose
Step 1	Server# **scope ldap**	Enters the BIOS command mode.
Step 2	Server# /ldap **set userSearchPrecedence** {*localUserDB* | *ldapUserDB*}	Sets the user search precedence to the LDAP database or the local user database depending on the option you choose.
Step 3	Server# /ldap * **commit**	Commits the transaction.
Step 4	Server# /ldap **show detail**	(Optional) Shows the LDAP details.

This example sets the user search precedence:

```
Server # scope ldap
Server /ldap # set userSearchPrecedence localUserDB
Server /ldap * # commit
Server /ldap # show detail
LDAP Settings:
Enabled: yes
Encrypted: no
Local User Search Precedence: localUserDB
Domain: new.com
Base DN: DC=new,DC=com
Timeout: 60
```

```
Filter Attribute: sAMAccountName
Attribute: CiscoAvPair
Server /ldap #
```

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.
User name column	The username for the user.
IP Address column	The IP address from which the user accessed the server. If this is a serial connection, it displays **N/A**.
Type column	The type of session the user chose to access the server. This can be one of the following: • **webgui—** indicates the user is connected to the server using the web UI. • **CLI—** indicates the user is connected to the server using CLI. • **serial—** indicates the user is connected to the server using the serial port.
Action column	This column displays **N/A** when the SOL is enabled and **Terminate** when the SOL is disabled. You can terminate a session by clicking **Terminate** on the web UI.

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** *session-number*	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 #
```

CHAPTER 8

Configuring Network-Related Settings

This chapter includes the following sections:

Server NIC Configuration

Server NICs

NIC Mode

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

- **Dedicated—**The management port that is used to access the Cisco IMC.
- **Shared LOM—**Any LOM (LAN on Motherboard) port that can be used to access Cisco IMC.
- **Shared LOM 10G—**Any 10G LOM port can be used to access the Cisco IMC.

- **Cisco Card**—Any port on the adapter card that can be used to access Cisco IMC. The Cisco adapter card has to be installed in a slot with Network the Communications Services Interface protocol support (NCSI).
- **Shared LOM Extended**—Any LOM port or Cisco adapter card port that can be used to access Cisco IMC. The Cisco adapter card has to be installed in a slot with NCSI support.

Note **Shared LOM Extended** and **Shared LOM 10G** are available only on some UCS C-Series servers.

NIC Redundancy

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

- **none**—Each port that is 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 that are associated with the configured NIC mode operate simultaneously. This feature increases throughput and provides multiple paths to Cisco IMC.

  Note When using **active-active**, do not configure a port-channel in the upstream switch for the member interfaces. A port-channel can be configured when using **active-standby**.

- **active-standby**—If a port that is associated with the configured NIC mode fails, traffic fails over to one of the other ports associated with the NIC mode.

  Note If you choose this option, make sure that all ports associated with the configured NIC mode are connected to the same VLAN 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 Cisco IMC command mode.
Step 2	Server /cimc # **scope network**	Enters the Cisco IMC 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: • Dedicated—The management Ethernet port is used to access the Cisco IMC. • Shared LOM—The LAN On Motherboard (LOM) Ethernet host ports are used to access the Cisco IMC. **Note** If you select Shared LOM, make sure that all host ports belong to the same subnet. • Shared LOM 10G—The 10G LOM Ethernet host ports are used to access the Cisco IMC. • 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 Cisco IMC.
Step 4	Server /cimc/network # **set vic-slot** {**none** | **riser1** | **riser2** | **flex-lom**}	VIC slot can be set to Cisco cards available in FLEX LOM or riser 1 or riser 2 slots. For C220 M4 servers, VIC slot options are as follows: • **Riser 1**—Slot 1 is selected. • **Riser 2**— Slot 2 is selected. • **FLEX LOM**—Slot 3 (MLOM) is selected. For C240 M4 servers, VIC slot options are as follows: • **Riser 1**—Slot 2 is the primary slot, but you can use slot 1. • **Riser 2**— Slot 5 is the primary slot, but you can use slot 4. • **FLEX LOM**—Slot 7 (MLOM) is selected. **Important** VIC slot is applicable for Cisco cards and on some UCS C-Series servers only.
Step 5	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: • **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.

	Command or Action	Purpose
		• **active-standby—**If one LOM Ethernet port fails, traffic fails over to another LOM port.
Step 6	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.
Step 7	At the prompt, enter y to confirm.	Configures the server NIC.

This example configures the Cisco IMC network interface:

```
scope cimc
Server /cimc # scope network
Server /cimc/network # set mode cisco_card
Server /cimc/network # set vic-slot <flex-lom>
Server /cimc/network *# set redundancy <active-active>
Server /cimc/network *# commit
Changes to the network settings will be applied immediately.
You may lose connectivity to the Cisco IMC and may have to log in again.
Do you wish to continue? [y/N] y
Server /cimc/network #
```

Common Properties Configuration

Overview to Common Properties Configuration

Hostname

The Dynamic Host Configuration Protocol (DHCP) enhancement is available with the addition of the hostname to the DHCP packet, which can either be interpreted or displayed at the DHCP server side. The hostname, which is now added to the options field of the DHCP packet, sent in the DHCP DISCOVER packet that 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, allows you to track and map the IP addresses that are leased out to Cisco IMC from the DHCP server. The default serial number is provided by the manufacturer as a sticker or label on the server to help you identify the server.

Dynamic DNS

Dynamic DNS (DDNS) is used to add or update the resource records on the DNS server from Cisco IMC. You can enable Dynamic DNS by using either the web UI or CLI. When you enable the DDNS option, the DDNS service records the current hostname, domain name, and the management IP address and updates the resource records in the DNS server from Cisco IMC.

> **Note** The DDNS server deletes the prior resource records (if any) and adds the new resource records to the DNS server if any one of the following DNS configuration is changed:
>
> - Hostname
> - Domain name in the LDAP settings
> - When DDNS and DHCP are enabled, if the DHCP gets a new IP address or DNS IP or domain name due to a change in a network or a subnet.
> - When DHCP is disabled and if you set the static IP address by using CLI or web UI.
> - When you enter the **dns-use-dhcp** command.

Dynamic DNS Update Domain— You can specify the domain. The domain could be either main domain or any sub-domain. This domain name is appended to the hostname of the Cisco IMC for the DDNS update.

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 Cisco IMC command mode.
Step 2	Server /cimc # **scope network**	Enters Cisco IMC network command mode.
Step 3	Server /cimc/network # **set hostname** *host-name*	Specifies the name of the host. When you modify the hostname, you are prompted to confirm whether you want to create a new self-signed certificate with Common Name (CN) as the new hostname. If you enter **y** at the prompt, a new self-signed certificate is created with CN as the new hostname. If you enter **n** at the prompt, only the hostname is changed and no certificate will be generated.
Step 4	Server /cimc/network # **set ddns-enabled**	(Optional) Enables the DDNS service for Cisco IMC
Step 5	Server /cimc/network # **set ddns-update-domain** *value*	(Optional) Updates the selected domain or its subdomain.

	Command or Action	Purpose
Step 6	Server /cimc/network # **commit**	Commits the transaction to the system configuration.
Step 7	At the prompt, enter y to confirm.	Configures common properties.

This example shows how to configure 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 # set ddns-enabled
Server /cimc/network # set ddns-update-domain 1.2.3.4
Server /cimc/network *# commit
Changes to the network settings will be applied immediately.
You may lose connectivity to the Cisco IMC and may have to log in again.
Do you wish to continue? [y/N] y
Server /cimc/network #
```

What to Do Next

Changes to the network are applied immediately. You might lose connectivity to Cisco IMC and 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 Cisco IMC command mode.
Step 2	Server /cimc # **scope network**	Enters the Cisco IMC network command mode.
Step 3	Server /cimc/network # **set dhcp-enabled** {**yes** | **no**}	Selects whether the Cisco IMC uses DHCP. **Note** If DHCP is enabled, we recommend that the DHCP server be configured to reserve a single IP address for the Cisco IMC. If the Cisco IMC 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** *ipv4-address*	Specifies the IP address for the Cisco IMC.

	Command or Action	Purpose
Step 5	Server /cimc/network # **set v4-netmask** *ipv4-netmask*	Specifies the subnet mask for the IP address.
Step 6	Server /cimc/network # **set v4-gateway** *gateway-ipv4-address*	Specifies the gateway for the IP address.
Step 7	Server /cimc/network # **set dns-use-dhcp** {**yes** | **no**}	Selects whether the Cisco IMC retrieves the DNS server addresses from DHCP.
Step 8	Server /cimc/network # **set preferred-dns-server** *dns1-ipv4-address*	Specifies the IP address of the primary DNS server.
Step 9	Server /cimc/network # **set alternate-dns-server** *dns2-ipv4-address*	Specifies the IP address of the secondary DNS server.
Step 10	Server /cimc/network # **commit**	Commits the transaction to the system configuration.
Step 11	At the prompt, enter y to confirm.	Configures IPv4.
Step 12	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
Changes to the network settings will be applied immediately.
You may lose connectivity to the Cisco IMC and may have to log in again.
Do you wish to continue? [y/N] y
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
    IPv6 Enabled: no
    IPv6 Address: ::
    IPv6 Prefix: 64
    IPv6 Gateway: ::
    IPv6 Link Local: ::
    IPv6 SLAAC Address: ::
    IPV6 DHCP Enabled: no
    IPV6 Obtain DNS Server by DHCP: no
    IPV6 Preferred DNS: ::
    IPV6 Alternate DNS: ::
    VLAN Enabled: no
    VLAN ID: 1
    VLAN Priority: 0
    Port Profile:
    Hostname: C240-FCH1938V17L
```

```
    MAC Address: E4:AA:5D:AD:19:81
    NIC Mode: shared_lom_ext
    NIC Redundancy: active-active
    VIC Slot: riser1
    Auto Negotiate: no
    Admin Network Speed: NA
    Admin Duplex: NA
    Operational Network Speed: NA
    Operational Duplex: NA

Server /cimc/network #
```

Configuring IPv6

Before You Begin

You must log in as a user with admin privileges to configure IPv6 network settings.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters the Cisco IMC command mode.
Step 2	Server /cimc # **scope network**	Enters the Cisco IMC network command mode.
Step 3	Server /cimc/network # **set v6-enabled** {**yes** | **no**}	Enables IPv6.
Step 4	Server /cimc/network # **set v6-dhcp-enabled** {**yes** | **no**}	Selects whether the Cisco IMC uses DHCP. **Note** If DHCP is enabled, we recommend that the DHCP server be configured to reserve a single IPv6 address for the Cisco IMC. If the Cisco IMC is reachable through multiple ports on the server, the single IPv6 address must be reserved for the full range of MAC addresses of those ports.
Step 5	Server /cimc/network # **set v6-addr** *ipv6-address*	Specifies the IP address for the Cisco IMC.
Step 6	Server /cimc/network # **set v6-prefix** *ipv6-prefix-length*	Specifies the prefix length for the IP address.
Step 7	Server /cimc/network # **set v6-gateway** *gateway-ipv6-address*	Specifies the gateway for the IP address.
Step 8	Server /cimc/network # **set v6-dns-use-dhcp** {**yes** | **no**}	Selects whether the Cisco IMC retrieves the DNS server addresses from DHCP. **Note** You can use this option only when DHCP enabled.
Step 9	Server /cimc/network # **set v6-preferred-dns-server** *dns1-ipv6-address*	Specifies the IP address of the primary DNS server.

	Command or Action	Purpose
Step 10	Server /cimc/network # **set v6-alternate-dns-server** *dns2-ipv6-address*	Specifies the IP address of the secondary DNS server.
Step 11	Server /cimc/network # **commit**	Commits the transaction to the system configuration.
Step 12	At the prompt, enter y to confirm.	Configures IPv6.
Step 13	Server /cimc/network # **show** [**detail**]	(Optional) Displays the IPv6 network settings.

This example enables static IPv6 and displays the IPv6 network settings:

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set v6-enabled yes
Server /cimc/network *# set v6-addr 2010:201::279
Server /cimc/network *# set v6-gateway 2010:201::1
Server /cimc/network *# set v6-prefix 64
Server /cimc/network *# set v6-dns-use-dhcp no
Server  /cimc/network *# set v6-preferred-dns-server 2010:201::100
Server  /cimc/network *# set v6-alternate-dns-server 2010:201::101
Changes to the network settings will be applied immediately.
You may lose connectivity to the Cisco IMC and may have to log in again.
Server /cimc/network *# commit
Changes to the network settings will be applied immediately.
You may lose connectivity to the Cisco IMC and may have to log in again.
Do you wish to continue? [y/N] y
Server /cimc/network # show detail
Network Setting:
    IPv4 Enabled: yes
    IPv4 Address: 10.106.145.76
    IPv4 Netmask: 255.255.255.0
    IPv4 Gateway: 10.106.145.1
    DHCP Enabled: yes
    DDNS Enabled: yes
    DDNS Update Domain: example.com
    Obtain DNS Server by DHCP: no
    Preferred DNS: 171.70.168.183
    Alternate DNS: 0.0.0.0
    IPv6 Enabled: yes
    IPv6 Address: 2010:201::279
    IPv6 Prefix: 64
    IPv6 Gateway: 2010:201::1
    IPv6 Link Local: fe80::523d:e5ff:fe9d:395d
    IPv6 SLAAC Address: 2010:201::523d:e5ff:fe9d:395d
    IPV6 DHCP Enabled: no
    IPV6 Obtain DNS Server by DHCP: no
    IPV6 Preferred DNS: 2010:201::100
    IPV6 Alternate DNS: 2010:201::101
    VLAN Enabled: no
    VLAN ID: 1
    VLAN Priority: 0
    Port Profile:
    Hostname: CIMC_C220
    MAC Address: 50:3D:E5:9D:39:5C
    NIC Mode: dedicated
    NIC Redundancy: none
    Network Speed: 100Mbps
    Duplex: full
    Auto Negotiate: no
   Admin Network Speed: NA
    Admin Duplex: NA
```

```
    Operational Network Speed: NA
    Operational Duplex: NA

Server /cimc/network #
```

This example enables DHCP for IPv6 and displays the IPv6 network settings:

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set v6-enabled yes
Server /cimc/network *# set v6-dhcp-enabled yes
Changes to the network settings will be applied immediately.
You may lose connectivity to the Cisco IMC and may have to log in again.
Server /cimc/network *# commit
Changes to the network settings will be applied immediately.
You may lose connectivity to the Cisco IMC and may have to log in again.
Do you wish to continue? [y/N] y
Server /cimc/network # show detail
Network Setting:
    IPv4 Enabled: yes
    IPv4 Address: 10.106.145.76
    IPv4 Netmask: 255.255.255.0
    IPv4 Gateway: 10.106.145.1
    DHCP Enabled: yes
    DDNS Enabled: yes
    DDNS Update Domain: example.com
    Obtain DNS Server by DHCP: no
    Preferred DNS: 171.70.168.183
    Alternate DNS: 0.0.0.0
    IPv6 Enabled: yes
    IPv6 Address: 2010:201::253
    IPv6 Prefix: 64
    IPv6 Gateway: fe80::222:dff:fec2:8000
    IPv6 Link Local: fe80::523d:e5ff:fe9d:395d
    IPv6 SLAAC Address: 2010:201::523d:e5ff:fe9d:395d
    IPV6 DHCP Enabled: yes
    IPV6 Obtain DNS Server by DHCP: no
    IPV6 Preferred DNS: ::
    IPV6 Alternate DNS: ::
    VLAN Enabled: no
    VLAN ID: 1
    VLAN Priority: 0
    Port Profile:
    Hostname: CIMC_C220
    MAC Address: 50:3D:E5:9D:39:5C
    NIC Mode: dedicated
    NIC Redundancy: none
    Network Speed: 100Mbps
    Duplex: full
    Auto Negotiate: no
    Admin Network Speed: NA
    Admin Duplex: NA
    Operational Network Speed: NA
    Operational Duplex: NA

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 Cisco IMC command mode.
Step 2	Server /cimc # **scope network**	Enters the Cisco IMC network command mode.
Step 3	Server /cimc/network # **set vlan-enabled** {**yes** | **no**}	Selects whether the Cisco IMC is connected to a VLAN.
Step 4	Server /cimc/network # **set vlan-id** *id*	Specifies the VLAN number.
Step 5	Server /cimc/network # **set vlan-priority** *priority*	Specifies the priority of this system on the VLAN.
Step 6	Server /cimc/network # **commit**	Commits the transaction to the system configuration.
Step 7	At the prompt, enter y to confirm.	Configures the server LAN.
Step 8	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
Changes to the network settings will be applied immediately.
You may lose connectivity to the Cisco IMC and may have to log in again.
Do you wish to continue? [y/N] y
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
    IPv6 Enabled: no
    IPv6 Address: ::
    IPv6 Prefix: 64
    IPv6 Gateway: ::
    IPv6 Link Local: ::
    IPv6 SLAAC Address: ::
    IPV6 DHCP Enabled: no
    IPV6 Obtain DNS Server by DHCP: no
    IPV6 Preferred DNS: ::
    IPV6 Alternate DNS: ::
    VLAN Enabled: yes
    VLAN ID: 10
    VLAN Priority: 32
    Port Profile:
    Hostname: C240-FCH1938V17L
    MAC Address: E4:AA:5D:AD:19:81
    NIC Mode: shared_lom_ext
    NIC Redundancy: active-active
    VIC Slot: riser1
```

```
    Auto Negotiate: no
    Admin Network Speed: NA
    Admin Duplex: NA
    Operational Network Speed: NA
    Operational Duplex: NA

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 Cisco IMC command mode.
Step 2	Server /cimc # **scope network**	Enters the Cisco IMC network command mode.
Step 3	Server /cimc/network # **set port-profile** *port_profile_name*	Specifies the port profile Cisco IMC should use to configure the management interface, the virtual Ethernet, and the VIF on supported adapter cards such as the Cisco UCS VIC 1225 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	At the prompt, enter y to confirm.	Connects to a port profile.
Step 6	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
Changes to the network settings will be applied immediately.
You may lose connectivity to the Cisco IMC and may have to log in again.
Do you wish to continue? [y/N] y
```

```
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
    IPv6 Enabled: no
    IPv6 Address: ::
    IPv6 Prefix: 64
    IPv6 Gateway: ::
    IPv6 Link Local: ::
    IPv6 SLAAC Address: ::
    IPV6 DHCP Enabled: no
    IPV6 Obtain DNS Server by DHCP: no
    IPV6 Preferred DNS: ::
    IPV6 Alternate DNS: ::
    VLAN Enabled: no
    VLAN ID: 1
    VLAN Priority: 0
    Port Profile: abcde12345
    Hostname: C240-FCH1938V17L
    MAC Address: E4:AA:5D:AD:19:81
    NIC Mode: shared_lom_ext
    NIC Redundancy: active-active
    VIC Slot: riser1
    Auto Negotiate: no
    Admin Network Speed: NA
    Admin Duplex: NA
    Operational Network Speed: NA
    Operational Duplex: NA

Server /cimc/network #
```

Network Interface Configuration

Overview to Network Interface Configuration

This support is added to configure network speed and duplex mode for the Cisco IMC management port. Auto Negotiation mode can be set for dedicated mode only. When auto negotiation is enabled the network port speed and duplex settings are ignored by the system and Cisco IMC retains the speed at which the switch is configured. When auto negotiation is disabled, you can configure the network port speed (10 Mbps, 100 Mbps, or 1 Gbps) and set the duplex value at either full or half.

Port Properties can be managed in the following two modes:

- **Admin Mode—**You can configure the network speed and duplex values by disabling the **Auto Negotiation** option. The default value of the network speed in the admin mode is 100 Mbps and the duplex mode is set to Full. Before changing the network speed ensure that the switch you connected to has the same port speed.
- **Operation Mode—**Displays the operation network port speed and duplex values. If you enabled auto negotiation mode, the network port speed and duplex details of the switch are displayed. If unchecked, the network port speed and duplex values that you set at the **Admin Mode** are displayed.

When you reset Cisco IMC 1.5(x), 2.0(1), and 2.0(3) versions to factory defaults, **Shared LOM** mode is configured by default.

For C3160 servers, if you reset to factory defaults, **Dedicated** mode is configured to **Full** duplex mode with 100 Mbps speed by default.

Configuring Interface Properties

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

Important This action is available only on some UCS C-Series servers.

Procedure

	Command or Action	Purpose
Step 1	Server # **scope cimc**	Enters the Cisco IMC 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. • If you enter **yes**, the network port speed and duplex settings are ignored by the system and Cisco IMC retains the speed at which the switch is configured. • If you enter **no**, you can configure the network port speed and duplex values.
Step 5	Server/cimc/network # **set net-speed** {**10 Mbps** | **100 Mbps** | **1 Gbps**}	Sets specified network port speed. **Note** This option is available only if **auto-negotiate** is set to **no**. Before changing the port speed, ensure that the switch you connected to has the same port speed. When **auto-negotiate** is set to **yes**, by default the network port speed is set to 100 Mbps.
Step 6	Server/cimc/network* # **set duplex** {**full** | **half**}	Sets specified duplex mode type. By default, the duplex mode is set to **Full**. **Note** For network speed of 1 Gbps, only full duplex mode is allowed.

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
 Please set speed and duplex
 If not set then a default speed of 100Mbps and duplex full will be applied
Server/cimc/network* # commit
Server/cimc/network* # set net-speed 100 Mbps
Server/cimc/network # set duplex full
```

```
Server/cimc/network* # commit
Changes to the network settings will be applied immediately.
You may lose connectivity to the Cisco IMC and may have to log in again.
Do you wish to continue? [y/N] y
Server/cimc/network #
```

Network Security Configuration

Network Security

The Cisco IMC 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. Cisco IMC 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 Cisco IMC command mode.
Step 2	Server /cimc # **scope network**	Enters the Cisco IMC 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** *fail-count*	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. The number of unsuccessful login attempts must occur within the time frame specified in the IP Blocking Fail Window field. Enter an integer between 3 and 10.
Step 6	Server /cimc/network/ipblocking # **set fail-window** *fail-seconds*	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.

	Command or Action	Purpose
Step 7	Server /cimc/network/ipblocking # **set penalty-time** *penalty-seconds*	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.
Step 9	Server /cimc/network/ipblocking # **exit**	Exits the IP blocking to the network command mode.
Step 10	Server /cimc/network # **scope ipfiltering**	Enters the IP filtering command mode.
Step 11	Server /cimc/network/ipfiltering # **set enabled** {**yes** | **no**}	Enables or disables IP filtering. At the prompt enter y to enable IP filtering.
Step 12	Server /cimc/network/ipfiltering # **set filter-1** *IPv4 or IPv6 address or a range of IP addresses*	You can set four IP filters. You can assign an IPv4 or IPv6 IP address or a range of IP addresses.
Step 13	Server /cimc/network/ipfiltering # **commit**	Commits the transaction to the system configuration.

This example configures network security:

```
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 #  exit
Server /cimc/network # scope ipfiltering
Server /cimc/network/ipfiltering # set enabled yes
This will enable IP Filtering
Do you wish to continue? [y/N] y
Server /cimc/network/ipfiltering *# set filter-1 1.1.1.1-255.255.255.255
                                    set filter-2 10.10.10.10
                                    set filter-3 2001:xxx::-2xxx:xx8::0001
                                    set filter-4
2001:xxx::-2xxx:xx8::0001-2001:xxx::-2xxx:xx8::0020
Server /cimc/network/ipfiltering *# commit
Changes to the ipfiltering will be applied immediately.
You may lose connectivity to the Cisco IMC and may have to log in again.
Do you wish to continue? [y/N] Y
```

Network Time Protocol Configuration

Configuring Network Time Protocol Settings

By default, when Cisco IMC is reset, it synchronizes the time with the host. With the introduction of the NTP service, you can configure Cisco IMC to synchronize the time with an NTP server. The NTP server does not run in Cisco IMC 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, Cisco IMC synchronizes the time with the configured NTP server. The NTP service can be modified only through Cisco IMC.

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 the Cisco IMC 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 #
```

Pinging an IP address

Ping an IP address when you want to validate network connectivity with the IP address in the Cisco IMC.

Before You Begin

You must log in as a user with administration privileges to ping an IP address.

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# **pingaddress** *IP address* | **retries***number* | **timeout***seconds*	Pings the IP address or host name for a specified number of times until timeout. • **IP address/hostname** - The IP address or the host name of the server. • **Number of retries** - The number of times the system tries to connect to the server. Default value is 3. Valid range is from 1 to 10. • **Timeout** - The number of seconds the system waits before it stops pinging. Default maximum value is 20 seconds. Valid range is from 1 to 20 seconds.
Step 4	Server /cimc/network # **commit**	Commits the transaction to the system configuration.
Step 5	At the prompt, enter y to confirm.	Pings the IP address.

This example pings an IP address:

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # ping 10.10.10.10
Server /cimc/network *# commit
Changes to the network settings will be applied immediately.
You may lose connectivity to the Cisco IMC and may have to log in again.
Do you wish to continue? [y/N] y
Server /cimc/network #
```

CHAPTER 9

Managing Network Adapters

This chapter includes the following sections:

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 VIC 1225 Virtual Interface Card
- Cisco UCS VIC 1385 Virtual Interface Card
- Cisco UCS VIC 1227T Virtual Interface Card
- Cisco UCS VIC 1387 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 polices 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 VIC 1225 Virtual Interface Card

The Cisco UCS VIC 1225 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.

Cisco UCS VIC 1385 Virtual Interface Card

The Cisco UCS VIC 1385 Virtual Interface Cardis a dual-port Enhanced Quad Small Form-Factor Pluggable (QSFP) 40 Gigabit Ethernet and Fibre Channel over Ethernet (FCoE)-capable half-height PCI Express (PCIe) card designed exclusively for Cisco UCS C-Series Rack Servers. It incorporates Cisco's next-generation converged network adapter (CNA) technology, with a comprehensive feature set, providing investment protection for future feature software releases. The card enables a policy-based, stateless, agile server infrastructure that can present over 256 PCIe standards-compliant interfaces to the host that can be dynamically configured as either network interface cards (NICs) or host bus adapters (HBAs). In addition, the Cisco UCS VIC 1385 card supports Cisco Data Center Virtual Machine Fabric Extender (VM-FEX) technology, which extends the Cisco UCS fabric interconnect ports to virtual machines, simplifying server virtualization deployment.

The personality of the card is determined dynamically at boot time using the service profile associated with the server. The number, type (NIC or HBA), identity (MAC address and World Wide Name [WWN]), failover policy, bandwidth, and quality-of-service (QoS) policies of the PCIe interfaces are all determined using the service profile. The capability to define, create, and use interfaces on demand provides a stateless and agile server infrastructure. Additional features and capabilities include:

- Each PCIe interface created on the VIC is associated with an interface on the Cisco UCS fabric interconnect, providing complete network separation for each virtual cable between a PCIe device on the VIC and the interface on the fabric interconnect
- The Cisco UCS VIC 1385 Virtual Interface Card provides high network performance and low latency for the most demanding applications such as SMB-Direct, VMQ, DPDK, and Cisco NetFlow

Cisco UCS VIC 1227T Virtual Interface Card

The Cisco UCS VIC 1227T Virtual Interface Card is a dual-port 10GBASE-T (RJ-45) 10-Gbps Ethernet and Fibre Channel over Ethernet (FCoE)–capable PCI Express (PCIe) modular LAN-on-motherboard (mLOM) adapter designed exclusively for Cisco UCS C-Series Rack Servers. New to Cisco rack servers, the mLOM slot can be used to install a Cisco VIC without consuming a PCIe slot, which provides greater I/O expandability. It incorporates next-generation converged network adapter (CNA) technology from Cisco, providing Fibre Channel connectivity over low-cost twisted pair cabling with a bit error rate (BER) of 10 to 15 up to 30 meters and investment protection for future feature releases. The mLOM card enables a policy-based, stateless, agile server infrastructure that can present up to 256 PCIe standards-compliant interfaces to the host that can be dynamically configured as either network interface cards (NICs) or host bus adapters (HBAs). In addition, the Cisco UCS VIC 1227T Virtual Interface Card supports Cisco Data Center Virtual Machine Fabric Extender (VM-FEX) technology, which extends the Cisco UCS fabric interconnect ports to virtual machines, simplifying server virtualization deployment. Additional features and capabilities include:

- Stateless and agile design - The personality of the card is determined dynamically at boot time using the service profile associated with the server. The number, type (NIC or HBA), identity (MAC address and World Wide Name [WWN]), failover policy, bandwidth, and quality-of-service (QoS) policies of the PCIe interfaces are all determined using the service profile. The capability to define, create, and use interfaces on demand provides a stateless and agile server infrastructure.
- Each PCIe interface created on the VIC is associated with an interface on the Cisco UCS fabric interconnect, providing complete network separation for each virtual cable between a PCIe device on the VIC and the interface on the fabric interconnect.
- Cisco SingleConnect technology provides an exceptionally easy, intelligent, and efficient way to connect and manage computing in the data center. Cisco SingleConnect technology dramatically simplifies the way that data centers connect to rack and blade servers, physical servers, virtual machines, LANs, SANs, and management networks.

Cisco UCS VIC 1387 Virtual Interface Card

The Cisco UCS VIC 1387 Virtual Interface Card is a dual-port Enhanced Quad Small Form-Factor Pluggable (QSFP) 40 Gigabit Ethernet and Fibre Channel over Ethernet (FCoE)-capable half-height PCI Express (PCIe) card designed exclusively for Cisco UCS C-Series Rack Servers. It incorporates Cisco's next-generation converged network adapter (CNA) technology, with a comprehensive feature set, providing investment protection for future feature software releases. The card enables a policy-based, stateless, agile server infrastructure that can present over 256 PCIe standards-compliant interfaces to the host that can be dynamically configured as either network interface cards (NICs) or host bus adapters (HBAs). In addition, the Cisco UCS VIC 1387 card supports Cisco Data Center Virtual Machine Fabric Extender (VM-FEX) technology, which extends the Cisco UCS fabric interconnect ports to virtual machines, simplifying server virtualization deployment.

The personality of the card is determined dynamically at boot time using the service profile associated with the server. The number, type (NIC or HBA), identity (MAC address and World Wide Name [WWN]), failover policy, bandwidth, and quality-of-service (QoS) policies of the PCIe interfaces are all determined using the service profile. The capability to define, create, and use interfaces on demand provides a stateless and agile server infrastructure. Additional features and capabilities include:

- Each PCIe interface created on the VIC is associated with an interface on the Cisco UCS fabric interconnect, providing complete network separation for each virtual cable between a PCIe device on the VIC and the interface on the fabric interconnect
- The Cisco UCS VIC 1387 Virtual Interface Card provides high network performance and low latency for the most demanding applications such as SMB-Direct, VMQ, DPDK, and Cisco NetFlow

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** [*index*] [**detail**]	Displays adapter properties. To display the properties of a single adapter, specify the PCI slot number as the *index* 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** *index*	Enters the command mode for the adapter card at the PCI slot number specified by *index*. **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 lldp** {**disable** | **enable**}	Enables or disables Link Layer Discovery Protocol (LLDP) on the adapter card. LLDP is enabled by default. **Note** We recommend that you do not disable LLDP option, as it disables all the Data Center Bridging Capability Exchange protocol (DCBX) functionality.
Step 6	Server /chassis/adapter # **set vntag-mode** {**disabled** | **enabled**}	Enables or disables VNTAG on the adapter card. VNTAG is disabled by default. If VNTAG mode is enabled:

	Command or Action	Purpose
		• vNICs and vHBAs can be assigned to a specific channel. • vNICs and vHBAs can be associated to a port profile. • vNICs can fail over to another vNIC if there are communication problems.
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 *# set vntag-mode enabled
Server /chassis/adapter *# commit
Warning: Enabling VNTAG mode
All the vnic configuration will be reset to factory defaults
New VNIC adapter settings will take effect upon the next server reset
Server /chassis/adapter # show detail
PCI Slot 1:
    Product Name: UCS VIC xxxx
    Serial Number: FCHXXXXXZV4
    Product ID: UCSC-PCIE-xxx-04
    Adapter Hardware Revision: 3
    Current FW Version: x.0(0.345)
    VNTAG: Enabled
    FIP: Enabled
    LLDP: Enabled
    PORT CHANNEL: Disabled
    Configuration Pending: yes
    Cisco IMC Management Enabled: no
    VID: V00
    Vendor: Cisco Systems Inc
    Description:
    Bootloader Version: xxx
    FW Image 1 Version: x.0(0.345)
    FW Image 1 State: RUNNING ACTIVATED
    FW Image 2 Version: bodega-dev-170717-1500-orosz-ET
    FW Image 2 State: BACKUP INACTIVATED
    FW Update Status: Fwupdate never issued
    FW Update Error: No error
    FW Update Stage: No operation (0%)
    FW Update Overall Progress: 0%
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 VIC 1225 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 VIC 1225 Virtual Interface Card in an FCoE application, you must associate the vHBA with the FCoE VLAN. Follow the instructions in the **Modifying vHBA Properties** section 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** *index*	Enters the command mode for the adapter card at the PCI slot number specified by *index*. **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** | *name*] [**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** *index*	Enters the command mode for the adapter card at the PCI slot number specified by *index*. **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** | *name*}	Enters the host Fibre Channel interface command mode for the specified vHBA.
Step 5	Server /chassis/adapter/host-fc-if # **set wwnn** *wwnn*	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** *wwpn*	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** *mac-addr*	Specifies a MAC address for the vHBA.
Step 10	Server /chassis/adapter/host-fc-if # **set vlan** {**none** | *vlan-id*}	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** *cos-value*	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** {**off** | *rate*}	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** {**any** | *0-99*}	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** *msec*	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** *msec*	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** *size*	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** {**disable** | **enable**}	Enables or disables FCP Error Recovery. The default is disable.
Step 19	Server /chassis/adapter/host-fc-if/error-recovery # **set link-down-timeout** *msec*	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** *count*	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** *msec*	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: • **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-logi**	Enters the Fibre Channel fabric login command mode.
Step 31	Server /chassis/adapter/host-fc-if/port-f-logi # **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-logi # **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-logi # **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-logi**	Enters the Fibre Channel port login command mode.
Step 35	Server /chassis/adapter/host-fc-if/port-p-logi # **set plogi-retries** *count*	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-logi # **set plogi-timeout** *msec*	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-logi # **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** *count*	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** *size*	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** *size*	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** *size*	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 fc1
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** *index*	Enters the command mode for the adapter card at the PCI slot number specified by *index*. **Note** The server must be powered on before you can view or change adapter settings.
Step 3	Server /chassis/adapter # **create host-fc-if** *name*	Creates a vHBA and enters the host Fibre Channel interface command mode. The *name* argument can be up to 32 ASCII characters.

	Command or Action	Purpose
Step 4	Server /chassis/adapter/host-fc-if # **set channel-number** *number*	(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 138.

Deleting a vHBA

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 *index*. **Note** The server must be powered on before you can view or change adapter settings.
Step 3	Server /chassis/adapter # **delete host-fc-if** *name*	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** *index*	Enters the command mode for the adapter card at the PCI slot number specified by *index*. **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 # **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** *index*	Enters the command mode for the adapter card at the PCI slot number specified by *index*. **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 # **create-boot-entry** *wwpn lun-id*	Creates a boot table entry. • *wwpn* — The World Wide Port Name (WWPN) for the boot target in the form hh:hh:hh:hh:hh:hh:hh:hh. • *lun-id* —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** *index*	Enters the command mode for the adapter card at the PCI slot number specified by *index*. **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 *entry* 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** *index*	Enters the command mode for the adapter card at the PCI slot number specified by *index*. **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 # **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** *index*	Enters the command mode for the adapter card at the PCI slot number specified by *index*. **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 *index*. **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 VIC 1225 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.

Cisco C-series servers use Remote Direct Memory Access (RDMA) over Converged Ethernet (RoCE) for packet transfers. RoCE defines the mechanism of performing RDMA over ethernet, based on the similar mechanism of RDMA over Infiniband. However, RoCE, with its performance oriented characteristics, delivers a superior performance compared to traditional network socket implementation because of the lower latency, lower CPU utilization and higher utilization of network bandwidth. RoCE meets the requirement of moving large amount of data across networks very efficiently.

