# Cisco UCS C-Series Integrated Management Controller CLI Configuration Guide for C3X60 Servers

**First Published:** 2015-09-17

**Last Modified:** 2016-09-16

**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**.<br>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**.<br>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

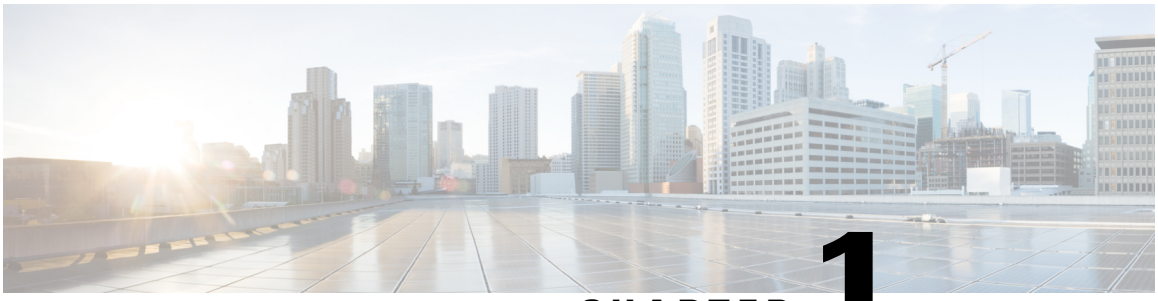
For a complete list of all B-Series documentation, see the *Cisco UCS B-Series Servers Documentation Roadmap* available at the following URL: http://www.cisco.com/go/unifiedcomputing/b-series-doc.

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 Server

The Cisco UCS C3260 is a modular, dense storage server with dual M3 or M4 server nodes, optimized for large datasets used in environments such as big data, cloud, object storage, and content delivery.

The UCS C3260 chassis is a modular architecture consisting of the following modules:

- Base chassis: contains four redundant, hot-pluggable power supplies, eight redundant, hot-pluggable fans, and a rail kit.
- Server Node: one or two M3 or M4 server nodes, each with two CPUs, 128, 256, or 512 GB of DIMM memory, and a pass-through controller or a RAID card with a 1 GB or 4 GB cache.
- System I/O Controller (SIOC): one or two System I/O Controllers, each of which includes an integrated 1300-series virtual interface capability.
- Optional Drive Expansion Node: Large Form Factor (LFF) 3.5-inch drives in a choice of capacities.
- Hard Drives: Up to 56 top-loading Large Form Factor (LFF) HDDs of 4TB, 6TB, 8TB and 10TB capacities.
- Solid State Drives: Optionally up to 28 solid-state disks (SSDs) of 400GB, 800 GB, 1.6TB, and 3.2 TB capacities.
- Solid-State Boot Drives: up to two SSDs per M3 or M4 server node.
- I/O Expander: provides two PCIe expansion slots and accommodates up to two NVMe SSDs.

The enterprise-class UCS C3260 storage server extends the capabilities of Cisco's Unified Computing System portfolio in a 4U form factor that delivers the best combination of performance, flexibility, and efficiency gains.

**Note** An M3 Server Node has Intel E5-2600 V2 CPUs and DDR-3 DIMMs. An M4 Server Node has Intel E5-2600 v4 CPUs and DDR-4 DIMMs

# 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.

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

# Cisco Integrated Management Controller

The 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
- 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
- Install and activate CMC 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.

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 | # |
| server | **scope server** *index* command from EXEC mode | /server # |
| bios | **scope bios** command from server mode | /server/bios # |
| advanced | **scope advanced** command from bios mode | /server/bios/advanced # |
| main | **scope main** command from bios mode | /server/bios/main # |
| server-management | **scope server-management** command from bios mode | /server/bios/server-management # |
| boot-device | **scope boot-device** command from bios mode | /server/bios/boot-device # |
| bmc | **scope bmc** command from server mode | /server/bmc # |
| firmware | **scope firmware** command from bmc mode | /server/bios/bmc # |
| import-export | **scope import-export** command from bmc mode | /server/bios/import-export # |
| network | **scope network** command from bmc mode | /server/bios/network # |
| power-restore-policy | **scope power-restore-policy** command from bmc mode | /server/bios/power-restore-policy # |
| kvm | **scope kvm** command from server mode | /server/kvm # |
| ipmi | **scope ipmi** command from server mode | /server/ipmi # |
| dimm-blacklisting | **scope dimm-blacklisting** command from server mode | /server/dimm-blacklisting # |

| Mode Name | Command to Access | Mode Prompt |
|---|---|---|
| reset-ecc | **scope reset-ecc** command from server mode | /server/reset-ecc # |
| sel | **scope sel** command from server mode | /server/sel # |
| sol | **scope sol** command from server mode | /server/sol # |
| vmedia | **scope vmedia** command from server mode | /server/vmedia # |
| certificate | **scope certificate** command from EXEC mode | /certificate # |
| fault | **scope fault** command from EXEC mode | /fault # |
| http | **scope http** command from EXEC mode | /http # |
| ldap | **scope ldap** command from EXEC mode | /ldap # |
| binding | **scope binding** command from ldap mode | /ldap/binding # |
| dns-search | **scope dns-search** command from ldap mode | /ldap/dns-search # |
| ldap-group-rule | **scope ldap-group-rule** command from ldap mode | /ldap/ldap-group-rule # |
| ldap-server | **scope ldap-server** command from ldap mode | /ldap/ldap-server # |
| role-group | **scope role-group** command from ldap mode | /ldap/role-group # |
| network | **scope network** command from EXEC mode | /network # |
| ipblocking | **scope ipblocking** command from network mode | /network/ipblocking # |
| chassis | **scope chassis** command from EXEC mode | /chassis # |
| adapter | | /chassis/adapter # |

| Mode Name | Command to Access | Mode Prompt |
|---|---|---|
| | **scope adapter** *index* command from chassis mode | |
| host-eth-if | **scope host-eth-if** command from adapter mode | /chassis/adapter/host-eth-if # |
| host-fc-if | **scope host-fc-if** command from adapter mode | /chassis/adapter/host-fc-if # |
| port-profiles | **scope port-profiles** command from adapter mode | /chassis/adapter/port-profiles # |
| vmfex | **scope vmfex** *index* command from adapter mode | /chassis/adapter/vmfex # |
| cmc | **scope cmc** *index* command from chassis mode | /chassis/cmc # |
| ipmi | **scope ipmi** command from cmc mode | /chassis/cmc/ipmi # |
| network | **scope network** command from cmc mode | /chassis/cmc/network # |
| firmware | **scope firmware** command from chassis mode | /chassis/firmware # |
| import-export | **scope import-export** command from chassis mode | /chassis/import-export # |
| log | **scope log** command from chassis mode | /chassis/log # |
| server | **scope server** command from log mode | /chassis/log/server # |
| sas-expander | **scope sas-expander** *index* command from chassis mode | /chassis/sas-expander # |
| phy-stats | **scope phy-stats** command from sas-expander mode | /chassis/sas-expander/phy-stats # |
| server | **scope server** *index* command from chassis mode | /chassis/server # |
| storageadapter | **scope storageadapter** command from server mode | /chassis/server/storageadapter # |
| dimm-summary | | /chassis/server/dimm-summary # |

| Mode Name | Command to Access | Mode Prompt |
|---|---|---|
| | **scope dimm-summary** command from server mode | |
| tech-support | **scope tech-support** command from chassis mode | /chassis/tech-support # |
| 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 # |
| ssh | **scope ssh** command from EXEC mode | /ssh # |
| time | **scope time** command from EXEC mode | /time # |
| ntp | **scope ntp** command from time mode | /time/ntp # |
| user | **scope user** *user-number* command from EXEC mode | /user # |
| user-policy | **scope user-policy** command from EXEC mode | /user-policy # |
| user-session | **scope user-session** *session-number* command from EXEC mode | /user-session # |
| xmlapi | **scope xmlapi** command from EXEC mode | /xmlapi # |

# Complete a Command

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

# Command History

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

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

# Committing, Discarding, and Viewing Pending Commands

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

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

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

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

# Command Output Formats

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

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

  This example shows command output in the default format:

```
Server /chassis # set cli output default
Server /chassis # show hdd detail
Name HDD_01_STATUS:
    Status : present
Name HDD_02_STATUS:
    Status : present
Name HDD_03_STATUS:
    Status : present
Name HDD_04_STATUS:
    Status : present

Server /chassis #
```

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

  This example shows command output in the YAML format:

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

---
    name: HDD_02_STATUS
    hdd-status: present

---
    name: HDD_03_STATUS
    hdd-status: present

---
    name: HDD_04_STATUS
    hdd-status: present

...

Server /chassis #
```

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

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

# Online Help for the CLI

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

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

# 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.

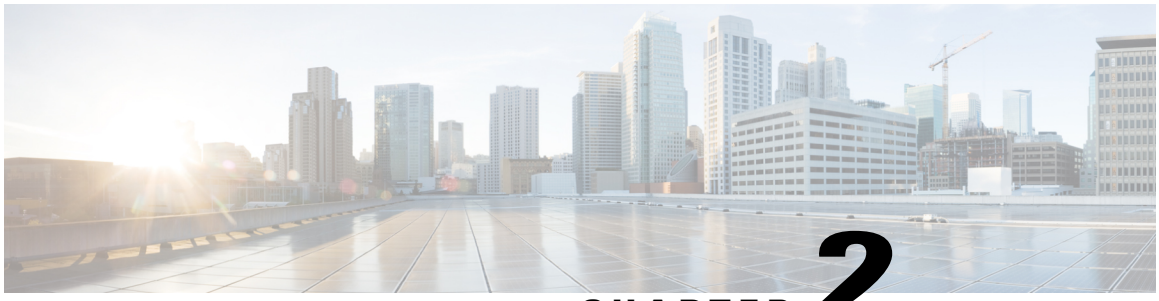
**Note** After an upgrade from Cisco IMC version 1.5(x) or 2.0(1) to the latest version, or when you do a factory reset, during first login Cisco IMC prompts for a password change. You cannot choose the word 'password' as your new password. If this creates problems for any scripts you may be running, 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** To configure the KVM console successfully for the Cisco UCS C3260 server, you need to configure IP addresses for the Cisco IMC, CMC, and BMC components. You can configure the IP addresses for these components using the CLI interface or Web UI. For the CLI, use the command **scope network**, or view the setting using **scope <chassis/server1/2><cmc/bmc><network>**.

To configure IP addresses for network components on the web interface, see the steps described in the section **Configuring Network-Related Settings**.

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

## Installing an OS Using the KVM Console

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

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

# PXE Installation Servers

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

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

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

# Installing an OS Using a PXE Installation Server

### Before You Begin

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

### Procedure

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

**Step 2** Reboot the server.
If a PXE install server is available on the VLAN, the installation process begins when the server reboots. PXE installations are typically automated and require no additional user input. Refer to the installation guide for the OS being installed to guide you through the rest of the installation process.

### What to Do Next

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

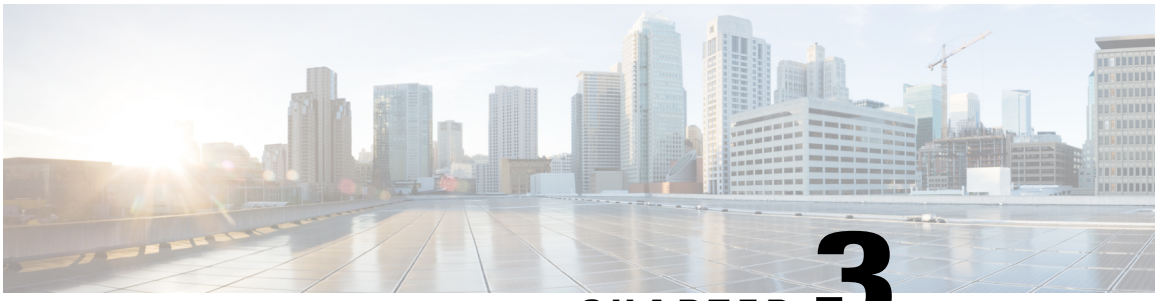
# Booting an Operating System from a USB Port

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

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

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

  http://www.cisco.com/en/US/products/ps10493/prod_installation_guides_list.html.
- After you boot the OS from the USB port, you must set the second-level boot order so that the server boots from that USB source every time.



CHAPTER 3

# Managing Chassis and Dynamic Storage

This chapter includes the following sections:



# Viewing Chassis Properties

## Viewing Chassis Summary

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server # **scope chassis** | Enters chassis command mode. |
| **Step 2** | Server /chassis # **show detail** | Displays the chassis' properties. |

This example displays the chassis' properties:

```
Server# scope chassis
Server /chassis # show detail
Chassis:
    Serial Number: FOX1843G9EM
    Product Name: UCS C3260
    PID : UCSC-C3X60-BASE
    Front Panel Locator LED: on
    Description:
    CMC-1 State: Active
    CMC-2 State: Standby

Server /chassis #
```

# Viewing CMC Firmware Versions

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server # **scope chassis** | Enters chassis command mode. |
| **Step 2** | Server /chassis # **show cmc** | Displays the CMC firmware versions. |

This example displays the CMC firmware versions.:

```
Server# scope chassis
Server /chassis # show cmc
ID    Name       Serial Number Update Stage Update Progress Current FW Version
----- ---------- ------------- ------------ --------------- ------------------
1     CMC1                     NONE         100             2.0(6.79)
2     CMC2                     NONE         100             2.0(6.79)

Server /chassis #
```

# Viewing LED Details

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server # **scope chassis** | Enters chassis command mode. |
| **Step 2** | Server /chassis # **show led** | Displays the LED details at the chassis level. |

This example the LED details at the chassis level:

```
Server# scope chassis
Server /chassis # show led
LED Name                  LED State  LED Color
------------------------- ---------- --------
CHS_FP_LED_ID             FAST BLINK BLUE
LED_HLTH_STATUS           ON         GREEN
LED_PSU_STATUS            ON         GREEN
LED_TEMP_STATUS           ON         GREEN
LED_FAN_STATUS            ON         GREEN
SERVER1_FP_ID_LED         OFF        BLUE
SERVER2_FP_ID_LED         OFF        BLUE
OVERALL_DIMM_STATUS       ON         GREEN

Server /chassis #
```

# Viewing the Details of the Servers on the Chassis

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server # **scope chassis** | Enters chassis command mode. |
| **Step 2** | Server /chassis # **show server** | Displays the high level details of the servers on the chassis. |

This example displays the high level details of the servers on the chassis:

```
Server# scope chassis
Server /chassis # show server
Server ID Power Serial Number Product Name  PID              UUID

--------- ----- ------------- ------------- ----------------
-------------------------------------
1         on    FCH1848794D   UCS C3160     UCSC-C3X60-SVRNB
60974271-A514-484C-BAE3-A5EE4FD16E06
2         on    FCH183978RD   UCS C3160     UCSC-C3X60-SVRNB
207BD0D4-C589-40C1-A73E-EF6E7F773198

Server /chassis #
```

# Viewing Physical Drive Properties

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server # **scope chassis** | Enters chassis command mode. |
| **Step 2** | Server /chassis # **scope dynamic-storage** | Enters the dynamic storage command mode. |
| **Step 3** | Server /chassis/dynamic-storage # **scope physical-drive drive number** | Enters the physical drive command mode. |
| **Step 4** | Server /chassis/dynamic-storage/physical-drive # **show detail** | Displays the details of the physical drive. |
| **Step 5** | Server /chassis/dynamic-storage/physical-drive # **exit** | Exits to the dynamic storage command mode. |
| **Step 6** | Server /chassis/dynamic-storage # **scope physical-drive-fw drive number** | Enters the physical drive firmware command mode. |
| **Step 7** | Server /chassis/dynamic-storage/physical-drive-fw # **show detail** | Displays the firmware details of the physical drive. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 8** | Server /chassis/dynamic-storage/physical-drive-fw # **exit** | Exits to the dynamic storage command mode. |
| **Step 9** | Server /chassis/dynamic-storage # **scope physical-drive-link drive number** | Enters the physical drive link command mode. |
| **Step 10** | Server /chassis/dynamic-storage/physical-drive-link # **show detail** | Displays the link details of the physical drive. |
| **Step 11** | Server /chassis/dynamic-storage/physical-drive-link # **exit** | Exits to the dynamic storage command mode. |
| **Step 12** | Server /chassis/dynamic-storage # **scope physical-slot-owner drive number** | Enters the physical slot ownership command mode. |
| **Step 13** | Server /chassis/dynamic-storage/physical-slot-owner # **show detail** | Displays details about which server the physical drive is assigned to. |

This example displays the physical drive properties:

```
Viewing Physical Drive Properties
Server# scope chassis
Server /chassis # scope dynamic-storage
Server /chassis/dynamic-storage # scope physical-drive 1
Server /chassis/dynamic-storage/physical-drive # show detail
Slot 1:
    Ownership: server1
    Health: good
    Vendor: TOSHIBA
    Product ID: MG03SCA400
    Product Rev Level: 5702
    Size: 3.63 TB
    Serial Number: 94E0A0T9FVU4
svbu-huu-sanity-col2-1-vcmc /chassis/dynamic-storage/physical-drive #

Viewing Firmware Details
Server /chassis/dynamic-storage/physical-drive # exit
Server /chassis/dynamic-storage # scope physical-drive-fw 1
Server /chassis/dynamic-storage/physical-drive-fw # show detail

Slot 1:
    Vendor: TOSHIBA
    Product ID: MG03SCA400
    Current_FW: 5702
    Update Stage: NONE
    Update Progress: 0
Server /chassis/dynamic-storage/physical-drive-fw #
Viewing Link Details
Server /chassis/dynamic-storage/physical-drive # exit
Server /chassis/dynamic-storage # scope physical-drive-link 1
Server /chassis/dynamic-storage/physical-drive-link # show detail
Slot 1:
    Ownership: server1
    EX1 Link: 6.0 Gb
    EX2 Link: 6.0 Gb
```

```
    SAS Adddress 1: 50000395c8d2a1fe
    SAS Adddress 2: 50000395c8d2a1ff
Server /chassis/dynamic-storage/physical-drive-link #
Viewing the slot owernship
Server /chassis/dynamic-storage/physical-drive-link # exit
Server /chassis/dynamic-storage # scope physical-slot-owner 1
Server /chassis/dynamic-storage/physical-drive-link # show detailSlot 1:
    Ownership: server1
Server /chassis/dynamic-storage/physical-slot-owner #
```

# Viewing Cisco VIC Adapter Properties

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server # **scope chassis** | Enters chassis command mode. |
| **Step 2** | Server /chassis # **show adapter** | Displays the high level details of the servers on the chassis. |
| **Step 3** | Server /chassis # **show adapter detail** | Displays the high level details of the servers on the chassis. |

This example displays the high level details of the Cisco Virtual Interface Card properties:

```
Server# scope chassis
Server /chassis # show adapter
Server ID Power Serial Number Product Name  PID              UUID

--------- ----- ------------- ------------- ----------------
-------------------------------------
1         on    FCH1848794D   UCS C3160     UCSC-C3X60-SVRNB
60974271-A514-484C-BAE3-A5EE4FD16E06
2         on    FCH183978RD   UCS C3160     UCSC-C3X60-SVRNB
207BD0D4-C589-40C1-A73E-EF6E7F773198
Server /chassis # show adapter detail
SIOC Slot 1:
    Product Name: UCSC-C3260-SIOC
    Serial Number: FCH18467P0U
    Product ID: UCSC-C3260-SIOC
    Adapter Hardware Revision:
    Current FW Version: 4.0(300.76)
    VNTAG: Disabled
    FIP: Enabled
    LLDP: Enabled
    Configuration Pending: no
    Cisco IMC Management Enabled: yes
    VID: V00
    Vendor: Cisco Systems Inc
    Description:
    Bootloader Version: 4.0(300.76)
    FW Image 1 Version: 4.0(300.76)
    FW Image 1 State: RUNNING ACTIVATED
    FW Image 2 Version: 4.0(300.71)
    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%
SIOC Slot 2:
```

```
    Product Name: UCSC-C3260-SIOC
    Serial Number: FCH18467P16
    Product ID: UCSC-C3260-SIOC
    Adapter Hardware Revision:
    Current FW Version: 4.0(300.61)
    VNTAG: Disabled
    FIP: Enabled
    LLDP: Enabled
    Configuration Pending: no
    Cisco IMC Management Enabled: yes
    VID: V00
    Vendor: Cisco Systems Inc
    Description:
    Bootloader Version: 4.0(300.61)
    FW Image 1 Version: 4.0(300.61)
    FW Image 1 State: RUNNING ACTIVATED
    FW Image 2 Version: 4.0(300.51)
    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 #
```

# Viewing Power Supply Properties

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server # **scope chassis** | Enters chassis command mode. |
| **Step 2** | Server /chassis # **show psu** | Displays the properties of each power supply on the chassis. |
| **Step 3** | Server /chassis # **show psu detail** | Displays the properties of each power supply on the chassis. |

This example displays the properties of each power supply on the chassis:

```
Server# scope chassis
Server /chassis # show psu
Name       In. Power (Watts)    Out. Power (Watts)   Firmware  Status     Product ID

---------- -------------------- -------------------- -------- ---------- ----------------
PSU1       101                  79                   10062012 Present    UCSC-PSU1-1050W
PSU2       89                   73                   10062012 Present    UCSC-PSU1-1050W
PSU3       96                   79                   10062012 Present    UCSC-PSU1-1050W
PSU4       92                   82                   10062012 Present    UCSC-PSU1-1050W
Server /chassis # show psu detail
Name PSU1:
    In. Power (Watts): 100
    Out. Power (Watts): 77
    Firmware : 10062012
    Status : Present
    Product ID : UCSC-PSU1-1050W
Name PSU2:
    In. Power (Watts): 89
    Out. Power (Watts): 75
    Firmware : 10062012
    Status : Present
    Product ID : UCSC-PSU1-1050W
Name PSU3:
```

```
    In. Power (Watts): 96
    Out. Power (Watts): 81
    Firmware : 10062012
    Status : Present
    Product ID : UCSC-PSU1-1050W
Name PSU4:
    In. Power (Watts): 91
    Out. Power (Watts): 77
    Firmware : 10062012
    Status : Present
    Product ID : UCSC-PSU1-1050W

Server /chassis #
```

# Chassis Management Tasks

## Toggling the Front Locator LED for the Chassis

### 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 #
```

## 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
```

# 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.

## Setting 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 time** | Enters time command mode. |
| **Step 2** | Server /time # **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 time
Server /time # 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: Wed Jul 1 02:21:15 2015 EST

Server /time #
```

# Managing Dynamic Storage

## Dynamic Storage Support

Effective with this release, The Cisco UCS C-Series rack-mount servers support dynamic storage of Serial Attached SCSI (SAS) drives in the Cisco Management Controller (CMC). This dynamic storage support is provided by the SAS fabric manager located in the CMC.