The RoCE firmware requires the following configuration parameters provided by Cisco UCS Manager for better vNIC performance:

- Queue Pairs
- Memory Regions
- Resource Groups

Guidelines and Limitations for SMB Direct with RoCE

- Microsoft SMB Direct with RoCE is supported:
  - On Windows 2012 R2.
  - On Windows 2016.
- Cisco UCS C-Series server does not support more than 4 RoCE-enabled vNICs per adapter.
- Cisco UCS C-Series server does not support RoCE with NVGRE, VXLAN, VMQ, or usNIC.
- Maximum number of queue pairs per adapter is 8192.

- Maximum number of memory regions per adapter is 524288.
- RoCE configuration is supported between Cisco adapters. Interoperability between Cisco adapters and third party adapters is not supported.

Important It is required to configure the no-drop QOS policy settings at the switches in the RDMA traffic path.

Viewing vNIC 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 *index*. **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** | *name*] [**detail**]	Displays properties of a single vNIC, if specified, or all vNICs.
Step 4	Server /chassis/adapter # **show ext-eth-if** [**detail**]	Displays the external ethernet interfaces' details.

Following examples display the brief properties of all vNICs and the detailed properties of eth0 and the external interfaces:

```
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 iSCSI Boot usNIC
----- ----- -----------  ------------- ---  ------------ --------------- ------
eth0   1500 0            74:A2:E6:28:C6:AE N/A N/A  disabled disabled   0
eth1   1500 1            74:A2:E6:28:C6:AF N/A N/A  disabled disabled   0
srg    1500 0            74:A2:E6:28:C6:B2 N/A N/A  disabled disabled   64
hhh    1500 0            74:A2:E6:28:C6:B3 N/A N/A  disabled disabled   0

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 Link: 0
    PCI Order: ANY
    VLAN: NONE
    VLAN Mode: TRUNK
    Rate Limiting: OFF
    PXE Boot: disabled
    iSCSI Boot: disabled
    usNIC: 0
    Channel Number: N/A
```

```
    Port Profile: N/A
    Uplink Failover: disabled
    Uplink Failback Timeout: 5
    aRFS: disabled
    VMQ: disabled
    NVGRE: disabled
    VXLAN: disabled
    RDMA Queue Pairs: 1
    RDMA Memory Regions: 4096
    RDMA Resource Groups: 1
    CDN Name: VIC-1-eth0

Server# scope chassis
Server /chassis # scope adapter 1
Server /chassis/adapter # show ext-eth-if
Port MAC Address       Link State Encap.. Mode Admin Speed Oper..Speed   Link Training
Connector Present Connector Supported
---- ----------------- ---------- ------------ ----------- ------------- -------------
----------------- -------------------
0    74:A2:E6:28:C6:A2 Link       CE           40Gbps      40Gbps          N/A
Yes               Yes
1    74:A2:E6:28:C6:A3 Link       CE           40Gbps      40Gbps          N/A
Yes               Yes

Server /chassis/adapter # show ext-eth-if detail

C220-FCH1834V23X /chassis/adapter # show ext-eth-if detail
Port 0:
    MAC Address: 74:A2:E6:28:C6:A2
    Link State: Link
    Encapsulation Mode: CE
    Admin Speed: 40Gbps
    Operating Speed: 40Gbps
    Link Training: N/A
    Connector Present: Yes
    Connector Supported: Yes
    Connector Type: QSFP_XCVR_CR4
    Connector Vendor: CISCO
    Connector Part Number: 2231254-3
    Connector Part Revision: B
Port 1:
    MAC Address: 74:A2:E6:28:C6:A3
    Link State: Link
    Encapsulation Mode: CE
    Admin Speed: 40Gbps
    Operating Speed: 40Gbps
    Link Training: N/A
    Connector Present: Yes
    Connector Supported: Yes
    Connector Type: QSFP_XCVR_CR4
    Connector Vendor: CISCO
    Connector Part Number: 2231254-3
    Connector Part Revision: B


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** *index*	Enters the command mode for the adapter card at the PCI slot number specified by *index*. **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** | *name*}	Enters the host Ethernet interface command mode for the specified vNIC.
Step 5	Server /chassis/adapter/host-eth-if # **set mtu** *mtu-value*	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** *mac-addr*	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** *cos-value*	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. **Note** • You must set the **COS** value to 5 for the RDMA enabled interfaces. • 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**}	Specifies whether the vNIC will trust host CoS or will remark packets. The behavior is as follows: • **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*}	Specifies the default VLAN for this vNIC. Valid VLAN numbers are 1 to 4094; the default is none. **Note** If NIV is enabled, this setting is determined by the switch, and the command is ignored.

	Command or Action	Purpose
Step 12	Server /chassis/adapter/host-eth-if # **set vlan-mode** {**access** | **trunk**}	Specifies the VLAN mode for the vNIC. The modes are as follows: • **access** —The vNIC belongs to only one VLAN. When the VLAN is set to access mode, any frame received from the specified default VLAN (1-4094) that is received from the switch with a TAG removes that TAG when it is sent to the host OS through the vNIC. • **trunk** —The vNIC can belong to more than one VLAN. This is the default. **Note** If NIV is enabled, this setting is determined by the switch, and the command is ignored.
Step 13	Server /chassis/adapter/host-eth-if # **set rate-limit** {**off** | *rate*}	Specifies a maximum data rate for the vNIC. The range is 1 to 10000 Mbps; the default is off. **Note** If NIV is enabled, this setting is determined by the switch, and the command is ignored.
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** *number*	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** *name*	If NIV mode is enabled for the adapter, select the port profile that should be associated with the vNIC. **Note** The *name* must be a port profile defined on the switch to which this server is connected.
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 secondary interface if there are communication problems.
Step 18	Server /chassis/adapter/host-eth-if # **set uplink-failback-timeout** *seconds*	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 *seconds* between 0 and 600.
Step 19	Server /chassis/adapter/host-eth-if # **set vmq** {**disable** | **enable**}	Enables or disables Virtual Machine Queue (VMQ) for this adapter. **Note** Ensure that VMQ is not enabled when SR-IOV or netflow is enabled on the adapter.

	Command or Action	Purpose
Step 20	Server /chassis/adapter/host-eth-if # **set arfs** {**disable** | **enable**}	Enables or disables Accelerated Receive Flow steering (aRFS) for this adapter.
Step 21	Server /chassis/adapter/host-eth-if # **scope interrupt**	Enters the interrupt command mode.
Step 22	Server /chassis/adapter/host-eth-if/interrupt # **set interrupt-count** *count*	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 23	Server /chassis/adapter/host-eth-if/interrupt # **set coalescing-time** *usec*	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 24	Server /chassis/adapter/host-eth-if/interrupt # **set coalescing-type** {**idle** | **min**}	The coalescing types are as follows: • **idle** —The system does not send an interrupt until there is a period of no activity lasting as least 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 25	Server /chassis/adapter/host-eth-if/interrupt # **set interrupt-mode** {**intx** | **msi** | **msix**}	Specifies the Ethernet interrupt mode. The modes are as follows: • **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 26	Server /chassis/adapter/host-eth-if/interrupt # **exit**	Exits to the host Ethernet interface command mode.
Step 27	Server /chassis/adapter/host-eth-if # **scope recv-queue**	Enters receive queue command mode.
Step 28	Server /chassis/adapter/host-eth-if/recv-queue # **set rq-count** *count*	The number of receive queue resources to allocate. The range is 1 to 256; the default is 4.
Step 29	Server /chassis/adapter/host-eth-if/recv-queue # **set rq-ring-size** *size*	The number of descriptors in the receive queue. The range is 64 to 4094; the default is 512.

	Command or Action	Purpose
Step 30	Server /chassis/adapter/host-eth-if/recv-queue # **exit**	Exits to the host Ethernet interface command mode.
Step 31	Server /chassis/adapter/host-eth-if # **scope trans-queue**	Enters transmit queue command mode.
Step 32	Server /chassis/adapter/host-eth-if/trans-queue # **set wq-count** *count*	The number of transmit queue resources to allocate. The range is 1 to 256; the default is 1.
Step 33	Server /chassis/adapter/host-eth-if/trans-queue # **set wq-ring-size** *size*	The number of descriptors in the transmit queue. The range is 64 to 4094; the default is 256.
Step 34	Server /chassis/adapter/host-eth-if/trans-queue # **exit**	Exits to the host Ethernet interface command mode.
Step 35	Server /chassis/adapter/host-eth-if # **scope comp-queue**	Enters completion queue command mode.
Step 36	Server /chassis/adapter/host-eth-if/comp-queue # **set cq-count** *count*	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 37	Server /chassis/adapter/host-eth-if/comp-queue # **exit**	Exits to the host Ethernet interface command mode.
Step 38	Server /chassis/adapter/host-eth-if/ # **set rdma_mr***number*	Sets the number of memory regions to be used per adapter. The values range from 4096 to 524288.
Step 39	Server /chassis/adapter/host-eth-if/ # **set rdma_qp***number*	Sets the number of queue pairs to be used per adapter. The values range from 1-8192 queue pairs.
Step 40	Server /chassis/adapter/host-eth-if/ # **set rdma_resgrp***number*	Sets the number of resource groups to be used. The values range from 1-128 resource groups. **Note** After committing the RoCE details, you are required to reboot the server for the changes to take place.
Step 41	Server /chassis/adapter/host-eth-if # **scope offload**	Enters TCP offload command mode.
Step 42	Server /chassis/adapter/host-eth-if/offload # **set tcp-segment-offload** {**disable** | **enable**}	Enables or disables TCP Segmentation Offload as follows: • **disable** —The CPU segments large TCP packets. • **enable** —The CPU sends large TCP packets to the hardware to be segmented. This option may

	Command or Action	Purpose
		reduce CPU overhead and increase throughput rate. This is the default. **Note** This option is also known as Large Send Offload (LSO).
Step 43	Server /chassis/adapter/host-eth-if/offload # **set tcp-rx-checksum-offload** {**disable** | **enable**}	Enables or disables TCP Receive Offload Checksum Validation as follows: • **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 44	Server /chassis/adapter/host-eth-if/offload # **set tcp-tx-checksum-offload** {**disable** | **enable**}	Enables or disables TCP Transmit Offload Checksum Validation as follows: • **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 45	Server /chassis/adapter/host-eth-if/offload # **set tcp-large-receive-offload** {**disable** | **enable**}	Enables or disables TCP Large Packet Receive Offload as follows: • **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 46	Server /chassis/adapter/host-eth-if/offload # **exit**	Exits to the host Ethernet interface command mode.
Step 47	Server /chassis/adapter/host-eth-if # **scope rss**	Enters Receive-side Scaling (RSS) command mode.
Step 48	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 49	Server /chassis/adapter/host-eth-if/rss # **set rss-hash-ipv4** {**disable** | **enable**}	Enables or disables IPv4 RSS. The default is enable.

	Command or Action	Purpose
Step 50	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 51	Server /chassis/adapter/host-eth-if/rss # **set rss-hash-ipv6** {**disable** | **enable**}	Enables or disables IPv6 RSS. The default is enable.
Step 52	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 53	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 54	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 55	Server /chassis/adapter/host-eth-if/rss # **exit**	Exits to the host Ethernet interface command mode.
Step 56	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   QCI1417A0QK    N2XX-ACPCI01   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 # enable vmq
Server /chassis/adapter/host-eth-if # enable arfs
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.

Enabling or Disabling Link Training on External Ethernet Interfaces

Link training for the port profile on the external ethernet interfaces of the specified vNIC can be enabled or disabled.

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** *index*	Enters the command mode for the adapter card at the PCI slot number specified by *index*. **Note** The server must be powered on before you can view or change adapter settings.
Step 4	Server /chassis / adapter # **scope ext-eth-if 0 | 1** *name*	Enters the external ethernet interface command mode for the specified vNIC.
Step 5	Server /chassis / adapter / ext-eth-if # **set link-training on | off**	Enables or disables the link training for the specified vNIC.
Step 6	Server /chassis / adapter / ext-eth-if * # **commit**	Commits the transaction to the system configuration.

This example shows how to enable or disable link training on the external ethernet interface.

```
Server# scope chassis
Server /chassis # scope adapter 1
Server /chassis/adapter # scope ext-eth-if 1
Server /chassis/adapter/ext-eth-if* # set link-training on
Server /chassis/adapter/ext-eth-if# commit
You may lose connectivity to the Cisco IMC and may have to log in again.
Do you wish to continue? [y/N] y
Port 1:
    MAC Address: 74:A2:E6:28:C6:A3
    Link State: Link
    Encapsulation Mode: CE
    Admin Speed: 40Gbps
    Operating Speed: -
    Link Training: N/A
    Connector Present: Yes
    Connector Supported: Yes
    Connector Type: QSFP_XCVR_CR4
    Connector Vendor: CISCO
    Connector Part Number: 2231254-3
    Connector Part Revision: B
```

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** *index*	Enters the command mode for the adapter card at the PCI slot number specified by *index*. **Note** The server must be powered on before you can view or change adapter settings.
Step 3	Server /chassis/adapter # **create host-eth-if** *name*	Creates a vNIC and enters the host Ethernet interface command mode. The *name* argument can be up to 32 ASCII characters.
Step 4	Server /chassis/adapter/host-eth-if # **set channel-number** *number*	(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** *index*	Enters the command mode for the adapter card at the PCI slot number specified by *index*. **Note** The server must be powered on before you can view or change adapter settings.
Step 3	Server /chassis/adapter # **delete host-eth-if** *name*	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 Cisco IMC 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 Cisco IMC 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** *index*	Enters the command mode for the adapter card at the PCI slot number specified by *index*. **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 you 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 Cisco IMC 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 value using the Cisco IMC CLI, on page 162.
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 6. 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. We recommend that you set this value to 6.
Step 7	server/chassis/adapter/host-eth-if/usnic-config# **set tq-count** *count*	Specifies the number of transmit queue resources to allocate. We recommend that you set this value to 6.
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.
Step 11	server/chassis/adapter/host-eth-if# **exit**	Exits to adapter interface command mode.

	Command or Action	Purpose
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 6
server /chassis/adapter/host-eth-if/usnic-config *# set rq-count 6
server /chassis/adapter/host-eth-if/usnic-config *# set tq-count 6
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# scope bios
server /bios # scope advanced
server /bios/advanced # set IntelVTD Enabled
server /bios/advanced *# set ATS Enabled*
server /bios/advanced *# set CoherencySupport Enabled
server /bios/advanced *# commit
Changes to BIOS set-up parameters will require a reboot.
Do you want to reboot the system?[y|N]y
A system reboot has been initiated.
```

Modifying a Cisco usNIC value using the Cisco IMC CLI

Before You Begin

You must log in to the Cisco IMC 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** *index*	Enters the command mode for the adapter card at the PCI slot number specified by *index*. **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 you 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 usnic-count** *number of usNICs* .	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 6	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 7	server/chassis/adapter/host-eth-if/usnic-config# **exit**	Exits to host Ethernet interface command mode.
Step 8	server/chassis/adapter/host-eth-if# **exit**	Exits to adapter interface command mode.
Step 9	server/chassis/adapter# **exit**	Exits to chassis interface command mode.
Step 10	server/chassis# **exit**	Exits to server interface command mode.

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 32
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
```

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** *index*	Enters the command mode for the adapter card at the PCI slot number specified by *index*. **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** | *name*}	Enters the host Ethernet interface command mode for the specified vNIC.
Step 4	Server /chassis/adapter/host-eth-if # **show usnic-config** *index*	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 Cisco IMC 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** *index*	Enters the command mode for the adapter card at the PCI slot number specified by *index*. **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 you 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/chassis/host-eth-if/iscsi-boot *# commit
New host-eth-if settings will take effect upon the next adapter reboot

server/chassis/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** *index*	Enters the command mode for the adapter card at the PCI slot number specified by *index*. **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** | *name*}	Enters the host Ethernet interface command mode for the specified vNIC.
Step 4	Server /chassis/adapter/host-eth-if # **create iscsi-boot** *index*	Creates the iSCSI boot index for the vNIC. At this moment, only 0 is allowed as the index.
Step 5	Server /chassis/adapter/host-eth-if/iscsi-boot* # **create iscsi-target** *index*	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** *string*	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 iqn.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** *index*	Enters the command mode for the adapter card at the PCI slot number specified by *index*. **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** | *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 #
```

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** *index*	Enters the command mode for the adapter card at the PCI slot number specified by *index*. **Note** The server must be powered on before you can view or change adapter settings.
Step 3	Server /chassis/adapter # **export-vnic** *protocol remote server IP address*	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: • TFTP • FTP • SFTP • SCP • HTTP

	Command or Action	Purpose
		Note The Cisco UCS C-Series server now supports fingerprint confirmation of the server when you update firmware through a remote server. This option is available only if you choose SCP or SFTP as the remote server type. If you chose SCP or SFTP as the remote server type while performing this action, a prompt with the message Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue? Click y or n depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.

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** *index*	Enters the command mode for the adapter card at the PCI slot number specified by *index*. **Note** The server must be powered on before you can view or change adapter settings.
Step 3	Server /chassis/adapter # **import-vnic** *tftp-ip-address path-and-filename*	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 *index* argument. **Note** Resetting the adapter to default settings sets the port speed to 4 X 10 Gbps. Choose 40 Gbps as the port speed only if you are using a 40 Gbps switch.

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 Cisco IMC 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 Cisco IMC. 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** *tftp-ip-address path-and-filename* {**activate** | **no-activate**} [*pci-slot*] [*pci-slot*]	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** [*pci-slot*] [*pci-slot*]	(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 171.

Activating Adapter Firmware

Important While the activation is in progress, do not:

- Reset, power off, or shut down the server.
- Reboot or reset Cisco IMC.
- 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.
Step 2	Server /chassis # **activate-adapter-fw** *pci-slot* {**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 suceeded
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** *index*	Resets the adapter at the PCI slot number specified by the *index* 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 #
```

CHAPTER 10

Managing Storage Adapters

This chapter includes the following sections:

Creating Virtual Drives 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	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 # **create virtual-drive**	At this point, you are prompted to enter information corresponding to the RAID level, the physical drives to be used, the size, enabling full disk encryption of the drive 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. **Note** Enabling full disk encryption secures the drive.

	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, 10, 50 --> 1

Please choose from the following 10 unused physical drives:
    ID  Size(MB)       Model        Interface  Type
     1  571776         SEAGATE      SAS        HDD
     2  571776         SEAGATE      SAS        HDD
     4  571776         SEAGATE      SAS        HDD
     5  428672         SEAGATE      SAS        HDD
     6  571776         SEAGATE      SAS        HDD
     7  571776         SEAGATE      SAS        HDD
     8  571776         SEAGATE      SAS        HDD
     9  428672         SEAGATE      SAS        HDD
    10  571776         SEAGATE      SAS        HDD
    11  953344         SEAGATE      SAS        HDD

Specify physical disks for span 0:
  Enter comma-separated PDs from above list--> 1,2
  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' --> 10 GB

Optional attribute:

  stripsize: defaults to 64K Bytes

     0: 8K Bytes
    1: 16K Bytes
    2: 32K Bytes
    3: 64K Bytes
    4: 128K Bytes
    5: 256K Bytes
    6: 512K Bytes
    7: 1024K Bytes
  Choose number from above options or hit return to pick default--> 2
stripsize will be set to 32K Bytes (6 and 'strip-size\:32k')

  Disk Cache Policy: defaults to Unchanged

     0: Unchanged
    1: Enabled
    2: Disabled
  Choose number from above options or hit return to pick default--> 0
Disk Cache Policy will be set to Unchanged (0 and 'disk-cache-policy\:unchanged'

         )

  Read Policy: defaults to No Read Ahead

     0: No Read Ahead
    1: Always
  Choose number from above options or hit return to pick default--> 0
Read Policy will be set to No Read Ahead (0 and 'read-policy\:no-read-ahead')

  Write Policy: defaults to Write Through

     0: Write Through
```

```
    1: Write Back Good BBU
    2: Always Write Back
  Choose number from above options or hit return to pick default--> 0
Write Policy will be set to Write Through (0 and 'write-policy\:write-through')

  IO Policy: defaults to Direct I/O

     0: Direct I/O
    1: Cached I/O
  Choose number from above options or hit return to pick default--> 0
IO Policy will be set to Direct I/O (0 and 'io-policy\:direct-io')

  Access Policy: defaults to Read Write

     0: Read Write
    1: Read Only
    2: Blocked
  Choose number from above options or hit return to pick default--> 0
Access Policy will be set to Read Write (0 and 'access-policy\:read-write')
Enable SED security on virtual drive (and underlying drive group)?
Enter y or n--> y
Virtual drive and drive group will be secured

New virtual drive will have the following characteristics:
  - Spans: '[1.2]'
  - RAID level: '1'
  - Name: 'test_v_drive'
  - Size: 10 GB
  - stripsize: 32K Bytes
  - Disk Cache Policy: Unchanged
  - Read Policy: No Read Ahead
  - Write Policy: Write Through
  - IO Policy: Direct I/O
  - Access Policy: Read Write
  - Encryption: FDE

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     10000 MB   RAID 1
false
4             Good           Optimal              new_from_test    500 MB     RAID 1
false

Server /chassis/storageadapter #
```

Creating 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)
----------------------------------------------------------------
0  RAID0_12          0   100 MB        Unknown         1,2

Please choose from the above list the virtual drive number
whose space the new virtual drive will share--> 0
New virtual drive will share space with VD 0

Please enter Virtual Drive name (15 characters maximum)--> test_v_drive
Please enter Virtual Drive size in MB, GB, or TB (maximum: Unknown)
  Example format: '400 GB' --> 10 GB

Optional attributes:

  stripsize: defaults to 64K Bytes
     0: 8K Bytes
    1: 16K Bytes
    2: 32K Bytes
    3: 64K Bytes
    4: 128K Bytes
    5: 256K Bytes
    6: 512K Bytes
    7: 1024K Bytes
  Choose number from above options or hit return to pick default--> 0
stripsize will be set to 8K Bytes (4 and 'strip-size\:8k')

  Disk Cache Policy: defaults to Unchanged
     0: Unchanged
    1: Enabled
    2: Disabled
  Choose number from above options or hit return to pick default--> 0
Disk Cache Policy will be set to Unchanged (0 and 'disk-cache-policy\:unchanged')

  Read Policy: defaults to No Read Ahead
```

```
      0: No Read Ahead
     1: Always
  Choose number from above options or hit return to pick default--> 0
Read Policy will be set to No Read Ahead (0 and 'read-policy\:no-read-ahead')

  Write Policy: defaults to Write Through
     0: Write Through
    1: Write Back Good BBU
    2: Always Write Back
  Choose number from above options or hit return to pick default--> 0
Write Policy will be set to Write Through (0 and 'write-policy\:write-through')

  IO Policy: defaults to Direct I/O
     0: Direct I/O
    1: Cached I/O
  Choose number from above options or hit return to pick default--> 0
IO Policy will be set to Direct I/O (0 and 'io-policy\:direct-io')

  Access Policy: defaults to Read Write
     0: Read Write
    1: Read Only
    2: Blocked
  Choose number from above options or hit return to pick default--> 0
Access Policy will be set to Read Write (0 and 'access-policy\:read-write')

New virtual drive will have the following characteristics:
  - It will share space with virtual drive 0
  - Name: 'amit'
  - Size: 10 GB
  - stripsize: 8K Bytes
  - Disk Cache Policy: Unchanged
  - Read Policy: No Read Ahead
  - Write Policy: Write Through
  - IO Policy: Direct I/O
  - Access Policy: Read Write

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     10000 MB   RAID 1
false
4             Good           Optimal              new_from_test    500 MB     RAID 1
false

Server /chassis/storageadapter #
```

Setting a Virtual Drive as Transport Ready

Before You Begin

- You must log in with admin privileges to perform this task.
- The virtual drive must be in optimal state to enable transport ready.

Procedure

	Command or Action	Purpose
Step 1	Server # **scope chassis**	Enters the chassis command mode.
Step 2	Server /chassis # **scope storageadapter** *slot ID*	Enters the command mode for an installed storage card.
Step 3	Server /chassis/storageadapter # **scope virtual-drive** *drive-number*	Enters the command mode for the specified virtual drive.
Step 4	Server /chassis/storageadapter/virtual-drive # **set-transport-ready** *{include-all | exclude-all | include-dhsp}*	Sets the virtual drive to transport ready and assigns the chosen properties. Enter the initialization type using which you can set the selected virtual drive as transport ready. This can be one of the following: • **exlude-all—** Excludes all the dedicated hot spare drives. • **include-all—** Includes any exclusively available or shared dedicated hot spare drives. • **include-dhsp—** Includes exclusive dedicated hot spare drives. When you are prompted to confirm the action. Enter y to confirm. **Note** When you set a virtual drive to transport ready all the physical drives associated with it are displayed as Ready to remove.
Step 5	Server /chassis/storageadapter/virtual-drive # **show detail**	(Optional) Display the virtual drive properties with the change.

This example shows how to set virtual drive 5 to transport ready:

```
Server # scope chassis
Server /chassis # scope storageadapter SLOT-HBA
Server /chassis/storageadapter # scope virtual-drive 5
Server /chassis/storageadapter/virtual-drive # set-transport-ready exclude-all
Since they belong to same drive group, all these virtual drives will be set to Transport
Ready - 0
Are you sure you want to proceed?[y|N]y
Server /chassis/storageadapter/virtual-drive # show detail
Virtual Drive 0:
    Health: Good
    Status: Optimal
    Visibility : Visible
    Name: RAID0_124_RHEL
    Size: 2858160 MB
    Physical Drives: 1, 2, 4
    RAID Level: RAID 0
    Boot Drive: false
    FDE Capable: 0
    FDE Enabled: 0
```

```
    Target ID: 0
    Strip Size: 64 KB
    Drives Per Span: 3
    Span Depth: 1
    Access Policy: Transport Ready
    Cache Policy: Direct
    Read Ahead Policy: None
    Requested Write Cache Policy: Write Through
    Current Write Cache Policy: Write Through
    Disk Cache Policy: Unchanged
    Auto Snapshot: false
    Auto Delete Oldest: true
    Allow Background Init: true
Server /chassis/storageadapter/virtual-drive #
```

Clearing a Virtual Drive as Transport Ready

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 ID*	Enters the command mode for an installed storage card.
Step 3	Server /chassis/storageadapter # **scope virtual-drive** *drive-number*	Enters the command mode for the specified virtual drive.
Step 4	Server /chassis/storageadapter/virtual-drive # **clear-transport-ready**	This reverts the selected transport ready virtual drive to its original status. When you are prompted to confirm the action. Enter y to confirm.
Step 5	Server /chassis/storageadapter/virtual-drive # **show detail**	(Optional) Display the virtual drive properties with the change.

This example shows how to revert the selected transport ready virtual drive to its original state:

```
Server # scope chassis
Server /chassis # scope server 1
Server /chassis # scope storageadapter SLOT-HBA
Server /chassis/storageadapter # scope virtual-drive 5
Server /chassis/storageadapter/virtual-drive # clear-transport-ready
Since they belong to same drive group, all these virtual drives will be moved out of Transport
 Ready - 0
Are you sure you want to proceed?[y|N]y
Server /chassis/storageadapter/virtual-drive # show detail
Virtual Drive 0:
    Health: Good
    Status: Optimal
    Visibility : Visible
```

```
    Name: RAID0_124_RHEL
    Size: 2858160 MB
    Physical Drives: 1, 2, 4
    RAID Level: RAID 0
    Boot Drive: false
    FDE Capable: 0
    FDE Enabled: 0
    Target ID: 0
    Strip Size: 64 KB
    Drives Per Span: 3
    Span Depth: 1
    Access Policy: Read-Write
    Cache Policy: Direct
    Read Ahead Policy: None
    Requested Write Cache Policy: Write Through
    Current Write Cache Policy: Write Through
    Disk Cache Policy: Unchanged
    Auto Snapshot: false
    Auto Delete Oldest: true
    Allow Background Init: true
Server /chassis/storageadapter/virtual-drive #
```

Importing Foreign Configuration

When one or more physical drives that have previously been configured with a different controller are inserted into a server, they are identified as foreign configurations. You can import these foreign configurations to a controller.

Important You cannot import a foreign configuration in the following two scenarios:

1. When the secure virtual drive was created on server 1 (from which you want to import the configuration) using the remote key, and on server 2 (to which you want to import) using the local key.
2. When server 2 is configured with another KMIP server, which is not a part of the server 1 KMIP server cluster.

In order to import the foreign configuration in these scenarios, change the controller security on server 2 from local key management to remote key management, and use the same KMIP server from the same cluster where the server 1 KMIP is configured.

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 # **import-foreign-config**	You are prompted to confirm the action. Enter **yes** to confirm.

	Command or Action	Purpose
		Note If you do not enter **yes**, the action is aborted.

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

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter # import-foreign-config
Are you sure you want to import all foreign configurations on this controller?
Enter 'yes' to confirm -> yes
Server /chassis/storageadapter #
```

Unlocking Foreign Configuration Drives

When a set of physical drives hosting a secured drive group are inserted into a different server or controller (or the same controller but whose security-key has been changed while they were not present), they become foreign configurations. Since they are secured, these foreign configurations must be unlocked before they can be imported. The following procedure explains how to unlock a foreign configuration 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 # **unlock-foreign-configuration**	At the prompt, enter the security key and enter **yes** at the confirmation prompt.
Step 4	Server /chassis/storageadapter # **scope physical-drive 2**	(Optional) Enters the physical drive command mode.
Step 5	Server /chassis/storageadapter/physicsl-drive # **show detail**	(Optional) Displays the status of the unlocked foreign drive.

This example shows how to unlock a foreign configuration drive:

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter # unlock-foreign-configuration
Please enter the security key to unlock the foreign configuration -> testSecurityKey
Server /chassis/storageadapter # import-foreign-config
Are you sure you want to import all foreign configurations on this controller?
Enter 'yes' to confirm -> yes
```

```
Server /chassis/storageadapter # scope physical-drive 2
Server /chassis/storageadapter/physical-drive # show detail
Physical Drive Number 2:
    Controller: SLOT-HBA
    Health: Good
    Status: Online
    .
    .
    FDE Capable: 1
    FDE Enabled: 1
    FDE Secured: 1
    FDE Locked: 0
    FDE locked foreign config: 0

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

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 #
```

Enabling JBOD

Note You can enable Just a Bunch of Disks (JBOD) only on some UCS C-Series servers.

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 # **enable-jbod-mode**	Enables the JBOD Mode for the selected controller

This example enables the JBOD mode for the selected controller:

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter # enable-jbod-mode
Are you sure you want to enable JBOD mode?
Enter 'yes' to confirm -> yes
Server/chassis/storageadapter # show settings
PCI Slot SLOT-3:
    Info Valid: Yes
    Enable JBOD Mode: true
```

Disabling JBOD

Note This option is available only on some UCS C-Series servers.

Before You Begin

JBOD mode must be enabled for the selected controller.

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 # **disable-jbod-mode**	Disables the JBOD Mode for the selected controller

This example disables the JBOD mode for the selected controller:

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter # disable-jbod-mode
Are you sure you want to disable JBOD mode?
Enter 'yes' to confirm -> yes
Server/chassis/storageadapter # show settings
PCI Slot SLOT-3:
    Info Valid: Yes
    Enable JBOD Mode: false
```

Clearing a Boot Drive

Important This task clears the boot drive configuration on the controller. 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-boot-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 clear the boot drive configuration on the MegaRAID controller in slot 3:

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

Enabling Security on a JBOD

you can enable security on a physical drive only if it is a JBOD. The following procedure explains how to enable security on a JBOD:

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 2**	Enters the physical drive command mode.
Step 4	Server /chassis/storageadapter # **enable-security-on-jbod**	At the confirmation prompt, enter **yes**. Enables security on the JBOD.
Step 5	Server /chassis/storageadapter/physicsl-drive # **show detail**	(Optional) Displays details of the physical drive.

This example shows how to enable security on a JBOD:

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
savbu-stordev-dn1-2-cimc /chassis/storageadapter # scope physical-drive 2
server /chassis/storageadapter/physical-drive # enable-security-on-jbod
Are you sure you want to enable security on this JBOD?
NOTE: this is not reversible!
Enter 'yes' to confirm -> yes
server /chassis/storageadapter/physical-drive # show detail
Physical Drive Number 2:
    .
    .
    Status: JBOD
    .
    .
    FDE Capable: 1
    FDE Enabled: 1
    FDE Secured: 1
server /chassis/storageadapter/physical-drive #
```

Clearing a Secure Physical Drive

Clearing a secure drive converts an FDE drive from secured to unsecured. The Physical drive status must be Unconfigured good to perform this action. This erases the data on the physical drive. The following procedure explains how to clear a secure SED physical 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 physical-drive 2**	Enters the physical drive command mode.
Step 4	Server /chassis/storageadapter/physicsl-drive # **clear-secure-drive**	At the confirmation prompt, enter **yes**. This clears the secure SED physical drive and all the data will be lost.
Step 5	Server /chassis/storageadapter/physicsl-drive # **show detail**	(Optional) Displays the physical drive details.

This example shows how to clear an SED foreign configuration physical drive:

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter # scope physical-drive 2
Server /chassis/storageadapter/physical-drive #  clear-secure-drive
Are you sure you want to erase all data from this physical drive?
NOTE: this is not reversible!  ALL DATA WILL BE LOST!!
Enter 'yes' to confirm -> yes
Server /chassis/storageadapter/physical-drive # show detail
Physical Drive Number 2:
    Controller: SLOT-HBA
    Health: Good
    Status: Unconfigured Good
    .
    .
    FDE Capable: 1
    FDE Enabled: 0
    FDE Secured: 0


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

Clearing a Secure SED Foreign Configuration Physical Drive

Coverts a locked foreign configuration Full Disk Encryption drive to a unsecured and unlocked drive. This erases the data on the physical drive. The following procedure explains how to clear a secure SED foreign configuration physical 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 physical-drive 2**	Enters the physical drive command mode.
Step 4	Server /chassis/storageadapter/physicsl-drive # **clear-secure-foreign-config-drive**	At the confirmation prompt, enter **yes**. This clears the secure SED foreign configuration physical drive and all the data will be lost.
Step 5	Server /chassis/storageadapter/physicsl-drive # **show detail**	(Optional) Displays the physical drive details.

This example shows how to clear an SED foreign configuration physical drive:

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter # scope physical-drive 2
Server /chassis/storageadapter/physical-drive # clear-secure-foreign-config-drive
Are you sure you want to erase all data from this foreign-configuration physical drive?
NOTE: this is not reversible!  ALL DATA WILL BE LOST!!
Enter 'yes' to confirm -> yes
Server /chassis/storageadapter/physical-drive # show detail
Physical Drive Number 2:
    Controller: SLOT-HBA
    Health: Good
    Status: Unconfigured Good
    .
    .
    FDE Capable: 1
    FDE Enabled: 0
    FDE Secured: 0
    FDE Locked: 0
    FDE Locked Foreign Config: 0

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

Retrieving Storage Firmware Logs for a Controller

This task retrieves the Storage Firmware Logs for the controller and places it in the `/var/log` location. This ensures that this log data is available when Technical Support Data is requested.

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 # **get-storage-fw-log**	
Step 4	Server /chassis/storageadapter # **show detail**	Displays the status of the retrieval process. **Important** Retrieving Storage Firmware Logs for a controller could take up to 2-4 minutes. Until this process is complete, do not initiate exporting technical support data.