The fabric manager interacts with the PMC SAS expanders over an Out-of-Band ethernet connection. SAS Expanders allow you to maximize the storage capability of an SAS controller card. Using these expanders, you can employ SAS controllers support up to 60 hard drives. In CMC, an active SIOC configures the expander zoning, where you can assign the drives to the server nodes through the Web UI, command line interface or Cisco UCS Manager. The standby CMC is updated with the current state, so during a CMC fail-over standby, the CMC can take over the zoning responsibilities. Once the drives are visible to a particular server node, you can manage these using RAID controller.

**Note** The SAS controller support 56 hard disk drives (HDD) by default. There is also a provision to to replace Server node 2 with an additional four HDDs on Server 2. In that case the total number of HDDs shown in the Zoning page is 60. However, CMC would not support zoning for the additional HDDs 57, 58, 59, 60.

The SAS fabric manager provides an API library for other processes to configure and monitor the expanders and drives. Configuration of the fabric involves zoning the drives, updating the firmware for expanders and drives.

Dynamic Storage supports the following options:

- Assigning physical disks to server 1 and server 2
- Chassis Wide Hot Spare (supported only on RAID controllers)
- Shared mode (supported only in HBAs)
- Unassigning physical disks

# Viewing SAS Expander Properties

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server # **scope chassis** | Enters chassis command mode. |
| **Step 2** | Server /chassis # **show sas-expander** | Displays the SAS expander properties. |
| **Step 3** | Server /chassis # **show sas-expander detail** | Displays detailed SAS expander properties. |
| **Step 4** | Server /chassis # **scope sas-expander sas expander ID** | Enters SAS expander mode. |
| **Step 5** | Server /chassis/sas-expander # **show detail** | Displays the properties of the chosen SAS expander. |

This example displays the SAS expander properties:

```
Server# scope chassis
Server /chassis # show sas-expander
ID    Name       Update Stage Update Progress Current FW Version
----- ---------- ------------ --------------- ------------------
1     SASEXP1    NONE         100             04.08.01_B055
2     SASEXP2    NONE         100             04.08.01_B055

Server /chassis # show sas-expander detail
Firmware Image Information:
    ID: 1
    Name: SASEXP1
    Update Stage: NONE
    Update Progress: 100
    Current FW Version: 04.08.01_B056
    FW Image 1 Version: 04.08.01_B056
    FW Image 1 State: RUNNING ACTIVATED
    FW Image 2 Version: 04.08.01_B056
    FW Image 2 State: BACKUP INACTIVATED
Firmware Image Information:
    ID: 2
    Name: SASEXP2
    Update Stage: NONE
    Update Progress: 100
    Current FW Version: 04.08.01_B056
    FW Image 1 Version: 04.08.01_B056
    FW Image 1 State: RUNNING ACTIVATED
    FW Image 2 Version: 04.08.01_B056
    FW Image 2 State: BACKUP INACTIVATED

Server /chassis # scope sas-expander 1
Server /chassis/sas-expander # show detail
Firmware Image Information:
    ID: 1
    Name: SASEXP1
    Update Stage: NONE
    Update Progress: 100
    Current FW Version: 04.08.01_B056
    FW Image 1 Version: 04.08.01_B056
    FW Image 1 State: RUNNING ACTIVATED
    FW Image 2 Version: 04.08.01_B056
    FW Image 2 State: BACKUP INACTIVATED
```

```
Server /chassis/sas-expander #
```

# Viewing Dynamic Storage and Physical Drive Details

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server # **scope chassis** | Enters chassis command mode. |
| **Step 2** | Server /chassis # **show dynamic-storage** | Displays the physical drives and the servers they are assigned to. |
| **Step 3** | Server /chassis/dynamic-storage # **scope dynamic-storage** | Enters dynamic storage command mode. |
| **Step 4** | Server /chassis/dynamic-storage # **show physical-drive** | Displays the physical drive properties. |
| **Step 5** | Server /chassis/dynamic-storage # **show physical-drive-fw** | Displays the firmware of the physical drives. |
| **Step 6** | Server /chassis/dynamic-storage # **show physical-drive-link** | Displays the links of the physical drives. |
| **Step 7** | Server /chassis/dynamic-storage # **show physical-slot-owner** | Displays the physical drives association with the servers. |

This example displays the dynamic storage properties:

```
Server# scope chassis
Server /chassis # show dynamic-storage
Slot  Ownership
----- ----------
1     server1
2     server1
3     server1
4     server1
5     server1
6     server1
7     server1
8     server1
9     server1
.
.
.
Server /chassis # scope dynamic-storage
Server /chassis/dynamic-storage # show detail
Slot 1:
    Ownership: server1
Slot 2:
    Ownership: server1
Slot 3:
    Ownership: server1
Slot 4:
    Ownership: server1
Slot 5:
    Ownership: server1
Slot 6:
    Ownership: server1
```

```
Slot 7:
    Ownership: server1
Slot 8:
.
.
.

Server /chassis/dynamic-storage # show physical-drive
Slot  Ownership  Health  Vendor    Product ID          Size       Serial Number
----- ---------- ------- --------- ------------------ ---------- --------------
1     server1    good    TOSHIBA   MG03SCA400         3.63 TB    94E0A0T9FVU4
2     server1    good    TOSHIBA   MG03SCA400         3.63 TB    94D0A0F7FVU4
3     server1    good    TOSHIBA   MG03SCA400         3.63 TB    94B0A12YFVU4
4     server1    good    TOSHIBA   MG03SCA400         3.63 TB    94B0A131FVU4
5     server1    good    TOSHIBA   MG03SCA400         3.63 TB    94C0A0I9FVU4
6     server1    good    TOSHIBA   MG03SCA400         3.63 TB    94B0A12ZFVU4
7     server1    good    TOSHIBA   MG03SCA400         3.63 TB    94B0A02AFVU4
8     server1    good    TOSHIBA   MG03SCA400         3.63 TB    94B0A00LFVU4
9     server1    good    TOSHIBA   MG03SCA400         3.63 TB    94B0A00WFVU4
10    server1    good    TOSHIBA   MG03SCA400         3.63 TB    94B0A00QFVU4
11    server1    good    TOSHIBA   MG03SCA400         3.63 TB    94B0A00MFVU4
12    server1    good    TOSHIBA   MG03SCA400         3.63 TB    94B0A00NFVU4
13    server1    good    TOSHIBA   MG03SCA400         3.63 TB    94B0A130FVU4
14    server1    good    TOSHIBA   MG03SCA400         3.63 TB    94B0A00OFVU4

Server /chassis/dynamic-storage # show physical-drive-fw

Slot  Vendor    Product ID          Current_FW Update Stage Update Progress
----- --------- ------------------- ---------- ------------ --------------------
1     TOSHIBA   MG03SCA400          5702       NONE         0
2     TOSHIBA   MG03SCA400          5702       NONE         0
3     TOSHIBA   MG03SCA400          5702       NONE         0
4     TOSHIBA   MG03SCA400          5702       NONE         0
5     TOSHIBA   MG03SCA400          5702       NONE         0
6     TOSHIBA   MG03SCA400          5702       NONE         0
7     TOSHIBA   MG03SCA400          5702       NONE         0
8     TOSHIBA   MG03SCA400          5702       NONE         0
9     TOSHIBA   MG03SCA400          5702       NONE         0
10    TOSHIBA   MG03SCA400          5702       NONE         0
11    TOSHIBA   MG03SCA400          5702       NONE         0
12    TOSHIBA   MG03SCA400          5702       NONE         0
13    TOSHIBA   MG03SCA400          5702       NONE         0
14    TOSHIBA   MG03SCA400          5702       NONE         0

Server /chassis/dynamic-storage show physical-drive-link
Slot  Ownership  EX1 Link EX2 Link SAS Adddress 1    SAS Adddress 2
----- ---------- -------- -------- ----------------- -----------------
1     server1    6.0 Gb   6.0 Gb   50000395c8d2a1fe  50000395c8d2a1ff
2     server1    6.0 Gb   6.0 Gb   50000395c8d1f6de  50000395c8d1f6df
3     server1    6.0 Gb   6.0 Gb   50000395c8d0e93a  50000395c8d0e93b
4     server1    6.0 Gb   6.0 Gb   50000395c8d0e946  50000395c8d0e947
5     server1    6.0 Gb   6.0 Gb   50000395c8d17d2e  50000395c8d17d2f
6     server1    6.0 Gb   6.0 Gb   50000395c8d0e93e  50000395c8d0e93f
7     server1    6.0 Gb   6.0 Gb   50000395c8d09ace  50000395c8d09acf
8     server1    6.0 Gb   6.0 Gb   50000395c8d099ce  50000395c8d099cf
9     server1    6.0 Gb   6.0 Gb   50000395c8d099fa  50000395c8d099fb
10    server1    6.0 Gb   6.0 Gb   50000395c8d099e2  50000395c8d099e3
11    server1    6.0 Gb   6.0 Gb   50000395c8d099d2  50000395c8d099d3
12    server1    6.0 Gb   6.0 Gb   50000395c8d099d6  50000395c8d099d7
13    server1    6.0 Gb   6.0 Gb   50000395c8d0e942  50000395c8d0e943
14    server1    6.0 Gb   6.0 Gb   50000395c8d099da  50000395c8d099db

Server /chassis/dynamic-storage show physical-slot-owner
Slot  Ownership
----- ----------
1     server1
2     server1
3     server1
4     server1
5     hotspare
6     server1
7     server1
8     server1
```

```
9     server1
10    server1
.
.
.
Server /chassis/dynamic-storage #
```

# Managing Physical Drives

## Assigning Physical Drives to Servers

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server # **scope chassis** | Enters chassis command mode. |
| **Step 2** | Server /chassis/dynamic-storage # **scope dynamic-storage** | Enters dynamic storage command mode. |
| **Step 3** | Server /chassis/dynamic-storage # **assign-drive server ID<drive-slotid-list>** | Assigns the chosen physical drive to the server. |

Example for assigning a physical drive to the servers:

```
Server# scope chassis
Server /chassis # scope dynamic-storage
svbu-huu-sanity-col2-1-vcmc /chassis/dynamic-storage # assign-drive server2 27
Are you sure you want to assign drives 27 to server2
Enter 'yes' to confirm -> yes
assign-drive operation successful.

Server /chassis/dynamic-storage #
```

## Unassigning Physical Drives to Servers

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server # **scope chassis** | Enters chassis command mode. |
| **Step 2** | Server /chassis # **show dynamic-storage** | Displays the physical drives and the servers they are assigned to servers. |
| **Step 3** | Server /chassis/dynamic-storage # **scope dynamic-storage** | Enters dynamic storage command mode. |
| **Step 4** | Server /chassis/dynamic-storage # **unassign-drive <drive-slotid-list>** | Unassign the chosen physical drive. |

This example unassigning a physical drive:

```
Server# scope chassis
Server /chassis # scope dynamic-storage
Server /chassis/dynamic-storage # unassign-drive 27
Are you sure you want to unassign drives 27
Host will loose access to drive(s). Enter 'yes' to confirm -> yes
unassign-drive operation successful.

Server /chassis/dynamic-storage #
```

## Assigning Physical Drives as Chassis Wide Hot Spare

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server # **scope chassis** | Enters chassis command mode. |
| **Step 2** | Server /chassis/dynamic-storage # **scope dynamic-storage** | Enters dynamic storage command mode. |
| **Step 3** | Server /chassis/dynamic-storage # **assign-drive hotspare <drive-slotid-list>** | Assigns the physical drive as a global hotspare at the chassis level. |

Example for assigning a physical drive as a global hotspare at the chassis level:

```
Server# scope chassis
Server /chassis # scope dynamic-storage
Server /chassis/dynamic-storage # assign-drive hotspare 5
Are you sure you want to assign drives 5 as hotspare
Enter 'yes' to confirm -> yes
assign-drive operation successful.

Server /chassis/dynamic-storage #
```

## Sharing Physical Drives with Servers

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server # **scope chassis** | Enters chassis command mode. |
| **Step 2** | Server /chassis/dynamic-storage # **scope dynamic-storage** | Enters dynamic storage command mode. |
| **Step 3** | Server /chassis/dynamic-storage # **assign-drive shared <drive-slotid-list>** | Assigns the chosen physical drive for both the servers. |

Example for assigning the same physical drive for both the servers:

```
Server# scope chassis
Server /chassis # scope dynamic-storage
svbu-huu-sanity-col2-1-vcmc /chassis/dynamic-storage # assign-drive shared 4
Are you sure you want to assign drives 4 as shared
Enter 'yes' to confirm -> yes
assign-drive operation successful.

Server /chassis/dynamic-storage #
```

# Managing SAS Expander and HDD Firmware

## Updating and Activating SAS Expander Firmware

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server # **scope chassis** | Enters chassis command mode. |
| **Step 2** | Server /chassis # **scope sas-expandersas expander ID** | Enters SAS expander mode. |
| **Step 3** | Server /chassis/sas-expander # **update** *protocol IP Address path* | Initiates the firmware update by specifying 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:<br>• TFTP<br>• FTP<br>• SFTP<br>• SCP<br>• HTTP<br>**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.<br>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.<br>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 /chassis/sas-expander # **show detail** | (Optional)<br>Displays the status of the firmware upgrade. |

This example shows how to update and activate the SAS expander firmware:

```
Server# scope chassis
Server /chassis # scope sas-expander 1
Updating the firmware
Server /chassis/sas-expander# update tftp 10.10.10.10 /tftpboot/skasargo/<firmware file>
updating the firmware.
Checking the status of the upgrade
Server /chassis/sas-expander# show detail
Firmware Image Information:
    ID: 1
    Name: SASEXP1
    Update Stage: In Progress
    Update Progress: 25
    Current FW Version: 04.08.01_B056
    FW Image 1 Version: 04.08.01_B056
    FW Image 1 State: RUNNING ACTIVATED
    FW Image 2 Version: 04.08.01_B056
    FW Image 2 State: BACKUP INACTIVATED

Activating the firmware
svbu-huu-sanity-col2-1-vcmc /chassis/sas-expander # activate
This operation will activate backup firmware and reboot the SAS-Expander.
Continue?[y|N]y

Server /chassis/sas-expander #
```

## Updating HDD Firmware

### Procedure

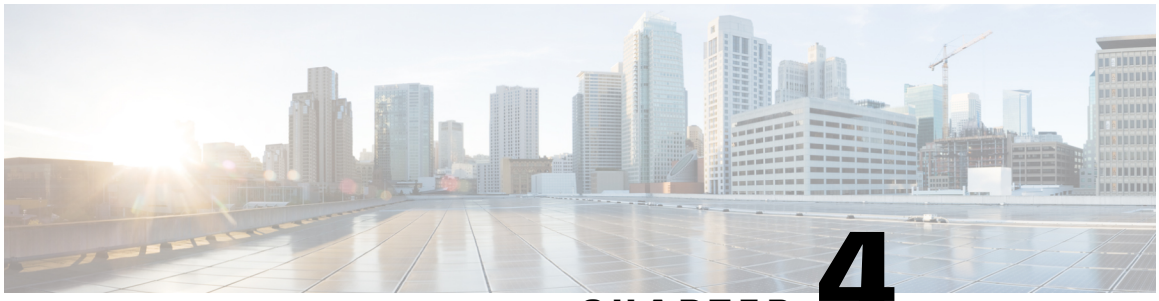
| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server # **scope chassis** | Enters chassis command mode. |
| **Step 2** | Server /chassis/dynamic-storage # **scope dynamic-storage** | Enters dynamic storage command mode. |
| **Step 3** | Server /chassis/dynamic-storage # **update-drive** *protocol IP Address path HDD slot-ids* | 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:<br>• TFTP<br>• FTP<br>• SFTP<br>• SCP<br>• 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.<br>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.<br>The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.<br>**Note** You can update firmware for multiple servers from the same vendor. |
| **Step 4** | Server /chassis/dynamic-storage # **show physical-drive-fw** | (Optional)<br>Displays the status of the firmware upgrade. |

This example provides steps to update the HDD firmware:

```
Server# scope chassis
Server /chassis # scope dynamic-storage
Updating for a single HDD
Server /chassis/dynamic-storage #update-drive tftp 10.10.10.10 /tftpboot/skasargo/sg4.lod
14
updating FW for slot 1 HDD
Updating for Multiple HDD
Server /chassis/dynamic-storage#update-drive tftp 10.10.10.10 /tftpboot/skasargo/sg4.lod
1-14
updating fw for multiple HDDs
Viewing the Status of the Upgrade
Server /chassis/dynamic-storage# show physical-drive-fw

Slot  Vendor    Product ID          Current_FW Update Stage Update Progress
----- --------- ------------------- ---------- ------------ --------------------
1     TOSHIBA   MG03SCA400          5702       Progress        25
2     TOSHIBA   MG03SCA400          5702       NONE            0
3     TOSHIBA   MG03SCA400          5702       NONE            0
4     TOSHIBA   MG03SCA400          5702       NONE            0
5     TOSHIBA   MG03SCA400          5702       NONE            0
6     TOSHIBA   MG03SCA400          5702       NONE            0
7     TOSHIBA   MG03SCA400          5702       NONE            0
8     TOSHIBA   MG03SCA400          5702       NONE            0
9     TOSHIBA   MG03SCA400          5702       NONE            0
10    TOSHIBA   MG03SCA400          5702       NONE            0
11    TOSHIBA   MG03SCA400          5702       NONE            0
12    TOSHIBA   MG03SCA400          5702       NONE            0
13    TOSHIBA   MG03SCA400          5702       NONE            0
14    TOSHIBA   MG03SCA400          5702       NONE            0
Server /chassis/dynamic-storage #
```



CHAPTER 4

# Managing the Server

This chapter includes the following sections:



## Toggling the Server 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 server server ID** | Enters server command mode. |
| **Step 2** | Server /server # **set locator-led** {**on** \| **off**} | Enables or disables the server locator LED. |
| **Step 3** | Server /server # **commit** | Commits the transaction to the system configuration. |

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

```
Server# scope server 1
Server /server # set locator-led off
Server /server *# commit

Server /server #
```

# Toggling the Locator LED for a Hard Drive

### Before You Begin

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

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server # **scope server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 2** | Server /server # **scope sensor** | Enters sensor command. |
| **Step 3** | Server /server/sensor # **scope hdd** | Enters hard disk drive (HDD) command mode. |
| **Step 4** | Server /server/sensor/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 server 1
Server /server # scope sensor
Server /server/sensor # scope hdd
Server /server/sensor/hdd # locateHDD 2 1
HDD Locate LED Status changed to 1
Server /server/sensor/hdd # show
Name                 Status               LocateLEDStatus
-------------------- -------------------- --------------------
HDD1_STATUS          present              TurnOFF
HDD2_STATUS          present              TurnON
HDD3_STATUS          absent               TurnOFF
HDD4_STATUS          absent               TurnOFF

Server /server/sensor/hdd #
```

# 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**

- C3260 M4 servers support both Legacy and Precision Boot order configuration through Web UI and CLI.
- 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 server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 2** | Server /server# **scope bios** | Enters BIOS command mode. |
| **Step 3** | Server /serve/bios # **show boot-device [detail]**. | Displays the detailed information of the boot devices. |

This example displays the details of the created bootable devices:

```
Server# scope server 1
Server /server # scope bios
Server /server/bios # show boot-device
Boot Device          Device Type  Device State       Device Order
-------------------- ------------ ------------------ ----------------
TestUSB              USB          Enabled            1
TestPXE              PXE          Enabled            2
Server /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 server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 2** | Server /server# **scope bios** | Enters BIOS command mode. |
| **Step 3** | Server /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:<br>• **HDD—**Hard disk drive<br>• **PXE—**PXE boot<br>• **SAN** boot<br>• **iSCSI** boot<br>• **USB**<br>• **Virtual Media**<br>• **PCHStorage**<br>• **UEFISHELL** |
| **Step 4** | Server /server/bios # **scope boot-device** *created boot device name*. | Enters the management of the created bootable devices. |
| **Step 5** | Server /server/bios/boot-device # **set** *values* | Specifies the property values for particular bootable device. You can set one or more of the following:<br>• cli**—** CLI options<br>• state**—** Whether the device will be visible by BIOS. By default the device is disabled. |

| | Command or Action | Purpose |
|---|---|---|
| | | **Note** If enabled, the device will overwrite the legacy boot order configuration.<br>• slot— Slot id where the device is plugged in.<br>• port— Port of the slot in which the device is present.<br>• LUN— Logical unit in a slot where the device is present.<br>• sub-type—Sub device type under a certain device type.<br>• order—The order of the device in the available list of devices. |
| **Step 6** | Server /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 server 1
Server /server # scope bios
Server /server/bios #  create boot-device TestPXE PXE
Server /server/bios #  scope boot-device TestPXE
Server /server/bios /boot-device #  set state Enabled
Server /server/bios /boot-device #  set slot L
Server /server/bios /boot-device #  set port 1
Server /server/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 /server/bios /boot-device #  y
Commiting device configuration
Server /server/bios/boot-device # show detail
BBIOS:
    BIOS Version: C3X60M3.2.0.7c.0.071620151216
    Backup BIOS Version: C3X60M3.2.0.7c.0.071620151216
    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

Server /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 server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 2** | Server /server# **scope bios** | Enters BIOS command mode. |
| **Step 3** | Server /server/bios # **scope boot-device** *created boot device name*. | Enters the management of the created bootable devices. |
| **Step 4** | Server /server/bios /boot-device # **set state** {*Enabled*\|*Disabled*}. | Enables or disables the device. The default state is disabled.<br>**Note** If enabled, the device will overwrite the legacy boot order configuration. |
| **Step 5** | Server /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.<br>**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 6** | Server /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 7** | Server /server/bios /boot-device* # **commit** | Commits the transaction to the system configuration. |

This example modifies the attributes of an existing device:

```
Server# scope server 1
Server /server # scope bios
Server /server/bios *# scope boot-device scu-device-hdd
Server /server/bios/boot-device # set status enabled
Server /server/bios/boot-device *# set order 2
Server /server/bios/boot-device *# set port 1
Server /server/bios/boot-device *# commit
Enabling boot device will overwrite boot order Level 1 configuration
Continue?[y|N]y
Server /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 server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 2** | Server /server# **scope bios** | Enters BIOS command mode. |
| **Step 3** | Server /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 server 1
Server /server # scope bios
Server /server/bios # rearrange-boot-device  TestPXE:1,TestUSB:2
 Server /server/bios # show boot-device
Boot Device          Device Type  Device State       Device Order
-------------------- ------------ ------------------ ----------------
TestPXE              PXE          Disabled           1
TestUSB              USB          Disabled           2

Server /server/bios #
```

# Reapplying 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 server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | Server /server# **scope bios** | Enters BIOS command mode. |
| **Step 3** | Server /server/bios # **re-apply**. | Re-applies the boot order to BIOS, if the last configured boot order source is BIOS.. |

This example reapplies the boot order to BIOS:

```
Server# scope server 1
Server /server # scope bios
Server /server/bios # re-apply
Server /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 server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 2** | Server /server# **scope bios** | Enters BIOS command mode. |
| **Step 3** | Server /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 server 1
Server /server # scope bios
Server /server/bios # remove-boot-device scu-device-hdd
Server /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<br>• Windows Server 2012 R2 |
| **QLogic PCI adapters** | • 8362 dual port adapter<br>• 2672 dual port adapter |
| **Fusion-io** | |

| Components | Types |
|---|---|
| **LSI** | • LSI MegaRAID SAS 9240-8i<br>• LSI MegaRAID SAS 9220-8i<br>• LSI MegaRAID SAS 9265CV-8i<br>• LSI MegaRAID SAS 9285CV-8e<br>• LSI MegaRAID SAS 9285CV-8e<br>• LSI MegaRAID SAS 9266-8i<br>• LSI SAS2008-8i mezz<br>• LSI Nytro card<br>• RAID controller for UCS C3X60 Storage (SLOT-MEZZ)<br>• Host Bus Adapter (HBA) |

# Enabling or Disabling UEFI Secure Boot Mode

### Before You Begin

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

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server # **scope server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 2** | Server /server# **scope bios** | Enters BIOS command mode. |
| **Step 3** | Server /server/bios # **set secure-boot**{ **enable** \| **disable** } | Enables or disables UEFI secure boot.<br>**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. |
| **Step 4** | Server /server/bios # **show detail** | (Optional)<br>Displays the details of the BIOS settings. |

The following examples show how to enable or disable secure boot and commit the transaction:

```
Server# scope server 1
Server /server # scope bios
Server /server/bios # set secure-boot enable
Setting Value : enable
Commit Pending.
```

```
Server /server/bios *# commit
UEFI Secure boot state changed successfully. Execute 'show detail' command to check the
current status
Server /server/bios # show detail
BIOS:
    BIOS Version: C3X60M3.2.0.7c.0.071620151216
    Backup BIOS Version: C3X60M3.2.0.8.0.071620152203
    Boot Order: (none)
    Boot Override Priority:
    FW Update/Recovery Status: None, OK
    UEFI Secure Boot: enabled
    Configured Boot Mode: Legacy
    Actual Boot Mode: Legacy
    Last Configured Boot Order Source: CIMC
Server /server/bios #
Server /server/bios #
erver# scope server 1
Server /server # scope bios
Server /server/bios # set secure-boot disable
Setting Value : disable
Commit Pending.
Server /server/bios *# commit
UEFI Secure boot state changed successfully. Execute 'show detail' command to check the
current status
Server /server/bios # show detail
BIOS:
    BIOS Version: C3X60M3.2.0.7c.0.071620151216
    Backup BIOS Version: C3X60M3.2.0.8.0.071620152203
    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
Server /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 server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 2** | Server /server# **scope bios** | Enters BIOS command mode. |
| **Step 3** | Server /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 server 1
Server /server # scope bios
Server /server/bios #  show actual-boot-order
```

```
Boot Order   Boot Device                          Device Type     Boot Policy
------------ ----------------------------------- --------------- -------------------
1            Cisco CIMC-Mapped vDVD1.22          VMEDIA          NIHUUCIMCDVD
2            Cisco vKVM-Mapped vDVD1.22          VMEDIA          dvd
3            Cisco vKVM-Mapped vHDD1.22          VMEDIA          dvd2
4            Cisco CIMC-Mapped vHDD1.22          VMEDIA          dvd3
5            (Bus 14 Dev 00)PCI RAID Adapter     HDD             NonPolicyTarget
6            "P1: INTEL SSDSC2BB120G4      "     PCHSTORAGE      NonPolicyTarget
7            "UEFI: Built-in EFI Shell "         EFI             NonPolicyTarget
8            "P0: INTEL SSDSC2BB120G4      "     PCHSTORAGE      NonPolicyTarget
9            Cisco vKVM-Mapped vFDD1.22          VMEDIA          NonPolicyTarge

Server /server/bios #
```

# 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 # **scope server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 3** | Server /chassis/server # **power on** | Powers on the server. |
| **Step 4** | At the prompt, enter y to confirm. | Power on the server. |

This example shows how to power on the server:

```
Server# scope chassis
Server# /chassis scope server 1
Server /chassis/server # power on
This operation will change the server's power state.
Do you want to continue with power control for Server 1 ?[y|N] y
```

```
Server /chassis/server # show
Server ID Power Serial Number Product Name  PID              UUID

--------- ----- ------------- ------------- ----------------
-----------------------------------
1         On    FCH1848794D   UCS C3160     UCSC-C3X60-SVRNB
60974271-A514-484C-BAE3-A5EE4FD16E06

Server /chassis/server#
```

# Powering Off the Server

**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** | Serve /chassis # **scope server 1** | Enters the server command mode. |
| **Step 3** | Server /chassis/server # **power off** | Powers off the server. |
| **Step 4** | At the prompt, enter y to confirm. | Power off the server. |

This example shows how to power off the server:

```
Server# scope chassis
Server# /chassis scope server 1
Server /chassis/server # power off
This operation will change the server's power state.
Do you want to continue with power control for Server 1 ?[y|N] y

Server /chassis/server # show
Server ID Power Serial Number Product Name  PID              UUID

--------- ----- ------------- ------------- ----------------
-----------------------------------
1         Off   FCH1848794D   UCS C3x60     UCSC-C3X60-SVRNB
60974271-A514-484C-BAE3-A5EE4FD16E06

Server /chassis/server#
```

# Powering Cycling the Server

**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** | Serve /chassis # **scope server 1** | Enters the server command mode. |
| **Step 3** | Server /chassis/server # **power cycle** | Power off and then powers on the server. |
| **Step 4** | At the prompt, enter y to confirm. | Power off and then powers on the server. |

This example shows how to power cycle the server:

```
Server# scope chassis
Server# /chassis scope server 1
Server /chassis/server # power cycle
This operation will change the server's power state.
Do you want to continue with power control for Server 1 ?[y|N] y

Server /chassis/server # show
Server ID Power Serial Number Product Name  PID             UUID

--------- ----- ------------- ------------- ----------------
-----------------------------------
1         On    FCH1848794D   UCS C3x60     UCSC-C3X60-SVRNB
60974271-A514-484C-BAE3-A5EE4FD16E06

Server /chassis/server#
```

# 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 /server # **scope server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 2** | server /server # **scope bmc** | Enters bmc command mode. |
| **Step 3** | Server /server/bmc # **scope power-restore-policy** | Enters the power restore policy command mode. |
| **Step 4** | Server /server/bmc/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:<br>• **power-off—**Server power will remain off until manually turned on. This is the default action.<br>• **power-on—**Server power will be turned on when chassis power is restored.<br>• **restore-last-state—**Server power will return to the state before chassis power was lost.<br>When the selected action is **power-on**, you can select a delay in the restoration of power to the server. |
| **Step 5** | Server /server/bmc/power-restore-policy # **set delay** {**fixed** \| **random**} | (Optional)<br>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 6** | Server /server/bmc/power-restore-policy # **set delay-value** *delay* | (Optional)<br>Specifies the delay time in seconds. The range is 0 to 240; the default is 0. |
| **Step 7** | 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 /server/bmc/power-restore-policy # set policy power-on
Server /server/bmc/power-restore-policy *# commit
Server /server/bmc/power-restore-policy # set delay fixed
Server /server/bmc/power-restore-policy *# set delay-value 180
Server /server/bmc/power-restore-policy *# commit
Server /server/bmc/power-restore-policy #  show detail
Power Restore Policy:
    Power Restore Policy: power-on
    Power Delay Type: fixed
    Power Delay Value(sec): 180

Server /server/bmc/power-restore-policy #
```

# Power Characterization

The chassis power characterization range is calculated and derived from individual server node power characterization status, and from the power requirements of all the unmanageable components of the chassis.

This range varies for each configuration, so you need to run the power characterization every time a configuration changes.

To help you use the power characterization range appropriately for the different power profiles, the system represents the chassis' minimum power as auto profile minimum and custom profile minimum. However, custom power profile minimum is the actual minimum power requirement of the current chassis configuration. For more information see the section Run Power Characterization.

# Power Profiles

**Note** Power Management is available only on some 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.

You can configure multiple profiles with the following combinations: automatic and thermal profiles; and custom and thermal profiles. These profiles are configured by using either the web user interface, command line interface, or XML API. In the web UI, the profiles are listed under the Power Capping area. In the CLI, the profiles are configured when you enter the **power-cap-config** command. You can configure the following power profiles for power capping feature:

- Automatic Power Limiting Profile
- Custom Power Limiting Profile
- Thermal Power Limiting Profile

Automatic power limiting profile sets the power limit of the individual server boards based on server priority selected by you, or as detected by the system, based on the server utilization sensor (which is known as manual or dynamic priority selection). The limiting values are calculated within the manageable chassis power budget and applied to the individual server, and the priority server is allocated with its maximum power limiting value, while the other server with the remaining of the manageable power budget. Power limiting occurs at each server board platform level that affects the overall chassis power consumption.

Custom power limiting profile allows you to set an individual server board's power limit from the Web UI or command line interface within the chassis power budget. In this scenario you can specify an individual server power limit.

Thermal power profile allows you to enable thermal failure power capping, which means you can set a specific platform temperature threshold and it sets P (min-x) as the power limit to be applied on the temperature threshold.

# Enabling Chassis Global Power Capping

## 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 power-cap-config** | Enters power cap configuration command mode. |
| **Step 3** | Server /chassis/power-cap-config # **set pow-cap-enable** {**yes** \| **no**} | Enables or disables the power configuration. |
| **Step 4** | Server /chassis/power-cap-config *# **set chassis-budget***power limit* | Sets the chassis power limit. |
| **Step 5** | Server /chassis/power-cap-config *# **commit** | Commits the transaction to the system. |
| **Step 6** | Server /chassis/power-cap-config # **show detail** | (Optional)<br>Displays the chassis power configuration details. |

The following example shows how to enable chassis global power capping:

```
Server # scope chassis
Server /chassis # scope power-cap-config
Server /chassis/power-cap-config # set pow-cap-enable yes
Server /chassis/power-cap-config *# set chassis-budget 1000
Server /chassis/power-cap-config *# commit
Server /chassis/power-cap-config # show detail
Chassis :
    Power Capping: yes
    Power Characterization Status: Completed
    Chassis Minimum (W): 756
    Chassis Maximum (W): 1089
    Chassis Budget (W): 1000
    Chassis Manageable Power Budget (W): 530
    Auto Balance Minimum Power Budget (W) : 966
Server 1 :
    Power Characterization Status: Completed
    Platform Minimum (W): 163
    Platform Maximum (W): 362
    Memory Minimum (W): 1
    Memory Maximum (W): 0
    CPU Minimum (W): 95
    CPU Maximum (W): 241
Server 2 :
    Power Characterization Status: Completed
    Platform Minimum (W): 136
    Platform Maximum (W): 253
    Memory Minimum (W): 1
    Memory Maximum (W): 0
    CPU Minimum (W): 57
    CPU Maximum (W): 139
Server /chassis/power-cap-config #
```

## Enabling Auto Balance Profile

### 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 chassis command mode. |
| **Step 2** | Server /chassis # **scope power-cap-config** | Enters power cap configuration command mode. |
| **Step 3** | Server /chassis/power-cap-config # **scope power-profile auto_balance** | Enters auto balance power profile command mode. |
| **Step 4** | Server /chassis/power-cap-config/power-profile # **set enabled** {**yes** \| **no**} | Enables or disables the power profile. |
| **Step 5** | Server /chassis/power-cap-config/power-profile *# **set priority-selection** {**dynamic** \| **manual**} | Sets the priority type to the chosen value. |
| **Step 6** | Server /chassis/power-cap-config/power-profile *# **set priority-server-id** {**1** \| **2**} | Assigns priority to the chosen server. |
| **Step 7** | Server /chassis/power-cap-config/power-profile *# **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.<br>The range is from 1 and 600 seconds. The default is 1 seconds. |
| **Step 8** | 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 9** | 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 will not be active. |
| **Step 10** | Server /chassis/power-cap-config/power-profile *# **commit** | Commits the transaction to the system configuration. |
| **Step 11** | Server /chassis/power-cap-config/power-profile # **show detail** | (Optional)<br>Displays the auto balance power profile details. |

The following example shows how to enable auto balance profile and setting the priority selection:

```
Setting Priority Using Dynamic Option
Server # scope chassis
Server /chassis # scope power-cap-config
Server /chassis/power-cap-config # scope power-profile auto_balance
Server /chassis/power-cap-config/power-profile # set enabled yes
Server /chassis/power-cap-config/power-profile *# set priority-selection dynamic
Server /chassis/power-cap-config/power-profile *# set corr-time 1
Server /chassis/power-cap-config/power-profile *# set allow-throttle yes
Server /chassis/power-cap-config/power-profile *# set susp-pd "2:0-4:30|All"
Server /chassis/power-cap-config/power-profile *# commit
Server /chassis/power-cap-config/power-profile # show detail
Profile Name : auto_balance
    Enabled: yes
    Priority Selection: dynamic
    Priority Server: 2
    Server1 Power Limit: 362
    Server2 Power Limit: 253
   Suspend Period: 2:0-4:30|All
    Exception Action: alert
    Correction Time: 1
    Throttling: no
Server /chassis/power-cap-config/power-profile #

Setting Priority Using the Manual Option
Server # scope chassis
Server /chassis # scope power-cap-config
Server /chassis/power-cap-config # scope power-profile auto_balance
Server /chassis/power-cap-config/power-profile # set enabled yes
Server /chassis/power-cap-config/power-profile *# set priority-selection manual
Server /chassis/power-cap-config/power-profile *# set priority-server-id 1
Server /chassis/power-cap-config/power-profile *# set corr-time 1
Server /chassis/power-cap-config/power-profile *# set allow-throttle yes
Server /chassis/power-cap-config/power-profile *# set susp-pd "2:0-4:30|All"
Server /chassis/power-cap-config/power-profile *# commit
Server /chassis/power-cap-config/power-profile # show detail
Profile Name : auto_balance
    Enabled: yes
    Priority Selection: manual
    Priority Server: 1
    Server1 Power Limit: 362
    Server2 Power Limit: 253
    Suspend Period: 2:0-4:30|All
    Exception Action: alert
    Correction Time: 1
    Throttling: no
Server /chassis/power-cap-config/power-profile #
```

## Disabling Auto Balance Power Profile

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server # **scope chassis** | Enters the chassis command mode. |
| **Step 2** | Server /chassis # **scope power-cap-config** | Enters the power cap configuration mode. |
| **Step 3** | Server /chassis/power-cap-config # **scope power-profile auto_balance** | Enters the auto balance power profile mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | Server /chassis/power-cap-config/power-profile # **set enabled no** | Disables the auto balance power profile. |
| **Step 5** | Server /chassis/power-cap-config/power-profile # **commit** | Commits the transaction to the system configuration. |

This example shows how to disable the auto balance profile:

```
Server # scope chassis
Server /chassis # scope power-cap-config
Server /chassis/power-cap-config # scope power-profile auto_balance
Server /chassis/power-cap-config/power-profile # set enabled no
Server /chassis/power-cap-config/power-profile *# commit
```

## Enabling Custom Profile on Server

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server # **scope chassis** | Enters the chassis command mode. |
| **Step 2** | Server /chassis # **scope power-cap-config** | Enters the power cap configuration mode. |
| **Step 3** | Server /chassis/power-cap-config # **scope power-profile custom** | Enters the custom power profile mode. |
| **Step 4** | Server /chassis/power-cap-config/power-profile # **set enabled yes** | Enables the custom power profile. |
| **Step 5** | Server /chassis/power-cap-config/power-profile *# **set power-limit** *value* | Specifies the power limit. Enter a value within the specified range. |
| **Step 6** | Server /chassis/power-cap-config/power-profile *# **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.<br>The range is from 1 and 600 seconds. The default is 1 seconds |
| **Step 7** | Server /chassis/power-cap-config/power-profile *# **set allow-throttle yes** | Enables the system to maintain the power limit by forcing the processor to use the throttling state (T-state) and memory throttle. |
| **Step 8** | Server /chassis/power-cap-config/power-profile *# **commit** | Commits the transaction to the system configuration. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 9** | At the prompt, enter the server ID for which you want to apply the custom power profile. | |
| **Step 10** | Server /chassis/power-cap-config/power-profile # **show detail** | Displays the power profile details. |

This example shows how to enable the custom profile on any server node:

```
Server # scope chassis
Server /chassis # scope power-cap-config
Server /chassis/power-cap-config # scope power-profile custom
Server /chassis/power-cap-config/power-profile # set enabled yes
Server /chassis/power-cap-config/power-profile *# set power-limit 253
Server /chassis/power-cap-config/power-profile *# set corr-time 1
Server /chassis/power-cap-config/power-profile *# set allow-throttle no
Server /chassis/power-cap-config/power-profile *# commit
Please enter server Id for which 'custom' power profile setting needs to be done
[1|2]?2
Server /chassis/power-cap-config/power-profile # show detail
Profile Name : custom
Server Id  1:
    Enabled: no
    Power Limit: N/A
    Suspend Period:
    Exception Action: alert
    Correction Time: 1
    Throttling: no
Server Id  2:
    Enabled: yes
    Power Limit: 253
    Suspend Period:
    Exception Action: alert
    Correction Time: 1
    Throttling: yes
```

## Disabling Custom Profile on Server

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server # **scope chassis** | Enters the chassis command mode. |
| **Step 2** | Server /chassis # **scope power-cap-config** | Enters the power cap configuration mode. |
| **Step 3** | Server /chassis/power-cap-config # **scope power-profile custom** | Enters the custom power profile mode. |
| **Step 4** | Server /chassis/power-cap-config/power-profile # **set enabled no** | Disables the custom power profile. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | Server /chassis/power-cap-config/power-profile *# **commit** | Commits the transaction to the system configuration. |
| **Step 6** | At the prompt, enter the server ID for which you want to disable the custom power profile. | |
| **Step 7** | Server /chassis/power-cap-config/power-profile # **show detail** | Displays the power profile details. |

This example shows how to disable the custom profile on any server node:

```
Server # scope chassis
Server /chassis # scope power-cap-config
Server /chassis/power-cap-config # scope power-profile custom
Server /chassis/power-cap-config/power-profile # set enabled no
Server /chassis/power-cap-config/power-profile *# commit
Please enter server Id for which 'custom' power profile setting needs to be done
[1|2]?2
Server /chassis/power-cap-config/power-profile # show detail
Profile Name : custom
Server Id  1:
    Enabled: no
    Power Limit: N/A
    Suspend Period:
    Exception Action: alert
    Correction Time: 1
    Throttling: no
Server Id  2:
    Enabled: no
    Power Limit: 253
    Suspend Period:
    Exception Action: alert
    Correction Time: 1
    Throttling: yes
```

## Enabling Thermal Profile on Server

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server # **scope chassis** | Enters the chassis command mode. |
| **Step 2** | Server /chassis # **scope power-cap-config** | Enters the power cap configuration mode. |
| **Step 3** | Server /chassis/power-cap-config # **scope power-profile thermal** | Enters the thermal power profile mode. |
| **Step 4** | Server /chassis/power-cap-config/power-profile # **set enabled yes** | Enables or disables the thermal power profile. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | Server /chassis/power-cap-config/power-profile *# **set temperature** *value* | Enter power in watts within the range specified. Enter the temperature in Celsius. |
| **Step 6** | Server /chassis/power-cap-config/power-profile *# **commit** | Commits the transaction to the system configuration. |
| **Step 7** | At the prompt, enter the server ID for which you want to enable the thermal power profile. | |
| **Step 8** | Server /chassis/power-cap-config/power-profile # **show detail** | Displays the power profile details. |

This example shows how to enable the thermal profile on any server node:

```
Server # scope chassis
Server /chassis # scope power-cap-config
Server /chassis/power-cap-config # scope power-profile thermal
Server /chassis/power-cap-config/power-profile # set enabled yes
Server /chassis/power-cap-config/power-profile *# set temperature 26
Server /chassis/power-cap-config/power-profile *# commit
Please enter server Id for which 'thermal' power profile setting needs to be done
[1|2]?1
Server /chassis/power-cap-config/power-profile # show detail
Profile Name : thermal
Server Id 1:
    Enabled: yes
    Temperature Threshold (deg C): 26
    Power Limit: 163
```

## Disabling Thermal Profile on Server

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server # **scope chassis** | Enters the chassis command mode. |
| **Step 2** | Server /chassis # **scope power-cap-config** | Enters the power cap configuration mode. |
| **Step 3** | Server /chassis/power-cap-config # **scope power-profile thermal** | Enters the thermal power profile mode. |
| **Step 4** | Server /chassis/power-cap-config/power-profile # **set enabled no** | Disables the thermal power profile. |
| **Step 5** | Server /chassis/power-cap-config/power-profile *# **commit** | Commits the transaction to the system configuration. |
| **Step 6** | At the prompt, enter the server ID for which you want to disable the thermal power profile. | |

| | Command or Action | Purpose |
|---|---|---|
| **Step 7** | Server /chassis/power-cap-config/power-profile # **show detail** | Displays the power profile details. |

This example shows how to disable the thermal profile on any server node:

```
Server # scope chassis
Server /chassis # scope power-cap-config
Server /chassis/power-cap-config # scope power-profile thermal
Server /chassis/power-cap-config/power-profile # set enabled no
Server /chassis/power-cap-config/power-profile *# commit
Please enter server Id for which 'thermal' power profile setting needs to be done
[1|2]?1
Server /chassis/power-cap-config/power-profile # show detail
Profile Name : thermal
Server Id 1:
    Enabled: no
    Temperature Threshold (deg C): 26
    Power Limit: 163
Server Id 2:
    Enabled: no
    Temperature Threshold (deg C): 0
    Power Limit: N/A
Server /chassis/power-cap-config/power-profile #
```

# Viewing Power Cap Configuration Details

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server # **scope chassis** | Enters the chassis command mode. |
| **Step 2** | Server /chassis # **scope power-cap-config** | Enters the power cap configuration mode. |
| **Step 3** | Server /chassis/power-cap-config # **show detail** | Displays the power characterization status of the chassis and servers. |

This example shows how to view power cap configuration details:

```
Server # scope chassis
Server /chassis # scope power-cap-config
Server /chassis/power-cap-config # show detail
Chassis :
    Power Capping: yes
    Power Characterization Status: Completed
    Chassis Minimum (W): 756
    Chassis Maximum (W): 1089
    Chassis Budget (W): 1000
    Chassis Manageable Power Budget (W): 530
    Auto Balance Minimum Power Budget (W) : 966
Server 1 :
    Power Characterization Status: Completed
    Platform Minimum (W): 163
```

```
    Platform Maximum (W): 362
    Memory Minimum (W): 1
    Memory Maximum (W): 0
    CPU Minimum (W): 95
    CPU Maximum (W): 241
Server 2 :
    Power Characterization Status: Completed
    Platform Minimum (W): 136
    Platform Maximum (W): 253
    Memory Minimum (W): 1
    Memory Maximum (W): 0
    CPU Minimum (W): 57
    CPU Maximum (W): 139
```