This example shows how to retrieve Storage Firmware Logs for a MegaRAID controller in slot 3:

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter # get-storage-fw-log
Server /chassis/storageadapter # show detail
PCI Slot SLOT-3:
TTY Log Status: In progress (8192 bytes fetched)
Server /chassis/storageadapter # show detail
PCI Slot SLOT-3:
TTY Log Status: In progress (90112 bytes fetched)
Server /chassis/storageadapter # show detail
PCI Slot SLOT-3:
TTY Log Status: Complete (172032 bytes fetched)
```

Self Encrypting Drives (Full Disk Encryption)

Cisco IMC supports self encrypting drives (SED). A special hardware in the drives encrypts incoming data and decrypts outgoing data in real-time. This feature is also called Full Disk Encryption (FDE).

The data on the drive is encrypted on its way into the drive and decrypted on its way out. However, if you lock the drive, no security key is required to retrieve the data.

When a drive is locked, an encryption key is created and stored internally. All data stored on this drive is encrypted using that key, and stored in encrypted form. Once you store the data in this manner, a security key is required in order to un-encrypt and fetch the data from the drive. Unlocking a drive deletes that encryption key and renders the stored data unusable. This is called a Secure Erase. The FDE comprises a key ID and a security key.

The FDE feature supports the following operations:

- Enable and disable security on a controller
- Create a secure virtual drive
- Secure a non-secure drive group

- Unlock foreign configuration drives
- Enable security on a physical drive (JBOD)
- Clear secure SED drives
- Clear secure foreign configuration

Scenarios to consider While Configuring Controller Security in a Dual SIOC Environment

Note Dual SIOC connectivity is available only on some servers.

Controller security can be enabled, disabled, or modified independently. However, local and remote key management applies to all the controllers on the server. Therefore security action involving switching the key management modes must be performed with caution. In a scenario where both controllers are secure, and you decide to move one of the controllers to a different mode, you need to perform the same operation on the other controller as well.

Consider the following two scenarios:

- Scenario 1—Key management is set to remote; both controllers are secure and use remote key management. If you now wish to switch to local key management, switch the key management for each controller and disable remote key management.
- Scenario 2—Key management is set to local; both controllers are secure and use local key management. If you now wish to switch to remote key management, enable remote key management and switch the key management for each controller.

If you do not modify the controller security method on any one of the controllers, it renders the secure key management in an unsupported configuration state.

Enabling Drive Security on a Controller

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 # **enable-controller-security**	At this point, you are prompted to enter a security key, you can either enter a security key of your choice or you can use the suggested security key. If you choose to assign a security key of your choice, enter the security key at the prompt.

	Command or Action	Purpose
		Depending on whether you want to use the suggested security key or a security key of your choice, enter **y** (yes) to confirm, or **n** (no) to cancel the operation at the appropriate prompt.
Step 4	Server /chassis/storageadapter # **show detail**	Displays the storage drive details.

The following example shows how to enable security on a controller:

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter # enable-controller-security
Use generated key-id 'UCSC-MRAID12G_FHH18250010_1d85dcd3'?  (y or n)--> y
Use suggested security-key '6ICsmuX@oVB7e9wXt79qsTgp6ICsmuX@'?  (y or n)--> n
Enter security-key --> testSecurityKey
Will use security-key 'testSecurityKey'
Server /chassis/storageadapter show detail
PCI Slot SLOT-HBA:
    <stuff deleted>
    Controller is Secured: 1

Server /chassis/storageadapter #
```

Disabling Drive Security on a Controller

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 # **disable-controller-security**	A confirmation prompt appears. At the confirmation prompt, enter **yes** to confirm, or **n** (no) to cancel the operation. Another prompt to enter the security key appears. Enter the security key. This disables the controller security.
Step 4	Server /chassis/storageadapter # **show detail**	Displays the storage drive details.

The following example shows how to disable security on a controller:

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter #  disable-controller-security
Note: this operation will fail if any secured drives are present.
Are you sure you want to disable security on this controller?
Enter 'yes' to confirm -> yes
Please enter the controller's security-key -> testSecurityKey
savbu-stordev-dn1-2-cimc /chassis/storageadapter # show detail
PCI Slot SLOT-HBA:
    <stuff deleted>
    Controller is Secured: 0

Server /chassis/storageadapter #
```

Modifying Controller Security Settings

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 # **modify-controller-security**	At this point, you are prompted to enter the current security key, option to choose whether you want to reset the key-id and the new security key. Enter the appropriate information. At the confirmation prompt, enter **y** (yes) to confirm, or **n** (no) to cancel the operation.

The following example shows how to modify the security settings of a controller:

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter # modify-controller-security
Please enter current security-key --> testSecurityKey
Keep current key-id 'UCSC-MRAID12G_FHH18250010_1d85dcd3'? (y or n)--> n
Enter new key-id: NewKeyId
Will change key-id to 'NewKeyId'
Keep current security-key? (y or n)--> y

Server /chassis/storageadapter #
```

Verifying the Security Key Authenticity

If you are not sure about the security key, you can use this procedure to verify whether the security key that you provide matches the controller security key.

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 # **verify-controller-security-key**	At the prompt, enter the security key and press Enter. If you enter a security key that does not match the controller security key, a verification failure message appears.

The following example shows how to verify the security key of a controller:

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter #  verify-controller-security-key
Please enter the security key to verify -> WrongSecurityKey
verify-controller-security-key failed.
Error: "r-type: RAID controller: SLOT-HBA command-status: Lock key from backup failed
verification"
savbu-stordev-dn1-2-cimc /chassis/storageadapter #
savbu-stordev-dn1-2-cimc /chassis/storageadapter # verify-controller-security-key
Please enter the security key to verify -> testSecurityKey

Server /chassis/storageadapter #
```

Switching Controller Security From Remote to Local Key Management

This task allows you to switch controller security from local management to remote management, and from remote to local management.

Before You Begin

- You must log in with admin privileges to perform this task.
- KMIP must be enabled.

Procedure

	Command or Action	Purpose
Step 1	Server # **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **scope storageadapter** *Slot-ID*	Enters storage adapter command mode.

	Command or Action	Purpose
Step 3	Server /chassis/storageadapter # **switch-to-local-key-mgmt**	Enter y at the confirmation prompt. **Note** If you have multiple controller you must switch the security on those as well.
Step 4	Server /chassis/server/storageadapter # *key id*	Enter the new key ID at the prompt. Switches to local key management.

The following example shows how to switch controller security from remote to local key management:

```
Server # scope chassis
Server /chassis # scope storageadapter SLOT-HBA 1
Server /chassis/storageadapter # switch-to-local-key-mgmt
Executing this command will require you to disable remote key management once switch is
complete.
Do you want to continue(y or n)?y
Proceeding to switch to local key management.
Enter new security-key: test
Will change security-key to 'test'
Switch to local key management complete on controller in SLOT-HBA.
***Remote key management needs to be disabled***
Please disable remote key management.
Server /chassis/server/storageadapter #
```

What to Do Next

After you switch from Remote to Local Key Management, ensure that you disable KMIP secure key management.

Switching Controller Security From Local to Remote Key Management

This task allows you to switch controller security from local management to remote management, and from remote to local management.

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 chassis command mode.
Step 2	Server /chassis # **scope storageadapter** *Slot-ID*	Enters storage adapter command mode.
Step 3	Server /chassis/storageadapter # **switch-to-remote-key-mgmt**	Enter y at the confirmation prompt.
Step 4	Server /chassis/storageadapter # *security id*	Enter the security key at the prompt. Switches to remote key management.

The following example shows how to switch controller security from local to remote key management:

```
Server # scope chassis
Server /chassis # scope storageadapter SLOT-HBA 1
Server /chassis/server/storageadapter # switch-to-remote-key-mgmt
Changing the security key requires existing security key.
Please enter current security-key --> test
Switch to remote key management complete on controller in SLOT-HBA.
Server /chassis/server/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.

	Command or Action	Purpose
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 # **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 #
```

Editing 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 # **modify-attributes**	Prompts you to select a different current policy.
Step 5	Server chassis /storageadapter /virtual-drive# **set raid-level** *value*	Specifies the RAID level for the specified virtual drive.
Step 6	Server chassis /storageadapter /virtual-drive# **set physical-drive** *value*	Specifies the physical drive for the specified virtual drive.

This example shows to edit a virtual drive:

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

```
Server /chassis/storageadapter # scope virtual-drive 3
Server /chassis/storageadapter/virtual-drive #set raid-level 1
Server /chassis/storageadapter/virtual-drive *# physical-drive 1
Server /chassis/storageadapter/virtual-drive* #commit
Server /chassis/storageadapter /virtual-drive # modify-attribute
Current write policy: Write Back Good BBU

    0: Write Through
    1: Write Back Good BBU
    2: Always Write Back
  Choose number from above options--> 0
The following attribute will be modified:
  - Write Policy: Write Through

OK? (y or n)--> y
Server /chassis/storageadapter/virtual-drive #
```

Securing a Virtual Drive

Important This task secures all the VDs in an existing drive group, where virtual-drive is the target ID of a virtual drive in the 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 # **scope virtual-drive** *drive-number*	Enters command mode for the specified virtual drive.
Step 4	Server /chassis/storageadapter/virtual-drive # **secure-drive-group**	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 secure the virtual drive group.

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter # scope virtual-drive 3
Server /chassis/storageadapter/virtual-drive # secure-drive-group
This will enable security for virtual drive 16, and all virtual drives sharing this drive
group.
It is not reversible.  Are you quite certain you want to do this?
Enter 'yes' to confirm -> yes
server /chassis/storageadapter/virtual-drive # show detail
```

```
Virtual Drive 16:
    .
    .
    FDE Capable: 1
    FDE Enabled: 1
    .
    .
 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** *slot*	Enters command mode for an installed storage card.
Step 3	Server /chassis/storageadapter # **scope virtual-drive** *3*	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.

	Command or Action	Purpose
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 #
```

Toggling Physical Drive Status

Before You Begin

- You must log in with admin privileges to perform this task.
- The controller must support the JBOD mode and the JBOD mode must be enabled.

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 4**	Enters command mode for the physical drive.
Step 4	Server /chassis/storageadapter/physical-drive # **make-unconfigured-good**	Modifies the status of the drive to Unconfigured good.
Step 5	Server /chassis/storageadapter/physical-drive # **make-jbod**	Enables the JBOD mode on the physical drive.

This example shows how to toggle between the status of the physical drive:

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter # scope physical-drive 4
Server /chassis/storageadapter/physical-drive # show detail
Physical Drive Number 4:
    Controller: SLOT-4
    Health: Good
    Status: JBOD
    Boot Drive: true
    Manufacturer: ATA
    Model: ST500NM0011
    Predictive Failure Count: 0
    Drive Firmware: CC02
    Coerced Size: 476416 MB
    Type: HDD
Server /chassis/storageadapter/physical-drive # make-unconfigured-good
Server /chassis/storageadapter/physical-drive # show detail
Physical Drive Number 4:
    Controller: SLOT-4
    Health: Good
    Status: Unconfigured Good
    Boot Drive: true
    Manufacturer: ATA
    Model: ST500NM0011
    Predictive Failure Count: 0
    Drive Firmware: CC02
    Coerced Size: 476416 MB
    Type: HDD
Server /chassis/storageadapter/physical-drive # make-jbod
Server /chassis/storageadapter/physical-drive # show detail
Physical Drive Number 4:
```

```
    Controller: SLOT-4
    Health: Good
    Status: JBOD
    Boot Drive: true
    Manufacturer: ATA
    Model: ST500NM0011
    Predictive Failure Count: 0
    Drive Firmware: CC02
    Coerced Size: 476416 MB
    Type: HDD
```

Setting a Physical Drive as a Controller Boot Drive

Before You Begin

- You must log in with admin privileges to perform this task.
- The controller must support the JBOD mode and the JBOD mode must be enabled.

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 4**	Enters command mode for the physical drive.
Step 4	Server /chassis/storageadapter/physical-drive # **set-boot-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 set a physical drive as a boot drive for a controller:

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter # show detail
PCI Slot SLOT-4:
    Health: Good
    Controller Status: Optimal
    ROC Temperature: Not Supported
    Product Name: MegaRAID 9240-8i (RAID 0,1,10,5)
    Serial Number: SP23807413
    Firmware Package Build: 20.11.1-0159
    Product ID: LSI Logic
    Battery Status: no battery
    Cache Memory Size: 0 MB
    Boot Drive: none
    Boot Drive is PD: false
    TTY Log Status: Not Downloaded
Server /chassis/storageadapter # scope physical-drive 4
Server /chassis/storageadapter/physical-drive # set-boot-drive
Are you sure you want to set physical drive 4 as the boot drive?
Enter 'yes' to confirm -> yes
```

```
Server /chassis/storageadapter/physical-drive # exit
Server /chassis/storageadapter # show detail
PCI Slot SLOT-4:
    Health: Good
    Controller Status: Optimal
    ROC Temperature: Not Supported
    Product Name: MegaRAID 9240-8i (RAID 0,1,10,5)
    Serial Number: SP23807413
    Firmware Package Build: 20.11.1-0159
    Product ID: LSI Logic
    Battery Status: no battery
    Cache Memory Size: 0 MB
    Boot Drive: 4
    Boot Drive is PD: true
    TTY Log Status: Not Downloaded
```

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.
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 #
```

Clear Controller Configuration

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 chassis command mode.

	Command or Action	Purpose
Step 2	Server /chassis # **scope storageadapter** *Slot-ID*	Enters storage adapter command mode.
Step 3	Server /chassis/storageadapter # **clear-all-config**	Enter yes at the confirmation prompt. Clears the controller configuration.

The following example shows how to clear the controller configuration:

```
Server # scope chassis
Server /chassis # scope storageadapter SLOT-HBA 1
Server /chassis/storageadapter # clear-all-config
Are you sure you want to clear the controller's config and delete all VDs?
Enter 'yes' to confirm -> yes
Enter administrative password to proceed with operation\n
Password -> Password accepted. Performing requested operation.
Server /chassis/storageadapter #
```

Restoring Storage Controller to Factory 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 chassis command mode.
Step 2	Server /chassis # **scope storageadapter** *Slot-ID*	Enters storage adapter command mode.
Step 3	Server /chassis/storageadapter # **set-factory-defaults**	Enter yes at the confirmation prompt. Restores the controller configuration parameters to factory defaults.

The following example shows how to restore the controller configuration parameters to factory defaults:

```
Server # scope chassis
Server /chassis # scope storageadapter SLOT-HBA 1
Server /chassis/storageadapter # set-factory-defaults
This operation will restore controller settings to factory default values. Do you want to
proceed?
Enter 'yes' to confirm -> yes
Server /chassis/storageadapter #
```

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 #
```

Viewing Physical Drive Details

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 2**	Enters the physical drive command mode.
Step 4	Server /chassis/storageadapter/physicsl-drive # **show detail**	Displays the physical drive details.

This example shows how to view the physical drive information:

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter # scope physical-drive 202
Server /chassis/storageadapter/physical-drive # show detail
Physical Drive Number 202:
    Controller: SLOT-HBA
    Info Valid: Yes
    Info Invalid Cause:
    Enclosure Device ID: 252
    Device ID: 8
    Drive Number: 202
    Health: Good
    Status: Online
    Boot Drive: false
    Manufacturer: ATA
    Model: INTEL SSDSC2BB480G4
    Predictive Failure Count: 0
    Drive Firmware: 0370
    Type: SSD
    Block Size: 512
    Physical Block Size: 4096
    Negotiated Link Speed: 6.0 Gb/s
    Locator LED: false
    FDE Capable: 0
    FDE Enabled: 0
    FDE Secured: 0
    FDE Locked: 0
    FDE Locked Foreign Config: 0
    Enclosure Association: Direct Attached
    Enclosure Logical ID: N/A
    Enclosure SAS Address[0]: N/A
    Enclosure SAS Address[1]: N/A
    Power Cycle Count: 106
    Power On Hours: 10471
    Percentage Life Left: 100
    Wear Status in Days: 1825
    Percentage Reserved Capacity Consumed: 0
    Time of Last Refresh : 2017-03-04 13:47
    Operating Temperature: 34
    Media Error Count: 0
    Other Error Count: 0
    Interface Type: SATA
    Block Count: 937703088
    Raw Size: 457862 MB
    Non Coerced Size: 457350 MB
    Coerced Size: 456809 MB
    SAS Address 0: 4433221108000000
    SAS Address 1: 0x0
    Power State: active
```

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 Cisco IMC 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 Cisco IMC 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:

Note

- If you want to upgrade from version 1.4(5e) to 1.5(4) or higher versions, you must first upgrade to version1.5(2) and then upgrade to a higher version of Cisco IMC.
- Reset the Cisco Flexible Flash controller to load the latest Flex Flash firmware after every Cisco IMC firmware upgrade.

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.

Scenario	Behavior
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 card to the server, and then upgrade its firmware to the latest version.
- 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 Cisco IMC GUI or from the Cisco IMC CLI. To mark the state of the card as primary healthy, you can either use the **Reset Configuration** option in the Cisco IMC GUI or run the **reset-config** command in the Cisco IMC 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 accidently 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 Cisco IMC 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 Cisco IMC 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 for C220 M4 and C240 M4 Servers

Note

- In the **Mirror** mode, **Slot1 Read/Write Error Threshold** is applicable to both the SD cards, if two cards are present.
- In the **Util** Mode, **Slot1 Read/Write Error Threshold** is applicable to the card in slot 1 and **Slot2 Read/Write Error Threshold** is applicable to the card in slot 2.

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**	Enters the Cisco Flexible Flash controller command mode for the specified controller.
Step 3	Server /chassis/flexflash # **scope operational-profile**	Enters the operational profile command mode.
Step 4	Server /chassis/flexflash/operational-profile # **set read-error-count-slot1-threshold** *threshold*	Specifies the number of read errors that are permitted while accessing the Cisco Flexible Flash card in slot 1. If the number of errors exceeds this threshold, the Cisco Flexible Flash card is disabled and you must reset it manually before Cisco IMC 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 5	Server /chassis/flexflash/operational-profile	Specifies the number of read errors that are permitted while accessing the Cisco Flexible Flash card in slot 2. If the number

	Command or Action	Purpose
	# **set read-error-count-slot2-threshold** *threshold*	of errors exceeds this threshold, the Cisco Flexible Flash card is disabled and you must reset it manually before Cisco IMC 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 6	Server /chassis/flexflash/operational-profile # **set write-error-count-slot2-threshold** *threshold*	Specifies the number of write errors that are permitted while accessing the Cisco Flexible Flash card in slot 2. If the number of errors exceeds this threshold, the Cisco Flexible Flash card is disabled and you must reset it manually before Cisco IMC 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).
Step 7	Server /chassis/flexflash/operational-profile # **commit**	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-err-count-slot1-threshold 9
Server /chassis/flexflash/operational-profile *# set read-err-count-slot2-threshold 10
Server /chassis/flexflash/operational-profile *# set write-err-count-slot1-threshold 11
Server /chassis/flexflash/operational-profile *# set write-err-count-slot2-threshold 12
Server /chassis/flexflash/operational-profile *# commit
Server /chassis/flexflash/operational-profile # show detail
FlexFlash Operational Profile:
    Firmware Operating Mode: util
    SLOT1 Read Error Threshold: 9
    SLOT1 Write Error Threshold: 11
    SLOT2 Read Error Threshold: 10
    SLOT2 Write Error Threshold: 12
```

Configuring the Flexible Flash Controller Properties for C220 M3, C240 M3, and C460 M4 Servers

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 *index* 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 Cisco IMC 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 Cisco IMC 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).
Step 8	Server /chassis/flexflash/operational-profile # **set virtual-drives-enabled** *list*	Specifies a list of virtual drives to be made available to the server as a USB-style drive. The options are as follows: • **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.

	Command or Action	Purpose
		• **HUU**—The server can access the Cisco Host Upgrade Utility. When specifying more than one option, you must enclose the list in quotation marks (").
Step 9	Server /chassis/adapter # **commit**	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 verison of Cisco IMC 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** | **HV**}	The virtual drive from which the server attempts to boot the next time it is restarted. This can be one of the following: • **None**—The server uses the default boot order

	Command or Action	Purpose
		• **HV—**The server boots from the hypervisor virtual drive
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 HV
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** *index*	Enters the Cisco Flexible Flash controller command mode for the specified controller. At this time, the only permissible *index* 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 #
```

Configuring the Flexible Flash Controller Cards in Mirror Mode

Configuring controller cards in mirror mode:

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**	Enters the Cisco Flexible Flash controller command mode for the specified controller.
Step 3	Server /chassis/flexflash # **configure-cards-mirror SLOT-1**.	Configures SLOT-1 as healthy primary.
Step 4	Enter **y** at the **Enable auto sync(by default auto sync is disabled)?[y|N]** prompt.	Sync the card on slot 1 with the card on slot 2.
Step 5	Enter **y** at the **Set Mirror Partition Name(Default name is Hypervisor)?[y|N]** prompt.	Enables you to set the name of the mirror partition.
Step 6	Enter the name of the mirror partition at the **Enter Partition Name Mirror Partition Name :***Hypervisor* prompt.	Sets the name of the mirror partition.
Step 7	Enter **y** at the **Set Virtual Drive as non-removable (Default is removable)?[y|N]** prompt.	Enables you to set the VD as non-removable. The following message displays: This action will mark the SLOT-1 as healthy primary slot and SLOT-2 (if card existing) as unhealthy secondary. This operation may disturb the host connectivity as well.
Step 8	Enter **y** at the **Continue?[y|N]y** prompt.	Configures the cards in Mirror mode and sets the card in SLOT-1 as primary healthy and SLOT-2 (if card existing) as unhealthy secondary.

	Command or Action	Purpose
Step 9	Server /chassis/flexflash # **show physical-drive**	(Optional) Displays the status of the configured cards. **Note** • When the cards are configured in auto sync mode and if the cards go out of sync then syncing from a good card with the bad card will start automatically. • If the cards are configured in auto sync mode and if a card goes out of sync, then syncing from a good card starts automatically. • If the server is running with one auto mirror healthy card and if a new card is inserted then the metadata is automatically created on the new card and data syncing starts from auto mirror configured card to the new paired card.

This example shows how to configure the controller cards in mirror mode:

```
Server# scope chassis
Server /chassis # scope flexflash
Server /chassis/flexflash #  configure-cards-mirror SLOT-1
Enable auto sync(by default auto sync is disabled)?[y|N]y
Set Mirror Partition Name(Default name is Hypervisor)?[y|N]y
Enter Partition Name Mirror Partition Name :HV
Set Virtual Drive as non-removable (Default is removable)?[y|N]y
This action will mark the SLOT-1 as healthy primary slot and SLOT-2 (if card existing) as
unhealthy secondary.
This operation may disturb the host connectivity as well.
Continue?[y|N]y
Server /chassis/flexflash # show detail
Controller FlexFlash-0:
    Product Name: Cisco FlexFlash
    Controller HW: FX3S
    Vendor: Cypress
    Firmware Version: 1.3.2 build 159
    Firmware Operating Mode: mirror
    Firmware Configured Mode: mirror
    Has Error: No
    Error Description:
    Internal State: Disconnected
    Controller Status: OK
    Cards Manageable: Yes
    Startup Firmware Version: 1.3.2 build 159

Server /chassis/flexflash # show physical-drive
Physical Drive  Status    Controller   Card Type         Card mode         Health     Sync
 Mode
--------------- --------- ------------ ----------------- ----------------- ----------
----------
SLOT-1          present   FlexFlash-0  FX3S configured   mirror-primary    healthy    auto
SLOT-2          present   FlexFlash-0  FX3S configured   mirror-secondary  unhealthy  auto

Server /chassis/flexflash #
```

Configuring Controller Cards in Util Mode

Procedure

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters the chassis command mode.
Step 2	Server /chassis # **scope flexflash**	Enters the Cisco Flexible Flash controller command mode for the specified controller.
Step 3	Server /chassis/flexflash # **configure-cards-util SLOT-1**	Configures card in slot-1 as Util card with four partitions - scu, huu, drivers, and user partition).
Step 4	Enter **y** at the **Set User Partition Name on Util Card (Default name is UserPartition)?[y|N]** prompt.	Enables you to set the name of the user partition.
Step 5	Enter the name of the user partition at the **Enter User Partiton Name:***UserPartition* prompt.	Sets the name of the user partition.
Step 6	Enter **y** at the **Set Partition Name on Non Util Card(Default name is Hypervisor)?[y|N]** prompt.	Enables you to set the name of the single partition on non-Util card.
Step 7	Enter the name of the mirror partition at the **Enter Partition Name of Non Util Card:***Hypervisor* prompt.	Sets the name of the non-Util partition. The following message displays: This action will create util configuration (4 partition) on SLOT-1 card and non-util configuration(1 partition) on SLOT-2 (if card existing). This operation may disturb the host connectivity as well.
Step 8	Enter **y** at the **Continue?[y|N]y** prompt.	Configures the cards in the Util mode; creates four partitions of the card on SLOT-1 and sets it as primary healthy, and SLOT-2 (if card existing) as healthy secondary.
Step 9	Server /chassis/flexflash # **show physical-drive**	(Optional) Displays the status of the configured cards. **Note** On a Util card with four partitions, an extra partition is created and used during OOB update of SCU, HUU, and drivers.

This example shows how to configure the controller cards in Util mode:

```
Server# scope chassis
Server /chassis # scope flexflash
Server /chassis/flexflash #  configure-cards-mirror SLOT-1
Set User Partiton Name on Util Card (Default name is UserPartition)?[y|N]y
Enter User Partiton Name :UserPartition
Set Partition Name on Non Util Card(Default name is Hypervisor)?[y|N]y
```

```
Enter Partition Name of Non Util Card :Hypervisor
This action will create util configuration (4 partitons) on SLOT-1 card and
non-util configuration(1 partition) on SLOT-2 (if card existing)
This operation may disturb the host connectivity as well.
Continue?[y|N]y

Server /chassis/flexflash # show detail
Controller FlexFlash-0:
    Product Name: Cisco FlexFlash
    Controller HW: FX3S
    Vendor: Cypress
    Firmware Version: 1.3.2 build 159
    Firmware Operating Mode: util
    Firmware Configured Mode: util
    Has Error: No
    Error Description:
    Internal State: Disconnected
    Controller Status: OK
    Cards Manageable: Yes
    Startup Firmware Version: 1.3.2 build 159

Server /chassis/flexflash # show physical-drive
Physical Drive  Status    Controller   Card Type         Card mode         Health     Sync
 Mode
--------------- --------- ------------ ----------------- ----------------- ----------
----------
SLOT-1          present   FlexFlash-0  FX3S configured   util              healthy    NA
SLOT-2          present   FlexFlash-0  FX3S configured   util              healthy    NA

Server /chassis/flexflash #
```

Configuring the Flexible Flash Controller Firmware Mode

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**	Enters the Cisco Flexible Flash controller command mode for the specified controller.
Step 3	Server /chassis/flexflash # **configure-firmware-mode** .	Switches the firmware mode from the current state to the other. The following messages appear: This action will switch firmware mode from util to mirror This operation may disturb the host connectivity as well.
Step 4	Enter **y** at the **Continue?[y|N]y** prompt.	Switches the firmware mode from mirror to Util or Util to mirror.

This example shows how to configure the firmware mode of a controller:

```
Server# scope chassis
Server /chassis # scope flexflash
Server /chassis/flexflash #  configure-firmware-mode
This action will switch fimrware mode from util to mirror
This operation may disturb the host connectivity as well.
Continue?[y|N]y
Server /chassis/flexflash # show detail
Controller FlexFlash-0:
    Product Name: Cisco FlexFlash
    Controller HW: FX3S
    Vendor: Cypress
    Firmware Version: 1.3.2 build 159
    Firmware Operating Mode: mirror
    Firmware Configured Mode: mirror
    Has Error: Yes
    Error Description:
    Internal State: Failed
    Controller Status: Mode Mismatch SDcard(s)
    Cards Manageable: NO
    Startup Firmware Version: 1.3.2 build 159

*+----------------------------------------------------------------------------+
+ Based on type and number of cards please execute mirror/util Configuration +
+ (configure-mirror/configure-util) commands to start monitoring/managing SD cards +
+                              OR                                             +
+                      Switch Firmware Operating Mode                         +
+----------------------------------------------------------------------------+

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 *index* 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 *index* value is **FlexFlash-0**.
Step 3	Server /chassis/flexflash # **synchronize-card-configuration***primary slot ID*	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 #
```

Adding an ISO Image Configuration

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters the chassis command mode.
Step 2	Server/chassis # **scope flexflash**	Enters the Cisco Flexible Flash controller command mode for the specified controller.
Step 3	Server/chassis/flexflash/ # **scope vd-image-configs**	Enters the virtual drive configuration command mode.
Step 4	Server/chassis/flexflash/vd-image-configs # **vd-image-cifs** *virtual_drive //serverip/remote_share <remote_file>*	`Server username`: prompt is displayed. **1** Server username: *server username* Enter a server username. **2** Server password: *server password* Enter a server password.

	Command or Action	Purpose
		3 Confirm password: *server password* Repeat the server password.
Step 5	Server/chassis/flexflash/vd-image-configs # **vd-image-nfs** *virtual_drive serverip:/remote_share <remote_file>*	`Server username:` prompt is displayed.
Step 6	Server/chassis/flexflash/vd-image-configs # **show detail**	(Optional) Displays the details of the virtual drives.

```
Server # scope chassis
Server/chassis # scope flexflash
Server/chassis/flexflash # scope vd-image-configs
Server/chassis/flexflash/vd-image-configs # vd-image-cifs SCU //10.106.146.69/pdagguma
/softwares/ucs-cxx-scu-3.1.9.iso
Server/chassis/flexflash/vd-image-configs # show detail
Vritual Drive SCU:
    Mount Type: cifs
    Remote Share: //10.106.146.69/pdagguma
    Remote File: /softwares/ucs-cxx-scu-3.1.9.iso
    Mount Options:
"username=pdagguma,password*********,soft,nounix,noserverino,rsize=3072,wsize=3072"
Vritual Drive HUU:
    Mount Type: cifs
    Remote Share: //10.101
    Remote File: DFLJD_huu.iso
    Mount Options:
"username=pdagguma,password*********,soft,nounix,noserverino,rsize=3072,wsize=3072"
Vritual Drive Drivers:
    Mount Type: None
    Remote Share: None
    Remote File: None
    Mount Options: None
Server/chassis/flexflash/vd-image-configs #
```

Enabling Virtual Drives

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**	Enters the Cisco Flexible Flash controller command mode for the specified controller.

	Command or Action	Purpose
Step 3	Server /chassis/ flexflash # **scope virtual-drive**	Enters the virtual drive command mode for the specified controller.
Step 4	Server /chassis/flexflash/virtual-drive # **enable-vds** *"SCU HUU dlfd"*	Enables the virtual drives to the host.

This example shows how to enable the virtual drives to the host:

```
Server# scope chassis
Server /chassis # scope flexflash
Server /chassis/flexflash #  scope virtual-drive
Server /chassis/flexflash/virtual-drive # enable-vds "SCU HUU dlfd"
Server /chassis/flexflash/virtual-drive # show detail

Virtual Drive SCU:
    VD ID: 1
    Size: 2560 MB
    VD Scope: Non-Raid
    VD Status: Healthy
    VD Type: Removable
    Read/Write: R/W
    Host Accessible: Connected
    Operation in progress: NA
    Last Operation completion status: none
Virtual Drive HUU:
    VD ID: 2
    Size: 1536 MB
    VD Scope: Non-Raid
    VD Status: Healthy
    VD Type: Removable
    Read/Write: R/W
    Host Accessible: Connected
    Operation in progress: NA
    Last Operation completion status: none
Virtual Drive Drivers:
    VD ID: 3
    Size: 8192 MB
    VD Scope: Non-Raid
    VD Status: Healthy
    VD Type: Removable
    Read/Write: R/W
    Host Accessible: Not-Connected
    Operation in progress: NA
    Last Operation completion status: none
Virtual Drive dlfd:
    VD ID: 4
    Size: 9952 MB
    VD Scope: Non-Raid
    VD Status: Healthy
    VD Type: Removable
    Read/Write: R/W
    Host Accessible: Connected
    Operation in progress: NA
    Last Operation completion status: none
Virtual Drive dfdff:
    VD ID: 5
    Size: 30432 MB
    VD Scope: Non-Raid
    VD Status: Healthy
    VD Type: Removable
    Read/Write: R/W
    Host Accessible: Not-Connected
    Operation in progress: NA
    Last Operation completion status: none
```

```
Server /chassis/flexflash/virtual-drive #
```

Erasing Virtual Drives

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**	Enters the Cisco Flexible Flash controller command mode for the specified controller.
Step 3	Server /chassis/ flexflash # **scope virtual-drive**	Enters the virtual drive command mode for the specified controller.
Step 4	Server /chassis/flexflash/virtual-drive # **erase-vds "SCU HUU"**	Initiates erasing FAT32.

This example shows how to erase data on the virtual drives:

```
Server# scope chassis
Server /chassis # scope flexflash
Server /chassis/flexflash #  scope virtual-drive
Server /chassis/flexflash/virtual-drive #  erase-vds "SCU HUU"
Server /chassis/flexflash/virtual-drive # show detail

Virtual Drive SCU:
    VD ID: 1
    Size: 2560 MB
    VD Scope: Non-Raid
    VD Status: Healthy
    VD Type: Removable
    Read/Write: R/W
    Host Accessible: Not-Connected
    Operation in progress: Erasing
    Last Operation completion status: none
Virtual Drive HUU:
    VD ID: 2
    Size: 1536 MB
    VD Scope: Non-Raid
    VD Status: Healthy
    VD Type: Removable
    Read/Write: R/W
    Host Accessible: Connected
    Operation in progress: Erase-Pending
    Last Operation completion status: none
Virtual Drive Drivers:
    VD ID: 3
    Size: 8192 MB
    VD Scope: Non-Raid
    VD Status: Healthy
    VD Type: Removable
```

```
    Read/Write: R/W
    Host Accessible: Not-Connected
    Operation in progress: NA
    Last Operation completion status: none
Virtual Drive dlfd:

Server /chassis/flexflash/virtual-drive #
```

Syncing Virtual Drives

Before You Begin

- You must log in with admin privileges to perform this task.
- Cisco Flexible Flash must be supported by your platform.
- The cards must be configured in manual mirror mode.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters the chassis command mode.
Step 2	Server /chassis # **scope flexflash**	Enters the Cisco Flexible Flash controller command mode for the specified controller.
Step 3	Server /chassis/ flexflash # **scope virtual-drive**	Enters the virtual drive command mode for the specified controller.
Step 4	Server /chassis/flexflash/virtual-drive # **sync-vds** *Hypervisor*	Syncs the virtual drives. **Note** • If the cards are configured in auto sync mode and if a card goes out of sync, then syncing from a good card starts automatically. • If the server is running with one auto mirror healthy card and if a new card is inserted then the metadata is automatically created on the new card and data syncing starts from auto mirror configured card to the new paired card.

This example shows how to sync the virtual drives:

```
Server# scope chassis
Server /chassis # scope flexflash
Server /chassis/flexflash #  scope virtual-drive
Server /chassis/flexflash/virtual-drive # sync-vds Hypervisor
Server /chassis/flexflash/virtual-drive # show detail

Virtual Drive Hypervisor:
    VD ID: 1
    Size: 30432 MB
    VD Scope: Raid
    VD Status: Degraded
    VD Type: Removable
    Read/Write: R/W
```

```
    Host Accessible: Not-Connected
    Operation in progress: Syncing(Manual)10% done
    Last Operation completion status: none

Server /chassis/flexflash/virtual-drive #
```

CHAPTER 11

Configuring Communication Services

This chapter includes the following sections:

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 Cisco IMC.
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.

	Command or Action	Purpose
Step 5	Server /http # **set http-redirect** {**yes** | **no**}	Enables or disables the redirection of an HTTP request to HTTPS.
Step 6	Server /http # **set timeout** *seconds*	Sets the number of seconds to wait between HTTP requests before the Cisco IMC 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 Cisco IMC:

```
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 Cisco IMC.
Step 3	Server /ssh # **set ssh-port** *number*	Sets the port to use for secure shell access. The default is 22.
Step 4	Server /ssh # **set timeout** *seconds*	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.

	Command or Action	Purpose
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 Cisco IMC:

```
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 Cisco IMC

The Cisco Cisco IMC XML application programming interface (API) is a programmatic interface to Cisco IMC 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 Cisco IMC 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 Cisco IMC.
Step 3	Server /xmlapi # **commit**	Commits the transaction to the system configuration.

This example enables XML API control of Cisco IMC 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 #
```

Enabling Redfish

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 redfish**	Enters redfish command mode.
Step 2	Server /redfish # **set enabled** {**yes** | **no**}	Enables or disables redfish control of Cisco IMC.
Step 3	Server /redfish* # **commit**	Commits the transaction to the system configuration.

This example enables redfish control of Cisco IMC and commits the transaction:

```
Server# scope redfish
Server /redfish # set enabled yes
Server /redfish *# commit
Server /redfish #  show detail
REDFISH Settings:
    Enabled: yes
    Active Sessions: 0
    Max Sessions: 4

Server /redfish #
```

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 Cisco IMC 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: • **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.
Step 4	Server /ipmi # **set encryption-key** *key*	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.
Step 6	Server /ipmi # **randomise-key**	Sets the IPMI encryption key to a random value. **Note** You can perform the Step 6 action instead of Steps 4 and 5.
Step 7	At the prompt, enter y to randomize the encryption key.	Sets the IPMI encryption key to a random value.

This example configures IPMI over LAN for the Cisco IMC:

```
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 # randomise-key
This operation will change the IPMI Encryption Key to a random value
Continue?[y|N]y
Setting IPMI Encryption Key to a random value...

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 Cisco IMC, see the *MIB Quick Reference for Cisco UCS* at this URL: http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/mib/b-series/b_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.
Step 4	Server /snmp # **set enable-serial-num** {**yes** | **no**}	Prefixes the traps with the serial number of the server.

	Command or Action	Purpose
Step 5	Server /snmp # **set snmp-port** *port number*	Sets the port number on which the SNMP agent runs. You can choose a number within the range 1 to 65535. The default port number is 161. **Note** The port numbers that are reserved for system calls, such as 22,23,80,123,443,623,389,636,3268,3269 and 2068, cannot be used as an SNMP port.
Step 6	Server /snmp # **set community-str** *community*	Specifies the default SNMP v1 or v2c community name that Cisco IMC includes on any trap messages it sends to the SNMP host. The name can be up to 18 characters.
Step 7	Server /snmp # **set community-access**	This can be one of the following : Disabled, Limited, or Full.
Step 8	Server /snmp # **set trap-community-str**	Specifies the SNMP community group to which trap information should be sent. The name can be up to 18 characters
Step 9	Server /snmp # **set sys-contact** *contact*	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 10	Server /snmp # **set sys-location** *location*	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 11	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 enable-serial-num yes
Server /snmp *# set snmp-port 20000
Server /snmp *# set community-str cimcpublic
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: 20000
    System Contact: User Name <username@example.com> +1-408-555-1212
    System Location: San Jose, California
    SNMP Community: cimcpublic
    SNMP Trap Community: public
    SNMP Community access: Full
    Enabled: yes
    Serial Number Enabled: yes

Server /snmp #
```

What to Do Next

Configure SNMP trap settings as described in Configuring SNMP Trap Settings, on page 238.

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** *number*	Enters the SNMP trap destination command mode for the specified destination. Four SNMP trap destinations are available. The destination *number* 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** { | **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** *user*	
Step 7	Server /snmp/trap-destination # **set trap-addr** *trap destination address*	Specifies the trap destination address to which the trap information is sent. You can set an IPv4 or IPv6 address or a domain name as the trap destination. **Note** When IPv6 is enabled, the SNMP Trap destination source address can either be the SLAAC IPv6 address (if available) or a user assigned IPv6 address. Both these are valid SNMP IPv6 destination addresses that uniquely identify the server.
Step 8	Server /snmp/trap-destinations # **set trap-port** *trap destination port*	Sets the port number the server uses to communicate with the trap destination. You can choose a number within the range 1 to 65535.

	Command or Action	Purpose
Step 9	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 trap-addr www.cisco.com
Server /snmp/trap-destination *# set trap-port 10000
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
    Trap Address: www.cisco.com
    Trap Port: 10000
    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 # **send-test-trap**	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 #  send-test-trap
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** *number*	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: • **yes—**This user is enabled as an SNMPv3 user and is allowed to access the SNMP OID tree. **Note** The security name and security level must also be configured at this time or the user addition will fail. • **no—**This user configuration is deleted.
Step 4	Server /snmp/v3users # **set v3security-name** *security-name*	Enter an SNMP username for this user.
Step 5	Server /snmp/v3users # **set v3security-level** {**noauthnopriv** | **authnopriv** | **authpriv**}	Select a security level for this user. This can be one of the following: • **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** *auth-key*	Enter an authorization password for this user.

	Command or Action	Purpose
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** *priv-auth-key*	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:ex4mp1ek3y
Please confirm v3auth-key:ex4mp1ek3y
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 #
```

Configuring a Server to Send Email Alerts Using SMTP

The Cisco IMC supports email-based notification of server faults to recipients without relying on the SNMP. The system uses the Simple Mail Transfer Protocol (SMTP) to send server faults as email alerts to the configured SMTP server.

A maximum of four recipients is supported.

Configuring SMTP Servers for Receiving E-Mail Alerts

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 smtp**	Enters the SMTP command mode.
Step 2	Server /smtp # **set enabled** {**yes** | **no**}	Enables or disables the SMTP feature.
Step 3	Server /smtp * # **set server-addr** *IP_Address*	Assigns the SMTP server IP address.
Step 4	Server /smtp * # **set fault-severity** {**critical** | **major** | **minor** | **warning** | **condition**}	Assigns the fault severity to the mail alerts.
Step 5	Server /smtp * # **set port** *port_number*	Sets the port number for the SMTP server.
Step 6	Server /smtp * # **commit**	Commits the transaction to the system configuration.
Step 7	Server /smtp # **set-mail-addr** {**recipient1** | **recipient2** | **recipient3** | **recipient4**} *email_address*	Sends a test mail alert to the email address assigned to the chosen recipient.
Step 8	Server /smtp # **send-test-mail recipient1**	Sends a test mail alert to the email address assigned to the chosen recipient.

This example shows how to configure SMTP for receiving mail alerts:

```
Server # scope smtp
Server /smtp # set enabled yes
Server /smtp *# set server-addr 10.10.10.10
Server /smtp *# set fault-severity major
Server /smtp *# set port 25
There is no change in the configured port number.
Please verify if you wish to choose a different one before commit.
Server /smtp *# commit
Server /smtp # set-mail-addr recipient1 test@cisco.com
Server /smtp # show detail
SMTP Setting:
    Enabled: yes
    Port Number: 25
    Server Address: 10.104.10.10
    Minimum Severity to Report: critical
    Recipient1:
        Name     : seduggir@fpmr2.com
        Reachable: na
    Recipient2:
        Name     :
        Reachable: na
    Recipient3:
        Name     :
        Reachable: na
    Recipient4:
        Name     :
        Reachable: na

Server /smtp # send-test-mail recipient1
Test mail sent Successful.
Server /smtp # show detail
SMTP Setting:
    Enabled: yes
```

```
    Port Number: 25
    Server Address: 10.10.10.10
    Minimum Severity to Report: critical
    Recipient1:
        Name     : test@cisco.com
        Reachable: yes
    Recipient2:
        Name     :
        Reachable: na
    Recipient3:
        Name     :
        Reachable: na
    Recipient4:
        Name     :
        Reachable: na

Server /smtp #
```

CHAPTER 12

Managing Certificates and Server Security

This chapter includes the following sections:

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 Cisco IMC 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. The generated certificate key length is 2048 bits.

Note Before performing any of the following tasks in this chapter, ensure that the Cisco IMC time is set to the current time.

Procedure

Step 1 Generate the CSR from the Cisco IMC.

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 Cisco IMC.

Note The uploaded certificate must be created from a CSR generated by the Cisco IMC. 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 the **Configuring Common Properties** section.

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.
- Ensure that the Cisco IMC time is set to the current time.

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:

Name	Description
Common Name field	The fully qualified name of the Cisco IMC. By default the CN of the servers appears in CXXX-YYYYYY format, where XXX is the model number and YYYYYY is the serial number of the server. When you upgrade to latest version, CN is retained as is.
Organization Name field	The organization requesting the certificate.
Organization Unit field	The organizational unit.
Locality field	The city or town in which the company requesting the certificate is headquartered.
State Name field	The state or province in which the company requesting the certificate is headquartered.
Country Code drop-down list	The country in which the company resides.
Email field	The 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/zCCAWgCAQAwgZkxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJDQTEVMBMGA1UE
BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
ZgAMivyCsKgb/6CjQtsofvzxmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKONDl
GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
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 Cisco IMC 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.
- Ensure that the certificate is of type **Server**.

If you did not use the first option, in which Cisco IMC internally generates and uploads a self-signed certificate, you must upload the new certificate using the **upload** command in certificate command mode.

Creating an Untrusted CA-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 Cisco IMC.

Before You Begin

- Obtain and install a certificate server software package on a server within your organization.
- Ensure that the Cisco IMC time is set to the current time.

Procedure

	Command or Action	Purpose
Step 1	**openssl genrsa -out** *CA_keyfilename keysize* **Example:** `# openssl genrsa -out ca.key 2048`	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** *numdays* **-key** *CA_keyfilename* **-out** *CA_certfilename* **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** *numdays* **-in** *CSR_filename* **-CA** *CA_certfilename* **-set_serial 04 -CAkey** *CA_keyfilename* **-out** *server_certfilename* **-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.

	Command or Action	Purpose
	Example: `# openssl x509 -req -days 365 -in csr.txt -CA ca.crt -set_serial 04 -CAkey ca.key -out myserver05.crt -extfile openssl.conf`	
Step 5	**openssl x509 -noout -text -purpose -in <cert file>** **Example:** `openssl x509 -noout -text -purpose -in <cert file>`	Verifies if the generated certificate is of type **Server**. **Note** If the values of the fields **Server SSL** and **Netscape SSL** server are not yes, ensure that openssl.conf is configured to generate certificates of type server.
Step 6	If the generated certificate does not have the correct validity dates, ensure the Cisco IMC time is set to the current time, and regenerate the certificate by repeating steps 1 through 5.	(Optional) Certificate with the correct validity dates is created.

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 2048
Generating RSA private key, 2048 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 Cisco IMC.

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.
- Ensure that the generated certificate is of type **Server**.

Note You must first generate a CSR using the Cisco IMC 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/zCCAWgCAQAwgZkxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJDQTEVMBMGA1UE
BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
ZgAMivyCsKgb/6CjQtsofvzxmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKONDl
GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
mK3Ku+YiORnv6DhxrOoqau8r/hyI/L43l7IPN1HhOi3oha4=
-----END CERTIFICATE-----
```

```
<CTRL+D>
```

Key Management Interoperability Protocol

Key Management Interoperability Protocol (KMIP) is a communication protocol that defines message formats to handle keys or classified data on a key management server. KMIP is an open standard and is supported by several vendors. Key management involves multiple interoperable implementations, so a KMIP client works effectively with any KMIP server.

Note The KMIP feature is supported only on the C220 M4, C240 M4 and S3260 M4 servers.

Self-Encrypting Drives(SEDs) contain hardware that encrypts incoming data and decrypts outgoing data in realtime. A drive or media encryption key controls this function. However, the drives need to be locked in order to maintain security. A security key identifier and a security key (key encryption key) help achieve this goal. The key identifier provides a unique ID to the drive.

Different keys have different usage requirements. Currently, the responsibility of managing and tracking local keys lies primarily with the user, which could result in human error. The user needs to remember the different keys and their functions, which could prove to be a challenge. KMIP addresses this area of concern to manage the keys effectively without human involvement.

Enabling or Disabling KMIP

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 kmip**	Enters the KMIP command mode.
Step 2	Server/kmip# **set enabled** {**yes** | **no**}	Enables or disables KMIP.
Step 3	Server/kmip*# **commit**	Commits the transaction to the system configuration.
Step 4	Server/kmip # **show detail**	(Optional) Displays the KMIP status.

This example enables KMIP:

```
Server # scope kmip
Server /kmip # set enabled yes
Server /kmip *# commit
Server /kmip # show detail
  Enabled: yes
Server /kmip #
```

Creating a Client Private Key and Client Certificate for KMIP Configuration

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 Cisco IMC.

Before You Begin

- Obtain and install a certificate server software package on a server within your organization.
- Ensure that the Cisco IMC time is set to the current time.

Procedure

	Command or Action	Purpose
Step 1	**openssl genrsa -out** *Client_Privatekeyfilename keysize* **Example:** `# openssl genrsa –out client_private.pem 2048`	This command generates a client private key that will be used to generate the client certificate. The specified file name contains an RSA key of the specified key size.
Step 2	**openssl req -new -x509 -days** *numdays* **-key** *Client_Privatekeyfilename* **-out** *Client_certfilename* **Example:** `# openssl req -new -x509 -key client_private.pem -out client.pem -days 365`	This command generates a new self-signed client certificate using the client private key obtained from the previous step. The certificate is valid for the specified period. The command prompts the user for additional certificate information. A new self-signed client certificate is created.
Step 3	Obtain the KMIP root CA certificate from the KMIP server.	Refer to the KMIP vendor documentation for details on obtaining the root CA certificate.

What to Do Next

Upload the new certificate to the Cisco IMC.

Downloading a KMIP Client Certificate

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 kmip**	Enters the KMIP command mode.
Step 2	Server/kmip # **set enabled yes**	Enables KMIP.
Step 3	Server/kmip*# **commit**	Commits the transaction to the system configuration.
Step 4	Server/kmip # **scope kmip-client-certificate**	Enters the KMIP client certificate command mode.
Step 5	Server /kmip/kmip-client-certificate # **download-client-certificate** *remote-protocol IP Address KMIP client certificate file*	Specifies the protocol to connect to the remote server. It can be of the following types: • TFTP • FTP • SFTP • SCP • HTTP **Note** The Cisco UCS C-Series server now supports fingerprint confirmation of the server when you update firmware through a remote server. This option is available only if you choose SCP or SFTP as the remote server type. If you chose SCP or SFTP as the remote server type while performing this action, a prompt with the message Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue? Click y or n depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.
Step 6	At the confirmation prompt, enter **y**.	This begins the download of the KMIP client certificate.
Step 7	Server /kmip/kmip-client-certificate # **paste-client-certificate**	(Optional) At the prompt, paste the content of the signed certificate and press CTRL+D. **Note** You can either use the remote server method from the previous steps or use the paste option to download the client certificate.

This example downloads the KMIP client certificate:

```
Server # scope kmip
Server /kmip # set enabled yes
Server /kmip *# commit
Server /kmip # scope kmip-client-certificate
Server /kmip/kmip-client-certificate # show detail
    KMIP client certificate Available: 1
    Download client certificate Status: COMPLETED
    Export client certificate Status: NONE
Server /kmip/kmip-client-certificate #  download-client-certificate tftp 10.10.10.10
KmipCertificates/
svbu-xx-blr-dn1-13_ClientCert.pem
  You are going to overwrite the KMIP client certificate.
  Are you sure you want to proceed and overwrite the KMIP client certificate? [y|N]y
KMIP client certificate downloaded successfully

You can  either use the remote server method from the previous steps or use the paste option
 to download the client certificate.

Server /kmip/kmip-client-certificate # paste-client-certificate
Please paste your certificate here, when finished, press CTRL+D.
----BEGIN CERTIFICATE-----
MIIDTzCCAjegAwIBAgIQXuWPdBbyTb5M7/FT8aAjZTANBgkqhkiG9w0BAQUFADA6
MRMwEQYKCZImiZPyLGQBGRYDY29tMRMwEQYKCZImiZPyLGQBGRYDbmV3MQ4wDAYD
VQQDEwVuZXdDQTAeFw0xNTAzMTIxMTM5MTZaFw0yMDAzMTIxMTQ5MTVaMDoxEzAR
BgoJkiaJk/IsZAEZFgNjb20xEzARBgoJkiaJk/IsZAEZFgNuZXcxDjAMBgNVBAMT
BW5ld0NBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuPSAwHtk0IbM
Cd5tYdCa498bfX5Nfdgnq5zE+cGIOqv0dAkucofC/Y0+m7hne9H12aQ9SqTOK1+L
5IT3PVCczhasI7L7jAa+Oe5AOYw7Nsugw5Bd23n42BTVMMp7xsgr1mVfFoHXbBkQ
wiT9DieyImSyGiq5n0/8Iooc0iN5WPMVcHO2ysz76jR8p07xRqgYNCl6cbKAhWfZ
oYIwjhpZv0+SXEs8sEJZKDUhWIfOIpnDL7MoZYgl/kymgs/0hsW4L338jy303c7T
TwnG2/7BOMK0YFkEhqcjlkamGP7MKB2T9e/Cug6VkvFSkkim8M1eHx1gEnQxRtAG
YGp1n55iHQIDAQABo1EwTzALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAd
BgNVHQ4EFgQUl2F3U7cggzCuvRWliZWg91n5lccwEAYJKwYBBAGCNxUBBAMCAQAw
DQYJKoZIhvcNAQEFBQADggEBAJXoJJDDB3QH0q8VY8G/oC1SkAwyOE1dH0NdxFES
tNqQMTaRB2Sb2L/ZzAtfIaZ0Xab9Ig4MqNIMBbHDCwlzhD5gX42GPYWhA/GjRj3O
Q5KcRaEFomxp+twRrJ25ScVSczKJaRonWqKDVL9TwoSuDar3ObiS9ZC0KuBBf0vu
dzrJEYY/1zz7WVPZVyevhba3VSt4LW75URTqOKBSuKO+fvGyyNHWvMPFEIEnJAKt
7QmhO2fiWhD8CxaPFIByqkvrJ96no6oBxdEcjm9n1MttF/UJcpypSPH+46mRn5Az
SzgCBftYNjBPLcwbZGJkF/GpPwjd0TclMM08UOdqiTxR7Ts=
-----END CERTIFICATE-----
  You are going to overwrite the KMIP Client Certificate.
  Are you sure you want to proceed and overwrite the KMIP Client Certificate? [y|N]
y
Server /kmip/kmip-client-certificate #
```

Exporting a KMIP Client Certificate

Before You Begin

- You must log in as a user with admin privileges to perform this task.
- You should have downloaded KMIP client certificate before you can export it.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope kmip**	Enters the KMIP command mode.

	Command or Action	Purpose
Step 2	Server /kmip # **scope kmip-client-certificate**	Enters the KMIP client certificate command mode.
Step 3	Server /kmip/kmip-client-certificate # **export-client-certificate** *remote-protocol IP Adderss KMIP root CA Certificate file*	Specifies the protocol to connect to the remote server. It can be of the following types: • TFTP • FTP • SFTP • SCP • HTTP **Note** The Cisco UCS C-Series server now supports fingerprint confirmation of the server when you update firmware through a remote server. This option is available only if you choose SCP or SFTP as the remote server type. If you chose SCP or SFTP as the remote server type while performing this action, a prompt with the message Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue? Click y or n depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to. Initiates the export of the certificate.
Step 4	Server /kmip/kmip-client-certificate # **show detail**	(Optional) Displays the status of the certificate export.

This example exports the KMIP client certificate:

```
Server # scope kmip
Server /kmip # scope kmip-client-certificate
Server /kmip/kmip-client-certificate #  export-client-certificate ftp 10.10.10.10
/TFTP_DIR/KmipCertificates
/svbu-xx-blr-dn1-13_ClientCert.pem_exported_ftp
Username: username
Password:
KMIP Client Certificate exported successfully
Server /kmip/kmip-client-certificate # show detail
    KMIP Client Certificate Available: 1
    Download KMIP Client Certificate Status: COMPLETED
    Export KMIP Client Certificate Status: COMPLETED
Server /kmip/kmip-client-certificate #
```

Deleting a KMIP Client Certificate

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 kmip**	Enters the KMIP command mode.
Step 2	Server# /kmip **scope kmip-client-certificate**	Enters the KMIP client certificate binding command mode.
Step 3	Server /kmip/kmip-client-certificate # **delete-client-certificate**	Confirmation prompt appears.
Step 4	At the confirmation prompt, enter **y**.	This deletes the KMIP client certificate.

This example deletes the KMIP client certificate:

```
Server # scope kmip
Server /kmip # scope kmip-client-certificate
Server /kmip/kmip-client-certificate # delete-client-certificate
  You are going to delete the KMIP Client Certificate.
  Are you sure you want to proceed and delete the KMIP Client Certificate? [y|N]y
 KMIP Client Certificate deleted successfully.
```

Downloading a KMIP Root CA Certificate

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 kmip**	Enters the KMIP command mode.
Step 2	Server/kmip # **set enabled yes**	Enables KMIP.
Step 3	Server/kmip * # **commit**	Commits the transaction to the system configuration.
Step 4	Server /kmip # **scope kmip-root-ca-certificate**	Enters the KMIP root CA certificate command mode.
Step 5	Server /kmip/kmip-root-ca-certificate # **download-root-ca-certificate**	Specifies the protocol to connect to the remote server. It can be of the following types: • TFTP

	Command or Action	Purpose
	remote-protocol IP Address KMIP CA Certificate file	• FTP • SFTP • SCP • HTTP **Note** The Cisco UCS C-Series server now supports fingerprint confirmation of the server when you update firmware through a remote server. This option is available only if you choose SCP or SFTP as the remote server type. If you chose SCP or SFTP as the remote server type while performing this action, a prompt with the message Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue? Click y or n depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.
Step 6	At the confirmation prompt, enter **y**.	This begins the download of the KMIP root CA certificate.
Step 7	Server /kmip/kmip-root-ca-certificate # **paste-root-ca-certificate**	(Optional) At the prompt, paste the content of the root CA certificate and press CTRL+D. **Note** You can either use the remote server method from the previous steps or use the paste option to download the root CA certificate.

This example downloads the KMIP root CA certificate:

```
Server # scope kmip
Server /kmip # set enabled yes
Server /kmip *# commit
Server /kmip # scope kmip-root-ca-certificate
Server /kmip/kmip-root-ca-certificate # show detail
    KMIP Root CA Certificate Available: 1
    Download Root CA Certificate Status: COMPLETED
    Export Root CA Certificate Status: NONE
Server /kmip/kmip-root-ca-certificate # download-root-ca-certificate tftp 10.10.10.10
KmipCertificates/
svbu-xx-blr-dn1-13_ServerCert.pem
  You are going to overwrite the KMIP Root CA Certificate.
  Are you sure you want to proceed and overwrite the KMIP Root CA Certificate? [y|N]y
KMIP Root CA Certificate downloaded successfully

You can  either use the remote server method from the previous steps or use the paste option
 to download the client certificate.

Server /kmip/kmip-root-ca-certificate # paste-root-ca-certificate
Please paste your certificate here, when finished, press CTRL+D.
```

```
----BEGIN CERTIFICATE-----
MIIDTzCCAjegAwIBAgIQXuWPdBbyTb5M7/FT8aAjZTANBgkqhkiG9w0BAQUFADA6
MRMwEQYKCZImiZPyLGQBGRYDY29tMRMwEQYKCZImiZPyLGQBGRYDbmV3MQ4wDAYD
VQQDEwVuZXdDQTAeFw0xNTAzMTIxMTM5MTZaFw0yMDAzMTIxMTQ5MTVaMDoxEzAR
BgoJkiaJk/IsZAEZFgNjb20xEzARBgoJkiaJk/IsZAEZFgNuZXcxDjAMBgNVBAMT
BW5ld0NBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuPSAwHtk0IbM
Cd5tYdCa498bfX5Nfdgnq5zE+cGIOqv0dAkucofC/Y0+m7hne9H12aQ9SqTOK1+L
5IT3PVCczhasI7L7jAa+Oe5AOYw7Nsugw5Bd23n42BTVMMp7xsgr1mVfFoHXbBkQ
wiT9DieyImSyGiq5n0/8Iooc0iN5WPMVcHO2ysz76jR8p07xRqgYNCl6cbKAhWfZ
oYIwjhpZv0+SXEs8sEJZKDUhWIfOIpnDL7MoZYgl/kymgs/0hsW4L338jy303c7T
TwnG2/7BOMK0YFkEhqcjlkamGP7MKB2T9e/Cug6VkvFSkkim8M1eHx1gEnQxRtAG
YGp1n55iHQIDAQABo1EwTzALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAd
BgNVHQ4EFgQUl2F3U7cggzCuvRWliZWg91n5lccwEAYJKwYBBAGCNxUBBAMCAQAw
DQYJKoZIhvcNAQEFBQADggEBAJXoJJDDB3QH0q8VY8G/oC1SkAwyOE1dH0NdxFES
tNqQMTaRB2Sb2L/ZzAtfIaZ0Xab9Ig4MqNIMBbHDCwlzhD5gX42GPYWhA/GjRj3O
Q5KcRaEFomxp+twRrJ25ScVSczKJaRonWqKDVL9TwoSuDar3ObiS9ZC0KuBBf0vu
dzrJEYY/1zz7WVPZVyevhba3VSt4LW75URTqOKBSuKO+fvGyyNHWvMPFEIEnJAKt
7QmhO2fiWhD8CxaPFIByqkvrJ96no6oBxdEcjm9n1MttF/UJcpypSPH+46mRn5Az
SzgCBftYNjBPLcwbZGJkF/GpPwjd0TclMM08UOdqiTxR7Ts=
-----END CERTIFICATE-----
  You are going to overwrite the KMIP Root CA Certificate.
  Are you sure you want to proceed and overwrite the KMIP Root CA Certificate? [y|N]
y
Server /kmip/kmip-root-ca-certificate #
```

Exporting a KMIP Root CA Certificate

Before You Begin

- You must log in as a user with admin privileges to perform this task.
- You should have downloaded KMIP root CA certificate before you can export it.

Procedure

	Command or Action	Purpose
Step 1	Server # **scope kmip**	Enters the KMIP command mode.
Step 2	Server /kmip # **scope kmip-root-ca-certificate**	Enters the KMIP root CA certificate command mode.
Step 3	Server /kmip/kmip-root-ca-certificate # **export-root-ca-certificate** *remote-protocol IP Adderss KMIP root CA Certificate file*	Specifies the protocol to connect to the remote server. It can be of the following types: • TFTP • FTP • SFTP • SCP • HTTP

	Command or Action	Purpose
		Note The Cisco UCS C-Series server now supports fingerprint confirmation of the server when you update firmware through a remote server. This option is available only if you choose SCP or SFTP as the remote server type. If you chose SCP or SFTP as the remote server type while performing this action, a prompt with the message Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue? Click y or n depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to. Initiates the export of the certificate.
Step 4	Server /kmip/kmip-root-ca-certificate # **show detail**	(Optional) Displays the status of the certificate export.

This example exports the KMIP root CA certificate:

```
Server # scope kmip
Server /kmip # scope kmip-root-ca-certificate
Server /kmip/kmip-root-ca-certificate #  export-root-ca-certificate tftp 10.10.10.10
KmipCertificates/
svbu-xx-blr-dn1-13_ServerCert.pem_exported_tftp
KMIP Root CA Certificate exported successfully
Server /kmip/kmip-root-ca-certificate # show detail
    KMIP Root CA Certificate Available: 1
    Download Root CA Certificate Status: COMPLETED
    Export Root CA Certificate Status: COMPLETED
Server /kmip/kmip-root-ca-certificate #
```

Deleting a KMIP Root CA Certificate

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 kmip**	Enters the KMIP command mode.
Step 2	Server# /kmip **scope kmip-root-ca-certificate**	Enters the KMIP root CA certificate binding command mode.

	Command or Action	Purpose
Step 3	Server /kmip/kmip-root-ca-certificate # **delete-root-ca-certificate**	Confirmation prompt appears.
Step 4	At the confirmation prompt, enter **y**.	This deletes the KMIP root CA certificate.

This example deletes the KMIP root CA certificate:

```
Server # scope kmip
Server /kmip # scope kmip-root-ca-certificate
Server /kmip/kmip-root-ca-certificate # delete-root-ca-certificate
  You are going to delete the KMIP root CA certificate.
  Are you sure you want to proceed and delete the KMIP root CA certificate? [y|N]y
 KMIP root CA certificate deleted successfully.
```

Downloading a KMIP Client Private Key

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 kmip**	Enters the KMIP command mode.
Step 2	Server/kmip# **set enabled yes**	Enables KMIP.
Step 3	Server/kmip*# **commit**	Commits the transaction to the system configuration.
Step 4	Server/kmip # **scope kmip-client-private-key**	Enters the KMIP client private key command mode.
Step 5	Server /kmip/kmip-client-private-key # **download-client-pvt-key** *remote-protocol IP Address KMIP client private key file*	Specifies the protocol to connect to the remote server. It can be of the following types: • TFTP • FTP • SFTP • SCP • HTTP

	Command or Action	Purpose
		Note The Cisco UCS C-Series server now supports fingerprint confirmation of the server when you update firmware through a remote server. This option is available only if you choose SCP or SFTP as the remote server type. If you chose SCP or SFTP as the remote server type while performing this action, a prompt with the message Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue? Click y or n depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.
Step 6	At the confirmation prompt, enter **y**.	This begins the download of the KMIP client private key.
Step 7	Server /kmip/kmip-client-private-key # **paste-client-pvt-key**	(Optional) At the prompt, paste the content of the private key and press CTRL+D. **Note** You can either use the remote server method from the previous steps or use the paste option to download the client private key.

This example downloads the KMIP client private key:

```
Server # scope kmip
Server /kmip # set enabled yes
Server /kmip *# commit
Server /kmip # scope kmip-client-private-key
Server /kmip/kmip-client-private-key # show detail
    KMIP Client Private Key Available: 1
    Download Client Private Key Status: COMPLETED
    Export Client Private Key Status: NONE
Server /kmip/kmip-client-private-key #  download-client-pvt-key tftp 10.10.10.10
KmipCertificates/
svbu-xx-blr-dn1-13_ClientPvtKey.pem
  You are going to overwrite the KMIP Client Private Key.
  Are you sure you want to proceed and overwrite the KMIP Client Private Key? [y|N]y
KMIP Client Private Key downloaded successfully

You can  either use the remote server method from the previous steps or use the paste option
 to download the client certificate.

Server /kmip/kmip-client-private-key # paste-client-pvt-key
Please paste your client private here, when finished, press CTRL+D.
----BEGIN CERTIFICATE-----
MIIDTzCCAjegAwIBAgIQXuWPdBbyTb5M7/FT8aAjZTANBgkqhkiG9w0BAQUFADA6
MRMwEQYKCZImiZPyLGQBGRYDY29tMRMwEQYKCZImiZPyLGQBGRYDbmV3MQ4wDAYD
VQQDEwVuZXdDQTAeFw0xNTAzMTIxMTM5MTZaFw0yMDAzMTIxMTQ5MTVaMDoxEzAR
BgoJkiaJk/IsZAEZFgNjb20xEzARBgoJkiaJk/IsZAEZFgNuZXcxDjAMBgNVBAMT
BW51d0NBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuPSAwHtk0IbM
Cd5tYdCa498bfX5Nfdgnq5zE+cGIOqv0dAkucofC/Y0+m7hne9H12aQ9SqTOK1+L
5IT3PVCczhasI7L7jAa+Oe5AOYw7Nsugw5Bd23n42BTVMMp7xsgr1mVfFoHXbBkQ
wiT9DieyImSyGiq5n0/8Iooc0iN5WPMVcHO2ysz76jR8p07xRqgYNCl6cbKAhWfZ
```

```
oYIwjhpZv0+SXEs8sEJZKDUhWIfOIpnDL7MoZYgl/kymgs/0hsW4L338jy303c7T
TwnG2/7BOMK0YFkEhqcjlkamGP7MKB2T9e/Cug6VkvFSkkim8M1eHx1gEnQxRtAG
YGp1n55iHQIDAQABo1EwTzALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAd
BgNVHQ4EFgQUl2F3U7cggzCuvRWliZWg91n5lccwEAYJKwYBBAGCNxUBBAMCAQAw
DQYJKoZIhvcNAQEFBQADggEBAJXoJJDDB3QH0q8VY8G/oC1SkAwyOE1dH0NdxFES
tNqQMTaRB2Sb2L/ZzAtfIaZ0Xab9Ig4MqNIMBbHDCwlzhD5gX42GPYWhA/GjRj3O
Q5KcRaEFomxp+twRrJ25ScVSczKJaRonWqKDVL9TwoSuDar3ObiS9ZC0KuBBf0vu
dzrJEYY/1zz7WVPZVyevhba3VSt4LW75URTqOKBSuKO+fvGyyNHWvMPFEIEnJAKt
7QmhO2fiWhD8CxaPFIByqkvrJ96no6oBxdEcjm9n1MttF/UJcpypSPH+46mRn5Az
SzgCBftYNjBPLcwbZGJkF/GpPwjd0TclMM08UOdqiTxR7Ts=
-----END CERTIFICATE-----
  You are going to overwrite the KMIP client private key.
  Are you sure you want to proceed and overwrite the KMIP Client Private Key? [y|N]
y
Server /kmip/kmip-client-private-key #
```

Exporting KMIP Client Private Key

Before You Begin

- You must log in as a user with admin privileges to perform this task.
- You should have downloaded KMIP client private key before you can export it.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope kmip**	Enters the KMIP command mode.
Step 2	Server /kmip # **scope kmip-client-private-key**	Enters the KMIP client private key command mode.
Step 3	Server /kmip/kmip-client-private-key # **export-client-pvt-key** *remote-protocol IP Adderss KMIP root CA Certificate file*	Specifies the protocol to connect to the remote server. It can be of the following types: • TFTP • FTP • SFTP • SCP • HTTP

	Command or Action	Purpose
		Note The Cisco UCS C-Series server now supports fingerprint confirmation of the server when you update firmware through a remote server. This option is available only if you choose SCP or SFTP as the remote server type. If you chose SCP or SFTP as the remote server type while performing this action, a prompt with the message Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue? Click y or n depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to. Initiates the export of the certificate.
Step 4	Server /kmip/kmip-client-private-key # **show detail**	(Optional) Displays the status of the certificate export.

This example exports the KMIP client private key:

```
Server # scope kmip
Server /kmip # scope kmip-client-private-key
Server /kmip/kmip-client-private-key #  export-client-pvt-key tftp 10.10.10.10
KmipCertificates
/svbu-xx-blr-dn1-13_ClientPvtKey.pem_exported_tftp
KMIP Client Private Key exported successfully
Server /kmip/kmip-client-private-key # show detail
    KMIP Client Private Key Available: 1
    Download Client Private Key Status: COMPLETED
    Export Client Private Key Status: COMPLETED
Server /kmip/kmip-client-private-key #
```

Deleting a KMIP Client Private Key

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 kmip**	Enters the KMIP command mode.
Step 2	Server# /kmip **scope kmip-client-private-key**	Enters the KMIP client private key binding command mode.
Step 3	Server /kmip/kmip-client-private-key # **delete-client-pvt-key**	Confirmation prompt appears.

	Command or Action	Purpose
Step 4	At the confirmation prompt, enter **y**.	This deletes the KMIP client private key.

This example deletes the KMIP client private key:

```
Server # scope kmip
Server /kmip # scope kmip-client-private-key
Server /kmip/kmip-client-private-key # delete-client-pvt-key
  You are going to delete the KMIP client private key.
  Are you sure you want to proceed and delete the KMIP client private key? [y|N]y
 KMIP client private key deleted successfully.
```

Configuring KMIP Server Login Credentials

This procedure shows you how to configure the login credentials for the KMIP server and make the KMIP server login credentials mandatory for message authentication.

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 kmip**	Enters the KMIP command mode.
Step 2	Server /kmip # **scope kmip-login**	Enters the KMIP login command mode.
Step 3	Server/kmip/kmip-login # **set login** *username*	Sets the KMIP server user name.
Step 4	Server/kmip/kmip-login * # **set password**	Enter the password at the prompt and enter the same password again at the confirm password prompt. This sets the KMIP server password.
Step 5	Server/kmip/kmip-login * # **set use-kmip-cred** {**yes** | **no**}	Decides whether the KMIP server login credentials should be mandatory for message authentication.
Step 6	Server/kmip/kmip-login * # **commit**	Commits the transaction to the system configuration.
Step 7	Server/kmip/kmip-login # **restore**	(Optional) Restores the KMIP settings to defaults.