# Viewing Power Monitoring Details

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server # **scope chassis** | Enters the chassis command mode. |
| **Step 2** | Server /chassis # **show power-monitoring** | Displays the power monitoring details. |

This example shows how to view power monitoring details:

```
Server # scope chassis
Server /chassis # show power-monitoring
Chassis :
Current (W)  Minimum (W)  Maximum (W)  Average (W)  Period
------------ ------------ ------------ ------------ ------------
408          311          471          392          0days 9:5...
Server 1 :
Domain     Current (W)  Minimum (W)  Maximum (W)  Average (W)  Period
---------- ------------ ------------ ------------ ------------ ------------
Platform   68           61           178          68           0days 21:...
CPU        30           28           133          30           0days 21:...
Memory     1            0            1            1            0days 21:...
Server 2 :
Domain     Current (W)  Minimum (W)  Maximum (W)  Average (W)  Period
---------- ------------ ------------ ------------ ------------ ------------
Platform   97           62           200          100          1days 7:1:2
CPU        46           16           140          48           1days 7:1:2
Memory     1            0            1            1            1days 7:1:2
Server /chassis/server/pid-catalog #
```

# Viewing CUPS Utilization Details

### Procedure

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

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | Server /chassis # **show cups-utilization** | Displays the server utilization value on all the available CPUs. |

This example shows how to view CUPS utilization details:

```
Server # scope chassis
Server /chassis # show cups-utilization
Server 1 :
CPU Utilization (%)  Memory Utilization (%)  I/O Utilization (%)  Overall Utilization (%)
-------------------- ----------------------- -------------------- -----------------------
0                    0                       0                    0
Server 2 :
CPU Utilization (%)  Memory Utilization (%)  I/O Utilization (%)  Overall Utilization (%)
-------------------- ----------------------- -------------------- -----------------------
7                    0                       0                    8
```

# Resetting the Server

**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** | Serve /chassis # **scope server 1** | Enters the server command mode. |
| **Step 3** | Server /chassis/server # **power hard-reset** | Reset the server, this is equivalent to pressing the reset button on the front panel or IPMI reset. |
| **Step 4** | At the prompt, enter y to confirm. | Reset the server, this is equivalent to pressing the reset button on the front panel or IPMI reset. |

This example shows how to power hard reset the server:

```
Server# scope chassis
Server# /chassis scope server 1
Server /chassis/server # power hard-reset
This operation will change the server's power state.
Do you want to continue with power control for Server 1 ?[y|N] y

Server /chassis/server # show
Server ID Power Serial Number Product Name  PID             UUID
```

```
--------- ----- ------------- ------------- ----------------
-----------------------------------
1         Off   FCH1848794D   UCS C3260     UCSC-C3X60-SVRNB
60974271-A514-484C-BAE3-A5EE4FD16E06

Server /chassis/server#
```

# Shutting Down the Server

**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** | Serve /chassis # **scope server 1** | Enters the server command mode. |
| **Step 3** | Server /chassis/server # **power shutdown** | Shuts down the host OS and powers off the server. |
| **Step 4** | At the prompt, enter y to confirm. | Shuts down the host OS and powers off the server. |

This example shows how to shutdown the server:

```
Server# scope chassis
Server# /chassis scope server 1
Server /chassis/server # power shutdown
This operation will change the server's power state.
Do you want to continue with power control for Server 1 ?[y|N] y

Server /chassis/server # show
Server ID Power Serial Number Product Name  PID              UUID

--------- ----- ------------- ------------- ----------------
-----------------------------------
1         Off   FCH1848794D   UCS C3260     UCSC-C3X60-SVRNB
60974271-A514-484C-BAE3-A5EE4FD16E06

Server /chassis/server#
```

# 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 server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 2** | Server /server # **scope dimm-blacklisting** / | Enters the DIMM blacklisting mode. |
| **Step 3** | Server /server/dimm-blacklisting # **set enabled** {**yes** \| **no**} | Enables or disables DIMM blacklisting. |
| **Step 4** | Server /server/dimm-blacklisting* # **commit** | Commits the transaction to the system configuration. |

The following example shows how to enable DIMM blacklisting:

```
Server # scope server 1
Server /server # scope dimm-blacklisting
Server /server/dimm-blacklisting # set enabled yes
Server /server/dimm-blacklisting* # commit
Server /server/dimm-blacklisting #
Server /server/dimm-blacklisting # show detail
```

```
DIMM Blacklisting:
      Enabled: yes
Server /server/dimm-blacklisting #
```

# Configuring BIOS Settings

## Viewing BIOS Status

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server # **scope server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 2** | Server /sever # **scope bios** | Enters the BIOS command mode. |
| **Step 3** | Server /sever/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. |
| Backup BIOS Version | The backup version string of the 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 server 1
Server /sever # scope bios
```

```
Server /sever/bios # show detail
Server /sever/bios # show detail
BIOS:
    BIOS Version: C3X60M3.2.0.7c.0.071620151216
    Backup BIOS Version: C3X60M3.2.0.7c.0.071620151216
    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
Server /sever/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 server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 2** | Server /server # **scope bios** | Enters the BIOS command mode. |
| **Step 3** | Server /server /bios # **scope main** | Enters the main BIOS settings command mode. |
| **Step 4** | Server /server /bios # **set TPMAdminCtrl** {**Disbaled** \| **Enabled**} | Enables or disables TPM support. |
| **Step 5** | Server /server /bios/main # **commit** | Commits the transaction to the system configuration.<br>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 main BIOS parameter and commits the transaction:

```
Server /server # scope server 1
Server/server # scope bios
Server /server/bios # scope main
Server /server/bios/main # set TPMAdminCtrl Enabled
Server /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 /server/bios/main #
```

# Configuring Advanced 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 server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 2** | Server /sever # **scope bios** | Enters the BIOS command mode. |
| **Step 3** | Server /sever/bios # **scope advanced** | Enters the advanced BIOS settings command mode. |
| **Step 4** | Configure the BIOS settings. | BIOS Parameters by Server Model, on page 267 |
| **Step 5** | Server /sever/bios/advanced # **commit** | Commits the transaction to the system configuration.<br>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 all the USB drives and commits the transaction:

```
Server# scope server 1
Server/sever # scope bios
Server /sever/bios # scope advanced
Server /sever/bios/advanced # set AllUsbDevices Enabled
Server /sever/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 /sever/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 server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 2** | Server /sever # **scope bios** | Enters the BIOS command mode. |
| **Step 3** | Server /sever/bios # **scope server-management** | Enters the server management BIOS settings command mode. |
| **Step 4** | Configure the BIOS settings. | BIOS Parameters by Server Model, on page 267 |
| **Step 5** | Server /sever/bios/server-management # **commit** | Commits the transaction to the system configuration.<br>Changes are applied on the next server reboot. If server power is on, you are prompted to choose whether to reboot now. |

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

This example enables the OS watchdog timer and commits the transaction:

```
Server# scope bios
Server /sever # scope bios
Server /sever/bios # scope server-management
Server /sever/bios/server-management # set OSBootWatchdogTimer Enabled
Server /sever/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 /sever/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 server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 2** | Server /sever # **scope bios** | Enters the BIOS command mode. |
| **Step 3** | Server /sever/bios # **bios-setup-default** | Restores BIOS default settings. This command initiates a reboot. |

This example restores BIOS default settings:

```
Server# scope bios
Server/sever # scope bios
Server /sever/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 server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 2** | Server /sever # **scope bios** | Enters the BIOS command mode. |
| **Step 3** | Server /sever/bios # **enter-bios-setup** | Enters BIOS setup on reboot. |

This example enables you to enter BIOS setup:

```
Server# scope server 1
Server /sever # scope bios
Server /sever/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.

### 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 server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 2** | Server /sever # **scope bios** | Enters the BIOS command mode. |
| **Step 3** | Server /sever/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 /sever/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] y
Server /sever/bios #
```

# Viewing Product ID (PID) Catalog Details

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server # **scope chassis** | Enters chassis command mode. |
| **Step 2** | Server /chassis # **scope server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 3** | Server /chassis/server # **show cpu-pid** | Displays the CPU PID details. |
| **Step 4** | Server /chassis/server # **show dimm-pid** | Displays the memory PID details. |
| **Step 5** | Server /chassis/server # **show pciadapter-pid** | Displays the PCI adapters PID details. |
| **Step 6** | Server /chassis/server # **show hdd-pid** | Displays the HDD PID details. |

This example shows how to create view PID details

```
Server # scope chassis
Server /chassis # scope server 1
Viewing CPU PID details
Server /chassis/server # 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/server # 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/server # 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/server # show hdd-pid
Disk Controller  Product ID           Vendor     Model
---- ----------- -------------------- ---------- ------------
1    SBMezz1     UCSC-C3X60-HD6TB     SEAGATE    ST6000NM0014
2    SBMezz1     UCSC-C3X60-HD6TB     SEAGATE    ST6000NM0014
3    SBMezz1     UCSC-C3X60-HD6TB     SEAGATE    ST6000NM0014
```

```
4    SBMezz1     UCSC-C3X60-HD6TB     SEAGATE    ST6000NM0014
5    SBMezz1     UCSC-C3X60-HD6TB     SEAGATE    ST6000NM0014
6    SBMezz1     UCSC-C3X60-HD6TB     SEAGATE    ST6000NM0014
7    SBMezz1     UCSC-C3X60-HD6TB     SEAGATE    ST6000NM0014
8    SBMezz1     UCSC-C3X60-HD6TB     SEAGATE    ST6000NM0014
9    SBMezz1     UCSC-C3X60-HD6TB     SEAGATE    ST6000NM0014
10   SBMezz1     UCSC-C3X60-HD6TB     SEAGATE    ST6000NM0014
11   SBMezz1     UCSC-C3X60-HD6TB     SEAGATE    ST6000NM0014
12   SBMezz1     UCSC-C3X60-HD6TB     SEAGATE    ST6000NM0014
13   SBMezz1     UCSC-C3X60-HD6TB     SEAGATE    ST6000NM0014
14   SBMezz1     UCSC-C3X60-HD6TB     SEAGATE    ST6000NM0014
201  SBMezz1     UCSC-C3X60-12SSD     ATA        INTEL SSD...
202  SBMezz1     UCSC-C3X60-12SSD     ATA        INTEL SSD...

Server /chassis/server #
```

# Uploading and Activating PID Catalog

### Before You Begin

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

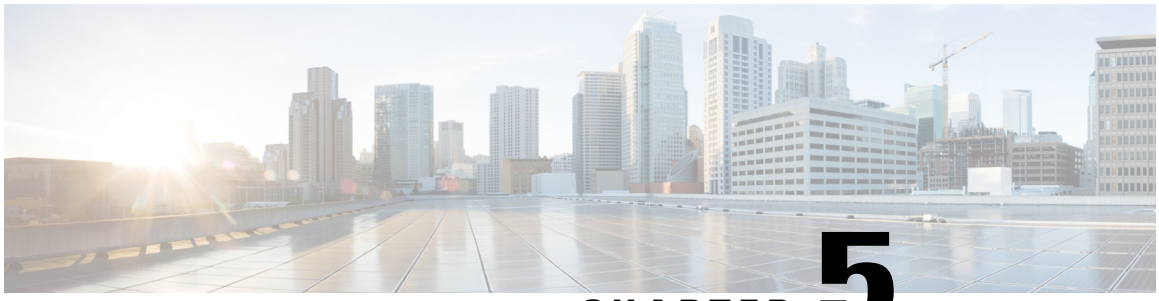
### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server # **scope chassis** | Enters the chassis command mode. |
| **Step 2** | Server /chassis # **scope pid-catalog** | Enters the server 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:<br>• TFTP<br>• FTP<br>• SFTP<br>• SCP<br>• HTTP<br>**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.<br>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.<br>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 |
|---|---|---|
| | | Initiates the upload of the PID catalog. |
| **Step 4** | Server /chassis/pid-catalog # **show detail** | (Optional)<br>Displays the status of the upload. |
| **Step 5** | Server /chassis/pid-catalog # **exit** | Returns to the chassis command mode. |
| **Step 6** | Server /chassis # **scope server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 7** | Server /chassis/server # **scope pid-catalog** | Enters server PID catalog command mode. |
| **Step 8** | Server /chassis/server/pid-catalog # **activate** | Activates the uploaded PID catalog. |
| **Step 9** | Server /chassis/server/pid-catalog # **show detail** | (Optional)<br>Displays the status of the activation. |

This example shows how to upload and activate 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 # show detail
    Upload Status: Upload Successful
Activating the uploaded PID catalog
Server /chassis/pid-catalog # exit
Server /chassis # scope server 2
Server /chassis/server # scope pid-catalog
Server /chassis/server/pid-catalog # activate
Successfully activated PID catalog
Server /chassis/server/pid-catalog # show detail
    Upload Status:
    Activation Status: Activation Successful
    Current Activated Version: 2.0(12.78).01
Server /chassis/server/pid-catalog #
```



CHAPTER 5

# Viewing Server Properties

This chapter includes the following sections:



## Viewing Server Properties

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server # **scope chassis** | Enters chassis command mode. |
| **Step 2** | Server /chassis # **scope server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 3** | Server /chassis /server # **show detail** | Displays server properties. |

This example displays server properties:

```
Server# scope chassis
Server /chassis #scope server 1
Server /chassis /Server #show
Server ID Power Serial Number Product Name  PID             UUID
```

```
--------- ----- ------------- ------------- ----------------
-----------------------------------
2         on    FCH183978RD   UCS C3260     UCSC-C3X60-SVRNB
207BD0D4-C589-40C1-A73E-EF6E7F773198

Server /chassis /Server #show detail
Server ID 1:
    Power: off
    Serial Number: FCH1848794D
    Product Name: UCS C3260
    PID: UCSC-C3X60-SVRNB
    UUID: 60974271-A514-484C-BAE3-A5EE4FD16E06
 Server /chassis /Server #
```

# Viewing CMC Properties

### 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 # **show detail** | Displays the CMC details for the chosen SIOC controller. |

This example shows how to view the CMC details:

```
server # scope chassis
server /chassis # scope cmc 1
server /chassis/cmc # show detail
CMC Firmware update initialized.
Please check the status using "show detail"
Server /chassis/cmc # show detail
Firmware Image Information:
    ID: 1
    Name: CMC1
    Serial Number: FCH19117MTU
    Update Stage: NONE
    Update Progress: 100
    Current FW Version: 2.0(10.97)
    FW Image 1 Version: 2.0(10.97)
    FW Image 1 State: RUNNING ACTIVATED
    FW Image 2 Version: 2.0(10.87)
    FW Image 2 State: BACKUP INACTIVATED
    Reset Reason: not-applicable (This provides the reason for the last Cisco IMC reboot.)
server /chassis/cmc #
```

# Viewing Server CPU Details

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server # **scope chassis** | Enters chassis command mode. |
| **Step 2** | Server /chassis # **scope server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 3** | Server /chassis /server # **show cpu** | Displays CPU details for the server. |
| **Step 4** | Server# **show cpu-pid** | Displays the CPU product IDs . |

This example displays the CPU details for the server:

```
Server# scope chassis
Server /chassis #scope server 1
Server /chassis /Server #show cpu
Name         Cores    Version
------------ -------- --------------------------------------------------
CPU1         6        Intel(R) Xeon(R) CPU E5-2620 v2 @ 2.10GHz
CPU2         6        Intel(R) Xeon(R) CPU E5-2620 v2 @ 2.10GHz

Server /chassis /Server #show cpu-pid
Socket Product ID           Model
------ -------------------- ----------------------------------------
CPU1   UCS-CPU-E52620B      Intel(R) Xeon(R) CPU E5-2620 v2 @ 2.1...
CPU2   UCS-CPU-E52620B      Intel(R) Xeon(R) CPU E5-2620 v2 @ 2.1...

 Server /chassis /Server #
```

# Viewing Memory Properties

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server # **scope chassis** | Enters chassis command mode. |
| **Step 2** | Server /chassis # **scope server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 3** | Server /chassis /server # **show dimm** | Displays DIMM details for the server. |
| **Step 4** | Server# **show dimm-pid** | Displays the DIMM product IDs. |
| **Step 5** | Server# **show dimm-summary** | Displays the DIMM summary information . |

This example displays the DIMM details for the server.:

```
Server# scope chassis
Server /chassis #scope server 1
```

```
Server /chassis /Server #show dimm
Name                 Capacity        Channel Speed (MHz) Channel Type
-------------------- --------------- ------------------- ---------------
DIMM_A1              16384 MB        1866                DDR3
DIMM_A2              16384 MB        1866                DDR3
DIMM_B1              16384 MB        1866                DDR3
DIMM_B2              16384 MB        1866                DDR3
DIMM_C1              16384 MB        1866                DDR3
DIMM_C2              16384 MB        1866                DDR3
DIMM_D1              16384 MB        1866                DDR3
DIMM_D2              16384 MB        1866                DDR3
DIMM_E1              16384 MB        1866                DDR3
DIMM_E2              16384 MB        1866                DDR3
DIMM_F1              16384 MB        1866                DDR3
DIMM_F2              16384 MB        1866                DDR3
DIMM_G1              16384 MB        1866                DDR3
DIMM_G2              16384 MB        1866                DDR3
DIMM_H1              16384 MB        1866                DDR3
DIMM_H2              16384 MB        1866                DDR3

Server /chassis /Server #show dimm-pid
Name               Product ID           Vendor ID  Capacity  Speed
------------------ -------------------- ---------- --------- ------
DIMM_A1            UCS-MR-1X162RZ-A     0xCE00     16384 MB  1866
DIMM_A2            UCS-MR-1X162RZ-A     0xCE00     16384 MB  1866
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

Server /chassis /Server #show dimm-summary
DIMM Summary:
    Memory Speed: 1600 MHz
    Total Memory: 262144 MB
    Effective Memory: 262144 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: Independent Mirroring Lockstep
    Memory Configuration: Independent


 Server /chassis /Server #
```

# Viewing PCI Adapter Properties for a Server

### Procedure

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

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | Server /chassis # **scope server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 3** | Server /chassis /server # **show pci-adapter** | Displays PCI adapter details for the server. |
| **Step 4** | Server# **show pciadapter-pid** | Displays the PCI adapter product IDs. |

This example displays the PCI adapter details for the server.:

```
Server# scope chassis
Server /chassis #scope server 1
Server /chassis /Server #show pci-adapter
Slot       Vendor ID  Device ID  SubVendor ID  SubDevice ID  Firmware Version Product Name

---------- ---------- ---------- ------------- ------------- -------------
-------------------------
1          0x1137     0x0042     0x1137        0x0157        4.0(300.71)   UCSC-C3260-SIOC

M          0x1000     0x005d     0x1137        0x012d        24.7.3-0006   Cisco RAID
controller ...

Server /chassis /Server #show pciadapter-pid
Slot   Product ID           Vendor ID  Device ID   SubVendor ID  SubDevice ID
------ -------------------- ---------- ----------- ------------- -------------
1      UNKNOWN              0x1137     0x0042      0x1137        0x0157
M      UCSC-C3X60-RAID      0x1000     0x005d      0x1137        0x012d

 Server /chassis /Server #
```

# Viewing HDD Details for a Server

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server # **scope chassis** | Enters chassis command mode. |
| **Step 2** | Server /chassis # **scope server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 3** | Server /chassis /server # **show hdd-pid** | Displays HDD details for the server. |

This example displays the HDD details for the server:

```
Server# scope chassis
Server /chassis #scope server 1
Server /chassis /Server #show hdd-pid
Disk Controller  Product ID           Vendor     Model
---- ----------- -------------------- ---------- ------------
1    SLOT-MEZZ   UCS-HD4T7KS3-E       TOSHIBA    MG03SCA400
2    SLOT-MEZZ   UCS-HD4T7KS3-E       TOSHIBA    MG03SCA400
3    SLOT-MEZZ   UCS-HD4T7KS3-E       TOSHIBA    MG03SCA400
4    SLOT-MEZZ   UCS-HD4T7KS3-E       TOSHIBA    MG03SCA400
5    SLOT-MEZZ   UCS-HD4T7KS3-E       TOSHIBA    MG03SCA400
6    SLOT-MEZZ   UCS-HD4T7KS3-E       TOSHIBA    MG03SCA400
7    SLOT-MEZZ   UCS-HD4T7KS3-E       TOSHIBA    MG03SCA400
```

```
8    SLOT-MEZZ   UCS-HD4T7KS3-E       TOSHIBA    MG03SCA400
9    SLOT-MEZZ   UCS-HD4T7KS3-E       TOSHIBA    MG03SCA400
10   SLOT-MEZZ   UCS-HD4T7KS3-E       TOSHIBA    MG03SCA400
11   SLOT-MEZZ   UCS-HD4T7KS3-E       TOSHIBA    MG03SCA400
12   SLOT-MEZZ   UCS-HD4T7KS3-E       TOSHIBA    MG03SCA400
13   SLOT-MEZZ   UCS-HD4T7KS3-E       TOSHIBA    MG03SCA400
14   SLOT-MEZZ   UCS-HD4T7KS3-E       TOSHIBA    MG03SCA400

 Server /chassis /Server#
```

# Viewing Storage Adapter Properties for a Server

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server # **scope chassis** | Enters chassis command mode. |
| **Step 2** | Server /chassis # **scope server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 3** | Server /chassis /server # **show storageadapter** | Displays storage adapter details for the server. |

This example displays the storage adapter details for the server.:

```
Server# scope chassis
Server /chassis #scope server 1
Server /chassis /Server #show storageadapter
PCI Slot     Health         Controller Status ROC Temperature Product Name

------------ -------------- ----------------- ---------------
----------------------------------
SLOT-MEZZ    Good           Optimal           48 degrees C    RAID controller for UCS C3X60
 S...

Serial Number   Firmware Package Build  Product ID  D Battery Status  Cache Memory Size
--------------  ----------------------  ----------  ----------------  -----------------
FCH184972F5      24.7.3-0006            LSI Logic   Optimal            3534 MB

Boot Drive  Boot Drive is PD
----------  -----------------
 0           false
 Server /chassis /Server #
```

# Viewing TPM Properties

### Procedure

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

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | Server /chassis # **scope server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 3** | Server /chassis/server # **show tpm-inventory** | Displays TPM properties for the server. |

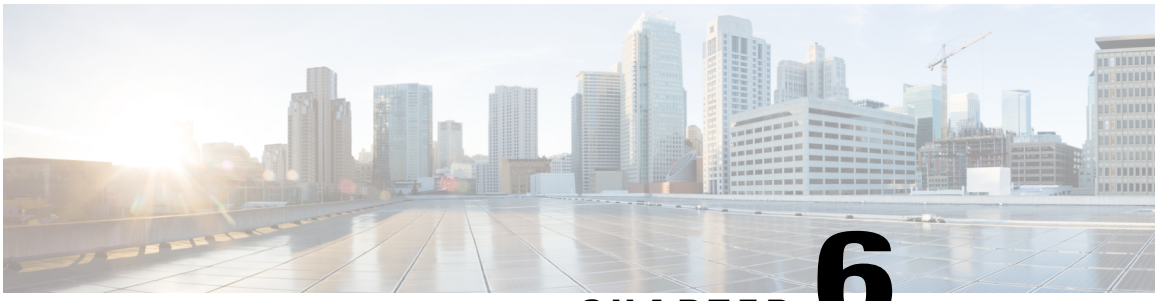
This example displays the TPM properties for the server:

```
Server# scope chassis
Server /chassis #scope server 1
Server /chassis /Server #show tpm-inventory
Version     Presence     Enabled-Status     Active-Status     Ownership Revision

----------- ------------ ------------------ ----------------- --------- ------------
NA          empty        unknown            unknown           unknown   NA

Model            Vendor               Serial
---------------- -------------------- ----------------

 Server chassis /Server#
```



CHAPTER 6

# Viewing Sensors

This chapter includes the following sections:



# Viewing Chassis Sensors

## 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 Current Sensors

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server# **scope sensor** | Enters sensor command mode. |
| **Step 2** | Server /sensor # **show current** | Displays current sensor statistics. |

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
------------ ------------- ---------- ------- ------------ ------------ ------------
------------
PSU1_IOUT    Normal          6.00       AMP        N/A          78.00        N/A
87.00
PSU2_IOUT    Normal          6.00       AMP        N/A          78.00        N/A
87.00
PSU3_IOUT    Normal          7.00       AMP        N/A          78.00        N/A
87.00
PSU4_IOUT    Normal          7.00       AMP        N/A          78.00        N/A
87.00

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** | Displays voltage sensor statistics. |

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
---------------- -------------- ---------- ------ ------------ ------------ ------------
------------
SIOC_P1V0        Normal         1.000      V          N/A          N/A          0.944
   1.064
SIOC_P1V2        Normal         1.208      V          N/A          N/A          1.128
   1.272
SIOC_P1V5        Normal         1.500      V          N/A          N/A          1.410
   1.590
SIOC_P2V5        Normal         2.478      V          N/A          N/A          2.338
   2.646
SIOC_P3V3        Normal         3.320      V          N/A          N/A          3.100
   3.500
SIOC_P12V_STBY   Normal         12.060     V          N/A          N/A          11.280
   12.720
SIOC_P3V3_STBY   Normal         3.360      V          N/A          N/A          3.140
   3.460
PSU1_VIN         Normal         228.000    V          N/A          N/A          N/A
   264.000
PSU2_VIN         Normal         228.000    V          N/A          N/A          N/A
   264.000
PSU3_VIN         Normal         228.000    V          N/A          N/A          N/A
   264.000
PSU4_VIN         Normal         228.000    V          N/A          N/A          N/A
   264.000
P5V_1            Normal         5.010      V          N/A          N/A          4.500
   5.640
P5V_2            Normal         5.010      V          N/A          N/A          4.500
   5.640
P5V_3            Normal         5.010      V          N/A          N/A          4.500
   5.640
P5V_4            Normal         5.010      V          N/A          N/A          4.500
   5.640
P0V9_EXP1_VCORE  Normal         0.872      V          N/A          N/A          0.836
   0.976
P0V9_EXP2_VCORE  Normal         0.872      V          N/A          N/A          0.836
   0.976
P0V9_EXP1_AVD    Normal         0.888      V          N/A          N/A          0.836
   0.976
P0V9_EXP2_AVD    Normal         0.904      V          N/A          N/A          0.836
   0.976
PSU1_VOUT        Normal         12.000     V          N/A          N/A          N/A
   12.600
PSU2_VOUT        Normal         12.000     V          N/A          N/A          N/A
   12.600
PSU3_VOUT        Normal         12.000     V          N/A          N/A          N/A
   12.600
PSU4_VOUT        Normal         12.000     V          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** | Displays temperature sensor statistics. |

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
----------------- -------------- ------- -------- ------------ ------------ ------------
------------
SIOC1_BACK_TEMP    Normal         37.0       C          N/A          70.0         N/A
     80.0
SIOC1_FRONT_TEMP   Normal         42.0       C          N/A          70.0         N/A
     80.0
SIOC1_MID_TEMP     Normal         41.0       C          N/A          70.0         N/A
     80.0
SIOC1_VIC_TEMP     Normal         44.0       C          N/A          70.0         N/A
     80.0
SIOC2_VIC_TEMP     Normal         44.0       C          N/A          70.0         N/A
     80.0
MOBO_R_BOT_TEMP    Normal         30.0       C          N/A          70.0         N/A
     80.0
MOBO_L_BOT_TEMP    Normal         31.0       C          N/A          70.0         N/A
     80.0
MOBO_R_MID_TEMP    Normal         25.0       C          N/A          50.0         N/A
     55.0
MOBO_R_IN_TEMP     Normal         24.0       C          N/A          50.0         N/A
     55.0
MOBO_L_IN_TEMP     Normal         26.0       C          N/A          50.0         N/A
     55.0
MOBO_L_MID_TEMP    Normal         26.0       C          N/A          50.0         N/A
     55.0
MOBO_R_OUT_TEMP    Normal         29.0       C          N/A          47.0         N/A
     52.0
MOBO_L_OUT_TEMP    Normal         29.0       C          N/A          46.0         N/A
     51.0
PSU1_TEMP          Normal         24.0       C          N/A          55.0         N/A
     60.0
PSU2_TEMP          Normal         27.0       C          N/A          55.0         N/A
     60.0
PSU3_TEMP          Normal         27.0       C          N/A          55.0         N/A
     60.0
PSU4_TEMP          Normal         25.0       C          N/A          55.0         N/A
     60.0
SIOC1_CMC_TEMP     Normal         51.0       C          N/A          75.0         N/A
     85.0
MOBO_R_EXP_TEMP    Normal         37.0       C          N/A          80.0         N/A
     90.0
MOBO_L_EXP_TEMP    Normal         40.0       C          N/A          80.0         N/A
     90.0
SIOC2_BACK_TEMP    Normal         36.0       C          N/A          70.0         N/A
     80.0
SIOC2_FRONT_TEMP   Normal         36.0       C          N/A          70.0         N/A
     80.0
SIOC2_MID_TEMP     Normal         36.0       C          N/A          70.0         N/A
     80.0
```

```
SIOC2_CMC_TEMP     Normal         36.0       C          N/A          75.0         N/A
     85.0
Server /sensor #
```

# Viewing LED Sensor

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server# **scope sensor** | Enters sensor command mode. |
| **Step 2** | Server /sensor # **show led** | Displays LED sensor statistics. |

This example displays LED sensor statistics:

```
Server# scope sensor
Server /sensor # show led
LED Name                  LED State  LED Color
------------------------- ---------- --------
LED_FAN12_FAULT           OFF        AMBER
LED_FAN34_FAULT           OFF        AMBER
LED_FAN56_FAULT           OFF        AMBER
LED_FAN78_FAULT           OFF        AMBER
CHS_FP_LED_ID             OFF        BLUE
LED_HLTH_STATUS           ON         GREEN
LED_PSU_STATUS            ON         GREEN
LED_TEMP_STATUS           ON         GREEN
LED_FAN_STATUS            ON         GREEN
SERVER1_FP_ID_LED         OFF        BLUE
SERVER2_FP_ID_LED         OFF        BLUE
OVERALL_DIMM_STATUS       ON         GREEN
Server /sensor #
```

# Viewing Server Sensors

# Viewing Storage Sensors

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server # **scope server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 2** | Server /server # **scope sensor** | Enters sensor command. |
| **Step 3** | Server /server /sensor #**show hdd** | Displays the storage sensors for the server. |

This example displays the storage sensors for the server:

```
Server# scope server 1
Server /server #scope sensor
Server /server /sensor #show hdd
Name                 Status
-------------------- --------------------
SSD1_PRS             inserted
SSD2_PRS             inserted

 Server server /sensor #
```

# Viewing Current Sensors

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server # **scope server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 2** | Server /server # **scope sensor** | Enters sensor command. |
| **Step 3** | Server /server /sensor #**show current** | Displays the current sensors for the server. |

This example displays the current sensors for the server:

```
Server# scope server 1
Server /server #scope sensor
Server /server /sensor #show current
Name           Sensor Status  Reading  Units   Min. Warning Max. Warning Min. Failure Max.
 Failure
-------------- -------------- -------- ------- ------------ ------------ ------------
------------
P12V_CUR_SENS  Normal         5.84       AMP        N/A          N/A          N/A
 56.90
Server server /sensor #
```

# Viewing LED Sensors

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server # **scope server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 2** | Server /server # **scope sensor** | Enters sensor command. |
| **Step 3** | Server /server /sensor #**show led** | Displays the LED sensors for the server. |

This example displays the LED sensors for the server:

```
Server# scope server 1
Server /server #scope sensor
Server /server /sensor #show led
LED Name                  LED State  LED Color
------------------------- ---------- --------
FP_ID_LED                 FAST BLINK BLUE
P1_DIMM_A1_LED            OFF        AMBER
P1_DIMM_A2_LED            OFF        AMBER
P1_DIMM_B1_LED            OFF        AMBER
P1_DIMM_B2_LED            OFF        AMBER
P1_DIMM_C1_LED            OFF        AMBER
P1_DIMM_C2_LED            OFF        AMBER
P1_DIMM_D1_LED            OFF        AMBER
P1_DIMM_D2_LED            OFF        AMBER
P2_DIMM_E1_LED            OFF        AMBER
P2_DIMM_E2_LED            OFF        AMBER
P2_DIMM_F1_LED            OFF        AMBER
P2_DIMM_F2_LED            OFF        AMBER
P2_DIMM_G1_LED            OFF        AMBER
P2_DIMM_G2_LED            OFF        AMBER
P2_DIMM_H1_LED            OFF        AMBER
P2_DIMM_H2_LED            OFF        AMBER
LED_HLTH_STATUS           ON         GREEN
LED_TEMP_STATUS           ON         GREEN
OVERALL_DIMM_STATUS       ON         GREEN

 Server server /sensor #
```

# Viewing Temperature Sensors

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server # **scope server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 2** | Server /server # **scope sensor** | Enters sensor command. |
| **Step 3** | Server /server /sensor #**show temperature** | Displays the temperature sensors for the server. |

This example displays the temperature sensors for the server:

```
Server# scope server 1
Server /server #scope sensor
Server /server /sensor #show temperature
Name            Sensor Status  Reading  Units    Min. Warning Max. Warning Min. Failure
Max. Failure
--------------- -------------- -------- -------- ------------ ------------ ------------
------------
TEMP_SENS_FRONT  Normal         24.0       C          N/A          60.0         N/A
   70.0
TEMP_SENS_REAR   Normal         25.0       C          N/A          80.0         N/A
   85.0
P1_TEMP_SENS     Normal         21.0       C          N/A          74.0         N/A
   79.0
P2_TEMP_SENS     Normal         23.5       C          N/A          74.0         N/A
   79.0
DDR3_P1_A1_TEMP  Normal         23.0       C          N/A          65.0         N/A
```

```
   85.0
DDR3_P1_A2_TEMP  Normal          23.0       C          N/A          65.0         N/A
   85.0
DDR3_P1_B1_TEMP  Normal          23.0       C          N/A          65.0         N/A
   85.0
DDR3_P1_B2_TEMP  Normal          23.0       C          N/A          65.0         N/A
   85.0
DDR3_P1_C1_TEMP  Normal          24.0       C          N/A          65.0         N/A
   85.0
DDR3_P1_C2_TEMP  Normal          24.0       C          N/A          65.0         N/A
   85.0
DDR3_P1_D1_TEMP  Normal          24.0       C          N/A          65.0         N/A
   85.0
DDR3_P1_D2_TEMP  Normal          23.0       C          N/A          65.0         N/A
   85.0
DDR3_P2_E1_TEMP  Normal          23.0       C          N/A          65.0         N/A
   85.0
DDR3_P2_E2_TEMP  Normal          23.0       C          N/A          65.0         N/A
   85.0
DDR3_P2_F1_TEMP  Normal          22.0       C          N/A          65.0         N/A
   85.0

Server server /sensor #
```

# Viewing Voltage Sensors

### Procedure

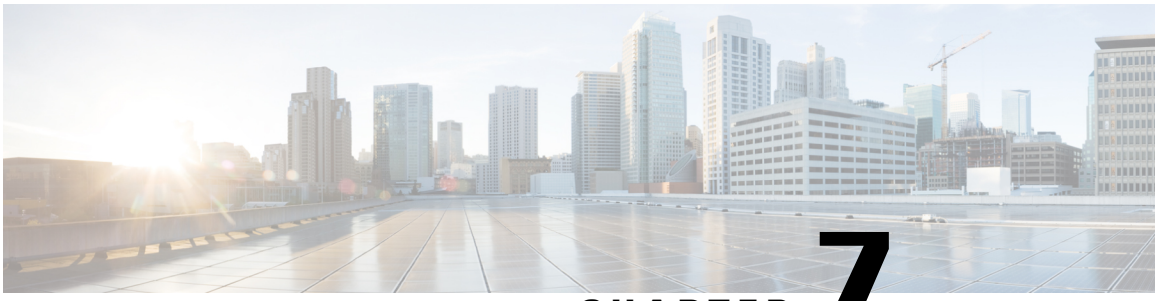
| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server # **scope server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 2** | Server /server # **scope sensor** | Enters sensor command. |
| **Step 3** | Server /server /sensor #**show voltage** | Displays the voltage sensors for the server. |

This example displays the voltage sensors for the server:

```
Server# scope server 1
Server /server #scope sensor
Server /server /sensor #show voltage
Name            Sensor Status  Reading  Units    Min. Warning Max. Warning Min. Failure
Max. Failure
--------------- -------------- -------- -------- ------------ ------------ ------------
------------
P3V_BAT_SCALED   Normal         2.973      V          N/A          N/A          2.154
   3.418
P5V_STBY         Normal         4.909      V          N/A          N/A          4.555
   5.452
P3V3_STBY        Normal         3.302      V          N/A          N/A          3.018
   3.602
P1V1_SSB_STBY    Normal         1.088      V          N/A          N/A          1.000
   1.205
P1V8_STBY        Normal         1.784      V          N/A          N/A          1.627
   1.980
P1V0_STBY        Normal         0.990      V          N/A          N/A          0.911
   1.088
P1V5_STBY        Normal         1.490      V          N/A          N/A          1.372
   1.637
P0V75_STBY       Normal         0.725      V          N/A          N/A          0.686
   0.823
P2V5_STBY        Normal         2.484      V          N/A          N/A          2.279
```

```
   2.734
P12V             Normal          11.977      V           N/A           N/A           11.210
   12.803
P5V              Normal          5.031       V           N/A           N/A           4.680
   5.335
P3V3             Normal          3.276       V           N/A           N/A           3.089
   3.526
P1V5_SSB         Normal          1.482       V           N/A           N/A           1.412
   1.607
P1V1_SSB         Normal          1.084       V           N/A           N/A           1.037
   1.178
PVTT_P1          Normal          0.991       V           N/A           N/A           0.944
   1.061
PVTT_P2          Normal          0.975       V           N/A           N/A           0.944
   1.061
PVSA_P1          Normal          0.959       V           N/A           N/A           0.593
   1.170

Server server /sensor #
```



CHAPTER 7

# 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** To configure the KVM console successfully for the Cisco UCS C3260 server, you need to configure IP addresses for the Cisco IMC, CMC, and BMC components. You can configure the IP addresses for these components using the CLI interface or Web UI. For the CLI, use the command **scope network**, or view the setting using **scope <chassis/server1/2><cmc/bmc><network>**.

To configure IP addresses for network components on the web interface, see the steps described in the section **Configuring Network-Related Settings**.

**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 server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 2** | Server /server # **scope kvm** | Enters KVM command mode. |
| **Step 3** | Server /server/kvm # **set enabled yes** | Enables the virtual KVM. |
| **Step 4** | Server /server/kvm # **commit** | Commits the transaction to the system configuration. |
| **Step 5** | Server /server/kvm # **show** [**detail**] | (Optional) Displays the virtual KVM configuration. |

This example enables the virtual KVM:

```
Server# scope server 1
Server /server # scope kvm
Server /server/kvm # set enabled yes
Server /server/kvm *# commit
Server /server/kvm # show detail
KVM Settings:
    Encryption Enabled: yes
    Max Sessions: 4
    Local Video: yes
    Active Sessions: 1
    Enabled: yes
    KVM Port: 2068

Server /server/kvm #
```

# Disabling 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 server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 2** | Server /server # **scope kvm** | Enters KVM command mode. |
| **Step 3** | Server /server /kvm # **set enabled no** | Disables the virtual KVM.<br>**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 4** | Server /server/kvm # **commit** | Commits the transaction to the system configuration. |
| **Step 5** | Server /server/kvm # **show** [**detail**] | (Optional) Displays the virtual KVM configuration. |

This example enables the virtual KVM:

```
Server# scope server 1
Server /server # scope kvm
Server /server/kvm # set enabled no
Server /server/kvm *# commit
Server /server/kvm # show detail
KVM Settings:
    Encryption Enabled: yes
    Max Sessions: 4
    Local Video: yes
    Active Sessions: 0
    Enabled: no
    KVM Port: 2068

Server /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 server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | Server /server# **scope kvm** | Enters KVM command mode. |
| **Step 3** | Server /server/kvm # **set enabled** {**yes** \| **no**} | Enables or disables the virtual KVM. |
| **Step 4** | Server /server/kvm # **set encrypted** {**yes** \| **no**} | If encryption is enabled, the server encrypts all video information sent through the KVM. |
| **Step 5** | Server /server/kvm # **set kvm-port** *port* | Specifies the port used for KVM communication. |
| **Step 6** | Server /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 7** | Server /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 8** | Server /server/kvm # **commit** | Commits the transaction to the system configuration. |
| **Step 9** | Server /server/kvm # **show** [**detail**] | (Optional) Displays the virtual KVM configuration. |

This example configures the virtual KVM and displays the configuration:

```
Server# scope server 1
Server /server # scope kvm
Server /server/kvm # set enabled yes
Server /server/kvm *# set encrypted no
Server /server/kvm *# set kvm-port 2068
Server /server/kvm *# set max-sessions 4
Server /server/kvm *# set local-video yes
Server /server/kvm *# commit
Server /server/kvm # show detail
KVM Settings:
    Encryption Enabled: no
    Max Sessions: 4
    Local Video: yes
    Active Sessions: 0
    Enabled: yes
    KVM Port: 2068

Server /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.<br>**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.<br>**Note** While mapping an ISO to a server which has a UCS VIC P81E card and the NIC is in Cisco Card mode:<br>• 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.<br>• 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. |
| **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 server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 2** | Server /server# **scope vmedia** | Enters the virtual media command mode. |
| **Step 3** | Server /server/vmedia # **map-cifs** {**volume-name** \| **remote-share** \| **remote-file-path** [*mount options*] | Maps a CIFS file for vMedia. You must specify the following:<br>• Name of the volume to create<br>• Remote share including IP address and the exported directory<br>• Path of the remote file corresponding to the exported directory.<br>• (Optional) Mapping options<br>• Username and password to connect to the server |
| **Step 4** | Server /server/vmedia # **map-nfs** {**volume-name** \| **remote-share** \| **remote-file-path**} [*mount options*] | Maps an NFS file for vMedia. You must specify the following:<br>• Name of the volume to create<br>• Remote share including IP address and the exported directory<br>• Path of the remote file corresponding to the exported directory.<br>• (Optional) Mapping options |
| **Step 5** | Server /server/vmedia # **map-www** {**volume-name** \| **remote-share** \| **remote-file-path** [*mount options*] | Maps an HTTPS file for vMedia. You must specify the following:<br>• Name of the volume to create<br>• Remote share including IP address and the exported directory<br>• Path of the remote file corresponding to the exported directory.<br>• (Optional) Mapping options<br>• Username and password to connect to the server |

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

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

```
Server # scope server 1
Server /server #scope vmedia
Server /server/vmedia # map-cifs sample-volume //10.10.10.10/project /test/sample
Server username:
Server password: ****
Confirm password: ****

Server /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 server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 2** | Server /server # **scope vmedia** | Enters the virtual media command mode. |
| **Step 3** | Server /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 server 1
Server /server/scope vmedia
Server /server/vmedia # show mappings

Volume  Map-status   Drive-type     remote-share        remote-file               mount-type
------  ----------  ------------  --------------------- --------------------      -----------

Huu     OK           removable    http://10.104.236.99/ rhel-server-6.1-x86_6.iso      www
Rhel    OK           CD           http://10.104.236.99/ rhel-server-6.1-x86_6.iso      www


Server /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).