This example shows how to configure the KMIP server credentials:

```
Server /kmip # scope kmip-login
Server /kmip/kmip-login # set login username
Server /kmip/kmip-login *# set password
Please enter password:
Please confirm password:
```

```
Server /kmip/kmip-login *# set use-kmip-cred yes
Server /kmip/kmip-login *# commit
Server /kmip/kmip-login # show detail
    Use KMIP Login: yes
    Login name to KMIP server: username
    Password to KMIP server: ******

You can restore the KMIP server credentials to default settings by preforming the following
 step:

Server /kmip/kmip-login # restore
Are you sure you want to restore KMIP settings to defaults?
Please enter 'yes' to confirm: yes
Restored factory-default configuration.
Server /kmip/kmip-login # show detail
    Use KMIP Login: no
    Login name to KMIP server:
    Password to KMIP server: ******
Server /kmip/kmip-login #
```

Configuring KMIP Server Properties

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	Server # **scope kmip**	Enters the KMIP command mode.
Step 2	Server /kmip # **scope kmip-server** *server ID*	Enters the chosen KMIP server command mode.
Step 3	Server /kmip/kmip-server # **set** *kmip-port*	Sets the KMIP port.
Step 4	Server /kmip/kmip-server *# **set** *kmip-server*	Sets the KMIP server ID.
Step 5	Server /kmip/kmip-server # **set** *kmip-timeout*	Sets the KMIP server timeout.
Step 6	Server /kmip/kmip-server # **commit**	Commits the transaction to system configuration.
Step 7	Server /kmip/kmip-server # **show detail**	(Optional) Displays the KMIP server details.

This example tests the KMIP server connection:

```
Server # scope kmip
Server /kmip # scope kmip-server 1
Server /kmip/kmip-server # set kmip-port  5696
Server /kmip/kmip-server * # set kmip-server  kmipserver.com
Server /kmip/kmip-server * # set kmip-timeout  10
Server /kmip/kmip-server * # commit
Server /kmip/kmip-server # show detail
Server number 1:
    Server domain name or IP address: kmipserver.com
    Port: 5696
```

```
    Timeout: 10
Server /kmip/kmip-server #
```

CHAPTER 13

Configuring Platform Event Filters

This chapter includes the following sections:

Platform Event Filters

A platform event filter (PEF) can trigger an action. For each PEF, you can choose the action to be taken (or take no action) when a platform event occurs.

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	Voltage Critical Assert Filter
3	Current Assert Filter
4	Fan Critical Assert Filter
5	Processor Assert Filter
6	Power Supply Critical Assert Filter
7	Memory Critical 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: • **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 # **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 *# commit
Server /fault/pef # show
Platform Event Filter Event                       Action
--------------------- -------------------------- -----------
11                    Memory Assert Filter        reboot

Server /fault/pef #
```

Resetting Event Platform Filters

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.
Step 3	Server /fault # **commit**	Commits the transaction to the system configuration.
Step 4	Server /fault # **reset-event-filters**	Resets the platform event filters.

	Command or Action	Purpose
Step 5	Server /fault # **show pef**	Displays the latest platform event filters.

The following example enables platform event alerts:

```
Server# scope fault
Server /fault # set platform-event-enabled yes
Server /fault *# commit
Server /fault # show
Platform Event Enabled
-----------------------
   yes

Server /fault # reset-event-filters
Server /fault # show pef
Platform Event Filter   Event                              Action
--------------------- ----------------------------------- -----------
1                     Temperature Critical Assert Filter  none
2                     Voltage Critical Assert Filter      none
3                     Current Assert Filter               none
4                     Fan Critical Assert Filter          none
5                     Processor Assert Filter             none
6                     Power Supply Critical Assert Filter none
7                     Memory Critical Assert Filter       none

Server /fault #
```

CHAPTER 14

Cisco IMC Firmware Management

This chapter includes the following sections:

Overview of Firmware

C-Series servers use Cisco-certified firmware that is 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 the new BIOS firmware, it must be from the same software release as the Cisco IMC firmware that is running on the server. Do not install the new BIOS firmware until after you have activated the matching Cisco IMC 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, Cisco IMC, 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 Cisco IMC 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 want to update the firmware manually, you must update the Cisco IMC firmware first. The Cisco IMC firmware update process is divided into the following stages to minimize the amount of time that the server is offline:

- Installation—During this stage, Cisco IMC installs the selected Cisco IMC firmware in the nonactive, or backup, slot on the server.
- Activation—During this stage, Cisco IMC sets the nonactive firmware version as active, causing a disruption in service. When the server reboots, the firmware in the new active slot becomes the running version.

After you activate the Cisco IMC firmware, you can update the BIOS firmware. You must power off server during the entire BIOS update process, so the process is not divided into stages. Instead, you only need to enter one command and Cisco IMC installs and updates the BIOS firmware as quickly as possible. After the Cisco IMC 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.
- This procedure only applies to the Cisco UCS C-Series server running on Stand-Alone mode. Contact Cisco Technical Assistance Center to upgrade firmware for UCS C-Series running on Cisco UCS Manager integrated mode.

Cisco IMC in a secure mode ensures that all the firmware images prior to loading and execution are digitally signed and are verified for authenticity and integrity to protect the device from running tampered software.

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 Cisco IMC 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 Cisco IMC 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 Cisco IMC and BIOS firmware manually, do the following:
Beginning with Release 3.0, the BIOS and Cisco IMC firmware files are no longer embedded inside the HUU as a standalone .zip file. BIOS and Cisco IMC firmware must now be extracted using the **getfw** utility, which is available in the GETFW folder of the HUU. Perform the following steps to extract the BIOS or Cisco IMC firmware files:

Note To perform this:

- Openssl must be installed in the target system.
- Squashfs kernel module must be loaded in the target system.

```
Viewing the GETFW help menu:
[root@RHEL65-***** tmp]# cd GETFW/
[root@RHEL65-***** GETFW]# ./getfw -h
Help:
  Usage: getfw {-b -c -C -H -S -V -h} [-s SRC] [-d DEST]
    -b      : Get BIOS Firmware
    -c      : Get CIMC Firmware
    -C      : Get CMC Firmware
    -H      : Get HDD Firmware
```

```
    -S      : Get SAS Firmware
    -V      : Get VIC Firmware
    -h      : Display Help
    -s SRC  : Source of HUU ISO image
    -d DEST : Destination to keep Firmware/s
  Note : Default BIOS & CIMC get extracted
```

Extracting the BIOS firmware:

```
[root@RHEL65-***** GETFW]# ./getfw -s /root/Desktop/HUU/ucs-c2xxx-huu-3.0.1c.iso -d /tmp/HUU
FW/s available at '/tmp/HUUucs-c2xxx-huu-3.0.1c'
[root@RHEL65-***** GETFW]# cd /tmp/HUU/
[root@RHEL65-***** HUU]# cd ucs-c2xxx-huu-3.0.1c/
[root@RHEL65-***** ucs-c2xxx-huu-3.0.1c]# ls
bios  cimc
[root@RHEL65-***** ucs-c2xxx-huu-3.0.1c]# cd bios/
[root@RHEL65-***** bios]# ls
bios.cap
[root@RHEL65-***** bios]#
```

Extracting the CIMC firmware:

```
[root@RHEL65-***** GETFW]# ./getfw -s /root/Desktop/HUU/ucs-c2xxx-huu-3.0.1c.iso -d /tmp/HUU
FW/s available at '/tmp/HUUucs-c2xxx-huu-3.0.1c'
[root@RHEL65-***** GETFW]# cd /tmp/HUU/
[root@RHEL65-***** HUU]# cd ucs-c2xxx-huu-3.0.1c/
[root@RHEL65-***** ucs-c2xxx-huu-3.0.1c]# ls
bios  cimc
[root@RHEL65-***** ucs-c2xxx-huu-3.0.1c]# cd cimc/
[root@RHEL65-***** cimc]# ls
cimc.cap
[root@RHEL65-***** cimc]#
```

Step 12 (Optional) If you plan to install the firmware from a remote server, copy the BIOS installation CAP file and the Cisco IMC 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.

Note The Cisco UCS C-Series server now supports fingerprint confirmation of the server when you update firmware through a remote server. This option is available only if you choose SCP or SFTP as the remote server type.

If you chose SCP or SFTP as the remote server type while performing this action, a prompt with the message Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue? Click y or n depending on the authenticity of the server fingerprint.

The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.

What to Do Next

Use the Cisco Host Upgrade Utility to upgrade all firmware on the server or manually install the Cisco IMC firmware on the server.

Introduction to Cisco IMC Secure Boot

About Cisco IMC Secure Mode

Note Cisco IMC secure boot mode is enabled by default only on some Cisco UCS C-Series servers.

You can update Cisco IMC to the latest version using Host Upgrade Utility (HUU), web UI, or CLI. If you use HUU to upgrade Cisco IMC, you are prompted to enable secure boot mode. If you choose **Yes**, the system enters a secure mode and install the firmware twice. If you choose **No**, it enters a nonsecure mode. If you use either the web UI or CLI to upgrade Cisco IMC, you must upgrade to version 2.0(x). After you boot the system with version 2.0(x), it boots in a nonsecure mode by default. You must enable secure mode. when you enable secure mode, you are automatically reinstalling the firmware. In the web UI, the secure mode option is available as a checkbox within the Cisco IMC firmware update page. In the CLI, you can enable the secure mode by using the **update-secure** command.

During the first upgrade to Cisco IMC version 2.0, a warning message might display stating that some of the features and applications are not installed correctly and a second upgrade is required. We recommend that you perform the second upgrade with or without the secure boot option enabled to correctly install the Cisco IMC firmware version 2.0(x) in a secure mode. After the installation is complete, you must activate the image. After you boot your system with the secure boot option enabled, Cisco IMC remains in secure mode and you cannot disable it later on. If you do not activate the image and reinstall any other firmware images, Cisco IMC may become unresponsive.

Warning After you install the firmware with the secure boot migration, you must activate the image before performing any other regular server-based tasks. If you do not activate this image, and if you reinstall any other firmware images, Cisco IMC might become unresponsive.

The secure boot is enabled only when the firmware installation is complete and you have activated the image.

Note When Cisco IMC is in a secure mode, it means the following:

- Only signed Cisco IMC firmware images can be installed and booted on the device.
- Secure Cisco IMC mode cannot be disabled later on.
- Any Cisco IMC versions can be upgraded to the latest version directly.
- Cisco IMC firmware versions cannot be installed or booted prior to version 1.5(3x).
- Cisco IMC version 2.0 cannot be downgraded to version 1.4(x), 1.5, 1.5(2x), or 1.5(1), 1.5(2) or to any nonsecure firmware version.

Supported Cisco IMC Version When Downgrading from the Latest Version

The following table lists the Cisco IMC versions in a secure mode that can be downgraded to prior versions.

From Cisco IMC Version	To Cisco IMC Version	Possibility
2.0(x)	Prior to 1.5(1)	Not possible
2.0(x)	1.5(3x) or later	Possible
2.0(x)	Prior to 1.5(3x)	Not possible

Note When the Cisco IMC verison you are using is in a nonsecure mode, you can downgrade Cisco IMC to any prior version.

Note If you use HUU to downgrade Cisco IMC versions prior to 1.5(4), you must first downgrade Cisco IMC and then downgrade other firmware. Activate the firmware and then downgrade the BIOS firmware.

Number of Updates Required for Cisco IMC Version 2.0(1)

Important This section is valid for Cisco IMC version 2.0(1) and prior releases.

Supported Cisco IMC Version When Upgrading to the Latest Version

The following table lists the number of updates required for Cisco IMC to correctly install all the applications of the latest version.

From Cisco IMC Version	To a Nonsecure Cisco IMC Version 2.0(x)	To a Secure Cisco IMC Version 2.0(x)
Prior to 1.5(2)	Double update	Double update
1.5(2)	Single update	Double update
1.5(3)	Single update	Double update
1.5(3x) or Later	Single update	Double update

Updating Cisco IMC in a Nonsecure Mode

Important This section is valid for Cisco IMC version 2.0(1) and prior releases.

You can upgrade Cisco IMC to the latest version in a nonsecure mode with all the latest feature and applications installed correctly. When you upgrade Cisco IMC to the latest version using the web UI or CLI, you might need to update the firmware twice manually depending upon the version you are using. See, Supported Cisco IMC Version when Upgrading to the Latest Version. If you use HUU to upgrade the Cisco IMC verison, it gets upgraded to the latest verison automatically.

Note If you are installing from a Cisco IMC version prior to 1.5(2x), the following message is displayed:

Warning "Some of the Cisco IMC firmware components are not installed properly! Please reinstall Cisco IMC firmware version 2.0(1) or higher to recover".

> **Note** If you are in the middle of (HUU) update, we recommend that you reconnect any KVM session to current status of the update.

When Cisco IMC runs in a nonsecure mode, it implies the following:

- Any signed or unsigned Cisco firmware images can be installed on the device.
- Any Cisco IMC versions can be upgraded to the latest version directly.
- Cisco IMC firmware versions can be installed or booted to any prior versions.

Installing Cisco IMC Firmware

- If you are updating the Cisco IMC firmware through a front panel USB device, make sure that the Smart Access USB option has been enabled.
- If you start an update while an update is already in process, both updates will fail.

Before You Begin

- Log in to the Cisco IMC 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 273.

Procedure

	Command or Action	Purpose
Step 1	server# **scope cimc**	Enters Cisco IMC command mode.
Step 2	server /cimc # **scope firmware**	Enters Cisco IMC firmware command mode.
Step 3	server /cimc /firmware # **update** *protocol IP Address path*	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: • TFTP • FTP • SFTP • SCP • HTTP **Note** The Cisco UCS C-Series server now supports fingerprint confirmation of the server when you update firmware through a remote server. This option is available only if you choose SCP or SFTP as the remote server type. If you chose SCP or SFTP as the remote server type while performing this action, a prompt with the message Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue? Click y or n depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.
Step 4	server /cimc/firmware # **update usb** *path and firmware file name*	Updates the Cisco IMC firmware from the connected USB.
Step 5	server /cimc/firmware # **update-secure** *protocol IP Address path*	(Optional) Migrates to the Cisco IMC secure boot option. Migration implies the following: • You can install and boot only signed Cisco IMC firmware images on the server. • You cannot install and boot Cisco IMC firmware versions prior to 1.5(3x).

	Command or Action	Purpose
		• You cannot disable Secure Boot later on. **Important** This action is available for Cisco IMC 2.0(1) version only. For later versions, it is enabled by default. **Warning** After installing the firmware with the secure boot migration, you must activate the image before performing any other regular server-based tasks. If you do not activate this image, and if you reinstall any other firmware images, Cisco IMC might become unresponsive. For Cisco IMC version 2.0(1), the secure boot is enabled only when the firmware installation is complete and you have activated the image.
Step 6	server /cimc /firmware # **show detail**	(Optional) Displays the progress of the firmware update.

This example shows how to update the Cisco IMC firmware and to migrate Cisco IMC from a nonsecure boot to secure boot for Cisco IMC version 2.0:

```
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
Firmware update has started.
Please check the status using "show detail"
Server /cimc /firmware # update-secure tftp 1.1.1.1 /cimc-pkg.bin
Migrating to Cisco IMC Secure Boot option implies:
-You can install and boot only signed Cisco IMC firmware images on the server.
-You cannot install and boot Cisco IMC firmware versions prior than 1.5(3x).
-You cannot disable Secure Boot later on.

After installing the firmware with the Secure Boot migration, you must
activate the image before performing any other regular server-based tasks.
The Secure Boot option is enabled only when the firmware installation
is complete and you have activated the image.

Continue?[y|N]y
Update to Secure Boot selected, proceed with update.
Firmware update initialized.
Please check the status using "show detail".
server /cimc /firmware # show detail
Firmware Image Information:
    Update Stage: DOWNLOAD
    Update Progress: 5
    Current FW Version: 2.0(0.29)
    FW Image 1 Version: 2.0(0.28)
    FW Image 1 State: BACKUP INACTIVATED
    FW Image 2 Version: 2.0(0.29)
    FW Image 2 State: RUNNING ACTIVATED
    Boot-loader Version: 2.0(0.9).35
    Secure Boot: DISABLED

*+----------------------------------------------------------------------+
 + Some of the Cisco IMC firmware components are not installed properly! +
 + Please reinstall Cisco IMC firmware version 2.0 or higher to recover. +
 +----------------------------------------------------------------------+
server /cimc /firmware #
```

This example shows how to update the Cisco IMC firmware:

```
server# scope cimc
server /cimc # scope firmware
```

```
server /cimc /firmware # update ftp 10.10.10.10 //test/dnld-ucs-k9-bundle.1.0.2h.bin
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

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 Cisco IMC as a user with admin privileges.
- Activate the Cisco IMC firmware that goes with the BIOS version you want to install, as described in Activating Installed CIMC Firmware, on page 280.
- Power off the server.

Note

- For C220 M4, C240 M4 and C3160, you do not have to power off the server.
- If you start an update while an update is already in process, both updates will fail.
- If you are updating the BIOS firmware through a front panel USB device, make sure that the Smart Access USB option has been enabled.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters the Cisco IMC 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 Cisco IMC firmware version does not match, activate the Cisco IMC firmware before continuing with this procedure or the server will not boot. For details, see Activating Installed CIMC Firmware, on page 280.
Step 5	Server /cimc/firmware # **top**	Returns to the server root level.
Step 6	Server# **scope bios**	Enters the BIOS command mode.
Step 7	Server /bios # **update** *protocol IP Address path*	It specifies the following: • Protocol, it can be TFTP, FTP, SFTP, SCP, or HTTP. **Note** The Cisco UCS C-Series server now supports fingerprint confirmation of the server when you update firmware through a remote server. This option is available only if you choose SCP or SFTP as the remote server type. If you chose SCP or SFTP as the remote server type while performing this action, a prompt with the message Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue? Click y or n depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to. • The IPv4 or IPv6 address or the host name of the remote server. • The file path to the BIOS firmware file on the remote server.
Step 8	Server /bios # **update usb** *path and firmware file name*	Updates the BIOS firmware from the connected USB.

This example updates the BIOS firmware:

```
Server# scope bios
Server /bios# show detail
BIOS:
```

```
    BIOS Version: CxxMx.2.0.3.0.080720142114
    Backup BIOS Version: CxxMx.2.0.2.68.073120141827
    Boot Order: (none)
    Boot Override Priority:
    FW Update/Recovery Status: None, OK
    UEFI Secure Boot: disabled
    Configured Boot Mode: None
    Actual Boot Mode: Unknown
    Last Configured Boot Order Source: UNKNOWN
Server /bios # update ftp 10.10.10.10 //upgrade_bios_files/Cxx-BIOS-1-4-3j-0.CAP
 <CR>  Press Enter key
Firmware update has started.
Please check the status using "show detail"

For updating the BIOS using the front panel USB:

Server /bios # update usb CxxMx-BIOS-3-1-0-289.cap
 User Options:USB Path[Cxxmx-BIOS-3-1-0-289.cap]
<CR> Press Enter key
Firmware update has started.
Please check the status using "show detail"
Server /bios # show detail
BIOS:
BIOS Version: CxxMx.3.1.0.289.0530172308
Boot Order: (none)
FW Update Status: None, OK
UEFI Secure Boot: disabled
Configured Boot Mode: Legacy
Actual Boot Mode: Legacy
Last Configured Boot Order Source: BIOS
One time boot device: (none)
Server /bios #
```

Activating Installed BIOS Firmware

Note **Activate BIOS Firmware** (**activate**) option is available only for some C-Series servers. For servers that do not have the this option, rebooting the server activates the installed BIOS firmware.

Before You Begin

- Install the BIOS firmware on the server.
- Power off the host.

Important While the activation is in progress, do not:

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

Procedure

	Command or Action	Purpose
Step 1	Server# **scope bios**	Enters the BIOS command mode.
Step 2	Server /bios # **show detail**	Displays the available firmware images and status.
Step 3	Server /bios # **activate**	Activates the currently inactive image.
Step 4	At the prompt, enter y to activate the selected firmware image.	

This example activates firmware and then verifies the activation:

```
Server# scope bios
Server /bios # show detail
BIOS
    Version: C240M4.2.0.2.67.072320142231
    Backup BIOS Version: C240M4.2.0.2.66.071820142034
    Boot Order: (none)
    Boot Override Priority:
    FW Update/Recovery Status: None, OK
    UEFI Secure Boot: disabled
    Configured Boot Mode: None
    Actual Boot Mode: Legacy
    Last Configured Boot Order Source: BIOS

Server /bios # activate
This operation will activate "C240M4.2.0.2.66.071820142034" after next host power off
Continue?[y|N]

Server# scope bios
Server /bios # show detail
BIOS
    Version: C240M4.2.0.2.66.071820142034
    Backup BIOS Version: C240M4.2.0.2.67.072320142231
    Boot Order: (none)
    Boot Override Priority:
    FW Update/Recovery Status: None, OK
    UEFI Secure Boot: disabled
    Configured Boot Mode: None
    Actual Boot Mode: Legacy
    Last Configured Boot Order Source: BIOS
```

Installing VIC Firmware

Before You Begin

- Log in as a user with admin privileges.
- If you are updating VIC firmware from a front panel USB device, make sure that the Smart USB option has been enabled and a valid VIC firmware is available in the USB device.
- If you start a new update when an update is already in process, both updates will fail.

Procedure

	Command or Action	Purpose
Step 1	server # **scope chassis**	Enters the chassis command mode
Step 2	server /chassis # **update-adapter-fw** *protocol remote server address image file path***activate|no-activate***PCI slot number*	The VIC firmware will be stored at the specified path and file name on a remote server at the specified IPv4 or IPv6 address or a hostname. The remote server could be one of the following types: • TFTP • FTP • SFTP • SCP • HTTP **Note** The Cisco UCS C-Series server now supports fingerprint confirmation of the server when you update firmware through a remote server. This option is available only if you choose SCP or SFTP as the remote server type. If you chose SCP or SFTP as the remote server type while performing this action, a prompt with the message Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue? Click y or n depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.
Step 3	server /chassis # **update-adapter-fw usb** *image file path* **activate|no-activate** *PCI slot number*	Provide the image file path in the USB device, and the VIC PCI slot number.
Step 4	server /cimc # **show adapter detail**	(Optional) Displays the progress of the firmware update.

This example shows how to update the VIC firmware:

```
Server# scope chassis
Server /chassis # update-adapter-fw update ftp 10.10.10.10 cruzfw_new.bin activate MLOM
Adapter firmware update has started.
Please check the status using "show adapter detail".
You have chosen to automatically activate the new firmware
image.  Please restart your host after the update finish.
Server /chassis # show adapter detail
PCI Slot MLOM:
    Product Name: UCS VIC 1387
    Serial Number: FCH2102J8SU
```

```
    Product ID: UCSC-MLOM-C40Q-03
    Adapter Hardware Revision: 3
    Current FW Version: 4.1(3.143)
    VNTAG: Disabled
    FIP: Enabled
    LLDP: Enabled
    Configuration Pending: no
    Cisco IMC Management Enabled: yes
    VID: V03
    Vendor: Cisco Systems Inc
    Description:
    Bootloader Version: 4.1(2d)
    FW Image 1 Version: 4.1(3.143)
    FW Image 1 State: RUNNING ACTIVATED
    FW Image 2 Version: N/A
    FW Image 2 State: N/A
    FW Update Status: Update in progress
    FW Update Error: No error
    FW Update Stage: Erasing (12%)
    FW Update Overall Progress: 19%
Server /chassis #
```

Installing CMC Firmware from a Remote Server

Before You Begin

- Log in to the Cisco IMC 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 273.
- This action is available only on some C-Series servers.
- **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 chassis**	Enters chassis command mode.
Step 2	server /chassis # **scope cmc** *1|2*	Enters CMC on the chosen SIOC controller command mode.
Step 3	server /chassis/cmc # **update** *protocol IP Address path*	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: • TFTP • FTP • SFTP • SCP • HTTP

	Command or Action	Purpose
		Note The Cisco UCS C-Series server now supports fingerprint confirmation of the server when you update firmware through a remote server. This option is available only if you choose SCP or SFTP as the remote server type. If you chose SCP or SFTP as the remote server type while performing this action, a prompt with the message Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue? Click y or n depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.
Step 4	server /chassis/cmc # **show detail**	(Optional) Displays the progress of the firmware update.

This example shows how to update the CMC firmware:

```
server # scope chassis
server /chassis # scope cmc 1
server /chassis/cmc # update  http 10.104.236.99 colusa_cmc.2.0.2a.img
CMC Firmware update initialized.
Please check the status using "show detail"
Server /chassis/cmc # show detail
Firmware Image Information:
    Name: CMC1
    Update Stage: DOWNLOAD
    Update Progress: 25
    Current FW Version: 2.0(2a)
    FW Image 1 Version: 2.0(2a)
    FW Image 1 State: RUNNING ACTIVATED
    FW Image 2 Version: 2.0(2a)
    FW Image 2 State: BACKUP INACTIVATED
server /chassis/cmc #
```

What to Do Next

Activate the new firmware.

Activating Installed CMC Firmware

Note CMCs are configured to have one in an active state while other acts as a backup, when you activate the backup CMC the previously active CMC changes to backup CMC activating the other.

Before You Begin

Install the CMC firmware on the server.

Important While the activation is in progress, do not:

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

- CMC-1 activation interrupts Cisco IMC network connectivity.

Procedure

	Command or Action	Purpose
Step 1	server # **scope chassis**	Enters chassis command mode.
Step 2	Server# **scope cmc***1|2*	Enters the CMC of the chosen SIOC slot command mode.
Step 3	Server /cmc # **activate**	Activates the selected image for the chosen CMC.
Step 4	At the prompt, enter y to activate the selected firmware image.	The CMC-1 reboots, terminating all CLI and GUI sessions until the reboot completes, but CMC-2 reboot will not affect any active sessions.

This example activates CMC firmware on the SIOC slot 1:

```
Server # scope chassis
Server /chassis # scope cmc 1
Server /chassis/cmc #  activate
Warning: The CMC will be rebooted immediately to complete the activation.
The network may go down temporarily till CMC boots up again
Continue?[y|N]y
```

Installing SAS Expander Firmware from a Remote Server

Before You Begin

- You must be logged in as admin to perform this action.
- 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 sas-expander {1 | 2}**	Enters the SAS expander command mode.
Step 3	Server /chassis/sas-expander # **show detail**	Displays the available firmware images and status.
Step 4	Server /chassis/sas-expander # **update** *protocol IP_Address path*	It specifies the following: • Protocol, it can be TFTP, FTP, SFTP, SCP or HTTP. **Note** The Cisco UCS C-Series server now supports fingerprint confirmation of the server when you update firmware through a remote server. This option is available only if you choose SCP or SFTP as the remote server type. If you chose SCP or SFTP as the remote server type while performing this action, a prompt with the message Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue? Click y or n depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to. • The IPv4 or IPv6 address or the host name of the remote server. • The file path to the SAS expander firmware file on the remote server.

This example updates the SAS expander firmware:

```
Server# scope chassis
Server /chassis # scope sas-expander 1
Server /chassis/sas-expander # show detail
Firmware Image Information:
    ID: 1
    Name: SASEXP1
    Update Stage: NONE
    Update Progress: 0
    Current FW Version: 65103900
    FW Image 1 Version: 65103900
    FW Image 1 State: RUNNING ACTIVATED
    FW Image 2 Version: 65103900
    FW Image 2 State: BACKUP INACTIVATED
Server /chassis/sas-expander # update ftp 192.0.20.34
//upgrade_sas_expander_files/sas-expander-2-0-12a.fw
 <CR>  Press Enter key
Firmware update has started.
```

```
Please check the status using "show detail"
Server /chassis/sas-expander #
```

Activating Installed SAS Expander Firmware

Before You Begin

- You must be logged in as admin to perform this action.
- Install the firmware on the expander.
- Host must be powered on.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters the chassis command mode.
Step 2	Server /chassis # **scope sas-expander {1 | 2}**	Enters the SAS expander command mode.
Step 3	Server /chassis/sas-expander # **activate**	Activates the currently inactive image.
Step 4	At the prompt, enter y to activate the selected firmware image.	

This example activates firmware and then verifies the activation:

```
Server# scope chassis
Server /chassis # scope sas-expander 1
Server /chassis/sas-expander # show detail
 ID: 1
    Name: SASEXP1
    Update Stage: NONE
    Update Progress: 0
    Current FW Version: 65103900
    FW Image 1 Version: 65103900
    FW Image 1 State: RUNNING INACTIVATED
    FW Image 2 Version: 65103900
    FW Image 2 State: BACKUP INACTIVATED

Server /chassis/sas-expander # activate
This operation will activate "65103900" after next host power off
Continue?[y|N] y

Server /chassis/sas-expander # show detail
ID: 1
    Name: SASEXP1
    Update Stage: NONE
    Update Progress: 0
    Current FW Version: 65103900
    FW Image 1 Version: 65103900
    FW Image 1 State: RUNNING ACTIVATED
    FW Image 2 Version: 65103900
    FW Image 2 State: BACKUP INACTIVATED
Server /chassis/sas-expander #
```

Installing SAS Expander Firmware from a Remote Server

Before You Begin

- You must be logged in as admin to perform this action.
- 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 sas-expander {1 | 2}**	Enters the SAS expander command mode.
Step 3	Server /chassis/sas-expander # **show detail**	Displays the available firmware images and status.
Step 4	Server /chassis/sas-expander # **update** *protocol IP_Address path*	It specifies the following: • Protocol, it can be TFTP, FTP, SFTP, SCP or HTTP. **Note** The Cisco UCS C-Series server now supports fingerprint confirmation of the server when you update firmware through a remote server. This option is available only if you choose SCP or SFTP as the remote server type. If you chose SCP or SFTP as the remote server type while performing this action, a prompt with the message Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue? Click y or n depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to. • The IPv4 or IPv6 address or the host name of the remote server. • The file path to the SAS expander firmware file on the remote server.

This example updates the SAS expander firmware:

```
Server# scope chassis
Server /chassis # scope sas-expander 1
Server /chassis/sas-expander # show detail
Firmware Image Information:
    ID: 1
```

```
    Name: SASEXP1
    Update Stage: NONE
    Update Progress: 0
    Current FW Version: 65103900
    FW Image 1 Version: 65103900
    FW Image 1 State: RUNNING ACTIVATED
    FW Image 2 Version: 65103900
    FW Image 2 State: BACKUP INACTIVATED
Server /chassis/sas-expander # update ftp 192.0.20.34
//upgrade_sas_expander_files/sas-expander-2-0-12a.fw
 <CR>  Press Enter key
Firmware update has started.
Please check the status using "show detail"
Server /chassis/sas-expander #
```

Activating Installed SAS Expander Firmware

Before You Begin

- You must be logged in as admin to perform this action.
- Install the firmware on the expander.
- Host must be powered on.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters the chassis command mode.
Step 2	Server /chassis # **scope sas-expander {1 | 2}**	Enters the SAS expander command mode.
Step 3	Server /chassis/sas-expander # **activate**	Activates the currently inactive image.
Step 4	At the prompt, enter y to activate the selected firmware image.	

This example activates firmware and then verifies the activation:

```
Server# scope chassis
Server /chassis # scope sas-expander 1
Server /chassis/sas-expander # show detail
 ID: 1
    Name: SASEXP1
    Update Stage: NONE
    Update Progress: 0
    Current FW Version: 65103900
    FW Image 1 Version: 65103900
    FW Image 1 State: RUNNING INACTIVATED
    FW Image 2 Version: 65103900
    FW Image 2 State: BACKUP INACTIVATED

Server /chassis/sas-expander # activate
This operation will activate "65103900" after next host power off
Continue?[y|N] y

Server /chassis/sas-expander # show detail
ID: 1
```

```
    Name: SASEXP1
    Update Stage: NONE
    Update Progress: 0
    Current FW Version: 65103900
    FW Image 1 Version: 65103900
    FW Image 1 State: RUNNING ACTIVATED
    FW Image 2 Version: 65103900
    FW Image 2 State: BACKUP INACTIVATED
Server /chassis/sas-expander #
```

CHAPTER 15

Viewing Faults and Logs

This chapter includes the following sections:

Fault Summary

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 #
```

Fault History

Viewing the Fault History

Procedure

	Command or Action	Purpose
Step 1	Server # **scope fault**	Enters fault command mode.
Step 2	Server # **show fault-history**	Displays the faults' history.

This example displays the faults' history:

```
Server # scope fault
Server /fault # show fault-history
Time                Severity  Source  Cause                 Description
------------------- --------- ------  --------------------
----------------------------------------
2014 Feb 6 23:24:49 error     %CIMC   PSU_REDUNDANCY-FAIL
"[F0743][major][psu-redundancy-fail].....
2014 Feb 6 23:24:49 error     %CIMC   EQUIPMENT_INOPERABLE
"[F0374][major][equipment-inoperable]...
2014 Feb 6 23:24:19 debug     %CIMC   2014 Feb 6 23        "24:19:7:%CIMC::: SEL INIT DONE"


Server /fault #
```

Cisco IMC Log

Viewing the Cisco IMC Log

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters the Cisco IMC command mode.
Step 2	Server /cimc # **scope log**	Enters the Cisco IMC log command mode.
Step 3	Server /cimc/log # **show entries** [**detail**]	Displays Cisco IMC events, including timestamp, the software module that logged the event, and a description of the event.

This example displays the log of Cisco IMC 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 Cisco IMC Log

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters the Cisco IMC command mode.
Step 2	Server /cimc # **scope log**	Enters the Cisco IMC log command mode.
Step 3	Server /cimc/log # **clear**	Clears the Cisco IMC log.

The following example clears the log of Cisco IMC events:

```
Server# scope cimc
Server /cimc # scope log
Server /cimc/log # clear
```

Configuring the Cisco IMC Log Threshold

You can specify the lowest level of messages that will be included in the Cisco IMC log.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters the Cisco IMC command mode.
Step 2	Server /cimc # **scope log**	Enters the Cisco IMC log command mode.
Step 3	Server /cimc/log # **set local-syslog-severity** *level*	The severity *level* can be one of the following, in decreasing order of severity: • emergency • alert • critical • error • warning • notice • informational • debug **Note** Cisco IMC does not log any messages with a severity below the selected severity. For example, if you select **error**, then the Cisco IMC 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 Cisco IMC Log to a Remote Server

You can configure profiles for one or two remote syslog servers to receive Cisco IMC 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 Cisco IMC command mode.
Step 2	Server /cimc # **scope log**	Enters the Cisco IMC log command mode.
Step 3	Server /cimc/log # **set remote-syslog-severity** *level*	(Optional) The severity *level* can be one of the following, in decreasing order of severity: • emergency • alert • critical • error • warning • notice • informational • debug **Note** Cisco IMC 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 Cisco IMC log messages with the severity Emergency, Alert, Critical, or Error. It will not show Warning, Notice, Informational, or Debug messages.
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.

	Command or Action	Purpose
Step 5	Server /cimc/log/server # **set server-ip** *ipv4 or ipv6 address or domain name*	Specifies the remote syslog server address. **Note** You can set an IPv4 or IPv6 address or a domain name as the remote server address.
Step 6	Server /cimc/log/server # **set server-port** *port number*	Sets the destination port number of the remote syslog server.
Step 7	Server /cimc/log/server # **set enabled** {**yes** | **no**}	Enables the sending of Cisco IMC log entries to this syslog server.
Step 8	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 Cisco IMC 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 1
Server /cimc/log/server *# set server-ip www.abc.com
Server /cimc/log/server *# set server-port 514
Server /cimc/log/server *# set enabled yes
Server /cimc/log/server *# commit
Server /cimc/log/server # exit
Server /cimc/log # show server
Syslog Server 1:
    Syslog Server Address: www.abc.com
    Syslog Server Port: 514
    Enabled: 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
```

Logging Controls

Configuring the Cisco IMC Log Threshold

You can specify the lowest level of messages that will be included in the Cisco IMC log.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters the Cisco IMC command mode.
Step 2	Server /cimc # **scope log**	Enters the Cisco IMC log command mode.
Step 3	Server /cimc/log # **set local-syslog-severity** *level*	The severity *level* can be one of the following, in decreasing order of severity: • emergency • alert • critical • error • warning • notice • informational • debug **Note** Cisco IMC does not log any messages with a severity below the selected severity. For example, if you select **error**, then the Cisco IMC 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 Cisco IMC Log to a Remote Server

You can configure profiles for one or two remote syslog servers to receive Cisco IMC 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 Cisco IMC command mode.
Step 2	Server /cimc # **scope log**	Enters the Cisco IMC log command mode.
Step 3	Server /cimc/log # **set remote-syslog-severity** *level*	(Optional) The severity *level* can be one of the following, in decreasing order of severity: • emergency • alert • critical • error • warning • notice • informational • debug **Note** Cisco IMC 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 Cisco IMC log messages with the severity Emergency, Alert, Critical, or Error. It will not show Warning, Notice, Informational, or Debug messages.
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.

	Command or Action	Purpose
Step 5	Server /cimc/log/server # **set server-ip** *ipv4 or ipv6 address or domain name*	Specifies the remote syslog server address. **Note** You can set an IPv4 or IPv6 address or a domain name as the remote server address.
Step 6	Server /cimc/log/server # **set server-port** *port number*	Sets the destination port number of the remote syslog server.
Step 7	Server /cimc/log/server # **set enabled** {**yes** | **no**}	Enables the sending of Cisco IMC log entries to this syslog server.
Step 8	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 Cisco IMC 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 1
Server /cimc/log/server *# set server-ip www.abc.com
Server /cimc/log/server *# set server-port 514
Server /cimc/log/server *# set enabled yes
Server /cimc/log/server *# commit
Server /cimc/log/server # exit
Server /cimc/log # show server
Syslog Server 1:
    Syslog Server Address: www.abc.com
    Syslog Server Port: 514
    Enabled: yes

Server /cimc/log # show remote-syslog-severity
    Remote Syslog Severity: warning

Server /cimc/log #
```

Sending a Test Cisco IMC Log to a Remote Server

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 Cisco IMC command mode.

	Command or Action	Purpose
Step 2	Server /cimc # **scope log**	Enters the Cisco IMC log command mode.
Step 3	Server /cimc/log # **send-test-syslog**	Sends a test Cisco IMC log to the configured remote servers.

This example shows how to send a test Cisco IMC syslog to the configured remote servers:

```
Server# scope cimc
Server /cimc # scope log
Server /cimc/log # send-test-syslog

Syslog Test message will be sent to configured Syslog destinations.
If no Syslog destinations configured, this command will be silently ignored.
Syslog Test message has been requested.

Server /cimc/log #
```

CHAPTER 16

Server Utilities

This chapter includes the following sections:

Enabling Or Disabling Smart Access USB

When you enable the smart access USB feature, the front panel USB device disconnects from the host operating system and connects to Cisco IMC. After enabling the smart access USB feature, you can use the front panel USB device to export technical support data, import or export Cisco IMC configuration, or update Cisco IMC, BIOS, and VIC firmware.
The supported file systems for smart access USB are as follows:

- EXT2
- EXT3
- EXT 4

- FAT 32
- FAT 16
- DOS

Note Huge file support is not supported in BMC. For EXT 4 file system, huge file support has to be turned off.

Before You Begin

You must be logged in with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server # **scope cimc**	Enters the Cisco IMC command mode.
Step 2	Server /cimc # **scope smart-access-usb**	Enters the smart access USB command mode.
Step 3	Server /cimc/smart-access-usb # **set enabled** { *yes* | *no* }	**set enabled yes** enables smart access USB. **set enabled no** disables the smart access USB. When you enable the smart access usb feature, the front panel USB device disconnects from the host operating system. When you disable the smart access usb feature, the front panel USB device disconnects from CIMC.
Step 4	Server /cimc/smart-access-usb *# **commit**	Commits the transaction to the system.
Step 5	Server /cimc/smart-access-usb # **show detail**	Displays the properties of the smart access USB.

This example shows how to enable smart access USB:

```
Server# scope cimc
Server /cimc # scope smart-access-usb
Server /cimc/smart-access-usb # set enabled yes
Enabling smart-access-usb feature will
disconnect front panel USB devices from
host operating system.
Do you wish to continue? [y/N] y
Server /cimc/smart-access-usb *# commit
Server /cimc/smart-access-usb # show detail
   Enabled: yes
   Storage Device attached: no
Server /cimc/smart-access-usb #
```

This example shows how to disable smart access USB:

```
Server# scope cimc
Server /cimc # scope smart-access-usb
Server /cimc/smart-access-usb # set enabled no
Disabling smart-access-usb feature will
disconnect front panel USB devices from CIMC.
Do you wish to continue? [y/N] y
Server /cimc/smart-access-usb *# commit
```

```
Server /cimc/smart-access-usb # show detail
   Enabled: no
   Storage Device attached: no
Server /cimc/smart-access-usb #
```

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 Cisco IMC 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.
Step 4	Server /cimc/tech-support # **set remote-path** *path/filename*	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** *protocol*	Specifies the protocol to connect to the remote server. It can be of the following types: • TFTP • FTP • SFTP • SCP • HTTP

	Command or Action	Purpose
		Note The Cisco UCS C-Series server now supports fingerprint confirmation of the server when you update firmware through a remote server. This option is available only if you choose SCP or SFTP as the remote server type. If you chose SCP or SFTP as the remote server type while performing this action, a prompt with the message Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue? Click y or n depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.
Step 6	Server /cimc/tech-support # **set remote-username** *name*	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** *password*	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.

Exporting Technical Support Data to Front Panel USB Device

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

- Make sure that the Smart USB option has been enabled and that the USB device is connected to the front panel.
- 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 Cisco IMC command mode.
Step 2	Server /cimc # **scope tech-support**	Enters the tech-support command mode.
Step 3	Server /cimc/tech-support # **scope fp-usb**	Enters the USB mode.
Step 4	Server /cimc/tech-support /fp-usb # **start** *filename*	Creates a technical support data file and transfers the file to a USB device. If you do not specify the file name, it will take a default file name.

This example creates a technical support data file and transfers the file to a USB device connected to the front panel:

```
Server# scope cimc
Server /cimc # scope tech-support
Server /cimc/tech-support # scope fp-usb
Server /cimc/tech-support/fp-usb # start techsupportUSB.tar.gz
Tech Support collection started.

Server /cimc/tech-support/fp-usb # show detail

Tech Support:
  Path(on USB device): techsupportUSB.tar.gz
  Progress(%): 6
  Status: COLLECTING
```

```
Server /cimc/tech-support/fp-usb #
```

What to Do Next

Provide the generated report file to Cisco TAC.

Rebooting the Cisco IMC

On rare occasions, such as an issue with the current running firmware, troubleshooting a server may require you to reboot the Cisco IMC. This procedure is not part of the normal maintenance of a server. After you reboot the Cisco IMC, you are logged off and the Cisco IMC will be unavailable for a few minutes.

Note If you reboot the Cisco IMC 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 Cisco IMC reboot is complete.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters the Cisco IMC command mode.
Step 2	Server /cimc # **reboot**	The Cisco IMC reboots.

This example reboots the Cisco IMC:

```
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.
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 Cisco IMC 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 Cisco IMC to Factory Defaults

On rare occasions, such as an issue with the current running firmware, troubleshooting a server may require you to reset the Cisco IMC 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 Cisco IMC, 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 Cisco IMC 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.

Note If you reset Cisco IMC 1.5(x), 2.0, and 2.0(3) versions to factory defaults, **Shared LOM** mode is configured by default. For C3160 servers, if you reset Cisco IMC to factory defaults, **Dedicated** mode is configured to **Full** duplex with 100 Mbps speed by default.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters the Cisco IMC command mode.
Step 2	Server /cimc # **factory-default**	After a prompt to confirm, the Cisco IMC resets to factory defaults.

The Cisco IMC factory defaults include the following conditions:

- SSH is enabled for access to the Cisco IMC CLI. Telnet is disabled.
- HTTPS is enabled for access to the Cisco IMC GUI.
- A single user account exists (user name is **admin** , password is **password**).
- DHCP is enabled on the management port.
- The previous actual boot order is retained.
- KVM and vMedia are enabled.
- USB is enabled.
- SoL is disabled.

This example resets the Cisco IMC 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]y
Server /cimc #
```

Resetting to Factory Defaults

Resetting to factory defaults will not reset the KMIP related information. You must run the individual restore commands from various KMIP scopes to reset the KMIP settings.

Important When you move VIC adapters from other generation C-Series servers (for example M4 servers) to the M5 generation C-Series servers or M5 servers to other generation servers, you must reset the adapters to factory 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 # **factory-default** {**all** | **bmc** | **storage** | **vic** }	Depending on the component that you choose to rest to factory default, the configuration parameters of that component is restored to factory defaults. You can choose one of the following components: • all—Resets the storage controllers, VIC, and BMC settings to factory defaults. • bmc —Resets the BMC settings to factory defaults. • storage —Resets the storage controller settings to factory default. • vic —Resets the VICs settings to factory default. Enter y at the confirmation prompt to reset the chosen component to default.
Step 3	Server /chassis # **show factory-reset-status**	(Optional) Displays the factory defaults status.

This example resets to factory defaults:

```
Server# scope chassis
Server /chassis # factory-default vic
```

```
his factory-default operation does the following on these components without any back-up:
VIC – all user configured data will deleted and controller properties reset to default values

(Host power-cycle is required for it to be effective)
Storage – all user configured data (including OS VD/drive if any) will be deleted,
controller properties and zoning settings reset to default values (Host power-cycle is
required for it to be effective)
BMC –  all Server BMC configuration reset to factory default values
CMC – all user configured data (including admin password) will be deleted and CMC settings
 reset to default values
Continue?[y|N]y
factory-default for ' vic' started. Please check the status using "show factory-reset-status".
Server /chassis # show factory-reset-status
Storage                              VIC                                  BMC
------------------------------------ ------------------------------------ ----------
NA                                   Pending                              NA
C240-FCH1828V0PN /chassis #
Server /chassis #
```

Exporting and Importing the Cisco IMC Configuration

Exporting the Cisco IMC Configuration

Note

- If any firmware or BIOS updates are in progress, do not export the Cisco IMC configuration until those tasks are complete.
- If you are exporting Cisco IMC configuration to a front panel USB device, make sure that the Smart Access USB option has been enabled.
- For security reasons, this operation does not export user accounts or the server certificate.

Before You Begin

Obtain the backup remote server IP address.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters the Cisco IMC command mode.
Step 2	Server /cimc # **scope import-export**	The configuration file is exported to the specified path and file name on the front panel USB device.
Step 3	Server /cimc/import-export # **export-config** *protocol ip-address path-and-filename*	The configuration file will be stored at the specified path and file name on a remote server at the specified IPv4 or IPv6 address or a hostname. The remote server could be one of the following types: • TFTP • FTP

	Command or Action	Purpose
		• SFTP • SCP • HTTP **Note** The Cisco UCS C-Series server now supports fingerprint confirmation of the server when you update firmware through a remote server. This option is available only if you choose SCP or SFTP as the remote server type. If you chose SCP or SFTP as the remote server type while performing this action, a prompt with the message Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue? Click y or n depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.
Step 4	Server /cimc/import-export # **export-config usb** *path-and-filename*	Exports the configuration data to the connected USB.
Step 5	Enter the Username, Password and Pass Phrase.	Sets the username, password and the pass phrase for the file being exported. Starts the backup operation.

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 Cisco IMC configuration:

```
Server# scope cimc
Server /cimc # scope import-export
Server /cimc/import-export # export-config tftp 192.0.2.34 /ucs/backups/cimc5.xml
Username:pynj
Password:****
Passphrase:***
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 #
```

Exporting and Importing the Cisco IMC Configuration

To perform a backup of the Cisco IMC configuration, you take a snapshot of the system configuration and export the resulting Cisco IMC 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 Cisco IMC configuration file to the same system or you can import it to another Cisco IMC 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 Cisco IMC configuration file is an XML text file whose structure and elements correspond to the Cisco IMC 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.

You can perform an import or an export operation on the following features:

- Cisco IMC version

  Note You can only export this information.

- Network settings
- Technical support
- Logging control for local and remote logs
- Power policies
- BIOS - BIOS Parameters

  Note Precision boot is not supported.

- Communication services
- Remote presence
- User management - LDAP
- Event management
- SNMP

Exporting the Cisco IMC Configuration

Note

- If any firmware or BIOS updates are in progress, do not export the Cisco IMC configuration until those tasks are complete.
- If you are exporting Cisco IMC configuration to a front panel USB device, make sure that the Smart Access USB option has been enabled.
- For security reasons, this operation does not export user accounts or the server certificate.

Before You Begin

Obtain the backup remote server IP address.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters the Cisco IMC command mode.
Step 2	Server /cimc # **scope import-export**	The configuration file is exported to the specified path and file name on the front panel USB device.
Step 3	Server /cimc/import-export # **export-config** *protocol ip-address path-and-filename*	The configuration file will be stored at the specified path and file name on a remote server at the specified IPv4 or IPv6 address or a hostname. The remote server could be one of the following types: • TFTP • FTP • SFTP • SCP • HTTP **Note** The Cisco UCS C-Series server now supports fingerprint confirmation of the server when you update firmware through a remote server. This option is available only if you choose SCP or SFTP as the remote server type. If you chose SCP or SFTP as the remote server type while performing this action, a prompt with the message Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue? Click y or n depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.

	Command or Action	Purpose
Step 4	Server /cimc/import-export # **export-config usb** *path-and-filename*	Exports the configuration data to the connected USB.
Step 5	Enter the Username, Password and Pass Phrase.	Sets the username, password and the pass phrase for the file being exported. Starts the backup operation.

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 Cisco IMC configuration:

```
Server# scope cimc
Server /cimc # scope import-export
Server /cimc/import-export # export-config tftp 192.0.2.34 /ucs/backups/cimc5.xml
Username:pynj
Password:****
Passphrase:***
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 Cisco IMC Configuration

Important

- If any firmware or BIOS updates are in progress, do not import the Cisco IMC configuration until those tasks are complete.
- If you are importing Cisco IMC configuration through a front panel USB device, make sure that the Smart Access USB option has been enabled.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters the Cisco IMC command mode.
Step 2	Server /cimc # **scope import-export**	Enters the import-export command mode.
Step 3	Server /cimc/import-export # **import-config** *protocol ip-address path-and-filename*	The configuration file at the specified path and file name on the remote server at the specified IPv4 or IPv6 address or a hostname will be imported. The remote server can be one of the following: • TFTP

	Command or Action	Purpose
		• FTP • SFTP • SCP • HTTP **Note** The Cisco UCS C-Series server now supports fingerprint confirmation of the server when you update firmware through a remote server. This option is available only if you choose SCP or SFTP as the remote server type. If you chose SCP or SFTP as the remote server type while performing this action, a prompt with the message Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue? Click y or n depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.
Step 4	Server /cimc/import-export # **import-config usb** *path and filename*	The configuration file is imported to the specified path and file name on the front panel USB device.
Step 5	Enter the Username, Password and Pass Phrase.	Sets the username, password and the pass phrase for the file being imported. Starts the import operation.

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 Cisco IMC configuration:

```
Server# scope cimc
Server /cimc # scope import-export
Server /cimc/import-export # import-config tftp 192.0.2.34 /ucs/backups/cimc5.xml
Username:pynj
Password:****
Passphrase:***
Import config started. Please check the status using "show detail".
Server /cimc/import-export # show detail
Import Export:
    Operation: Import
    Status: COMPLETED
    Error Code: 100 (No Error)
    Diagnostic Message: NONE
Server /cimc/import-export #
```

Exporting VIC Adapter Configuration

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

Procedure

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters the chassis command mode.
Step 2	Server /chassis # **export-all-adapters** *protocol ip-address path-and-filename*	The configuration file at the specified path and file name on the remote server at the specified IPv4 or IPv6 address or a hostname will be imported. The remote server can be one of the following: • TFTP • FTP • SFTP • SCP • HTTP **Note** The Cisco UCS C-Series server now supports fingerprint confirmation of the server when you update firmware through a remote server. This option is available only if you choose SCP or SFTP as the remote server type. If you chose SCP or SFTP as the remote server type while performing this action, a prompt with the message Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue? Click y or n depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.

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 export a VIC adapter configuration:

```
Server# scope chassis
Server /chassis # export-all-adapters tftp 10.10.10.10 /ucs/backups/cfdes.xml
Do you wish to continue? [y/N]y
Username: draf
Password:
Export config for all Adapters is triggered. Please check status using show adapter-ie-status
 detail.
Server /chassis # show adapter-ie-status detail
All VIC Import Export:
    Operation: ALL-VIC-EXPORT
```

```
    Status: COMPLETED
    Error Code: 100 (No Error)
    Diagnostic Message: NONE
Server /chassis #
```

Importing VIC Adapter Configuration

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

Procedure

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters the chassis command mode.
Step 2	Server /chassis # **import-all-adapters** *protocol ip-address path-and-filename*	The configuration file at the specified path and file name on the remote server at the specified IPv4 or IPv6 address or a hostname will be imported. The remote server can be one of the following: • TFTP • FTP • SFTP • SCP • HTTP **Note** The Cisco UCS C-Series server now supports fingerprint confirmation of the server when you update firmware through a remote server. This option is available only if you choose SCP or SFTP as the remote server type. If you chose SCP or SFTP as the remote server type while performing this action, a prompt with the message Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue? Click y or n depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.
Step 3	Enter the username, and password.	Starts the import operation.

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 the VIC adapter configuration:

```
Server# scope chassis
Server /chassis # import-all-adapters tftp 10.10.10.10 /ucs/backups/cfdes.xml
```

```
Do you wish to continue? [y/N]y
Username: gdts
Password:
Import config for all Adapters is triggered. Please check status using show adapter-ie-status
 detail.
Server /chassis # show adapter-ie-status detail
All VIC Import Export:
    Operation: ALL-VIC-IMPORT
    Status: COMPLETED
    Error Code: 100 (No Error)
    Diagnostic Message: NONE
Server /chassis #
```

Adding Cisco IMC Banner

Procedure

	Command or Action	Purpose
Step 1	Server # **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **upload-banner**	A prompt to enter the banner displays.
Step 3	Enter the banner and press CTRL+D.	At the prompt, enter y. This results in a loss of the current session, when you log back on again, the new banner appears.
Step 4	Server /chassis # **show-banner**	(Optional) The banner that you have added displays.

This example shows how to add the Cisco IMC banner:

```
Server # scope chassis
Server /chassis # upload-banner
Please paste your custom banner here, when finished, press enter and CTRL+D.
hello world
This will terminate all open SSH session to take an immediate action.
Do you wish to continue? [y/N] yy
Server /chassis # show-banner
hello world
Server /chassis #
```

Deleting Cisco IMC Banner

Procedure

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

	Command or Action	Purpose
Step 2	Server /chassis # **delete-banner**	At the prompt, enter y. This results in a loss of the current session, when you log back on again, the banner is deleted.
Step 3	Server /chassis # **show-banner**	(Optional) The banner that you have added displays.

This example shows how to delete the Cisco IMC banner:

```
Server # scope chassis
Server /chassis # delete-banner
This will terminate all open SSH session to take an immediate action.
Do you wish to continue? [y/N] yy
Server /chassis # show-banner

Server /chassis #
```

Enabling Secure Adapter Update

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters the Cisco IMC command mode.
Step 2	Server /cimc # **scope adapter-secure-update**	Enters the adapter-secure-update command mode.
Step 3	Server /cimc/adapter-secure-update # **enable-security-version-check** {**yes** | **no**}	Enter yes at the prompt. **Note** If you enter no at the prompt, secure adapter update is disabled.
Step 4	Server /cimc/adapter-secure-update # **enable-security-version-check status**	(Optional) Displays the secure update status.

This example shows how to enable the secure adapter update:

```
Server# scope cimc
Server /cimc # scope adapter-secure-update
Server /cimc/adapter-secure-update # enable-security-version-check yes
Server /cimc/adapter-secure-update # enable-security-version-check status
enable-security-version-check: Enabled
Server /cimc/adapter-secure-update #
```

Downloading and Viewing Inventory Details

You can retrieve and save in a file, the following inventory details from the Web UI:

- System Properties
- CPU Information
- Power supply unit inventory
- PCI adapters Cards
- Memory Details
- Trusted Platform Module information
- Disk Information
- Network interface card
- Storage adapter card
- Virtual interface card
- Fan status
- Flex flash card
- BBU Status

Procedure

	Command or Action	Purpose
Step 1	Server # **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **inventory-refresh**	Initiates the data collection activity and saves the data in a file.
Step 3	Server /chassis # **inventory-all**	Displays inventory information.

This example shows the inventory details and the status of inventory collection :

```
Server# scope chassis
Server /chassis #inventory-refresh

Inventory data collection started.

Server /chassis #inventory-all

Hardware Inventory Information:
Status: IN-PROGRESS
Progress(%): 5
...
Progress(%): 50
sysProductName: UCS C240 M3S
sysProductID: UCSC-C240-M3S
sysSerialNum: FCH1925V21U
...
CPU
```

```
id: 1
SocketDesignation: CPU1
ProcessorManufacturer: Intel(R) Corporation
ProcessorFamily: Xeon
ThreadCount: 4
Server /chassis #
```

APPENDIX A

BIOS Parameters by Server Model

This appendix contains the following sections:

C22 and C24 Servers

Main BIOS Parameters for C22 and C24 Servers

Name	Description
TPM Support **set TPMAdminCtrl**	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: • **Disabled**—The server does not use the TPM. • **Enabled**—The server uses the TPM. **Note** We recommend that you contact your operating system vendor to make sure the operating system supports this feature.

Advanced BIOS Parameters for C22 and C24 Servers

Processor Configuration Parameters

Name	Description
Intel Hyper-Threading Technology **set IntelHyperThread**	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: • **Disabled—**The processor does not permit hyperthreading. • **Enabled—**The processor allows for the parallel execution of multiple threads. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.
Number of Enabled Cores **set CoreMultiProcessing**	Allows you to disable one or more of the physical cores on the server. This can be one of the following: • **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. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.
Execute Disable **set ExecuteDisable**	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: • **Disabled—**The processor does not classify memory areas. • **Enabled—**The processor classifies memory areas. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.

Name	Description
Intel VT **set IntelVT**	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: • **Disabled—**The processor does not permit virtualization. • **Enabled—**The processor allows multiple operating systems in independent partitions. **Note** If you change this option, you must power cycle the server before the setting takes effect.
Intel VT-d **set IntelVTD**	Whether the processor uses Intel Virtualization Technology for Directed I/O (VT-d). This can be one of the following: • **Disabled—**The processor does not use virtualization technology. • **Enabled—**The processor uses virtualization technology.
Intel VT-d Coherency Support **set CoherencySupport**	Whether the processor supports Intel VT-d Coherency. This can be one of the following: • **Disabled—**The processor does not support coherency. • **Enabled—**The processor uses VT-d Coherency as required.
Intel VT-d ATS Support **set ATS**	Whether the processor supports Intel VT-d Address Translation Services (ATS). This can be one of the following: • **Disabled—**The processor does not support ATS. • **Enabled—**The processor uses VT-d ATS as required.

Name	Description
CPU Performance **set CPUPerformance**	Sets the CPU performance profile for the server. The performance profile consists of the following options: • DCU Streamer Prefetcher • DCU IP Prefetcher • Hardware Prefetcher • Adjacent Cache-Line Prefetch This can be one of the following: • **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**	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: • **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**	Whether the processor fetches cache lines in even/odd pairs instead of fetching just the required line. This can be one of the following: • **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**	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: • **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**	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: • **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**	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: • **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**	Enables you to configure the CPU power management settings for the following options: • Enhanced Intel Speedstep Technology • Intel Turbo Boost Technology • Processor Power State C6 Power Technology can be one of the following: • **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**	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: • **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. We recommend that you contact your operating system vendor to make sure the operating system supports this feature. **Note** **CPUPowerManagement** must be set to **Custom** or the server ignores the setting for this parameter.

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: • **Disabled**—The processor does not increase its frequency automatically. • **Enabled**—The processor utilizes Turbo Boost Technology if required. **Note** **CPUPowerManagement** must be set to **Custom** or the server ignores the setting for this parameter.
Processor Power State C6 **set ProcessorC6Report**	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: • **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. **Note** **CPUPowerManagement** must be set to **Custom** or the server ignores the setting for this parameter.
Processor Power State C1 Enhanced **set ProcessorC1EReport**	Whether the CPU transitions to its minimum frequency when entering the C1 state. This can be one of the following: • **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**	Whether the CPU is allowed to drop below the maximum non-turbo frequency when idle. This can be one of the following: • **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**	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. • **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. **Note** **CPUPowerManagement** must be set to **Custom** or the server ignores the setting for this parameter.
Energy Performance **set CpuEngPerfBias**	Allows you to determine whether system performance or energy efficiency is more important on this server. This can be one of the following: • **Balanced_Energy** • **Balanced_Performance** • **Energy_Efficient** • **Performance**

Memory Configuration Parameters

Name	Description
Select Memory RAS **set SelectMemoryRAS**	How the memory reliability, availability, and serviceability (RAS) is configured for the server. This can be one of the following: • **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**	Allows you to tune the system settings between the memory bandwidth and power consumption. This can be one of the following: • **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**	Whether the BIOS supports Non-Uniform Memory Access (NUMA). This can be one of the following: • **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**	Whether the system prioritizes low voltage or high frequency memory operations. This can be one of the following: • **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**	Allows you to set the rate at which the DRAM cells are refreshed. This can be one of the following: • **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**	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: • **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**	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: • **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**	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: • **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**	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: • **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**	The approximate number of meters above sea level at which the physical server is installed. This can be one of the following: • **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 Select **set QPILinkFrequency**	The Intel QuickPath Interconnect (QPI) link frequency, in gigatransfers per second (GT/s). This can be one of the following: • **Auto**—The CPU determines the QPI link frequency. • **6.4_GT/s** • **7.2_GT/s** • **8.0_GT/s**

Name	Description
QPI Snoop Mode **set QpiSnoopMode**	The Intel QuickPath Interconnect (QPI) snoop mode. This can be one of the following: • **Auto**—The CPU automatically recognizes this as Early Snoop mode. • **Early Snoop**— The distributed cache ring stops can send a snoop probe or a request to another caching agent directly. This mode has lower latency and it is best for workloads that have shared data sets across threads and can benefit from a cache-to-cache transfer, or for workloads that are not NUMA optimized. • **Home Snoop**— The snoop is always spawned by the home agent (centralized ring stop) for the memory controller. This mode has a higher local latency than early snoop, but it provides extra resources for a larger number of outstanding transactions. • **Home Directory Snoop**— The home directory is an optional enabled feature that is implemented at both the HA and iMC logic in the processor. The goal of the directory is to filter snoops to the remote sockets and a node controller in scalable platforms and 2S and 4S configurations. • **Home Directory Snoop with OSB**— In the Opportunistic Snoop Broadcast (OSB) directory mode, the HA could choose to do speculative home snoop broadcast under very lightly loaded conditions even before the directory information has been collected and checked.

Onboard Storage Parameters

Name	Description
Onboard SCU Storage Support **set DisableSCU**	Whether the onboard software RAID controller is available to the server. This can be one of the following: • **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**	Whether the system supports legacy USB devices. This can be one of the following: • **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**	Whether the system supports 60h/64h emulation for complete USB keyboard legacy support. This can be one of the following: • **Disabled**—60h/64 emulation is not supported. • **Enabled**—60h/64 emulation is supported. You should select this option if you are using a non-USB aware operating system on the server.
All USB Devices **set AllUsbDevices**	Whether all physical and virtual USB devices are enabled or disabled. This can be one of the following: • **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: • **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: • **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: • **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: • **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: • **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 MMIO above 4GB or not. This can be one of the following: • **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**	Allows you to set the level of ASPM (Active Power State Management) support in the BIOS. This can be one of the following: • **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**	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: • **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. **Note** The vKVM does not function when the onboard VGA is disabled.

Serial Configuration Parameters

Name	Description
Console Redirection **set ConsoleRedir**	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: • **Disabled—**No console redirection occurs during POST. • **Enabled—**Enables console redirection on serial port A during POST.
Terminal Type **set TerminalType**	What type of character formatting is used for console redirection. This can be one of the following: • **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. **Note** This setting must match the setting on the remote terminal application.

Name	Description
Bits per second **set BaudRate**	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: • **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. **Note** This setting must match the setting on the remote terminal application.
Flow Control **set FlowCtrl**	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: • **None**—No flow control is used. • **Hardware_RTS/CTS**—RTS/CTS is used for flow control. **Note** This setting must match the setting on the remote terminal application.
Putty KeyPad **set PuttyFunctionKeyPad**	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: • **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: • **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: • **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: • **Disabled—**All LOM ports are disabled. • **Enabled—**All LOM ports are enabled.
LOM Port *n* OptionROM **set LomOpromControlPort*n***	Whether Option ROM is available on the LOM port designated by ***n***. This can be one of the following: • **Disabled—**Option ROM is not available on LOM port ***n***. • **Enabled—**Option ROM is available on LOM port ***n***. • **UEFI_Only—**The expansion slot ***n*** is available for UEFI only. • **Legacy_Only—**The expansion slot ***n*** is available for legacy only.

Name	Description
All PCIe Slots OptionROM **set PcieOptionROMs**	Whether the server can use Option ROM present in the PCIe Cards. This can be one of the following: • **Disabled—**The Option ROM for all PCIe slots are not available. • **Enabled—**The Option ROMs for all the PCIe slots are available. • **UEFI_Only—**The Opiton ROMs for slot ***n*** are available for UEFI only. • **Legacy_Only—**The Option ROM for slot ***n*** are available for legacy only.
PCIe Slot:*n* OptionROM **set Slot-*n*-ROM**	Whether the server can use the Option ROMs present in the PCIe Cards. This can be one of the following: • **Disabled—**The Option ROM for slot ***n*** is not available. • **Enabled—**The Option ROM for slot ***n*** is available. • **UEFI_Only—**The Option ROM for slot ***n*** is available for UEFI only. • **Legacy_Only—**The Option ROM for slot ***n*** is available for legacy only.
PCIe Slot:*n* Link Speed **PCIe Slot:*n*LinkSpeed**	This option allows you to restrict the maximum speed of an adapter card installed in PCIe slot ***n***. This can be one of the following: • **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. 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.

Name	Description
CDN Support for LOM **set CdnSupport**	Whether the Ethernet Network naming convention is according to Consistent Device Naming (CDN) or the traditional way of naming conventions. This can be one of the following: • **Disabled—** OS Ethernet Networking Identifier is named in a default convention as ETH0, ETH1 and so on. By default, CDN option is disabled. • **LOMS Only—** OS Ethernet Network identifier is named in a consistent device naming (CDN) according to the physical LAN on Motherboard(LOM) port numbering; LOM Port 0, LOM Port 1 and so on. **Note** CDN is enabled for LOM ports and works with Windows 2012 or the latest OS only.
CDN Support for VIC **set CdnEnable**	Whether the Ethernet Network naming convention is according to Consistent Device Naming (CDN) or the traditional way of naming conventions. This can be one of the following: • **Disabled—** CDN support for VIC cards is disabled. • **Enabled—** CDN support is enabled for VIC cards. **Note** CDN support for VIC cards work with Windows 2012 or the latest OS only.

Server Management BIOS Parameters for C22 and C24 Servers

Name	Description
FRB-2 Timer **set FRB-2**	Whether the FRB2 timer is used by Cisco IMC to recover the system if it hangs during POST. This can be one of the following: • **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**	Whether the BIOS programs the watchdog timer with a specified timeout value. This can be one of the following: • **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 Cisco IMC logs an error and takes the action specified by the **set OSBootWatchdogTimerPolicy** command.
OS Watchdog Timer Timeout **set OSBootWatchdogTimerTimeOut**	If OS does not boot within the specified time, OS watchdog timer expires and system takes action according to timer policy. This can be one of the following: • **5_Minutes—**The OS watchdog timer expires 5 minutes after it begins to boot. • **10_Minutes—**The OS watchdog timer expires 10 minutes after it begins to boot. • **15_Minutes—**The OS watchdog timer expires 15 minutes after it begins to boot. • **20_Minutes—**The OS watchdog timer expires 20 minutes after it begins to boot. **Note** This option is only applicable if you enable the OS Boot Watchdog Timer.
OS Watchdog Timer Policy **set OSBootWatchdogTimerPolicy**	What action the system takes if the watchdog timer expires. This can be one of the following: • **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. **Note** This option is only applicable if you enable the OS Boot Watchdog Timer.

C220 and C240 Servers

Main BIOS Parameters for C220 and C240 Servers

Name	Description
TPM Support **set TPMAdminCtrl**	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: • **Disabled**—The server does not use the TPM. • **Enabled**—The server uses the TPM. **Note** We recommend that you contact your operating system vendor to make sure the operating system supports this feature.

Advanced BIOS Parameters for C220 and C240 Servers

Processor Configuration Parameters

Name	Description
Intel Hyper-Threading Technology **set IntelHyperThread**	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: • **Disabled**—The processor does not permit hyperthreading. • **Enabled**—The processor allows for the parallel execution of multiple threads. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.

Name	Description
Number of Enabled Cores **set CoreMultiProcessing**	Allows you to disable one or more of the physical cores on the server. This can be one of the following: • **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. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.
Execute Disable **set ExecuteDisable**	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: • **Disabled**—The processor does not classify memory areas. • **Enabled**—The processor classifies memory areas. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.
Intel VT **set IntelVT**	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: • **Disabled**—The processor does not permit virtualization. • **Enabled**—The processor allows multiple operating systems in independent partitions. **Note** If you change this option, you must power cycle the server before the setting takes effect.
Intel VT-d **set IntelVTD**	Whether the processor uses Intel Virtualization Technology for Directed I/O (VT-d). This can be one of the following: • **Disabled**—The processor does not use virtualization technology. • **Enabled**—The processor uses virtualization technology.

Name	Description
Intel VT-d Coherency Support **set CoherencySupport**	Whether the processor supports Intel VT-d Coherency. This can be one of the following: • **Disabled—**The processor does not support coherency. • **Enabled—**The processor uses VT-d Coherency as required.
Intel VT-d ATS Support **set ATS**	Whether the processor supports Intel VT-d Address Translation Services (ATS). This can be one of the following: • **Disabled—**The processor does not support ATS. • **Enabled—**The processor uses VT-d ATS as required.
CPU Performance **set CPUPerformance**	Sets the CPU performance profile for the server. The performance profile consists of the following options: • DCU Streamer Prefetcher • DCU IP Prefetcher • Hardware Prefetcher • Adjacent Cache-Line Prefetch This can be one of the following: • **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**	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: • **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**	Whether the processor fetches cache lines in even/odd pairs instead of fetching just the required line. This can be one of the following: • **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**	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: • **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**	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: • **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**	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: • **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**	Enables you to configure the CPU power management settings for the following options: • Enhanced Intel Speedstep Technology • Intel Turbo Boost Technology • Processor Power State C6 Power Technology can be one of the following: • **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**	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: • **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. We recommend that you contact your operating system vendor to make sure the operating system supports this feature. **Note** **CPUPowerManagement** must be set to **Custom** or the server ignores the setting for this parameter.