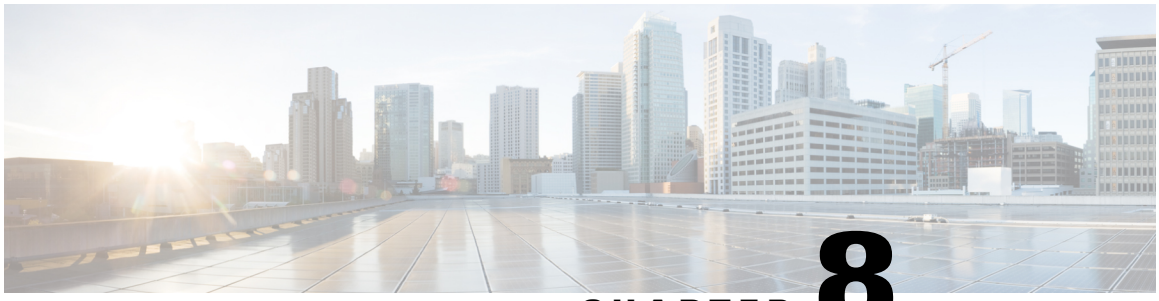
#### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server # **scope server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 2** | Server /server# **scope sol** | Enters SoL command mode. |
| **Step 3** | Server /server/sol # **set enabled** {**yes** \| **no**} | Enables or disables SoL on this server. |
| **Step 4** | Server /server/sol # **set baud-rate** {**9600** \| **19200** \| **38400** \| **57600** \| **115200**} | Sets the serial baud rate the system uses for SoL communication.<br>**Note** The baud rate must match the baud rate configured in the server serial console. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | Server /server/sol # **set comport** {**com0** \| **com1** | (Optional)<br>Sets the serial port through which the system routes SoL communications.<br>**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.<br>You can specify:<br>• **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.<br>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.<br>• **com1—**SoL communication is routed through COM port 1, an internal port accessible only through SoL.<br>If you select this option, you can use SoL on COM port 1 and the physical RJ45 connection on COM port 0.<br>**Note** Changing the comport setting disconnects any existing SoL sessions. |
| **Step 6** | Server /sol # **commit** | Commits the transaction to the system configuration. |
| **Step 7** | Server /sol # **show** [**detail**] | (Optional) Displays the SoL settings. |

This example configures SoL:

```
Server# scope server 1
Server /server #scope sol
Server /server/sol # set enabled yes
Server /server/sol *# set baud-rate 115200
Server /server/sol *# set comport com1
Server /server/sol *# commit
Server /server/sol # show
Enabled Baud Rate(bps)  Com Port
------- --------------- --------
yes     115200          com1
Server /sol # show detail
Serial Over LAN:
    Enabled: yes
    Baud Rate(bps): 115200
    Com Port: com1
Server /server/sol #
```



CHAPTER 8

# 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*. |
| **Step 2** | Server /user # **set enabled** {**yes** \| **no**} | Enables or disables the user account on the Cisco IMC. |

| | Command or Action | Purpose |
|---|---|---|
| **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.<br>**Note** When strong password is enabled, you must follow these guidelines while setting a password:<br>• The password must have a minimum of 8 and a maximum of 14 characters.<br>• The password must not contain the User's Name.<br>• The password must contain characters from three of the following four categories:<br>◦ English uppercase characters (A through Z)<br>◦ English lowercase characters (a through z)<br>◦ Base 10 digits (0 through 9)<br>◦ Non-alphabetic characters (!, @, #, $, %, ^, &, *, -, _, +, =)<br>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:<br>• readonly—This user can view information but cannot make any changes.<br>• user—This user can do the following:<br>• View all information<br>• Manage the power control options such as power on, power cycle, and power off<br>• Launch the KVM console and virtual media<br>• Clear all logs<br>• Toggle the locator LED<br>• Set the time zone<br>• Ping an IP address<br>• admin—This user can perform all actions available through the GUI, CLI, and IPMI. |
| **Step 6** | Server /user # **commit** | Commits the transaction to the system configuration. |

This example configures user 5 as an admin:

```
Server# scope user 5
Server /user # set enabled yes
Server /user *# set name john
Server /user *# set password
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 #
```

# 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.

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 |

| Properties | Value |
|---|---|
| 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. |
| **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.<br>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:<br>`1.3.6.1.4.1.9.287247.1`<br>**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:<br>• **admin—**The user can perform all actions available.<br>• **user—**The user can perform the following tasks:<br>◦ View all information |

| | Command or Action | Purpose |
|---|---|---|
| | | ◦ Manage the power control options such as power on, power cycle, and power off<br>◦ Launch the KVM console and virtual media<br>◦ Clear all logs<br>◦ Toggle the locator LED<br>• **readonly—**The user can view information but cannot make any changes. |
| **Step 8** | Server /ldap/role-group # **commit** | Commits the transaction to the system configuration. |

This example shows how to configure LDAP group authorization:

```
Server# scope ldap
Server /ldap # scope ldap-group-rule
Server /ldap/ldap-group-rule # set group-auth yes
Server /ldap *# scope role-group 5
Server /ldap/role-group # set name Training
Server /ldap/role-group* # set domain example.com
Server /ldap/role-group* # set role readonly
Server /ldap/role-group* # commit
ucs-c250-M2 /ldap # show role-group
Group  Group Name       Domain Name      Assigned Role
------ -----------     --------------   --------------
1      (n/a)            (n/a)            admin
2      (n/a)            (n/a)            user
3      (n/a)            (n/a)            readonly
4      (n/a)            (n/a)            (n/a)
5      Training         example.com      readonly

Server /ldap/role-group #
```

# 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. |

| | Command or Action | Purpose |
|---|---|---|
| **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. |

| | Command or Action | Purpose |
|---|---|---|
| **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:<br>• TFTP<br>• FTP<br>• SFTP<br>• SCP<br>• HTTP<br>**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.<br>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.<br>The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.<br>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. |
| **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. |
| **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 # **download-ca-certificate** *remote-protocol IP Address LDAP CA Certificate file* | Specifies the protocol to connect to the remote server. It can be of the following types:<br>• TFTP<br>• FTP<br>• SFTP<br>• SCP<br>• HTTP<br>**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.<br>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.<br>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 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 #  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 #
```

# 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 |
|---|---|
| **Terminate Session** button | If your user account is assigned the **admin** user role, this option enables you to force the associated user session to end.<br>**Note** You cannot terminate your current session from this tab. |
| **Session ID** column | The unique identifier for the session. |

| Name | Description |
|---|---|
| **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:<br>• **webgui—** indicates the user is connected to the server using the web UI.<br>• **CLI—** indicates the user is connected to the server using CLI.<br>• **serial—** indicates the user is connected to the server using the serial port. |

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

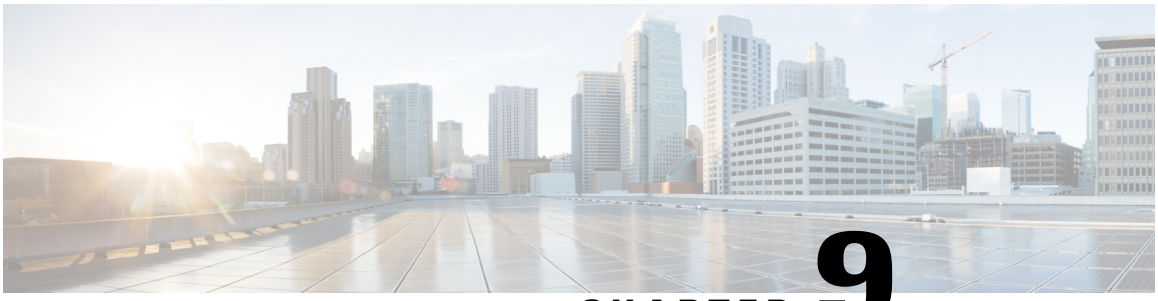
| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server# **show user-session** | Displays information about current user sessions. The user session to be terminated must be eligible to be terminated (killable) and must not be your own session. |
| **Step 2** | Server /user-session # **scope 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 9

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

### NIC Redundancy

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

- **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 the Cisco IMC.
- **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 subnet to ensure that traffic is secure regardless of which port is used.

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

# Configuring 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 network** | Enters the Cisco IMC network command mode. |
| **Step 2** | Server /network # **set mode** {**dedicated** \| **cisco_card**} | Sets the NIC mode to one of the following:<br>• Dedicated—The management Ethernet port is used to access the Cisco IMC.<br>• Cisco card—The ports on the adapter card are used to access the Cisco IMC. |
| **Step 3** | Server /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:<br>• **none—**The LOM Ethernet ports operate independently and do not fail over if there is a problem.<br>• **active-active—**If supported, all LOM Ethernet ports are utilized.<br>• **active-standby—**If one LOM Ethernet port fails, traffic fails over to another LOM port. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | Server /network # **commit** | Commits the transaction to the system configuration.<br>**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 5** | At the prompt, enter y to confirm. | Configures the server NIC. |

This example configures the Cisco IMC network interface:

```
Server  # scope network
Server /network # set mode cisco_card
Server /network *# set redundancy <active-active>
Server /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 /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 network** | Enters the Cisco IMC network command mode. |
| **Step 2** | Server /network # **set hostname-bmc1 hostname-bmc2hostname-cmc1hostname-cmc2***host-name* | Specifies the name of the host for the following components:<br>• **BMC 1**<br>• **BMC 2**<br>• **CMC 1**<br>• **CMC 2**<br>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.<br>If you enter **y** at the prompt, a new self-signed certificate is created with CN as the new hostname. |

| | Command or Action | Purpose |
|---|---|---|
| | | If you enter **n** at the prompt, only the hostname is changed and no certificate will be generated. |
| **Step 3** | Server /network # **set ddns-enabled** | (Optional)<br>Enables the DDNS service for Cisco IMC |
| **Step 4** | Server /network # **set ddns-update-domain** *value* | (Optional)<br>Updates the selected domain or its subdomain. |
| **Step 5** | Server /network # **commit** | Commits the transaction to the system configuration. |
| **Step 6** | At the prompt, enter y to confirm. | Configures common properties. |

This example shows how to configure the common properties:

```
Server # scope network
Server /network # set hostname-cmc1 cmc1
Server /network *# set ddns-enabled
Server /network *# set ddns-update-domain 1.2.3.4
Server /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 /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 network** | Enters the Cisco IMC network command mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | Server /network # **set dhcp-enabled** {**yes** \| **no**} | Selects whether the Cisco IMC uses DHCP.<br>**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 3** | Server /network # **set v4-addr** *ipv4-address* | Specifies the IP address for the Cisco IMC. |
| **Step 4** | Server /network # **set v4-netmask** *ipv4-netmask* | Specifies the subnet mask for the IP address. |
| **Step 5** | Server /network # **set v4-gateway** *gateway-ipv4-address* | Specifies the gateway for the IP address. |
| **Step 6** | Server /network # **set dns-use-dhcp** {**yes** \| **no**} | Selects whether the Cisco IMC retrieves the DNS server addresses from DHCP. |
| **Step 7** | Server /network # **set preferred-dns-server** *dns1-ipv4-address* | Specifies the IP address of the primary DNS server. |
| **Step 8** | Server /network # **set alternate-dns-server** *dns2-ipv4-address* | Specifies the IP address of the secondary DNS server. |
| **Step 9** | Server /network # **commit** | Commits the transaction to the system configuration. |
| **Step 10** | At the prompt, enter y to confirm. | Configures IPv4. |
| **Step 11** | Server /network # **show** [**detail**] | (Optional) Displays the IPv4 network settings. |

This example configures and displays the IPv4 network settings:

```
Server  # scope network
Server /network # set dhcp-enabled yes
Server /network *# set v4-addr 10.20.30.11
Server /network *# set v4-netmask 255.255.248.0
Server /network *# set v4-gateway 10.20.30.1
Server /network *# set dns-use-dhcp-enabled no
Server /network *# set preferred-dns-server 192.168.30.31
Server /network *# set alternate-dns-server 192.168.30.32
Server /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 /network # show detail
Network Setting:
    IPv4 Enabled: yes
    IPv4 Netmask: 255.255.248.0
    IPv4 Gateway: 10.20.30.1
    DHCP Enabled: no
    DDNS Enabled: yes
    DDNS Update Domain:
    Obtain DNS Server by DHCP: no
    Preferred DNS: 192.168.30.31
```

```
    Alternate DNS: 192.168.30.32
    IPv6 Enabled: no
    IPv6 Prefix: 64
    IPv6 Gateway: ::
    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
    NIC Mode: dedicated
    NIC Redundancy: none
    SIOC Slot: 1
    Management IPv4 Address: 10.106.145.202
    Management IPv6 Address: ::
    Management Hostname: C3260-FCH18207WF3
    Network Speed: 100Mbps
    Duplex: full
    Auto Negotiate: yes
    Admin Network Speed: auto
    Admin Duplex: auto
    Operational Network Speed: 1Gbps
    Operational Duplex: full
CMC 1 Network Setting:
    IPv4 Address CMC 1: 10.20.30.11
    IPv6 Address CMC 1: ::
    IPv6 Link Local CMC 1: ::
    IPv6 SLAAC Address CMC 1: ::
    Hostname CMC 1: UCS-C3260-FCH181772ZP-1
    MAC Address CMC 1: F4:CF:E2:77:7F:D2
CMC 2 Network Setting:
    IPv4 Address CMC 2: 10.20.30.11
    IPv6 Address CMC 2: ::
    IPv6 Link Local CMC 2: ::
    IPv6 SLAAC Address CMC 2: ::
    Hostname CMC 2: UCS-C3260--2
    MAC Address CMC 2: F4:CF:E2:77:80:83
BMC 1 Network Setting:
    IPv4 Address BMC 1: 10.20.30.11
    IPv6 Address BMC 1: ::
    IPv6 Link Local BMC 1: ::
    IPv6 SLAAC Address BMC 1: ::
    Hostname BMC 1: C3160-FCH1827K9YT
    MAC Address BMC 1: 7C:0E:CE:5A:EF:26
BMC 2 Network Setting:
    IPv4 Address BMC 2: 10.20.30.11
    IPv6 Address BMC 2: ::
    IPv6 Link Local BMC 2: ::
    IPv6 SLAAC Address BMC 2: ::
    Hostname BMC 2: C3160-FCH18407MYD
    MAC Address BMC 2: A0:EC:F9:85:90:3F


Server /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 network** | Enters the Cisco IMC network command mode. |
| **Step 2** | Server /network # **set v6-enabled** {**yes** \| **no**} | Enables IPv6. |
| **Step 3** | Server /network # **set v6-dhcp-enabled** {**yes** \| **no**} | Selects whether the Cisco IMC uses DHCP.<br>**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 4** | Server /network # **set v6-addr-bmc1v6-addr-bmc2v6-addr-cmc1v6-addr-cmc2 v6-addr-mgmt***ipv6-address* | Specifies the IP address for the following components:<br>• BMC1 IPv6 Address<br>• BMC2 IPv6 Address<br>• CMC1 IPv6 Address<br>• CMC2 IPv6 Address<br>• Management IPv6 Address |
| **Step 5** | Server /network # **set v6-prefix** *ipv6-prefix-length* | Specifies the prefix length for the IP address. |
| **Step 6** | Server /network # **set v6-gateway** *gateway-ipv6-address* | Specifies the gateway for the IP address. |
| **Step 7** | Server /network # **set v6-dns-use-dhcp** {**yes** \| **no**} | Selects whether the Cisco IMC retrieves the DNS server addresses from DHCP.<br>**Note** You can use this option only when DHCP enabled. |
| **Step 8** | Server /network # **set v6-preferred-dns-server** *dns1-ipv6-address* | Specifies the IP address of the primary DNS server. |
| **Step 9** | Server /network # **set v6-alternate-dns-server** *dns2-ipv6-address* | Specifies the IP address of the secondary DNS server. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 10** | Server /network # **commit** | Commits the transaction to the system configuration. |
| **Step 11** | At the prompt, enter y to confirm. | Configures IPv6. |
| **Step 12** | Server /network # **show** [**detail**] | (Optional) Displays the IPv6 network settings. |

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

```
Server # scope network
Server /network # set v6-enabled yes
Server /network *# set v6-addr-bmc1 2010:201::279
Server /network *# set v6-gateway 2010:201::1
Server /network *# set v6-prefix 64
Server /network *# set v6-dns-use-dhcp no
Server /network *# set v6-preferred-dns-server 2010:201::100
Server /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 /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 /network # show detail
Network Setting:
    IPv4 Enabled: yes
    IPv4 Netmask: 255.255.255.0
    IPv4 Gateway: 10.106.145.1
    DHCP Enabled: no
    DDNS Enabled: yes
    DDNS Update Domain:
    Obtain DNS Server by DHCP: no
    Preferred DNS: 171.70.168.183
    Alternate DNS: 0.0.0.0
    IPv6 Enabled: no
    IPv6 Prefix: 64
    IPv6 Gateway: 2010:201::1
    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: abcde12345
    NIC Mode: dedicated
    NIC Redundancy: none
    SIOC Slot: 1
    Management IPv4 Address: 10.106.145.202
    Management IPv6 Address: ::
    Management Hostname: C3260-FCH18207WF3
    Network Speed: 100Mbps
    Duplex: full
    Auto Negotiate: yes
    Admin Network Speed: auto
    Admin Duplex: auto
    Operational Network Speed: 1Gbps
    Operational Duplex: full
CMC 1 Network Setting:
    IPv4 Address CMC 1: 10.106.145.135
    IPv6 Address CMC 1:  ::
    IPv6 Link Local CMC 1: ::
    IPv6 SLAAC Address CMC 1: ::
```

```
    Hostname CMC 1: UCS-C3260-FCH181772ZP-1
    MAC Address CMC 1: F4:CF:E2:77:7F:D2
CMC 2 Network Setting:
    IPv4 Address CMC 2: 10.106.145.248
    IPv6 Address CMC 2:  ::
    IPv6 Link Local CMC 2: ::
    IPv6 SLAAC Address CMC 2: ::
    Hostname CMC 2: UCS-C3260--2
    MAC Address CMC 2: F4:CF:E2:77:80:83
BMC 1 Network Setting:
    IPv4 Address BMC 1: 10.106.145.41
    IPv6 Address BMC 1:  2010:201::279
    IPv6 Link Local BMC 1: ::
    IPv6 SLAAC Address BMC 1: ::
    Hostname BMC 1: C3160-FCH1827K9YT
    MAC Address BMC 1: 7C:0E:CE:5A:EF:26
BMC 2 Network Setting:
    IPv4 Address BMC 2: 10.106.145.39
    IPv6 Address BMC 2:  ::
    IPv6 Link Local BMC 2: ::
    IPv6 SLAAC Address BMC 2: ::
    Hostname BMC 2: C3160-FCH18407MYD
    MAC Address BMC 2: A0:EC:F9:85:90:3F

Server /network #
```

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

```
Server  # scope network
Server /network # set v6-enabled yes
Server /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 /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 /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: auto
    Admin Duplex: auto
    Operational Network Speed: 1Gbps
```

```
    Operational Duplex: full
CMC 1 Network Setting:
    IPv4 Address CMC 1: 10.106.145.135
    IPv6 Address CMC 1: ::
    IPv6 Link Local CMC 1: ::
    IPv6 SLAAC Address CMC 1: ::
    Hostname CMC 1: UCS-C3260-FCH181772ZP-1
    MAC Address CMC 1: F4:CF:E2:77:7F:D2
CMC 2 Network Setting:
    IPv4 Address CMC 2: 10.106.145.248
    IPv6 Address CMC 2: ::
    IPv6 Link Local CMC 2: ::
    IPv6 SLAAC Address CMC 2: ::
    Hostname CMC 2: UCS-C3260--2
    MAC Address CMC 2: F4:CF:E2:77:80:83
BMC 1 Network Setting:
    IPv4 Address BMC 1: 10.106.145.41
    IPv6 Address BMC 1: ::
    IPv6 Link Local BMC 1: ::
    IPv6 SLAAC Address BMC 1: ::
    Hostname BMC 1: C3160-FCH1827K9YT
    MAC Address BMC 1: 7C:0E:CE:5A:EF:26
BMC 2 Network Setting:
    IPv4 Address BMC 2: 10.106.145.39
    IPv6 Address BMC 2: ::
    IPv6 Link Local BMC 2: ::
    IPv6 SLAAC Address BMC 2: ::
    Hostname BMC 2: C3160-FCH18407MYD
    MAC Address BMC 2: A0:EC:F9:85:90:3F


Server /network #
```

# Configuring 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 network** | Enters the Cisco IMC network command mode. |
| **Step 2** | Server /network # **set vlan-enabled** {**yes** \| **no**} | Selects whether the Cisco IMC is connected to a VLAN. |
| **Step 3** | Server /network # **set vlan-id** *id* | Specifies the VLAN number. |
| **Step 4** | Server /network # **set vlan-priority** *priority* | Specifies the priority of this system on the VLAN. |
| **Step 5** | Server /network # **commit** | Commits the transaction to the system configuration. |
| **Step 6** | At the prompt, enter y to confirm. | Configures the server LAN. |
| **Step 7** | Server /network # **show** [**detail**] | (Optional) Displays the network settings. |

This example configures the VLAN:

```
Server # scope network
Server /network # set vlan-enabled yes
Server /network *# set vlan-id 5
Server /network *# set vlan-priority 7
Server /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 /network # show detail
Network Setting:
    IPv4 Enabled: yes
    IPv4 Netmask: 255.255.255.0
    IPv4 Gateway: 10.106.145.1
    DHCP Enabled: no
    DDNS Enabled: yes
    DDNS Update Domain:
    Obtain DNS Server by DHCP: no
    Preferred DNS: 171.70.168.183
    Alternate DNS: 0.0.0.0
    IPv6 Enabled: no
    IPv6 Prefix: 64
    IPv6 Gateway: ::
    IPV6 DHCP Enabled: no
    IPV6 Obtain DNS Server by DHCP: no
    IPV6 Preferred DNS: ::
    IPV6 Alternate DNS: ::
    VLAN Enabled: yes
    VLAN ID: 2
    VLAN Priority: 7
    Port Profile: abcde12345
    NIC Mode: dedicated
    NIC Redundancy: none
    SIOC Slot: 1
    Management IPv4 Address: 10.106.145.202
    Management IPv6 Address: ::
    Management Hostname: C3260-FCH18207WF3
    Network Speed: 100Mbps
    Duplex: full
    Auto Negotiate: yes
    Admin Network Speed: auto
    Admin Duplex: auto
    Operational Network Speed: 1Gbps
    Operational Duplex: full
CMC 1 Network Setting:
    IPv4 Address CMC 1: 10.106.145.135
    IPv6 Address CMC 1: ::
    IPv6 Link Local CMC 1: ::
    IPv6 SLAAC Address CMC 1: ::
    Hostname CMC 1: UCS-C3260-FCH181772ZP-1
    MAC Address CMC 1: F4:CF:E2:77:7F:D2
CMC 2 Network Setting:
    IPv4 Address CMC 2: 10.106.145.248
    IPv6 Address CMC 2: ::
    IPv6 Link Local CMC 2: ::
    IPv6 SLAAC Address CMC 2: ::
    Hostname CMC 2: UCS-C3260--2
    MAC Address CMC 2: F4:CF:E2:77:80:83
BMC 1 Network Setting:
    IPv4 Address BMC 1: 10.106.145.41
    IPv6 Address BMC 1: ::
    IPv6 Link Local BMC 1: ::
    IPv6 SLAAC Address BMC 1: ::
    Hostname BMC 1: C3160-FCH1827K9YT
    MAC Address BMC 1: 7C:0E:CE:5A:EF:26
BMC 2 Network Setting:
    IPv4 Address BMC 2: 10.106.145.39
    IPv6 Address BMC 2: ::
    IPv6 Link Local BMC 2: ::
    IPv6 SLAAC Address BMC 2: ::
```

```
    Hostname BMC 2: C3160-FCH18407MYD
    MAC Address BMC 2: A0:EC:F9:85:90:3F

Server /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 network** | Enters the Cisco IMC network command mode. |
| **Step 2** | Server /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.<br>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.<br>**Note** The port profile must be defined on the switch to which this server is connected. |
| **Step 3** | Server /network # **commit** | Commits the transaction to the system configuration. |
| **Step 4** | At the prompt, enter y to confirm. | Connects to a port profile. |
| **Step 5** | Server /network # **show** [**detail**] | (Optional)<br>Displays the network settings. |

This example connects to port profile abcde12345:

```
Server # scope network
Server /network # set port-profile abcde12345
Server /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 /network # show detail
Network Setting:
    IPv4 Enabled: yes
    IPv4 Netmask: 255.255.255.0
    IPv4 Gateway: 10.106.145.1
```