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: • **Disabled**—The processor does not increase its frequency automatically. • **Enabled**—The processor utilizes Turbo Boost Technology if required. **Note** **CPUPowerManagement** must be set to **Custom** or the server ignores the setting for this parameter.
Processor Power State C6 **set ProcessorC6Report**	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: • **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. **Note** **CPUPowerManagement** must be set to **Custom** or the server ignores the setting for this parameter.
Processor Power State C1 Enhanced **set ProcessorC1EReport**	Whether the CPU transitions to its minimum frequency when entering the C1 state. This can be one of the following: • **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**	Whether the CPU is allowed to drop below the maximum non-turbo frequency when idle. This can be one of the following: • **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**	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. • **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. **Note** **CPUPowerManagement** must be set to **Custom** or the server ignores the setting for this parameter.
Energy Performance **set CpuEngPerfBias**	Allows you to determine whether system performance or energy efficiency is more important on this server. This can be one of the following: • **Balanced_Energy** • **Balanced_Performance** • **Energy_Efficient** • **Performance**

Memory Configuration Parameters

Name	Description
Select Memory RAS **set SelectMemoryRAS**	How the memory reliability, availability, and serviceability (RAS) is configured for the server. This can be one of the following: • **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**	Allows you to tune the system settings between the memory bandwidth and power consumption. This can be one of the following: • **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**	Whether the BIOS supports Non-Uniform Memory Access (NUMA). This can be one of the following: • **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**	Whether the system prioritizes low voltage or high frequency memory operations. This can be one of the following: • **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**	Allows you to set the rate at which the DRAM cells are refreshed. This can be one of the following: • **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**	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: • **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**	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: • **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**	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: • **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**	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: • **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**	The approximate number of meters above sea level at which the physical server is installed. This can be one of the following: • **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 Select **set QPILinkFrequency**	The Intel QuickPath Interconnect (QPI) link frequency, in gigatransfers per second (GT/s). This can be one of the following: • **Auto**—The CPU determines the QPI link frequency. • **6.4_GT/s** • **7.2_GT/s** • **8.0_GT/s**

Name	Description
QPI Snoop Mode **set QpiSnoopMode**	The Intel QuickPath Interconnect (QPI) snoop mode. This can be one of the following: • **Auto**—The CPU automatically recognizes this as Early Snoop mode. • **Early Snoop**— The distributed cache ring stops can send a snoop probe or a request to another caching agent directly. This mode has lower latency and it is best for workloads that have shared data sets across threads and can benefit from a cache-to-cache transfer, or for workloads that are not NUMA optimized. • **Home Snoop**— The snoop is always spawned by the home agent (centralized ring stop) for the memory controller. This mode has a higher local latency than early snoop, but it provides extra resources for a larger number of outstanding transactions. • **Home Directory Snoop**— The home directory is an optional enabled feature that is implemented at both the HA and iMC logic in the processor. The goal of the directory is to filter snoops to the remote sockets and a node controller in scalable platforms and 2S and 4S configurations. • **Home Directory Snoop with OSB**— In the Opportunistic Snoop Broadcast (OSB) directory mode, the HA could choose to do speculative home snoop broadcast under very lightly loaded conditions even before the directory information has been collected and checked.

Onboard Storage Parameters

Name	Description
Onboard SCU Storage Support **set DisableSCU**	Whether the onboard software RAID controller is available to the server. This can be one of the following: • **Disabled**—The software RAID controller is not available. • **Enabled**—The software RAID controller is available.
Onboard SCU Storage SW Stack **set PchScuOromSelect**	Allows you to choose a pre-boot software stack for an onboard SCU storage controller. This can be one of the following: • **Intel RSTe(1)** • **LSI SW RAID (0)** **Note** This configuration parameter is valid only for the C220 servers.

USB Configuration Parameters

Name	Description
Legacy USB Support **set LegacyUSBSupport**	Whether the system supports legacy USB devices. This can be one of the following: • **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**	Whether the system supports 60h/64h emulation for complete USB keyboard legacy support. This can be one of the following: • **Disabled**—60h/64 emulation is not supported. • **Enabled**—60h/64 emulation is supported. You should select this option if you are using a non-USB aware operating system on the server.
All USB Devices **set AllUsbDevices**	Whether all physical and virtual USB devices are enabled or disabled. This can be one of the following: • **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: • **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: • **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: • **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: • **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: • **Disabled**—Disables the vMedia devices. • **Enabled**—Enables the vMedia devices.
USB Port: SD Card **set UsbPortSdCard**	Whether the SD card drives are enabled or disabled. This can be one of the following: • **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**	Whether to enable or disable MMIO above 4GB or not. This can be one of the following: • **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. **Note** PCI devices that are 64-bit compliant but use a legacy option ROM may not function correctly with this setting enabled.

Name	Description
MMCFG BASE **set MmcfgBaseSelect**	Sets the low base address for PCIe adapters within 4GB. This can be one of the following: • **1 GB** • **2 GB** • **2.5 GB** • **3 GB** • **Auto—** Automatically sets the low base address for PCIe adapters. **Note** This is valid for C240 servers only.
ASPM Support **set ASPMSupport**	Allows you to set the level of ASPM (Active Power State Management) support in the BIOS. This can be one of the following: • **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**	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: • **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. **Note** The vKVM does not function when the onboard VGA is disabled.

Serial Configuration Parameters

Name	Description
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: • **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.
Console Redirection **set ConsoleRedir**	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: • **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**	What type of character formatting is used for console redirection. This can be one of the following: • **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. **Note** This setting must match the setting on the remote terminal application.

Name	Description
Bits per second **set BaudRate**	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: • **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. **Note** This setting must match the setting on the remote terminal application.
Flow Control **set FlowCtrl**	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: • **None—**No flow control is used. • **Hardware_RTS/CTS—**RTS/CTS is used for flow control. **Note** This setting must match the setting on the remote terminal application.
Putty KeyPad **set PuttyFunctionKeyPad**	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: • **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: • **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
CDN Support for LOM **set CdnSupport**	Whether the Ethernet Network naming convention is according to Consistent Device Naming (CDN) or the traditional way of naming conventions. This can be one of the following: • **Disabled—** OS Ethernet Networking Identifier is named in a default convention as ETH0, ETH1 and so on. By default, CDN option is disabled. • **LOMS Only—** OS Ethernet Network identifier is named in a consistent device naming (CDN) according to the physical LAN on Motherboard(LOM) port numbering; LOM Port 0, LOM Port 1 and so on. **Note** CDN is enabled for LOM ports and works with Windows 2012 or the latest OS only.
CDN Support for VIC **set CdnEnable**	Whether the Ethernet Network naming convention is according to Consistent Device Naming (CDN) or the traditional way of naming conventions. This can be one of the following: • **Disabled—** CDN support for VIC cards is disabled. • **Enabled—** CDN support is enabled for VIC cards. **Note** CDN support for VIC cards work with Windows 2012 or the latest OS only.
All Onboard LOM Ports **set AllLomPortControl**	Whether all LOM ports are enabled or disabled. This can be one of the following: • **Disabled—**All LOM ports are disabled. • **Enabled—**All LOM ports are enabled.

Name	Description
LOM Port *n* OptionROM **set LomOpromControlPort*n***	Whether Option ROM is available on the LOM port designated by ***n***. This can be one of the following: • **Disabled**—The Option ROM for slot ***n*** is not available. • **Enabled**—The Option ROM for slot ***n*** is available. • **UEFI_Only**—The Option ROM for slot ***n*** is available for UEFI only. • **Legacy_Only**—The Option ROM for slot ***n*** is available for legacy only.
All PCIe Slots OptionROM **set PcieOptionROMs**	Whether the server can use Option ROM present in the PCIe Cards. This can be one of the following: • **Disabled**—The Option ROM for slot ***n*** is not available. • **Enabled**—The Option ROM for slot ***n*** is available. • **UEFI_Only**—The Option ROM for slot ***n*** is available for UEFI only. • **Legacy_Only**—The Option ROM for slot ***n*** is available for legacy only.
PCIe Slot:*n* OptionROM **set PcieSlot*n*OptionROM**	Whether the server can use the Option ROMs present in the PCIe Cards. This can be one of the following: • **Disabled**—The Option ROM for slot ***n*** is not available. • **Enabled**—The Option ROM for slot ***n*** is available. • **UEFI_Only**—The Option ROM for slot ***n*** is available for UEFI only. • **Legacy_Only**—The Option ROM for slot ***n*** 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: • **Disabled**—The Option ROM for slot ***n*** is not available. • **Enabled**—The Option ROM for slot ***n*** is available. • **UEFI_Only**—The Option ROM for slot ***n*** is available for UEFI only. • **Legacy_Only**—The Option ROM for slot ***n*** is available for legacy only.

Name	Description
PCIe Slot:*n* Link Speed **PCIe Slot:*n*LinkSpeed**	This option allows you to restrict the maximum speed of an adapter card installed in PCIe slot ***n***. This can be one of the following: • **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. 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.

Server Management BIOS Parameters for C220 and C240 Servers

Name	Description
FRB-2 Timer **set FRB-2**	Whether the FRB2 timer is used by Cisco IMC to recover the system if it hangs during POST. This can be one of the following: • **Disabled—**The FRB2 timer is not used. • **Enabled—**The FRB2 timer is started during POST and used to recover the system if necessary.
OS Watchdog Timer **set OSBootWatchdogTimer**	Whether the BIOS programs the watchdog timer with a specified timeout value. This can be one of the following: • **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 Cisco IMC logs an error and takes the action specified by the **set OSBootWatchdogTimerPolicy** command.

Name	Description
OS Watchdog Timer Timeout **set OSBootWatchdogTimerTimeOut**	If OS does not boot within the specified time, OS watchdog timer expires and system takes action according to timer policy. This can be one of the following: • **5_Minutes—**The OS watchdog timer expires 5 minutes after it begins to boot. • **10_Minutes—**The OS watchdog timer expires 10 minutes after it begins to boot. • **15_Minutes—**The OS watchdog timer expires 15 minutes after it begins to boot. • **20_Minutes—**The OS watchdog timer expires 20 minutes after it begins to boot. **Note** This option is only applicable if you enable the OS Boot Watchdog Timer.
OS Watchdog Timer Policy **set OSBootWatchdogTimerPolicy**	What action the system takes if the watchdog timer expires. This can be one of the following: • **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. **Note** This option is only applicable if you enable the OS Boot Watchdog Timer.

C460 M4 Servers

Main Tab for C460 M4 Servers

Main BIOS Parameters

Name	Description
Reboot Host Immediately checkbox	Upon checking, reboots the host server immediately. You must check the checkbox after saving changes.

Name	Description
TPM Support **set TPMAdminCtrl**	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: • **Disabled—**The server does not use the TPM. • **Enabled—**The server uses the TPM. **Note** We recommend that you contact your operating system vendor to make sure the operating system supports this feature.
Power ON Password Support drop-down	This token requires that you set a BIOS password before using the F2 BIOS configuration. If enabled, password needs to be validated before you access BIOS functions such as IO configuration, BIOS set up, and booting to an operating system using BIOS. It can be one of the following: • **Disabled—**Support is disabled. • **Enabled—**Support is enabled.

Actions Area

Name	Description
Save button	Saves the settings for the BIOS parameter and closes the dialog box. If the **Reboot Host Immediately** check box is checked, the server is rebooted immediately and the new BIOS settings go into effect. Otherwise the changes are saved until the server is manually rebooted.
Reset button	Resets the values for the BIOS parameters on all three tabs to the settings that were in effect when this dialog box was first opened.
Restore Defaults button	Sets the BIOS parameters on all three tabs to their default settings.

Advanced Tab for C460 M4 Servers

Reboot Server Option

If you want your changes applied automatically after you click **Save Changes**, check the **Reboot Host Immediately** check box. Cisco IMC immediately reboots the server and applies your changes.

If you want to apply your changes at a later time, clear the **Reboot Host Immediately** check box. Cisco IMC stores the changes and applies them the next time the server reboots.

Note If there are existing BIOS parameter changes pending, Cisco IMC automatically overwrites the stored values with the current settings when you click **Save Changes**.

Processor Configuration Parameters

Name	Description
Intel Hyper-Threading Technology **set IntelHyperThread**	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: • **Disabled—**The processor does not permit hyperthreading. • **Enabled—**The processor allows for the parallel execution of multiple threads. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.
Number of Enabled Cores **set CoreMultiProcessing**	Allows you to disable one or more of the physical cores on the server. This can be one of the following: • **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. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.
Execute Disable **set ExecuteDisable**	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: • **Disabled—**The processor does not classify memory areas. • **Enabled—**The processor classifies memory areas. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.

Name	Description
Intel VT **set IntelVT**	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: • **Disabled—**The processor does not permit virtualization. • **Enabled—**The processor allows multiple operating systems in independent partitions. **Note** If you change this option, you must power cycle the server before the setting takes effect.
Intel VT-d **set IntelVTD**	Whether the processor uses Intel Virtualization Technology for Directed I/O (VT-d). This can be one of the following: • **Disabled—**The processor does not use virtualization technology. • **Enabled—**The processor uses virtualization technology.
Intel(R) Interrupt Remapping drop-down list **set InterruptRemap**	Whether the processor supports Intel VT-d Interrupt Remapping. This can be one of the following: • **Disabled—**The processor does not support remapping. • **Enabled—**The processor uses VT-d Interrupt Remapping as required.
Intel(R) Passthrough DMA drop-down list **set PassThroughDMA**	Whether the processor supports Intel VT-d Pass-through DMA. This can be one of the following: • **Disabled—**The processor does not support pass-through DMA. • **Enabled—**The processor uses VT-d Pass-through DMA as required.
Intel VT-d Coherency Support **set CoherencySupport**	Whether the processor supports Intel VT-d Coherency. This can be one of the following: • **Disabled—**The processor does not support coherency. • **Enabled—**The processor uses VT-d Coherency as required.
Intel VT-d ATS Support **set ATS**	Whether the processor supports Intel VT-d Address Translation Services (ATS). This can be one of the following: • **Disabled—**The processor does not support ATS. • **Enabled—**The processor uses VT-d ATS as required.

Name	Description
CPU Performance **set CPUPerformance**	Sets the CPU performance profile for the server. The performance profile consists of the following options: • DCU Streamer Prefetcher • DCU IP Prefetcher • Hardware Prefetcher • Adjacent Cache-Line Prefetch This can be one of the following: • **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**	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: • **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**	Whether the processor fetches cache lines in even/odd pairs instead of fetching just the required line. This can be one of the following: • **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**	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: • **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**	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: • **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**	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: • **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**	Enables you to configure the CPU power management settings for the following options: • Enhanced Intel Speedstep Technology • Intel Turbo Boost Technology • Processor Power State C6 Power Technology can be one of the following: • **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**	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: • **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. We recommend that you contact your operating system vendor to make sure the operating system supports this feature. **Note** **CPUPowerManagement** must be set to **Custom** or the server ignores the setting for this parameter.

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: • **Disabled**—The processor does not increase its frequency automatically. • **Enabled**—The processor utilizes Turbo Boost Technology if required. **Note** **CPUPowerManagement** must be set to **Custom** or the server ignores the setting for this parameter.
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: • **Disabled**—BIOS does not send C3 report. • **Enabled**—BIOS sends the C3 report, allowing the OS to transition the processor to the C3 low power state. **Note** **CPUPowerManagement** must be set to **Custom** or the server ignores the setting for this parameter.
Processor C6 Report **set ProcessorC6Report**	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: • **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. **Note** **CPUPowerManagement** must be set to **Custom** or the server ignores the setting for this parameter.
Processor Power State C1 Enhanced **set ProcessorC1EReport**	Whether the CPU transitions to its minimum frequency when entering the C1 state. This can be one of the following: • **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.

Name	Description
P-STATE Coordination **set PsdCoordType**	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. • **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. **Note** **CPUPowerManagement** must be set to **Custom** or the server ignores the setting for this parameter.
SINGLE_PCTL drop-down list **get SinglePCTLEn**	Facilitates single PCTL support for better processor power management. This can be one of the following: • **No** • **Yes**
Config TDP drop-down list **get ConfigTDP**	Allows you to configure the Thermal Design Power (TDP) settings for the system. TDP is the maximum amount of power allowed for running applications without triggering an overheating event. This can be one of the following: • **Disabled—**Disables the TDP settings. This is the default value. • **Enabled—**Enables the TDP settings.
Energy Performance Tuning **set PwrPerfTuning**	Allows you to choose BIOS or Operating System for energy performance bias tuning. This can be one of the following: • **OS—** Chooses OS for energy performance tuning. • **BIOS—** Chooses BIOS for energy performance tuning.

Name	Description
Energy Performance **set CpuEngPerfBias**	Allows you to determine whether system performance or energy efficiency is more important on this server. This can be one of the following: • **Balanced_Energy** • **Balanced_Performance** • **Energy_Efficient** • **Performance**
Package C State Limit **set PackageCStateLimit**	The amount of power available to the server components when they are idle. This can be one of the following: • **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.
Extended APIC **set LocalX2Apic**	Allows you to enable or disable extended APIC support. This can be one of the following: • **XAPIC—**Enables APIC support. • **X2APIC—**Enables APIC and also enables Intel VT-d and Interrupt Remapping .

Name	Description
Workload Configuration **set WorkLdConfig**	Allows you to set a parameter to optimize workload characterization. This can be one of the following: • **Balanced—** Chooses balanced option for optimization. • **I/O Sensitive—** Chooses I/O sensitive option for optimization. **Note** We recommend you to set the workload configuration to **Balanced**.
IIO Error Enable drop-down list **get IohErrorEn**	Allows you to generate the IIO-related errors. This can be one of the following: • **Yes** • **No**

Memory Configuration Parameters

Name	Description
Select Memory RAS **set SelectMemoryRAS**	How the memory reliability, availability, and serviceability (RAS) is configured for the server. This can be one of the following: • **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.

Name	Description
DRAM Clock Throttling **set DRAMClockThrottling**	Allows you to tune the system settings between the memory bandwidth and power consumption. This can be one of the following: • **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.
Low Voltage DDR Mode **set LvDDRMode**	Whether the system prioritizes low voltage or high frequency memory operations. This can be one of the following: • **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.
Closed Loop Therm Throt drop-down list **set closedLoopThermThrotl**	Allows for the support of Closed-Loop Thermal Throttling, which improves reliability and reduces CPU power consumption through the automatic voltage control while the CPUs are in the idle state. This can be one of the following: • **Disabled—**Disables closed loop thermal throttling. • **Enabled—**Enables closed loop thermal throttling. This is the default value.
Channel Interleaving **set ChannelInterLeave**	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: • **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**	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: • **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**	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: • **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**	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: • **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**	The approximate number of meters above sea level at which the physical server is installed. This can be one of the following: • **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 Select **set QPILinkFrequency**	The Intel QuickPath Interconnect (QPI) link frequency, in gigatransfers per second (GT/s). This can be one of the following: • **Auto—**The CPU determines the QPI link frequency. • **6.4_GT/s** • **7.2_GT/s** • **8.0_GT/s**
QPI Snoop Mode **set QpiSnoopMode**	The Intel QuickPath Interconnect (QPI) snoop mode. This can be one of the following: • **Disabled—**Disables the QPI snoop mode. • **Cluster on Die—**Enables Cluster On Die. When enabled LLC is split into two parts with an independent caching agent for each. This helps increase the performance in some workloads. This mode is available only for processors that have 10 or more cores. It is the best mode for highly NUMA optimized workloads. • **Auto—**The CPU automatically recognizes this as Early Snoop mode. This is the default value.

USB Configuration Parameters

Name	Description
Legacy USB Support **set LegacyUSBSupport**	Whether the system supports legacy USB devices. This can be one of the following: • **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**	Whether the system supports 60h/64h emulation for complete USB keyboard legacy support. This can be one of the following: • **Disabled**—60h/64 emulation is not supported. • **Enabled**—60h/64 emulation is supported. You should select this option if you are using a non-USB aware operating system on the server.
All USB Devices **set AllUsbDevices**	Whether all physical and virtual USB devices are enabled or disabled. This can be one of the following: • **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: • **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: Internal **set UsbPortInt**	Whether the internal USB devices are enabled or disabled. This can be one of the following: • **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.

Name	Description
USB Port: KVM **set UsbPortKVM**	Whether the KVM ports are enabled or disabled. This can be one of the following: • **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: • **Disabled**—Disables the vMedia devices. • **Enabled**—Enables the vMedia devices.
xHCI Mode **set PchUsb30Mode**	Whether the xHCI controller legacy support is enabled or disabled. This can be one of the following: • **Disabled**—Disables the xHCI controller legacy support. • **Enabled**—Enables the xHCI controller legacy support.

PCI Configuration Parameters

Name	Description
Memory Mapped I/O Above 4GB **set MemoryMappedIOAbove4GB**	Whether to enable or disable MMIO above 4GB or not. This can be one of the following: • **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. **Note** PCI devices that are 64-bit compliant but use a legacy option ROM may not function correctly with this setting enabled.
SR-IOV Support drop-down list **set SrIov**	Whether SR-IOV (Single Root I/O Virtualization) is enabled or disabled on the server. This can be one of the following: • **Disabled**—SR-IOV is disabled. • **Enabled**—SR-IOV is enabled.

Serial Configuration Parameters

Name	Description
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: • **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.
Console Redirection **set ConsoleRedir**	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: • **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**	What type of character formatting is used for console redirection. This can be one of the following: • **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. **Note** This setting must match the setting on the remote terminal application.

Name	Description
Bits per second **set BaudRate**	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: • **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. **Note** This setting must match the setting on the remote terminal application.
Flow Control **set FlowCtrl**	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: • **None—**No flow control is used. • **Hardware_RTS/CTS—**RTS/CTS is used for flow control. **Note** This setting must match the setting on the remote terminal application.
Putty KeyPad **set PuttyFunctionKeyPad**	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: • **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: • **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
CDN Support for VIC **set CdnEnable**	Whether the Ethernet Network naming convention is according to Consistent Device Naming (CDN) or the traditional way of naming conventions. This can be one of the following: • **Disabled—** CDN support for VIC cards is disabled. • **Enabled—** CDN support is enabled for VIC cards. **Note** CDN support for VIC cards work with Windows 2012 or the latest OS only.
PCI ROM CLP **set PciRomClp**	PCI ROM Command Line Protocol (CLP) controls the execution of different Option ROMs such as PxE and iSCSI that are present in the card. By default, it is disabled. • **Enabled—** Enables you to configure execution of different option ROMs such as PxE and iSCSI for an individual ports separately. • **Disabled—**The default option. You cannot choose different option ROMs. A default option ROM is executed during PCI enumeration.
PCH SATA Mode **set SataModeSelect**	This options allows you to select the PCH SATA mode. This can be one of the following: • **AHCI—**Sets both SATA and sSATA controllers to AHCI mode. • **Disabled—**Disables both SATA and sSATA controllers. • **LSI SW Raid—** Sets both SATA and sSATA controllers to raid mode for LSI SW Raid

Name	Description
All Onboard LOM Ports **set AllLomPortControl**	Whether all LOM ports are enabled or disabled. This can be one of the following: • **Disabled**—All LOM ports are disabled. • **Enabled**—All LOM ports are enabled.
LOM Port *n* OptionROM **set LomOpromControlPort***n*	Whether Option ROM is available on the LOM port designated by ***n***. This can be one of the following: • **Disabled**—The Option ROM for slot ***n*** is not available. • **Enabled**—The Option ROM for slot ***n*** is available. • **UEFI_Only**—The Option ROM for slot ***n*** is available for UEFI only. • **Legacy_Only**—The Option ROM for slot ***n*** is available for legacy only.
All PCIe Slots OptionROM **set PcieOptionROMs**	Whether the server can use Option ROM present in the PCIe Cards. This can be one of the following: • **Disabled**—The Option ROM for slot ***n*** is not available. • **Enabled**—The Option ROM for slot ***n*** is available. • **UEFI_Only**—The Option ROM for slot ***n*** is available for UEFI only. • **Legacy_Only**—The Option ROM for slot ***n*** is available for legacy only.
PCIe Slot:*n* OptionROM **set PcieSlot*n*OptionROM**	Whether the server can use the Option ROMs present in the PCIe Cards. This can be one of the following: • **Disabled**—The Option ROM for slot ***n*** is not available. • **Enabled**—The Option ROM for slot ***n*** is available. • **UEFI_Only**—The Option ROM for slot ***n*** is available for UEFI only. • **Legacy_Only**—The Option ROM for slot ***n*** is available for legacy only.

Name	Description
PCIe Slot:MLOM OptionROM **set PcieSlotMLOMOptionROM**	This options allows you to control the Option ROM execution of the PCIe adapter connected to the MLOM slot. This can be one of the following: • **Enabled—**Executes both legacy and UEFI Option ROM. • **Disabled—**Both legacy and UEFI Option ROM will not be executed. • **UEFI Only—**Executes only UEFI Option ROM. • **Legacy Only—**Executes only Legacy Option ROM.
PCIe Slot:HBA OptionROM **set PcieSlotHBAOptionROM**	This options allows you to control the Option ROM execution of the PCIe adapter connected to the HBA slot. This can be one of the following: • **Enabled—**Executes both legacy and UEFI Option ROM. • **Disabled—**Both legacy and UEFI Option ROM will not be executed. • **UEFI Only—**Executes only UEFI Option ROM. • **Legacy Only—**Executes only Legacy Option ROM.
PCIe Slot:N1 OptionROM **set PcieSlotN1OptionROM**	This options allows you to control the Option ROM execution of the PCIe adapter connected to the SSD:NVMe1 slot. This can be one of the following: • **Enabled—**Executes both legacy and UEFI Option ROM. • **Disabled—**Both legacy and UEFI Option ROM will not be executed. • **UEFI Only—**Executes only UEFI Option ROM. • **Legacy Only—**Executes only Legacy Option ROM.
PCIe Slot:N2 OptionROM **set PcieSlotN2OptionROM**	This options allows you to control the Option ROM execution of the PCIe adapter connected to the SSD:NVMe2 slot. This can be one of the following: • **Enabled—**Executes both legacy and UEFI Option ROM. • **Disabled—**Both legacy and UEFI Option ROM will not be executed. • **UEFI Only—**Executes only UEFI Option ROM. • **Legacy Only—**Executes only Legacy Option ROM.

Name	Description
PCIe Slot:N2 OptionROM **set PcieSlotN2OptionROM**	This options allows you to control the Option ROM execution of the PCIe adapter connected to the SSD:NVMe2 slot. This can be one of the following: • **Enabled**—Executes both legacy and UEFI Option ROM. • **Disabled**—Both legacy and UEFI Option ROM will not be executed. • **UEFI Only**—Executes only UEFI Option ROM. • **Legacy Only**—Executes only Legacy Option ROM.
PCIe Slot:HBA Link Speed **PCIe SlotHBALinkSpeed**	This option allows you to restrict the maximum speed of an adapter card installed in PCIe HBA slot. This can be one of the following: • **Auto**— System selects the maximum speed allowed. • **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.

BIOS Configuration Dialog Box Button Bar

Important The buttons in this dialog box affect all BIOS parameters on all available tabs, not just the parameters on the tab that you are viewing.

Name	Description
Save Changes button	Saves the settings for the BIOS parameters on all three tabs and closes the dialog box. If the **Reboot Host Immediately** check box is checked, the server is rebooted immediately and the new BIOS settings go into effect. Otherwise the changes are saved until the server is manually rebooted.
Reset Values button	Restores the values for the BIOS parameters on all three tabs to the settings that were in effect when this dialog box was first opened.
Restore Defaults button	Sets the BIOS parameters on all three tabs to their default settings.
Cancel button	Closes the dialog box without making any changes.

Server Management Tab for C460 M4 Servers

Reboot Server Option

If you want your changes applied automatically after you click **Save Changes**, check the **Reboot Host Immediately** check box. Cisco IMC immediately reboots the server and applies your changes.

If you want to apply your changes at a later time, clear the **Reboot Host Immediately** check box. Cisco IMC stores the changes and applies them the next time the server reboots.

Note If there are existing BIOS parameter changes pending, Cisco IMC automatically overwrites the stored values with the current settings when you click **Save Changes**.

Server Management BIOS Parameters

Name	Description
FRB-2 Timer **set FRB-2**	Whether the FRB2 timer is used by Cisco IMC to recover the system if it hangs during POST. This can be one of the following: • **Disabled**—The FRB2 timer is not used. • **Enabled**—The FRB2 timer is started during POST and used to recover the system if necessary.
OS Watchdog Timer **set OSBootWatchdogTimer**	Whether the BIOS programs the watchdog timer with a specified timeout value. This can be one of the following: • **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 Cisco IMC logs an error and takes the action specified by the **set OSBootWatchdogTimerPolicy** command.

Name	Description
OS Watchdog Timer Timeout **set OSBootWatchdogTimerTimeOut**	If OS does not boot within the specified time, OS watchdog timer expires and system takes action according to timer policy. This can be one of the following: • **5_Minutes—**The OS watchdog timer expires 5 minutes after it begins to boot. • **10_Minutes—**The OS watchdog timer expires 10 minutes after it begins to boot. • **15_Minutes—**The OS watchdog timer expires 15 minutes after it begins to boot. • **20_Minutes—**The OS watchdog timer expires 20 minutes after it begins to boot. **Note** This option is only applicable if you enable the OS Boot Watchdog Timer.
OS Watchdog Timer Policy **set OSBootWatchdogTimerPolicy**	What action the system takes if the watchdog timer expires. This can be one of the following: • **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. **Note** This option is only applicable if you enable the OS Boot Watchdog Timer.

BIOS Configuration Dialog Box Button Bar

Important The buttons in this dialog box affect all BIOS parameters on all available tabs, not just the parameters on the tab that you are viewing.

Name	Description
Save Changes button	Saves the settings for the BIOS parameters on all three tabs and closes the dialog box. If the **Reboot Host Immediately** check box is checked, the server is rebooted immediately and the new BIOS settings go into effect. Otherwise the changes are saved until the server is manually rebooted.
Reset Values button	Restores the values for the BIOS parameters on all three tabs to the settings that were in effect when this dialog box was first opened.

Name	Description
Restore Defaults button	Sets the BIOS parameters on all three tabs to their default settings.
Cancel button	Closes the dialog box without making any changes.

C220 M4 and C240 M4 Servers

Main Tab for C220M4 and C240M4 Servers

Main BIOS Parameters

Name	Description
Reboot Host Immediately checkbox	Upon checking, reboots the host server immediately. You must check the checkbox after saving changes.
TPM Support **set TPMAdminCtrl**	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: • **Disabled—**The server does not use the TPM. • **Enabled—**The server uses the TPM. **Note** We recommend that you contact your operating system vendor to make sure the operating system supports this feature.
Power ON Password Support drop-down	This token requires that you set a BIOS password before using the F2 BIOS configuration. If enabled, password needs to be validated before you access BIOS functions such as IO configuration, BIOS set up, and booting to an operating system using BIOS. It can be one of the following: • **Disabled—**Support is disabled. • **Enabled—**Support is enabled.

Actions Area

Name	Description
Save button	Saves the settings for the BIOS parameters and closes the dialog box. If the **Reboot Host Immediately** check box is checked, the server is rebooted immediately and the new BIOS settings go into effect. Otherwise the changes are saved until the server is manually rebooted.
Reset button	Resets the values for the BIOS parameters on all three tabs to the settings that were in effect when this dialog box was first opened.
Restore Defaults button	Sets the BIOS parameters on all three tabs to their default settings.

Advanced Tab for C220M4 and C240M4 Servers

Reboot Server Option

If you want your changes applied automatically after you click **Save Changes**, check the **Reboot Host Immediately** check box. Cisco IMC immediately reboots the server and applies your changes.

If you want to apply your changes at a later time, clear the **Reboot Host Immediately** check box. Cisco IMC stores the changes and applies them the next time the server reboots.

Note If there are existing BIOS parameter changes pending, Cisco IMC automatically overwrites the stored values with the current settings when you click **Save Changes**.

Processor Configuration Parameters

Name	Description
Intel Hyper-Threading Technology **set IntelHyperThread**	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: • **Disabled**—The processor does not permit hyperthreading. • **Enabled**—The processor allows for the parallel execution of multiple threads. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.

Name	Description
Number of Enabled Cores **set CoreMultiProcessing**	Allows you to disable one or more of the physical cores on the server. This can be one of the following: • **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. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.
Execute Disable **set ExecuteDisable**	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: • **Disabled**—The processor does not classify memory areas. • **Enabled**—The processor classifies memory areas. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.
Intel VT **set IntelVT**	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: • **Disabled**—The processor does not permit virtualization. • **Enabled**—The processor allows multiple operating systems in independent partitions. **Note** If you change this option, you must power cycle the server before the setting takes effect.
Intel VT-d **set IntelVTD**	Whether the processor uses Intel Virtualization Technology for Directed I/O (VT-d). This can be one of the following: • **Disabled**—The processor does not use virtualization technology. • **Enabled**—The processor uses virtualization technology.

Name	Description
Intel VT-d Interrupt Remapping **set InterruptRemap**	Whether the processor supports Intel VT-d Interrupt Remapping. This can be one of the following: • **Disabled**—The processor does not support remapping. • **Enabled**—The processor uses VT-d Interrupt Remapping 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: • **Disabled**—The processor does not support pass-through DMA. • **Enabled**—The processor uses VT-d Pass-through DMA as required.
Intel VT-d Coherency Support **set CoherencySupport**	Whether the processor supports Intel VT-d Coherency. This can be one of the following: • **Disabled**—The processor does not support coherency. • **Enabled**—The processor uses VT-d Coherency as required.
Intel VT-d ATS Support **set ATS**	Whether the processor supports Intel VT-d Address Translation Services (ATS). This can be one of the following: • **Disabled**—The processor does not support ATS. • **Enabled**—The processor uses VT-d ATS as required.

Name	Description
CPU Performance **set CPUPerformance**	Sets the CPU performance profile for the server. The performance profile consists of the following options: • DCU Streamer Prefetcher • DCU IP Prefetcher • Hardware Prefetcher • Adjacent Cache-Line Prefetch This can be one of the following: • **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**	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: • **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**	Whether the processor fetches cache lines in even/odd pairs instead of fetching just the required line. This can be one of the following: • **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**	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: • **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**	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: • **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**	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: • **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**	Enables you to configure the CPU power management settings for the following options: • Enhanced Intel Speedstep Technology • Intel Turbo Boost Technology • Processor Power State C6 Power Technology can be one of the following: • **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**	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: • **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. We recommend that you contact your operating system vendor to make sure the operating system supports this feature. **Note** **CPUPowerManagement** must be set to **Custom** or the server ignores the setting for this parameter.

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: • **Disabled—**The processor does not increase its frequency automatically. • **Enabled—**The processor utilizes Turbo Boost Technology if required. **Note** **CPUPowerManagement** must be set to **Custom** or the server ignores the setting for this parameter.
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: • **Disabled—**BIOS does not send C3 report. • **Enabled—**BIOS sends the C3 report, allowing the OS to transition the processor to the C3 low power state. **Note** **CPUPowerManagement** must be set to **Custom** or the server ignores the setting for this parameter.
Processor C6 Report **set ProcessorC6Report**	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: • **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. **Note** **CPUPowerManagement** must be set to **Custom** or the server ignores the setting for this parameter.
Processor Power State C1 Enhanced **set ProcessorC1EReport**	Whether the CPU transitions to its minimum frequency when entering the C1 state. This can be one of the following: • **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.

Name	Description
P-STATE Coordination **set PsdCoordType**	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. • **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. **Note** **CPUPowerManagement** must be set to **Custom** or the server ignores the setting for this parameter.
Boot Performance Mode drop-down list **set BootPerformanceMode**	Allows the user to select the BIOS performance state that is set before the operating system handoff. This can be one of the following: • **Max Performance—**Processor P-state ratio is maximum • **Max Efficient—** Processor P-state ratio is minimum
Energy Performance Tuning **set PwrPerfTuning**	Allows you to choose BIOS or Operating System for energy performance bias tuning. This can be one of the following: • **OS—** Chooses OS for energy performance tuning. • **BIOS—** Chooses BIOS for energy performance tuning.
Energy Performance **set CpuEngPerfBias**	Allows you to determine whether system performance or energy efficiency is more important on this server. This can be one of the following: • **Balanced_Energy** • **Balanced_Performance** • **Energy_Efficient** • **Performance**

Name	Description
Package C State Limit **set PackageCStateLimit**	The amount of power available to the server components when they are idle. This can be one of the following: • **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.
Extended APIC **set LocalX2Apic**	Allows you to enable or disable extended APIC support. This can be one of the following: • **XAPIC—**Enables APIC support. • **X2APIC—**Enables APIC and also enables Intel VT-d and Interrupt Remapping .
Workload Configuration **set WorkLdConfig**	Allows you to set a parameter to optimize workload characterization. This can be one of the following: • **Balanced—** Chooses balanced option for optimization. • **I/O Sensitive—** Chooses I/O sensitive option for optimization. **Note** We recommend you to set the workload configuration to **Balanced**.