```
    DHCP Enabled: no
    DDNS Enabled: yes
    DDNS Update Domain:
    Obtain DNS Server by DHCP: no
    Preferred DNS: 171.70.168.183
    Alternate DNS: 0.0.0.0
    IPv6 Enabled: no
    IPv6 Prefix: 64
    IPv6 Gateway: ::
    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
    NIC Mode: dedicated
    NIC Redundancy: none
    SIOC Slot: 1
    Management IPv4 Address: 10.106.145.202
    Management IPv6 Address: ::
    Management Hostname: C3260-FCH18207WF3
    Network Speed: 100Mbps
    Duplex: full
    Auto Negotiate: yes
    Admin Network Speed: auto
    Admin Duplex: auto
    Operational Network Speed: 1Gbps
    Operational Duplex: full
CMC 1 Network Setting:
    IPv4 Address CMC 1: 10.106.145.135
    IPv6 Address CMC 1: ::
    IPv6 Link Local CMC 1: ::
    IPv6 SLAAC Address CMC 1: ::
    Hostname CMC 1: UCS-C3260-FCH181772ZP-1
    MAC Address CMC 1: F4:CF:E2:77:7F:D2
CMC 2 Network Setting:
    IPv4 Address CMC 2: 10.106.145.248
    IPv6 Address CMC 2: ::
    IPv6 Link Local CMC 2: ::
    IPv6 SLAAC Address CMC 2: ::
    Hostname CMC 2: UCS-C3260--2
    MAC Address CMC 2: F4:CF:E2:77:80:83
BMC 1 Network Setting:
    IPv4 Address BMC 1: 10.106.145.41
    IPv6 Address BMC 1: ::
    IPv6 Link Local BMC 1: ::
    IPv6 SLAAC Address BMC 1: ::
    Hostname BMC 1: C3160-FCH1827K9YT
    MAC Address BMC 1: 7C:0E:CE:5A:EF:26
BMC 2 Network Setting:
    IPv4 Address BMC 2: 10.106.145.39
    IPv6 Address BMC 2: ::
    IPv6 Link Local BMC 2: ::
    IPv6 SLAAC Address BMC 2: ::
    Hostname BMC 2: C3160-FCH18407MYD
    MAC Address BMC 2: A0:EC:F9:85:90:3F

Server /network #
```

# Configuring Interface Properties

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

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server # **scope network** | Enters the network command mode. |
| **Step 2** | Server /network* # **set mode dedicated** | Enters dedicated command mode. |
| **Step 3** | Server /network* # **set auto-negotiate** {**yes** \| **no**} | Enables or disables auto negotiation command mode.<br>• If you enter **yes**, the setting for duplex will be ignored by the system. The Cisco IMC retains the speed at which the switch is configured.<br>• If you enter **no**, you can set duplex. Else, a default speed of 100 Mbps will be applied, and duplex will retain its previous value. |
| **Step 4** | Server /network* # **set duplex** {**full** \| **half**} | Sets specified duplex mode type. By default, the duplex mode is set to **Full** |

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

```
Server # scope network
Server /network* # set mode dedicated
Server /network* # set auto-negotiate no
Warning: You have chosen to set auto negotiate to no
 If speed and duplex are not set then a default speed of 100Mbps will be applied
 Duplex will retain its previous value
Server /network* # commit
Server /network # set duplex full
Server /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 /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 network** | Enters the Cisco IMC network command mode. |
| **Step 2** | Server /network # **scope ipblocking** | Enters the IP blocking command mode. |
| **Step 3** | Server /network/ipblocking # **set enabled** {**yes** \| **no**} | Enables or disables IP blocking. |
| **Step 4** | 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.<br>The number of unsuccessful login attempts must occur within the time frame specified in the IP Blocking Fail Window field.<br>Enter an integer between 3 and 10. |
| **Step 5** | Server /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.<br>Enter an integer between 60 and 120. |
| **Step 6** | Server /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.<br>Enter an integer between 300 and 900. |
| **Step 7** | Server /network/ipblocking # **commit** | Commits the transaction to the system configuration. |

This example configures IP blocking:

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

# 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 time** | Enters time command mode. |
| **Step 2** | Server /time # **scope ntp** | Enters NTP service command mode. |
| **Step 3** | Server /time/ntp # **set enabled yes** | Enables the NTP service on the server. |
| **Step 4** | Server /time/ntp* # **commit** | Commits the transaction. |
| **Step 5** | Server /time/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 6** | Server /time/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 7** | Server /time/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 8** | Server /time/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 9** | Server /time/ntp # **commit** | Commits the transaction. |
| **Step 10** | Server /time/ntp # **show detail** | Displays the NTP configuration details. |

This example shows how to configure the NTP service:

```
Server  # scope time
Server /time # scope ntp
Server /time/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 /time/ntp* # commit
Server /time/ntp # set server-1 10.120.33.44
Server /time/ntp* # set server-2 10.120.34.45
Server /time/ntp* # set server-3 10.120.35.46
Server /time/ntp* # set server-4 10.120.36.48
Server /time/ntp* # commit
Server /time/ntp # show details
NTP Service Settings:
    NTP Enabled: yes
    NTP Server 1: 10.120.33.44
    NTP Server 2: 10.120.34.45
    NTP Server 3: 10.120.35.46
    NTP Server 4: 10.120.36.48
    Status: NTP service enabled
```

# 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.

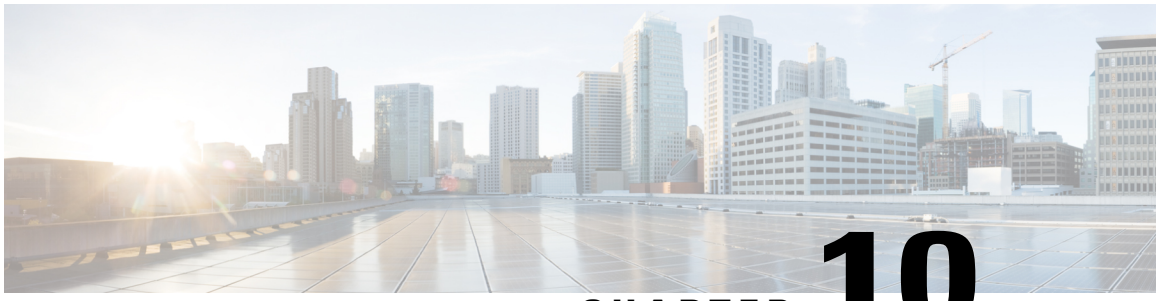
### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server # **scope network** | Enters the network command mode. |
| **Step 2** | Server /network# **ping** *IP address* \| **retries***number* \| **timeout***seconds* | Pings the IP address or host name for a specified number of times until timeout.<br>• **IP address/hostname** - The IP address or the host name of the server.<br>• **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.<br>• **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.<br>• **Component** - The controller that you can ping. |
| **Step 3** | Server /network # **commit** | Commits the transaction to the system configuration. |
| **Step 4** | At the prompt, enter y to confirm. | Pings the IP address. |

This example pings an IP address:

```
Server # scope network
Server /network # ping 10.10.10.10
PING 10.10.10.10 (10.10.10.10): 56 data bytes
64 bytes from 10.10.10.10: seq=0 ttl=238 time=146.343 ms
64 bytes from 10.10.10.10: seq=1 ttl=238 time=146.140 ms
64 bytes from 10.10.10.10: seq=2 ttl=238 time=146.238 ms

--- 10.10.10.10 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 146.140/146.240/146.343 ms
Server /cimc/network #
```



CHAPTER 10

# 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*.<br>**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.<br>**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.<br>**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 niv-mode** {**disable** \| **enable**} | Enables or disables Network Interface Virtualization (NIV) on the adapter card. NIV is disabled by default.<br>If NIV mode is enabled, vNICs: |

| | Command or Action | Purpose |
|---|---|---|
| | | • Can be assigned to a specific channel<br>• Can be associated with a port profile<br>• Can fail over to another vNIC if there are communication problems |
| **Step 7** | Server /chassis/adapter # **configure-vmfex** *port-count* | If NIV mode is enabled, *port-count* specifies the number of VM FEX interfaces you want Cisco IMC to create, from 0 to 112. |
| **Step 8** | Server /chassis/adapter # **commit** | Commits the transaction to the system configuration. |

This example configures the properties of adapter 1:

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

# Managing vHBAs

## Guidelines for Managing vHBAs

When managing vHBAs, consider the following guidelines and restrictions:

- The Cisco UCS P81E Virtual Interface Card and Cisco UCS 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*.<br>**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*.<br>**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.<br>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.<br>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.<br>This setting is not functional in NIV mode. |
| **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.<br>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. |

| | Command or Action | Purpose |
|---|---|---|
| **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. |
| **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:<br>• **intx —**Line-based interrupt (INTx) |

| | Command or Action | Purpose |
|---|---|---|
| | | • **msi —**Message-Signaled Interrupt (MSI)<br>• **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. |
| **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. |

| | Command or Action | Purpose |
|---|---|---|
| **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. |
| **Step 48** | Server /chassis/adapter/host-fc-if # **commit** | Commits the transaction to the system configuration.<br>**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*.<br>**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. |
| **Step 4** | Server /chassis/adapter/host-fc-if # **set channel-number** *number* | (Optional)<br>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.<br>**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 145.

# 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*.<br>**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.<br>**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.<br>**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*.<br>**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*.<br>**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. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | Server /chassis/adapter/host-fc-if # **create-boot-entry** *wwpn lun-id* | Creates a boot table entry.<br>• *wwpn* — The World Wide Port Name (WWPN) for the boot target in the form hh:hh:hh:hh:hh:hh:hh:hh.<br>• *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.<br>**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*.<br>**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. 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.<br>**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*.<br>**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. |

| | Command or Action | Purpose |
|---|---|---|
| **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*.<br>**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 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*.<br>**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

# 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*.<br>**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*.<br>**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.<br>**Note** If NIV is enabled, this setting is determined by the switch, and the command is ignored. |
| **Step 9** | Server /chassis/adapter/host-eth-if # **set trust-host-cos** {**disable** \| **enable**} | Specifies whether the vNIC will trust host CoS or will remark packets. The behavior is as follows:<br>• **disable —**Received packets are remarked with the configured CoS. This is the default.<br>• **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. |

| | Command or Action | Purpose |
|---|---|---|
| | | **Note** If NIV is enabled, this setting is determined by the switch, and the command is ignored. |
| **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:<br>• **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.<br>• **trunk —**The vNIC can belong to more than one VLAN. This is the default.<br>**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.<br>**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.<br>**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.<br>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.<br>**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.<br>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:<br>• **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.<br>• **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:<br>• **intx —**Line-based interrupt (PCI INTx)<br>• **msi —**Message-Signaled Interrupt (MSI)<br>• **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.<br>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.<br>**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:<br>• **disable —**The CPU segments large TCP packets.<br>• **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.<br>**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:<br>• **disable —**The CPU validates all packet checksums.<br>• **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:<br>• **disable —**The CPU validates all packet checksums.<br>• **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:<br>• **disable —**The CPU processes all large packets.<br>• **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.<br>**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*.<br>**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*.<br>**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)<br>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.<br>**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*.<br>**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.<br>**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*.<br>**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.<br>**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 169. |
| **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.<br>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.<br>**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.<br>**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*.<br>**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.<br>**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*.<br>**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*.<br>**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<br>**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 and Nexus 6000 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*.<br>**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.<br>**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*.<br>**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<br>**Note** The changes will take effect upon the next server reboot. |

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

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

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

# Managing VM FEX

## Virtual Machine Fabric Extender

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

For this release, VM FEX supports the following cards and Operating systems:

Cards - Cisco UCS 1225 Virtual Interface Card

Operating Systems:

- VMware ESXi 5.1 Update 2
- VMware ESXi 5.5

VM FEX is not supported on Microsoft Hyper-V and Red Hat KVM for this release.

## Viewing VM FEX Properties

### Before You Begin

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

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server# **scope chassis** | Enters the chassis command mode. |
| **Step 2** | Server /chassis # **scope adapter** *index* | Enters the command mode for the adapter card at the PCI slot number specified by *index*.<br>**Note** The server must be powered on before you can view or change adapter settings. |
| **Step 3** | Server /chassis/adapter # **show vmfex** [**detail**] | Displays the general VM FEX properties. For field descriptions, see General Properties Settings, on page 177. |
| **Step 4** | Server /chassis/adapter # **scope vmfex** *name* | Enters the command mode for the specified VM FEX interface. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | Server /chassis/adapter/vmfex # **show interrupt** [**detail**] | Displays Ethernet interrupt settings. For field descriptions, see Ethernet Interrupt Settings, on page 178. |
| **Step 6** | Server /chassis/adapter/vmfex # **show recv-queue** [**detail**] | Displays Ethernet receive queue settings. For field descriptions, see Ethernet Receive Queue Settings, on page 178. |
| **Step 7** | Server /chassis/adapter/vmfex # **show trans-queue** [**detail**] | Displays Ethernet transmit queue settings. For field descriptions, see Ethernet Transmit Queue Settings, on page 179. |
| **Step 8** | Server /chassis/adapter/vmfex # **show comp-queue** [**detail**] | Displays completion queue settings. For field descriptions, see Completion Queue Settings, on page 179. |
| **Step 9** | Server /chassis/adapter/vmfex # **show offload** [**detail**] | Displays TCP offload settings. For field descriptions, see TCP Offload Settings, on page 179. |
| **Step 10** | Server /chassis/adapter/vmfex # **show rss** [**detail**] | Displays RSS settings. For field descriptions, see Receive Side Scaling Settings, on page 180. |

This example displays the VM FEX properties:

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

Server /chassis/adapter # scope vmfex pts0

Server /chassis/adapter/vmfex # show interrupt
Interrupt Count Coalescing Time (us) Coalescing Type Interrupt Mode
--------------- -------------------- --------------- ---------------
6               125                  MIN             MSI

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

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

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

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

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

Server /chassis/adapter/vmfex #
```

# VM FEX Settings

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

### General Properties Settings

| Name | Description |
|---|---|
| **Name** | A user-defined name for the VM FEX. |
| **MTU** | The maximum transmission unit, or packet size, that this VM FEX accepts. |
| **Uplink Port** | The uplink port associated with this VM FEX. All traffic for this VM FEX goes through this uplink port. |
| **MAC Address** | The MAC address associated with the VM FEX. |
| **Class of Service** | The class of service to associate with traffic from this VM FEX. |
| **Trust Host CoS** | Whether the VM FEX can use the class of service provided by the host operating system. |
| **PCI Order** | The order in which this VM FEX will be used. |
| **Default VLAN** | The default VLAN for this VM FEX. |
| **VLAN Mode** | Whether VLAN trunking or access is configured. |
| **Rate Limit** | If rate limiting is configured, the maximum rate. |
| **Enable PXE Boot** | Whether the VM FEX can be used to perform a PXE boot. |
| **Channel Number** | If NIV mode is enabled for the adapter, the channel number assigned to this VM FEX. |

| Name | Description |
|---|---|
| **Port Profile** | If NIV mode is enabled for the adapter, the port profile associated with theVM FEX.<br>**Note** This field displays the port profiles defined on the switch to which this server is connected. |
| **Enable Uplink Failover** | If NIV mode is enabled for the adapter, whether traffic on this VM FEX should fail over to the secondary interface if there are communication problems. |
| **Failback Timeout** | After a VM FEX has started using its secondary interface, this setting controls how long the primary interface must be available before the system resumes using the primary interface for the VM FEX. |

### Ethernet Interrupt Settings

| Name | Description |
|---|---|
| **Interrupt Count** field | The number of interrupt resources allocated to this VM FEX. |
| **Coalescing Time** field | The time Cisco IMC waits between interrupts or the idle period that must be encountered before an interrupt is sent. |
| **Coalescing Type** field | This can be one of the following:<br>• **MIN—**The system waits for the time specified in the **Coalescing Time** field before sending another interrupt event.<br>• **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** field. |
| **Interrupt Mode** field | The preferred driver interrupt mode. This can be one of the following:<br>• **MSIx—**Message Signaled Interrupts (MSI) with the optional extension.<br>• **MSI—**MSI only.<br>• **INTx—**PCI INTx interrupts. |

### Ethernet Receive Queue Settings

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

### Ethernet Transmit Queue Settings

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

### Completion Queue Settings

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

### TCP Offload Settings

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

### Receive Side Scaling Settings

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

# 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*. |

| | Command or Action | Purpose |
|---|---|---|
| | | **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:<br>• TFTP<br>• FTP<br>• SFTP<br>• SCP<br>• HTTP<br>**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.<br>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.<br>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*.<br>**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.<br>**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)<br>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 184.

# 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

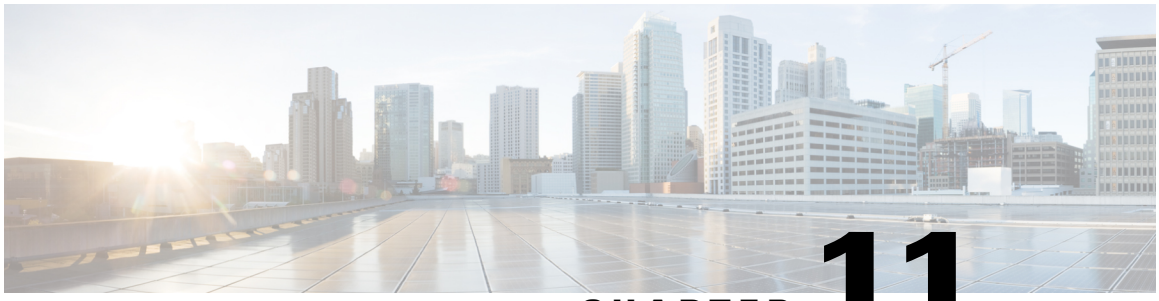
| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server# **scope chassis** | Enters the chassis command mode. |
| **Step 2** | Server /chassis # **activate-adapter-fw** *pci-slot* {**1** \| **2**} | Activates adapter firmware image 1 or 2 on the adapter in the specified PCI slot.<br>**Note** 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.



CHAPTER 11

# 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 chassis command mode. |
| **Step 2** | Server /chassis # **scope server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 3** | Server /chassis/server # **scope storageadapter** *Slot-ID* | Enters storage adapter command mode. |
| **Step 4** | Server /chassis/server/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 and the write policy for the new virtual drive. Enter the appropriate information at each prompt.<br>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 5** | 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 server 1
Server /chassis/server # scope storageadapter SLOT-3
Server /chassis/server/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')

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

OK? (y or n)--> y

Server /chassis/server/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 chassis command mode. |
| **Step 2** | Server /chassis # **scope server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 3** | Server /chassis/server # **scope storageadapter** *Slot-ID* | Enters storage adapter command mode. |
| **Step 4** | 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.<br>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 5** | Server /chassis/server/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 server 1
Server /chassis/server # scope storageadapter SLOT-3
Server /chassis/server/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/server/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 server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 3** | Server /chassis/server # **scope storageadapter** *slot ID* | Enters the command mode for an installed storage card. |
| **Step 4** | Server /chassis/server/storageadapter # **scope virtual-drive** *drive-number* | Enters the command mode for the specified virtual drive. |
| **Step 5** | Server /chassis/server/storageadapter/virtual-drive # **set-transport-ready** *{include-all \| exclude-all \| include-dhsp}* | Enter the initialization type using which you can set the selected virtual drive as transport ready. This can be one of the following:<br>• **exlude-all—** Excludes all the dedicated hot spare drives.<br>• **include-all—** Includes any exclusively available or shared dedicated hot spare drives.<br>• **include-dhsp—** Includes exclusive dedicated hot spare drives. |

| | Command or Action | Purpose |
|---|---|---|
| | | Sets the virtual drive to transport ready and assigns the chosen properties.<br>When you are prompted to confirm the action. Enter y to confirm.<br>**Note** When you set a virtual drive to transport ready all the physical drives associated with it are displayed as Ready to remove. |
| **Step 6** | Server /chassis/server/storageadapter/virtual-drive # **show detail** | (Optional)<br>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 server 1
Server /chassis/server # scope storageadapter SLOT-HBA
Server /chassis/server/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/server/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 server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 3** | Server /chassis/server # **scope storageadapter** *slot ID* | Enters the command mode for an installed storage card. |
| **Step 4** | Server /chassis/server/storageadapter # **scope virtual-drive** *drive-number* | Enters the command mode for the specified virtual drive. |
| **Step 5** | Server /chassis/server/storageadapter/virtual-drive # **clear-transport-ready** | This reverts the selected transport ready virtual drive to its original state.<br>When you are prompted to confirm the action. Enter y to confirm. |
| **Step 6** | Server /chassis/server/storageadapter/virtual-drive # **show detail** | (Optional)<br>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/server # scope storageadapter SLOT-HBA
Server /chassis/server/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/server/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.

### 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 server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 3** | Server /chassis/server # **scope storageadapter** *Slot-ID* | Enters storage adapter command mode. |
| **Step 4** | Server /chassis/server/storageadapter # **import-foreign-config** | You are prompted to confirm the action. Enter **yes** to confirm.<br>**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/server # scope storageadapter SLOT-3
Server /chassis/server/storageadapter # import-foreign-config
Are you sure you want to import all foreign configurations on this controller?
Enter 'yes' to confirm -> yes
Server /chassis/server/storageadapter #
```

# Clearing Foreign Configuration

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

### Before You Begin

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

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server # **scope chassis** | Enters chassis command mode. |
| **Step 2** | Server /chassis # **scope server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 3** | Server /chassis/server # **scope storageadapter** *Slot-ID* | Enters storage adapter command mode. |
| **Step 4** | Server /chassis/server/storageadapter # **clear-foreign-config** | You are prompted to confirm the action. Enter **yes** to confirm.<br>**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 server 1
Server /chassis/server # scope storageadapter SLOT-3
Server /chassis/server/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/server/storageadapter #
```

# Enabling and Disabling JBOD

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server # **scope chassis** | Enters chassis command mode. |
| **Step 2** | Server /chassis # **scope server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 3** | Server /chassis/server # **scope storageadapter** *Slot-ID* | Enters storage adapter command mode. |
| **Step 4** | Server /chassis/server/storageadapter # **enable-jbod-mode** | Enables the JBOD Mode for the selected controller |
| **Step 5** | Server /chassis/server/storageadapter # **disable-jbod-mode** | Disables the JBOD Mode for the selected controller |

This example enables and disables the JBOD mode for the selected controller:

```
Server# scope chassis
Server /chassis # scope server 1
Server /chassis/server # scope storageadapter SLOT-3
```

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

### What to Do Next

- 

# 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 chassis command mode. |
| **Step 2** | Server /chassis # **scope server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 3** | Server /chassis/server # **scope storageadapter** *Slot-ID* | Enters storage adapter command mode. |
| **Step 4** | Server /chassis/server/storageadapter # **clear-boot-drive** | You are prompted to confirm the action. Enter **yes** to confirm.<br>**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 server 1
Server /chassis/server # scope storageadapter SLOT-3
Server /chassis/server/storageadapter # clear-boot-drive
Are you sure you want to clear the controller's boot drive?
Enter 'yes' to confirm -> yes
Server /chassis/server/storageadapter #
```