Name	Description
CPU HWPM drop-down list **set HWPMEnable**	Enables the Hardware Power Management (HWPM) interface for better CPU performance and energy efficiency. This can be one of the following: • **Disabled—**The P-States are controlled the same way as on predecessor processor generations. • **Native Mode—**HWPM works with the operating system through a software interface. • **OOB Mode—**The CPU autonomously controls its frequency based on the operating system energy efficiency.
CPU Autonomous Cstate drop-down list **set AutonumousCstateEnable**	Enables CPU Autonomous C-State, which converts the HALT instructions to the MWAIT instructions. This can be one of the following: • **Disabled—**CPU Autonomous C-state is disabled. This is the default value. • **Enabled—**CPU Autonomous C-state is enabled.
Processor CMCI drop-down list **set CmciEnable**	Allows the CPU to trigger interrupts on corrected machine check events. The corrected machine check interrupt (CMCI) allows faster reaction than the traditional polling timer. This can be one of the following: • **Disabled—**Disables CMCI. • **Enabled—**Enables CMCI. This is the default value.

Memory Configuration Parameters

Name	Description
Select Memory RAS **set SelectMemoryRAS**	How the memory reliability, availability, and serviceability (RAS) is configured for the server. This can be one of the following: • **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.
NUMA **set NUMAOptimize**	Whether the BIOS supports Non-Uniform Memory Access (NUMA). This can be one of the following: • **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.
Channel Interleaving **set ChannelInterLeave**	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: • **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**	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: • **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**	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: • **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**	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: • **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**	The approximate number of meters above sea level at which the physical server is installed. This can be one of the following: • **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 Select **set QPILinkFrequency**	The Intel QuickPath Interconnect (QPI) link frequency, in gigatransfers per second (GT/s). This can be one of the following: • **Auto—**The CPU determines the QPI link frequency. • **6.4_GT/s** • **7.2_GT/s** • **8.0_GT/s**

Name	Description
QPI Snoop Mode **set QpiSnoopMode**	The Intel QuickPath Interconnect (QPI) snoop mode. This can be one of the following: • **Auto—**The CPU automatically recognizes this as Early Snoop mode. • **Early Snoop—**The distributed cache ring stops can send a snoop probe or a request to another caching agent directly. This mode has lower latency and it is best for workloads that have shared data sets across threads and can benefit from a cache-to-cache transfer, or for workloads that are not NUMA optimized. • **Home Snoop—**The snoop is always spawned by the home agent (centralized ring stop) for the memory controller. This mode has a higher local latency than early snoop, but it provides extra resources for a larger number of outstanding transactions. • **Home Directory Snoop—** The home directory is an optional enabled feature that is implemented at both the HA and iMC logic in the processor. The goal of the directory is to filter snoops to the remote sockets and a node controller in scalable platforms and 2S and 4S configurations. • **Home Directory Snoop with OSB—** In the Opportunistic Snoop Broadcast (OSB) directory mode, the HA could choose to do speculative home snoop broadcast under very lightly loaded conditions even before the directory information has been collected and checked. • **Cluster on Die—**Enables Cluster On Die. When enabled LLC is split into two parts with an independent caching agent for each. This helps increase the performance in some workloads. This mode is available only for processors that have 10 or more cores. It is the best mode for highly NUMA optimized workloads.

USB Configuration Parameters

Name	Description
Legacy USB Support **set LegacyUSBSupport**	Whether the system supports legacy USB devices. This can be one of the following: • **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
Port 60/64 Emulation **set UsbEmul6064**	Whether the system supports 60h/64h emulation for complete USB keyboard legacy support. This can be one of the following: • **Disabled**—60h/64 emulation is not supported. • **Enabled**—60h/64 emulation is supported. You should select this option if you are using a non-USB aware operating system on the server.
xHCI Mode **set PchUsb30Mode**	Whether the xHCI controller legacy support is enabled or disabled. This can be one of the following: • **Disabled**—Disables the xHCI controller legacy support. • **Enabled**—Enables the xHCI controller legacy support.
xHCI Legacy Support drop-down list **set UsbXhciSupport**	Whether the system supports legacy xHCI controller. This can be one of the following: • **Disabled**—Disables xHCI legacy support. • **Enabled**—Enables xHCI legacy support. This is the default value.
All USB Devices **set AllUsbDevices**	Whether all physical and virtual USB devices are enabled or disabled. This can be one of the following: • **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: • **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: • **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: • **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: • **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: • **Disabled**—Disables the vMedia devices. • **Enabled**—Enables the vMedia devices.

PCI Configuration Parameters

Name	Description
Memory Mapped I/O Above 4GB **set MemoryMappedIOAbove4GB**	Whether to enable or disable MMIO above 4GB or not. This can be one of the following: • **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. **Note** PCI devices that are 64-bit compliant but use a legacy option ROM may not function correctly with this setting enabled.
Sriov **set SrIov**	Whether SR-IOV (Single Root I/O Virtualization) is enabled or disabled on the server. This can be one of the following: • **Disabled**—SR-IOV is disabled. • **Enabled**—SR-IOV is enabled.

Name	Description
ASPM Support drop-down list **set ASPMSupport**	Allows you to set the level of ASPM (Active Power State Management) support in the BIOS. This can be one of the following: • **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
NVMe SSD Hot-Plug Support drop-down list **set PCIeSSDHotPlugSupport**	Allows you to replace an NVMe SSD without powering down the server. This can be one of the following: • **Disabled—**NVMe SSD hot-plug support is disabled. This is the default value. • **Enabled—**NVMe SSD hot-plug support is enabled.
VGA Priority drop-down list **set VgaPriority**	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: • **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.

Serial Configuration Parameters

Name	Description
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: • **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.

Name	Description
Console Redirection **set ConsoleRedir**	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: • **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**	What type of character formatting is used for console redirection. This can be one of the following: • **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. **Note** This setting must match the setting on the remote terminal application.
Bits per second **set BaudRate**	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: • **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. **Note** This setting must match the setting on the remote terminal application.

Name	Description
Flow Control **set FlowCtrl**	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: • **None—**No flow control is used. • **Hardware_RTS/CTS—**RTS/CTS is used for flow control. **Note** This setting must match the setting on the remote terminal application.
Putty KeyPad **set PuttyFunctionKeyPad**	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: • **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**	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: • **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
CDN Support for VIC **set CdnEnable**	Whether the Ethernet Network naming convention is according to Consistent Device Naming (CDN) or the traditional way of naming conventions. This can be one of the following: • **Disabled—** CDN support for VIC cards is disabled. • **Enabled—** CDN support is enabled for VIC cards. **Note** CDN support for VIC cards work with Windows 2012 or the latest OS only.
PCI ROM CLP **set PciRomClp**	PCI ROM Command Line Protocol (CLP) controls the execution of different Option ROMs such as PxE and iSCSI that are present in the card. By default, it is disabled. • **Enabled—** Enables you to configure execution of different option ROMs such as PxE and iSCSI for an individual ports separately. • **Disabled—**The default option. You cannot choose different option ROMs. A default option ROM is executed during PCI enumeration.
PCH SATA Mode **set SataModeSelect**	This options allows you to select the PCH SATA mode. This can be one of the following: • **AHCI—**Sets both SATA and sSATA controllers to AHCI mode. • **Disabled—**Disables both SATA and sSATA controllers. • **LSI SW Raid—** Sets both SATA and sSATA controllers to raid mode for LSI SW Raid
All Onboard LOM Ports **set AllLomPortControl**	Whether all LOM ports are enabled or disabled. This can be one of the following: • **Disabled—**All LOM ports are disabled. • **Enabled—**All LOM ports are enabled.
LOM Port *n* OptionROM **set LomOpromControlPort*n***	Whether Option ROM is available on the LOM port designated by ***n***. This can be one of the following: • **Disabled—**The Option ROM for slot ***n*** is not available. • **Enabled—**The Option ROM for slot ***n*** is available. • **UEFI_Only—**The Option ROM for slot ***n*** is available for UEFI only. • **Legacy_Only—**The Option ROM for slot ***n*** is available for legacy only.

Name	Description
All PCIe Slots OptionROM **set PcieOptionROMs**	Whether the server can use Option ROM present in the PCIe Cards. This can be one of the following: • **Disabled**—The Option ROM for slot ***n*** is not available. • **Enabled**—The Option ROM for slot ***n*** is available. • **UEFI_Only**—The Option ROM for slot ***n*** is available for UEFI only. • **Legacy_Only**—The Option ROM for slot ***n*** is available for legacy only.
PCIe Slot:*n* OptionROM **set PcieSlot*n*OptionROM**	Whether the server can use the Option ROMs present in the PCIe Cards. This can be one of the following: • **Disabled**—The Option ROM for slot ***n*** is not available. • **Enabled**—The Option ROM for slot ***n*** is available. • **UEFI_Only**—The Option ROM for slot ***n*** is available for UEFI only. • **Legacy_Only**—The Option ROM for slot ***n*** is available for legacy only.
PCIe Slot:MLOM OptionROM **set PcieSlotMLOMOptionROM**	This options allows you to control the Option ROM execution of the PCIe adapter connected to the MLOM slot. This can be one of the following: • **Enabled**—Executes both legacy and UEFI Option ROM. • **Disabled**—Both legacy and UEFI Option ROM will not be executed. • **UEFI Only**—Executes only UEFI Option ROM. • **Legacy Only**—Executes only Legacy Option ROM.
PCIe Slot:HBA OptionROM **set PcieSlotHBAOptionROM**	This options allows you to control the Option ROM execution of the PCIe adapter connected to the HBA slot. This can be one of the following: • **Enabled**—Executes both legacy and UEFI Option ROM. • **Disabled**—Both legacy and UEFI Option ROM will not be executed. • **UEFI Only**—Executes only UEFI Option ROM. • **Legacy Only**—Executes only Legacy Option ROM.

Name	Description
PCIe Slot:N1 OptionROM **set PcieSlotN1OptionROM**	This options allows you to control the Option ROM execution of the PCIe adapter connected to the SSD:NVMe1 slot. This can be one of the following: • **Enabled**—Executes both legacy and UEFI Option ROM. • **Disabled**—Both legacy and UEFI Option ROM will not be executed. • **UEFI Only**—Executes only UEFI Option ROM. • **Legacy Only**—Executes only Legacy Option ROM.
PCIe Slot:N2 OptionROM **set PcieSlotN2OptionROM**	This options allows you to control the Option ROM execution of the PCIe adapter connected to the SSD:NVMe2 slot. This can be one of the following: • **Enabled**—Executes both legacy and UEFI Option ROM. • **Disabled**—Both legacy and UEFI Option ROM will not be executed. • **UEFI Only**—Executes only UEFI Option ROM. • **Legacy Only**—Executes only Legacy Option ROM.
PCIe Slot:HBA Link Speed **PCIe SlotHBALinkSpeed**	This option allows you to restrict the maximum speed of an adapter card installed in PCIe HBA slot. This can be one of the following: • **Auto**— System selects the maximum speed allowed. • **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.

BIOS Configuration Dialog Box Button Bar

Important The buttons in this dialog box affect all BIOS parameters on all available tabs, not just the parameters on the tab that you are viewing.

Name	Description
Save Changes button	Saves the settings for the BIOS parameters on all three tabs and closes the dialog box. If the **Reboot Host Immediately** check box is checked, the server is rebooted immediately and the new BIOS settings go into effect. Otherwise the changes are saved until the server is manually rebooted.
Reset Values button	Restores the values for the BIOS parameters on all three tabs to the settings that were in effect when this dialog box was first opened.
Restore Defaults button	Sets the BIOS parameters on all three tabs to their default settings.
Cancel button	Closes the dialog box without making any changes.

Server Management Tab for C220M4 and C240M4 Servers

Reboot Server Option

If you want your changes applied automatically after you click **Save Changes**, check the **Reboot Host Immediately** check box. Cisco IMC immediately reboots the server and applies your changes.

If you want to apply your changes at a later time, clear the **Reboot Host Immediately** check box. Cisco IMC stores the changes and applies them the next time the server reboots.

Note If there are existing BIOS parameter changes pending, Cisco IMC automatically overwrites the stored values with the current settings when you click **Save Changes**.

Server Management BIOS Parameters

Name	Description
FRB-2 Timer **set FRB-2**	Whether the FRB2 timer is used by Cisco IMC to recover the system if it hangs during POST. This can be one of the following: • **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**	Whether the BIOS programs the watchdog timer with a specified timeout value. This can be one of the following: • **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 Cisco IMC logs an error and takes the action specified by the **set OSBootWatchdogTimerPolicy** command.
OS Watchdog Timer Timeout **set OSBootWatchdogTimerTimeOut**	If OS does not boot within the specified time, OS watchdog timer expires and system takes action according to timer policy. This can be one of the following: • **5_Minutes**—The OS watchdog timer expires 5 minutes after it begins to boot. • **10_Minutes**—The OS watchdog timer expires 10 minutes after it begins to boot. • **15_Minutes**—The OS watchdog timer expires 15 minutes after it begins to boot. • **20_Minutes**—The OS watchdog timer expires 20 minutes after it begins to boot. **Note** This option is only applicable if you enable the OS Boot Watchdog Timer.
OS Watchdog Timer Policy **set OSBootWatchdogTimerPolicy**	What action the system takes if the watchdog timer expires. This can be one of the following: • **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. **Note** This option is only applicable if you enable the OS Boot Watchdog Timer.

BIOS Configuration Dialog Box Button Bar

Important The buttons in this dialog box affect all BIOS parameters on all available tabs, not just the parameters on the tab that you are viewing.

Name	Description
Save Changes button	Saves the settings for the BIOS parameters on all three tabs and closes the dialog box. If the **Reboot Host Immediately** check box is checked, the server is rebooted immediately and the new BIOS settings go into effect. Otherwise the changes are saved until the server is manually rebooted.
Reset Values button	Restores the values for the BIOS parameters on all three tabs to the settings that were in effect when this dialog box was first opened.
Restore Defaults button	Sets the BIOS parameters on all three tabs to their default settings.
Cancel button	Closes the dialog box without making any changes.

C3160 Servers

Main BIOS Parameters for C3160 Servers

Main BIOS Parameters

Name	Description
Reboot Host Immediately checkbox	Upon checking, reboots the host server immediately. You must check the checkbox after saving changes.
TPM Support **set TPMAdminCtrl**	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: • **Disabled**—The server does not use the TPM. • **Enabled**—The server uses the TPM. **Note** We recommend that you contact your operating system vendor to make sure the operating system supports this feature.

Advanced BIOS Parameters for C3160 Servers

Processor Configuration Parameters

Name	Description
Intel Hyper-Threading Technology **set IntelHyperThread**	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: • **Disabled**—The processor does not permit hyperthreading. • **Enabled**—The processor allows for the parallel execution of multiple threads. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.
Number of Enabled Cores **set CoreMultiProcessing**	Allows you to disable one or more of the physical cores on the server. This can be one of the following: • **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. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.
Execute Disable **set ExecuteDisable**	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: • **Disabled**—The processor does not classify memory areas. • **Enabled**—The processor classifies memory areas. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.

Name	Description
Intel VT **set IntelVT**	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: • **Disabled**—The processor does not permit virtualization. • **Enabled**—The processor allows multiple operating systems in independent partitions. **Note** If you change this option, you must power cycle the server before the setting takes effect.
Intel VT-d **set IntelVTD**	Whether the processor uses Intel Virtualization Technology for Directed I/O (VT-d). This can be one of the following: • **Disabled**—The processor does not use virtualization technology. • **Enabled**—The processor uses virtualization technology.
Intel VT-d Coherency Support **set CoherencySupport**	Whether the processor supports Intel VT-d Coherency. This can be one of the following: • **Disabled**—The processor does not support coherency. • **Enabled**—The processor uses VT-d Coherency as required.
Intel VT-d ATS Support **set ATS**	Whether the processor supports Intel VT-d Address Translation Services (ATS). This can be one of the following: • **Disabled**—The processor does not support ATS. • **Enabled**—The processor uses VT-d ATS as required.

Name	Description
CPU Performance **set CPUPerformance**	Sets the CPU performance profile for the server. The performance profile consists of the following options: • DCU Streamer Prefetcher • DCU IP Prefetcher • Hardware Prefetcher • Adjacent Cache-Line Prefetch This can be one of the following: • **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**	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: • **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**	Whether the processor fetches cache lines in even/odd pairs instead of fetching just the required line. This can be one of the following: • **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**	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: • **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**	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: • **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**	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: • **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**	Enables you to configure the CPU power management settings for the following options: • Enhanced Intel Speedstep Technology • Intel Turbo Boost Technology • Processor Power State C6 Power Technology can be one of the following: • **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**	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: • **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. We recommend that you contact your operating system vendor to make sure the operating system supports this feature. **Note** **CPUPowerManagement** must be set to **Custom** or the server ignores the setting for this parameter.

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: • **Disabled—**The processor does not increase its frequency automatically. • **Enabled—**The processor utilizes Turbo Boost Technology if required. **Note** **CPUPowerManagement** must be set to **Custom** or the server ignores the setting for this parameter.
Processor Power State C6 **set ProcessorC6Report**	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: • **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. **Note** **CPUPowerManagement** must be set to **Custom** or the server ignores the setting for this parameter.
Processor Power State C1 Enhanced **set ProcessorC1EReport**	Whether the CPU transitions to its minimum frequency when entering the C1 state. This can be one of the following: • **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**	Whether the CPU is allowed to drop below the maximum non-turbo frequency when idle. This can be one of the following: • **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**	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. • **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. **Note** **CPUPowerManagement** must be set to **Custom** or the server ignores the setting for this parameter.
Energy Performance **set CpuEngPerfBias**	Allows you to determine whether system performance or energy efficiency is more important on this server. This can be one of the following: • **Balanced_Energy** • **Balanced_Performance** • **Energy_Efficient** • **Performance**

Memory Configuration Parameters

Name	Description
Select Memory RAS **set SelectMemoryRAS**	How the memory reliability, availability, and serviceability (RAS) is configured for the server. This can be one of the following: • **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**	Allows you to tune the system settings between the memory bandwidth and power consumption. This can be one of the following: • **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**	Whether the BIOS supports Non-Uniform Memory Access (NUMA). This can be one of the following: • **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**	Whether the system prioritizes low voltage or high frequency memory operations. This can be one of the following: • **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**	Allows you to set the rate at which the DRAM cells are refreshed. This can be one of the following: • **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**	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: • **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**	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: • **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**	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: • **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**	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: • **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**	The approximate number of meters above sea level at which the physical server is installed. This can be one of the following: • **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 Select **set QPILinkFrequency**	The Intel QuickPath Interconnect (QPI) link frequency, in gigatransfers per second (GT/s). This can be one of the following: • **Auto—**The CPU determines the QPI link frequency. • **6.4_GT/s** • **7.2_GT/s** • **8.0_GT/s**

SATA Configuration Parameters

Name	Description
SATA Mode **set SataMode**	Mode of operation of Serial Advanced Technology Attachment (SATA) Solid State Drives (SSD). • **Disabled—** All SATA ports is disabled, and drivers are not enumerated. • **IDE Mode—** Mode of operation follows previous hardware standards of Integrated Drive Electronics (IDE) interface • **AHCI Mode—**The default mode. Drives operate according to newer standard of Advance Host Controller Interface(AHCI).

USB Configuration Parameters

Name	Description
Legacy USB Support **set LegacyUSBSupport**	Whether the system supports legacy USB devices. This can be one of the following: • **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**	Whether the system supports 60h/64h emulation for complete USB keyboard legacy support. This can be one of the following: • **Disabled**—60h/64 emulation is not supported. • **Enabled**—60h/64 emulation is supported. You should select this option if you are using a non-USB aware operating system on the server.
All USB Devices **set AllUsbDevices**	Whether all physical and virtual USB devices are enabled or disabled. This can be one of the following: • **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: • **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: Internal **set UsbPortInt**	Whether the internal USB devices are enabled or disabled. This can be one of the following: • **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.

Name	Description
USB Port: KVM **set UsbPortKVM**	Whether the KVM ports are enabled or disabled. This can be one of the following: • **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: • **Disabled—**Disables the vMedia devices. • **Enabled—**Enables the vMedia devices.

PCI Configuration Parameters

Name	Description
PCI ROM CLP **set PciRomClp**	PCI ROM Command Line Protocol (CLP) controls the execution of different Option ROMs such as PxE and iSCSI that are present in the card. By default, it is disabled. • **Enabled—** Enables you to configure execution of different option ROMs such as PxE and iSCSI for an individual ports separately. • **Disabled—**The default option. You cannot choose different option ROMs. A default option ROM is executed during PCI enumeration.
ASPM Support **set ASPMSupport**	Allows you to set the level of ASPM (Active Power State Management) support in the BIOS. This can be one of the following: • **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.

Serial Configuration Parameters

Name	Description
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: • **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.
Console Redirection **set ConsoleRedir**	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: • **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**	What type of character formatting is used for console redirection. This can be one of the following: • **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. **Note** This setting must match the setting on the remote terminal application.

Name	Description
Bits per second **set BaudRate**	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: • **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. **Note** This setting must match the setting on the remote terminal application.
Flow Control **set FlowCtrl**	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: • **None—**No flow control is used. • **Hardware_RTS/CTS—**RTS/CTS is used for flow control. **Note** This setting must match the setting on the remote terminal application.
Putty KeyPad **set PuttyFunctionKeyPad**	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: • **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: • **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
CDN Support for VIC **set CdnEnable**	Whether the Ethernet Network naming convention is according to Consistent Device Naming (CDN) or the traditional way of naming conventions. This can be one of the following: • **Disabled**— OS Ethernet Networking Identifier is named in a default convention as ETH0, ETH1 and so on. By default, CDN option is disabled. • **LOMS Only**— OS Ethernet Network identifier is named in a consistent device naming (CDN) according to the physical LAN on Motherboard(LOM) port numbering; LOM Port 0, LOM Port 1 and so on. **Note** CDN is enabled for LOM ports and works with Windows 2012 or the latest OS only.
All PCIe Slots OptionROM **set PcieOptionROMs**	Whether the server can use Option ROM present in the PCIe Cards. This can be one of the following: • **Disabled**—The Option ROM for all PCIe slots are not available. • **Enabled**—The Option ROMs for all the PCIe slots are available. • **UEFI_Only**—The Opiton ROMs for slot ***n*** are available for UEFI only. • **Legacy_Only**—The Option ROM for slot ***n*** are available for legacy only.

Name	Description
PCIe Slot:*n* OptionROM **set PcieSlot*n*OptionROM**	Whether the server can use the Option ROMs present in the PCIe Cards. This can be one of the following: • **Disabled**—The Option ROM for slot ***n*** is not available. • **Enabled**—The Option ROM for slot ***n*** is available. • **UEFI_Only**—The Option ROM for slot ***n*** is available for UEFI only. • **Legacy_Only**—The Option ROM for slot ***n*** 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: • **Disabled**— The Option ROM for slot ***M*** is not available. • **Enabled**— The Option ROM for slot ***M*** is available. • **UEFI_Only**—The Option ROM for slot ***M*** is available for UEFI only. • **Legacy_Only**—The expansion slot for slot ***M*** is available for legacy only.
SIOC1 Link Speed **Set PcieSlot1LinkSpeed**	System IO Controller 1 (SIOC1) add-on slot 1 link speed. • **GEN1**— Link speed can reach up to first generation. • **GEN2**—The default link speed. Link speed can reach up to second generation. • **GEN3**— Link speed can reach up to third generation. • **Disabled**—Slot is disabled, and the card is not enumerated.
SIOC2 Link Speed **set PcieSlot2LinkSpeed**	System IO Controller 2 (SIOC2) add-on slot 2 link speed. • **GEN1**— Link speed can reach up to first generation. • **GEN2**—The default link speed. Link speed can reach up to second generation. • **GEN3**— Link speed can reach up to third generation. • **Disabled**—Slot is disabled, and the card is not enumerated.

Name	Description
Mezz Link Speed **set PcieSlotMLinkSpeed**	Mezz link speed. This can be one of the following: • **GEN 1—** Link speed can reach up to first generation. • **GEN 2—** Link speed can reach up to second generation. • **GEN 3—**The default link speed. Link speed can reach up to third generation. • **Disabled—**Slot is disabled, and the card is not enumerated.

Server Management Tab for C3160 Servers

Name	Description
FRB-2 Timer **set FRB-2**	Whether the FRB2 timer is used by Cisco IMC to recover the system if it hangs during POST. This can be one of the following: • **Disabled—**The FRB2 timer is not used. • **Enabled—**The FRB2 timer is started during POST and used to recover the system if necessary.
OS Watchdog Timer **set OSBootWatchdogTimer**	Whether the BIOS programs the watchdog timer with a specified timeout value. This can be one of the following: • **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 Cisco IMC logs an error and takes the action specified by the **set OSBootWatchdogTimerPolicy** command.

Name	Description
OS Watchdog Timer Timeout **set OSBootWatchdogTimerTimeOut**	If OS does not boot within the specified time, OS watchdog timer expires and system takes action according to timer policy. This can be one of the following: • **5_Minutes—**The OS watchdog timer expires 5 minutes after it begins to boot. • **10_Minutes—**The OS watchdog timer expires 10 minutes after it begins to boot. • **15_Minutes—**The OS watchdog timer expires 15 minutes after it begins to boot. • **20_Minutes—**The OS watchdog timer expires 20 minutes after it begins to boot. **Note** This option is only applicable if you enable the OS Boot Watchdog Timer.
OS Watchdog Timer Policy **set OSBootWatchdogTimerPolicy**	What action the system takes if the watchdog timer expires. This can be one of the following: • **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. **Note** This option is only applicable if you enable the OS Boot Watchdog Timer.

APPENDIX B

BIOS Token Name Comparison for Multiple Interfaces

This appendix contains the following section:

BIOS Token Name Comparison for Multiple Interfaces

The following table lists the BIOS token names used in the XML, CLI and Web GUI interfaces. You can use this list to map the names across these interfaces.

Note The parameters that are available depend on the type of Cisco UCS server you are using.

BIOS Token Group	BIOS Token Name	XML Object	CLI and Web GUI Object
Main	TPM Support	biosVfTPMSupport/ vpTPMSupport	TPMAdminCtrl
Process Configuration	Intel(R) Hyper-Threading Technology	biosVfIntelHyperThreadingTech/ vpIntelHyperThreadingTech	IntelHyperThread
	Number of Enable Cores	biosVfCoreMultiProcessing/ vpCoreMultiProcessing	CoreMultiProcessing
	Execute Disable	biosVfExecuteDisableBit/ vpExecuteDisableBit	ExecuteDisable
	Intel(R) VT	biosVfIntelVirtualizationTechnology/ vpIntelVirtualizationTechnology	IntelVT

BIOS Token Group	BIOS Token Name	XML Object	CLI and Web GUI Object
	Intel(R) VT-d	biosVfIntelVTForDirectedIO/ vpIntelVTForDirectedIO	IntelVTD
	Intel(R) VT-d Coherency Support	biosVfIntelVTForDirectedIO/ vpIntelVTDCoherencySupport	CoherencySupport
	Intel(R) VT-d ATS Support	biosVfIntelVTForDirectedIO/ vpIntelVTDATSSupport	ATS
	CPU Performance	biosVfCPUPerformance/ vpCPUPerformance	CpuPerformanceProfile
	Hardware Prefetcher	biosVfHardwarePrefetch/ vpHardwarePrefetch	HardwarePrefetch
	Adjacent Cache Line Prefetcher	biosVfAdjacentCacheLinePrefetch/ vpAdjacentCacheLinePrefetch	AdjacentCacheLinePrefetch
	DCU Streamer Prefetch	biosVfDCUPrefetch/ vvpStreamerPrefetch	DcuStreamerPrefetch
	DCU IP Prefetcher	biosVfDCUPrefetch/ vpIPPrefetch	DcuIpPrefetch
	Direct Cache Access Support	biosVfDirectCacheAccess/ vpDirectCacheAccess	DirectCacheAccess
	Power Technology	biosVfCPUPowerManagement/ vpCPUPowerManagement	CPUPowerManagement
	Enhanced Intel Speedstep(R) Technology	biosVfEnhancedIntelSpeedStepTech/ vpEnhancedIntelSpeedStepTech	EnhancedIntelSpeedStep
	Intel(R) Turbo Boost Technology	biosVfIntelTurboBoostTech/ vpIntelTurboBoostTech	IntelTurboBoostTech
	Processor Power state C6	biosVfProcessorCState/ vpProcessorCState	ProcessorC6Report

BIOS Token Name Comparison for Multiple Interfaces

BIOS Token Group	BIOS Token Name	XML Object	CLI and Web GUI Object
	Processor Power state C1 Enhanced	biosVfProcessorC1E/ vpProcessorC1E	ProcessorC1E
	Frequency Floor Override	biosVfCPUFrequencyFloor/ vpCPUFrequencyFloor	CpuFreqFloor
	P-STATE Coordination	biosVfPStateCoordType/ vpPStateCoordType	PsdCoordType
	Energy Performance	biosVfCPUEnergyPerformance/ vpCPUEnergyPerformance	CpuEngPerfBias
Memory Configuration	Select Memory RAS	biosVfSelectMemoryRASConfiguration/ vpSelectMemoryRASConfiguration	SelectMemoryRAS
	DRAM Clock Throttling	biosVfDRAMClockThrottling/ vpDRAMClockThrottling	DRAMClockThrottling
	NUMA	biosVfNUMAOptimized/ vpNUMAOptimized	NUMAOptimize
	Low Voltage DDR Mode	biosVfLvDIMMSupport/ vpNUMAOptimized	LvDDRMode
	DRAM Refresh rate	biosVfDramRefreshRate/ vpDramRefreshRate	DramRefreshRate
	Channel Interleaving	biosVfMemoryInterleave/ vpChannelInterLeave	ChannelInterLeave
	Rank Interleaving	biosVfMemoryInterleave/ vpRankInterLeave	RankInterLeave
	Patrol Scrub	biosVfPatrolScrub/ vpPatrolScrub	PatrolScrub
	Demand Scrub	biosVfDemandScrub/ vpDemandScrub	DemandScrub
	Altitude	biosVfAltitude/ vpAltitude	Altitude

BIOS Token Group	BIOS Token Name	XML Object	CLI and Web GUI Object
QPI Configuration	QPI Link Frequency Select	biosVfQPIConfig/ vpQPILinkFrequency	QPILinkFrequency
	Cluster on Die	biosVfCODEnable/ vpCODEnable	CODEnable
	Snoop Mode	biosVfEarlySnoop/ vpEarlySnoop	EarlySnoop
SATA Configuration	SATA Mode	Not supported	SATAMode
Onboard Storage	Onboard SCU Storage Support	biosVfOnboardStorage/ vpOnboardSCUStorageSupport	DisableSCU
	Onboard SCU Storage SW Stack	biosVfOnboardStorageSWStack vpOnboardSCUStorageSWStack	PchScuOromSelect
USB Configuration	Legacy USB Support	biosVfLegacyUSBSupport/ vpLegacyUSBSupport	LegacyUSBSupport
	Port 60/64 Emulation	biosVfUSBEmulation/ vpUSBEmul6064	UsbEmul6064
	All USB Devices	biosVfUSBPortsConfig/ vpAllUsbDevices	AllUsbDevices
	USB Port:Rear	biosVfUSBPortsConfig/ vpUsbPortRear	UsbPortRear
	USB Port:Front	biosVfUSBPortsConfig/ vpUsbPortFront	UsbPortFront
	USB Port:Internal	biosVfUSBPortsConfig/ vpUsbPortInternal	UsbPortInt
	USB Port:KVM	biosVfUSBPortsConfig/ vpUsbPortKVM	UsbPortKVM
	USB Port:Vmedia	biosVfUSBPortsConfig/ vpUsbPortVMedia	UsbPortVMedia

BIOS Token Name Comparison for Multiple Interfaces

BIOS Token Group	BIOS Token Name	XML Object	CLI and Web GUI Object
	USB Port:SD Card	biosVfUSBPortsConfig/ vpUsbPortSDCard	UsbPortSdCard
	xHCI Mode	biosVfPchUsb30Mode/ vpPchUsb30Mode	PchUsb30Mode
PCI Configuration	PCI ROM CLP	Not Supported	PciRomClp
	MMIO above 4GB	biosVfMemoryMappedIOAbove4GB/ vpMemoryMappedIOAbove4GB	MemoryMappedIOAbove4GB
	ASPM Support	biosVfASPMSupport/ vpASPMSupport	ASPMSupport
	VGA Priority	biosVfVgaPriority/ vpVgaPriority	VgaPriority
Serial Configuration	Console Redirection	biosVfConsoleRedirection/ vpConsoleRedirection	ConsoleRedir
	Terminal Type	biosVfConsoleRedirection/ vpTerminalType	TerminalType
	Bits per second	biosVfConsoleRedirection/ vpBaudRate	BaudRate
	Flow Control	biosVfConsoleRedirection/ vpFlowControl	FlowCtrl
	Putty KeyPad	biosVfConsoleRedirection/ vpPuttyKeyPad	PuttyFunctionKeyPad
	Redirection After BIOS POST	biosVfConsoleRedirection/ vpLegacyOSRedirection	RedirectionAfterPOST
LOM and PCIe Slots Configuration	PCH SATA Mode	biosVfSataModeSelect/ vpSataModeSelect	SataModeSelect
	All Onboard LOM Ports	biosVfSataModeSelect/ vpSataModeSelect	AllLomPortControl

BIOS Token Name Comparison for Multiple Interfaces

BIOS Token Group	BIOS Token Name	XML Object	CLI and Web GUI Object
	LOM Port 0 OptionROM	biosVfLOMPortOptionROM/ vpLOMPort0State	LomOpromControlPort0
	LOM Port 1 OptionROM	biosVfLOMPortOptionROM/ vpLOMPort1State	LomOpromControlPort1
	All PCIe Slots OptionROM	biosVfPCIOptionROMs/ vpPCIOptionROMs	PcieOptionROMs
	PCIe Slot:*n* OptionROM	biosVfPCISlotOptionROMEnable/ vpSlot*n*State	PcieSlot*n*OptionROM
	PCIe Mezzanine OptionROM	biosVfPCISlotOptionROMEnable/ vpSlotMezzState	PcieMezzOptionROM
	PCIe Slot:1 Link Speed or SIOC1 Link Speed	biosVfPCISlotOptionROMEnable/ vpSlot1LinkSpeed	PcieSlot1LinkSpeed
	PCIe Slot:2 Link Speed or SIOC2 Link Speed	biosVfPCISlotOptionROMEnable/ vpSlot2LinkSpeed	PcieSlot2LinkSpeed
	PCIe Slot:MLOM OptionROM	biosVfPCISlotOptionROMEnable/ vpSlotMLOMState	PcieSlotMLOMOptionROM
	PCIe Slot:HBA OptionROM	biosVfPCISlotOptionROMEnable/ vpSlotHBAState	PcieSlotHBAOptionROM
	PCIe Slot:N1 OptionROM	biosVfPCISlotOptionROMEnable/ vpSlotN1State	PcieSlotN1OptionROM
	PCIe Slot:N2 OptionROM	biosVfPCISlotOptionROMEnable/ vpSlotN2State	PcieSlotN2OptionROM
Server Management	FRB-2 Timer	biosVfFRB2Enable/ vpFRB2Enable	FRB-2

BIOS Token Name Comparison for Multiple Interfaces

BIOS Token Group	BIOS Token Name	XML Object	CLI and Web GUI Object
	OS Watchdog Timer	biosVfOSBootWatchdogTimer/ vpOSBootWatchdogTimer	OSBootWatchdogTimer
	OS Watchdog Timer Timeout	biosVfOSBootWatchdogTimerPolicy/ vpOSBootWatchdogTimerPolicy	OSBootWatchdogTimerTimeout
	OS Watchdog Timer Policy	biosVfOSBootWatchdogTimerTimeOut/ vpOSBootWatchdogTimerPolicy	OSBootWatchdogTimerPolicy
	Boot Order Rules	biosVfUCSMBootOrderRuleControl/ vpUCSMBootOrderRule	UCSMBootOrderRule

BIOS Token Name Comparison for Multiple Interfaces

INDEX

H

I

K

L

M

N

O

T

U

V

X

Y