# Retrieving Storage Firmware Logs for a Controller

This task retrieves the 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 the command mode for an installed storage card. |
| **Step 3** | Server /chassis/storageadapter # **get-storage-fw-log** | Retrieves the storage firmware log file to the specified controller. |
| **Step 4** | At the prompt, enter yes. | Begins download of the storage firmware log files. |

This example shows how to view the download status of the retrieved storage firmware log files:

```
Server # scope chassis
Server /chassis # scope storageadapter SLOT-HBA
Server /chassis/storageadapter # get-storage-fw-log

You are initiating the retrieval of the storage firmware log to Cisco IMC.
This task will take a few minutes to complete. You may monitor the status
  of the retrieval by running the 'get-storage-fw-log-download-progress' command.
When the download is finished, the 'Storage Firmware Log Status' value will be
  'Complete', along with the size of the logfile.
You may then download the log file using the Technical Support facility,
  accessible from /cimc/tech-support scope, or the WebUI's Utilities page.

Do you want to proceed?
Enter 'yes' to confirm -> yes
Server /chassis/storageadapter # get-storage-fw-log-download-progress
Storage Firmware Log Status: Complete (total size 61906 bytes)
```

# 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 chassis command mode. |
| **Step 2** | Server /chassis # **scope server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 3** | Server /chassis/server # **scope storageadapter** *Slot-ID* | Enters storage adapter command mode. |
| **Step 4** | Server /chassis/server/storageadapter # **scope virtual-drive** *drive-number* | Enters command mode for the specified virtual drive. |
| **Step 5** | Server /chassis/server/storageadapter/virtual-drive # **delete-virtual-drive** | You are prompted to confirm the action. Enter **yes** to confirm.<br>**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 server 1
Server /chassis/server # scope storageadapter SLOT-3
Server /chassis/server/storageadapter # scope virtual-drive 3
Server /chassis/server/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/server/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 chassis command mode. |
| **Step 2** | Server /chassis # **scope server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 3** | Server /chassis/server # **scope storageadapter** *Slot-ID* | Enters storage adapter command mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | Server /chassis/server/storageadapter # **scope virtual-drive** *drive-number* | Enters command mode for the specified virtual drive. |
| **Step 5** | Server /chassis/server/storageadapter/virtual-drive # **start-initialization** | Initializes the specified virtual drive. |
| **Step 6** | Server /chassis/server/storageadapter/virtual-drive # **cancel-initialization** | (Optional) Cancels the initialization of the specified virtual drive. |
| **Step 7** | Server /chassis/server/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/server # scope storageadapter SLOT-3
Server /chassis/storageadapter # scope virtual-drive 3
Server /chassis/server/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/server/storageadapter/virtual-drive # get-operation-status

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

Server /chassis/server/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 chassis command mode. |
| **Step 2** | Server /chassis # **scope server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 3** | Server /chassis/server # **scope storageadapter** *Slot-ID* | Enters storage adapter command mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | Server /chassis/server/storageadapter # **scope virtual-drive** *drive-number* | Enters command mode for the specified virtual drive. |
| **Step 5** | Server /chassis/server/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 server 1
Server /chassis/server # scope storageadapter SLOT-3
Server /chassis/server/storageadapter # scope virtual-drive 3
Server /chassis/server/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/server/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 chassis command mode. |
| **Step 2** | Server /chassis # **scope server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 3** | Server /chassis/server # **scope storageadapter** *Slot-ID* | Enters storage adapter command mode. |
| **Step 4** | Server chassis/server/storageadapter # **scope virtual-drive** *drive number* | Enters command mode for the specified virtual drive. |
| **Step 5** | Server chassis/server/storageadapter /virtual-drive # **modify-attributes** | Prompts you to select a different current policy. |
| **Step 6** | Server chassis/server/storageadapter/virtual-drive# **set raid-level** *value* | Specifies the RAID level for the specified virtual drive. |
| **Step 7** | Server chassis/server/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 chassis
Server /chassis/server # scope storageadapter slot-3
Server /chassis/server/storageadapter # scope virtual-drive 3
Server /chassis/server/storageadapter/virtual-drive #set raid-level 1
Server /chassis/server/storageadapter/virtual-drive *# physical-drive 1
Server /chassis/server/storageadapter/virtual-drive* #commit
Server /chassis/server/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/server/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 chassis command mode. |
| **Step 2** | Server /chassis # **scope server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 3** | Server /chassis/server # **scope storageadapter** *Slot-ID* | Enters storage adapter command mode. |
| **Step 4** | Server /chassis/server/storageadapter # **scope virtual-drive** *3* | Enters the command mode for the virtual drive. |
| **Step 5** | Server /chassis/server/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 server 1
Server /chassis/server # scope storageadapter SLOT-3
Server /chassis/server/storageadapter # scope virtual-drive
Server /chassis/server/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/server/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 chassis command mode. |
| **Step 2** | Server /chassis # **scope server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 3** | Server /chassis/server # **scope storageadapter** *Slot-ID* | Enters storage adapter command mode. |
| **Step 4** | Server /chassis/server/storageadapter # **scope physical-drive** *drive-number* | Enters command mode for the specified physical drive. |
| **Step 5** | Server /chassis/server/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 server 1
Server /chassis/server # scope storageadapter SLOT-3
Server /chassis/server/storageadapter # scope physical-drive 3
Server /chassis/server/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/server/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 chassis command mode. |
| **Step 2** | Server /chassis # **scope server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 3** | Server /chassis/server # **scope storageadapter** *Slot-ID* | Enters storage adapter command mode. |
| **Step 4** | Server /chassis/server/storageadapter # **scope physical-drive** *drive-number* | Enters command mode for the specified physical drive. |
| **Step 5** | Server /chassis/server/storageadapter/physical-drive # **make-global-hot-spare** | |
| **Step 6** | Server /chassis/server/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 server 1
Server /chassis/server # scope storageadapter SLOT-3
Server /chassis/server/storageadapter # scope physical-drive 3
Server /chassis/server/storageadapter/physical-drive # make-global-hot-spare
Server /chassis/server/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 chassis command mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | Server /chassis # **scope server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 3** | Server /chassis/server # **scope storageadapter** *Slot-ID* | Enters storage adapter command mode. |
| **Step 4** | Server /chassis/server/storageadapter # **scope physical-drive** *drive-number* | Enters command mode for the specified physical drive. |
| **Step 5** | Server /chassis/server/storageadapter/physical-drive # **prepare-for-removal** | |

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

```
Server# scope chassis
Server /chassis # scope server 1
Server /chassis/server # scope storageadapter SLOT-3
Server /chassis/server/storageadapter # scope physical-drive 3
Server /chassis/server/storageadapter/physical-drive # prepare-for-removal
Server /chassis/server/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 chassis command mode. |
| **Step 2** | Server /chassis # **scope server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 3** | Server /chassis/server # **scope storageadapter** *Slot-ID* | Enters storage adapter command mode. |
| **Step 4** | Server /chassis/server/storageadapter # **scope physical-drive 4** | Enters command mode for the physical drive. |
| **Step 5** | Server /chassis/server/storageadapter/physical-drive # **make-unconfigured-good** | Modifies the status of the drive to Unconfigured good. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | Server /chassis/server/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 chassis
Server /chassis/server # scope storageadapter SLOT-3
Server /chassis/server/storageadapter # scope physical-drive 4
Server /chassis/server/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/server/storageadapter/physical-drive # make-unconfigured-good
Server /chassis/server/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/server/storageadapter/physical-drive # make-jbod
Server /chassis/server/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 chassis command mode. |
| **Step 2** | Server /chassis # **scope server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 3** | Server /chassis/server # **scope storageadapter** *Slot-ID* | Enters storage adapter command mode. |
| **Step 4** | Server /chassis/server/storageadapter # **scope physical-drive 4** | Enters command mode for the physical drive. |
| **Step 5** | Server /chassis/server/storageadapter/physical-drive # **set-boot-drive** | You are prompted to confirm the action. Enter **yes** to confirm.<br>**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 server 1
Server /chassis/server # scope storageadapter SLOT-3
Server /chassis/server/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/server/storageadapter # scope physical-drive 4
Server /chassis/server/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/server/storageadapter/physical-drive # exit
Server /chassis/server/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 chassis command mode. |
| **Step 2** | Server /chassis # **scope server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 3** | Server /chassis/server # **scope storageadapter** *Slot-ID* | Enters storage adapter command mode. |
| **Step 4** | Server /chassis/server/storageadapter # **scope physical-drive** *drive-number* | Enters command mode for the specified physical drive. |
| **Step 5** | Server /chassis/server/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 server 1
Server /chassis/server # scope storageadapter SLOT-3
Server /chassis/server/storageadapter # scope physical-drive 3
Server /chassis/server/storageadapter/physical-drive # remove-hot-spare
Server /chassis/server/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 chassis command mode. |
| **Step 2** | Server /chassis # **scope server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 3** | Server /chassis/server # **scope storageadapter** *Slot-ID* | Enters storage adapter command mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | Server /chassis/server/storageadapter # **scope physical-drive** *drive-number* | Enters command mode for the specified physical drive. |
| **Step 5** | Server /chassis/server/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 server 1
Server /chassis/server # scope storageadapter SLOT-3
Server /chassis/server/storageadapter # scope physical-drive 3
Server /chassis/server/storageadapter/physical-drive # undo-prepare-for-removal
Server /chassis/server/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 chassis command mode. |
| **Step 2** | Server /chassis # **scope server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 3** | Server /chassis/server # **scope storageadapter** *Slot-ID* | Enters storage adapter command mode. |
| **Step 4** | Server /chassis/server/storageadapter # **scope bbu** | Enter the battery backup unit command mode. |
| **Step 5** | Server /chassis/server/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 server 1
Server /chassis/server # scope storageadapter SLOT-2
Server /chassis/server/storageadapter # scope bbu
Server /chassis/server/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/server/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 chassis command mode. |
| **Step 2** | Server /chassis # **scope server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 3** | Server /chassis/server # **scope storageadapter** *Slot-ID* | Enters storage adapter command mode. |
| **Step 4** | Server /chassis/server/storageadapter # **scope bbu** | Enter the battery backup unit command mode. |
| **Step 5** | Server /chassis/server/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 server 1
Server /chassis/server # scope storageadapter SLOT-2
Server /chassis/server/storageadapter # scope bbu
Server /chassis/server/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/server/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 chassis command mode. |
| **Step 2** | Server /chassis # **scope server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | Server /chassis/server # **scope storageadapter** *Slot-ID* | Enters storage adapter command mode. |
| **Step 4** | Server /chassis/server/storageadapter # **scope bbu** | Enter the battery backup unit command mode. |
| **Step 5** | Server /chassis/server/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 server 1
Server /chassis/server # scope storageadapter SLOT-2
Server /chassis/server/storageadapter # scope bbu
Server /chassis/server/storageadapter/bbu # start-learn-cycle
Server /chassis/server/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 chassis command mode. |
| **Step 2** | Server /chassis # **scope server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 3** | Server /chassis/server # **scope storageadapter** *Slot-ID* | Enters storage adapter command mode. |
| **Step 4** | Server /chassis/server/storageadapter # **scope physical-drive 3** | Enters the physical drive command mode. |
| **Step 5** | Server /chassis/server/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 server 1
Server /chassis/server # scope storageadapter SLOT-2
Server /chassis/server/storageadapter # scope physical-drive 3
Server /chassis/server/storageadapter/physical-drive # locator-led on
Server /chassis/server/storageadapter/physical-drive* # commit
Server /chassis/server/storageadapter/physical-drive #
```

# Viewing Storage Controller Logs

### Before You Begin

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

### Procedure

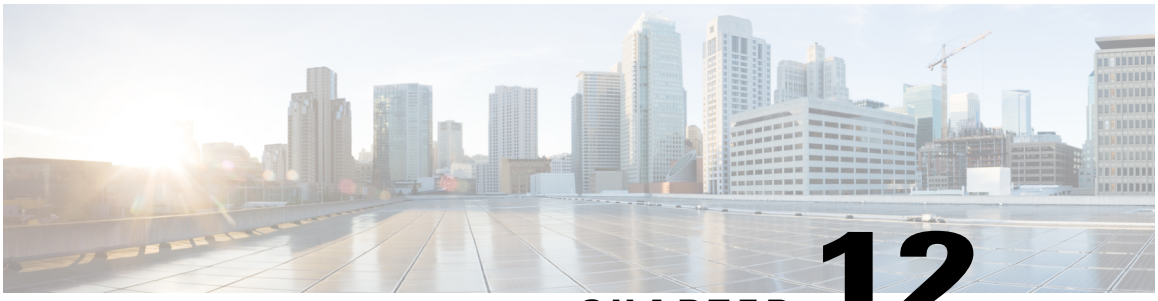
| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server # **scope chassis** | Enters chassis command mode. |
| **Step 2** | Server /chassis # **scope server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 3** | Server /chassis/server # **scope storageadapter** *Slot-ID* | Enters storage adapter command mode. |
| **Step 4** | Server /chassis/server/storageadapter # **show log** | Displays the storage controller logs. |

This example shows how to display storage controller logs:

```
Server # scope chassis
Server /chassis # scope server 1
Server /chassis/server # scope storageadapter SLOT-3
Server /chassis/server/storageadapter # show log

Time                        Severity         Description
----                        --------        -------------
Fri March 1 09:52:19 2015   Warning      Predictive Failure
Fri March 1 07:50:19 2015   Info         Battery charge complete
Fri March 1 07:50:19 2015   Info         Battery charge started
Fri March 1 07:48:19 2015   Info         Battery relearn complete
Fri March 1 07:47:19 2015   Info         Battery is discharging
Fri March 1 07:45:19 2015   Info         Battery relearn started

Server /chassis/server/storageadapter #
```



CHAPTER 12

# 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. |
| **Step 5** | Server /http # **set http-redirect** {**yes** \| **no**} | Enables or disables the redirection of an HTTP request to HTTPS. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | Server /http # **set timeout** *seconds* | Sets the number of seconds to wait between HTTP requests before the Cisco IMC times out and terminates the session.<br>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.<br>Enter an integer between 60 and 10,800. The default is 300 seconds. |
| **Step 5** | Server /ssh # **commit** | Commits the transaction to the system configuration. |
| **Step 6** | Server /ssh # **show** [**detail**] | (Optional) Displays the SSH configuration. |

This example configures SSH for the 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 #
```

# 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 for Cisco IMC

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 server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 2** | Server /server # **scope ipmi** | Enters the IPMI command mode. |
| **Step 3** | Server /server/ipmi # **set enabled** {**yes** \| **no**} | Enables or disables IPMI access on this server. |
| **Step 4** | Server /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:<br>• **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.<br>• **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.<br>• **admin —** IPMI users can perform all available actions. If you select this option, IPMI users with the |

| | Command or Action | Purpose |
|---|---|---|
| | | "Administrator" user role can create admin, user, and read-only sessions on this server. |
| **Step 5** | Server /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 6** | Server /server/ipmi # **commit** | Commits the transaction to the system configuration. |
| **Step 7** | Server /server/ipmi # **randomise-key** | Sets the IPMI encryption key to a random value.<br>**Note** You can perform the Step 6 action instead of Steps 4 and 5. |
| **Step 8** | 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 server 1
Server /server # scope ipmi
Server /server/ipmi # set enabled yes
Server /server/ipmi *# set privilege-level admin
Server /server/ipmi *# set encryption-key abcdef01234567890abcdef01234567890abcdef
Server /server/ipmi *# commit
Server /server/ipmi *# show
Enabled Encryption Key                          Privilege Level Limit
------- --------------------------------------- ---------------------
yes     ABCDEF01234567890ABCDEF01234567890ABCDEF admin

Server /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 /server/ipmi # show
Enabled Encryption Key                          Privilege Level Limit
------- --------------------------------------- ---------------------
yes     abcdef01234567890abcdef01234567890abcdef admin

Server /server/ipmi #
```

# Configuring IPMI over LAN for CMCs

Configure IPMI over LAN when you want to manage the CMC 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 chassis** | Enters server command mode of server 1 or 2. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | Server /chassis # **scope cmc** {**1** \| **2**} | Enters CMC command mode. |
| **Step 3** | Server /server # **scope ipmi** | Enters the IPMI command mode. |
| **Step 4** | Server /chassis/cmc/ipmi # **set enabled** {**yes** \| **no**} | Enables or disables IPMI access on this server. |
| **Step 5** | Server /chassis/cmc/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:<br>• **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.<br>• **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.<br>• **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 6** | Server /chassis/cmc/ipmi # **set encryption-key** *key* | Sets the IPMI encryption key to use for IPMI communications. The key value must be 40 hexadecimal numbers. |
| **Step 7** | Server /chassis/cmc/ipmi # **commit** | Commits the transaction to the system configuration. |
| **Step 8** | Server /chassis/cmc/ipmi # **randomise-key** | Sets the IPMI encryption key to a random value.<br>**Note** You can perform the Step 6 action instead of Steps 4 and 5. |
| **Step 9** | 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 CMC 1:

```
Server # scope chassis
Server # scope cmc 1
Server /chassis # scope ipmi
Server /chassis/cmc/ipmi # set enabled yes
Server /chassis/cmc/ipmi *# set privilege-level admin
Server /chassis/cmc/ipmi *# set encryption-key abcdef01234567890abcdef01234567890abcdef
Server /chassis/cmcipmi *# commit
Server /chassis/cmc/ipmi *# show
Enabled Encryption Key                          Privilege Level Limit
------- --------------------------------------- ---------------------
```

```
yes     ABCDEF01234567890ABCDEF01234567890ABCDEF admin

Server /chassis/cmc/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 /chassis/cmc/ipmi # show
Enabled Encryption Key                          Privilege Level Limit
------- --------------------------------------- ---------------------
yes     abcdef01234567890abcdef01234567890abcdef admin

Server /chassis/cmc/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.<br>**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. |
| **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.<br>**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. |

| | Command or Action | Purpose |
|---|---|---|
| **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 219.

# 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.<br>**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.<br>**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.<br>**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. |
| **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.<br>**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.

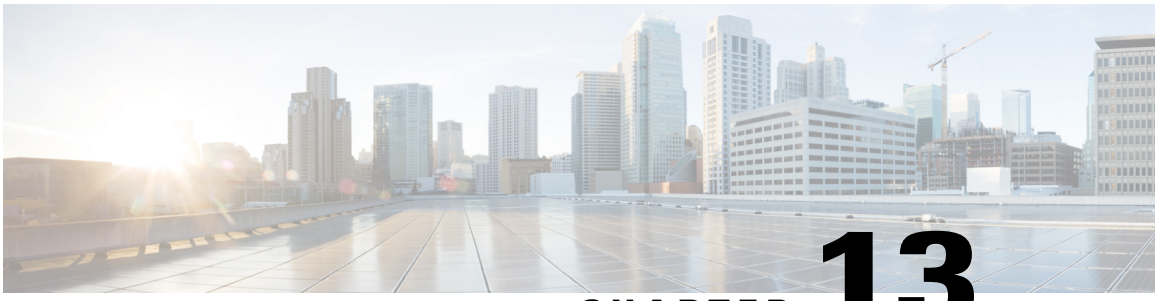
### Procedure

| | 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:<br>• **yes—**This user is enabled as an SNMPv3 user and is allowed to access the SNMP OID tree.<br>**Note** The security name and security level must also be configured at this time or the user addition will fail.<br>• **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:<br>• **noauthnopriv—**The user does not require an authorization or privacy password.<br>• **authnopriv—**The user requires an authorization password but not a privacy password. If you select this option, you must configure an authentication key.<br>• **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. |
| **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 #
```



CHAPTER 13

# Managing Certificates

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 Configuring Common Properties, on page 122.

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.<br>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.<br>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*<br><br>**Example:**<br>`# openssl genrsa -out ca.key 2048` | This command generates an RSA private key that will be used by the CA.<br>**Note** To allow the CA to access the key without user input, do not use the -des3 option for this command.<br>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*<br><br>**Example:**<br>`# 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.<br>The certificate server is an active CA. |
| **Step 3** | **echo "nsCertType = server" > openssl.conf**<br><br>**Example:**<br>`# 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.<br>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.<br>Your server certificate is contained in the output file. |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:**<br>`# 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>**<br><br>**Example:**<br>`openssl x509 -noout -text -purpose -in <cert file>` | Verifies if the generated certificate is of type **Server**.<br>**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)<br>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

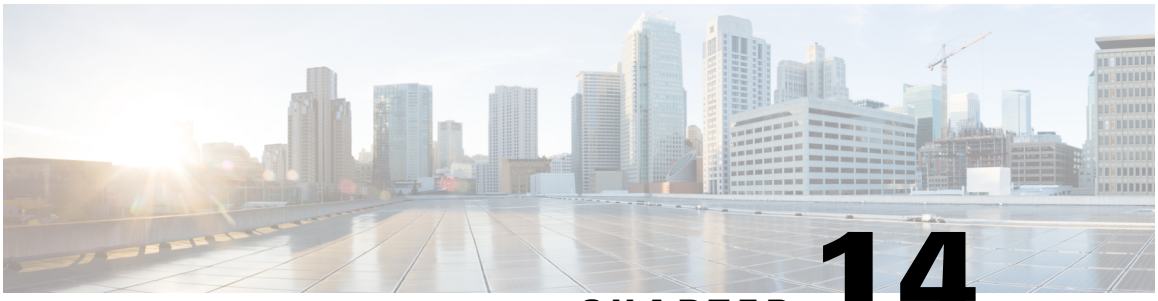
| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server# **scope certificate** | Enters the certificate command mode. |
| **Step 2** | Server /certificate # **upload** | Launches a dialog for entering and uploading the new server certificate. |

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/SINv7wd6Vv2pBt6ZpXgD4VBNKOND1
GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
mK3Ku+YiORnv6DhxrOoqau8r/hyI/L43l7IPN1HhOi3oha4=
-----END CERTIFICATE-----
```

```
<CTRL+D>
```



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.

**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:

a) From the ISO file, open the ZIP file containing the firmware installation files.
The ZIP file is on the top-level of the ISO file, and its name follows the format *ServerModel_ReleaseNumber*.ZIP.

For example, C240M3_1.4.4A.ZIP.

You do not need to extract all of the files contained in this ZIP file. Instead, you only need to open it so that you can access the BIOS firmware installation CAP file and the ZIP file containing the Cisco IMC firmware installation BIN file.

b) From the *ServerModel_ReleaseNumber*.ZIP file, extract the BIOS firmware installation CAP file and save it to your local drive.
The CAP file is in the *ReleaseNumber*/bios/cisco imc folder, and its name follows the format *Server*-BIOS-*Release-Number*.CAP.

For example, 1.4.4a/bios/cisco imc/C240-BIOS-1-4-4c-0.CAP.

c) From the *ServerModel_ReleaseNumber*.ZIP file, open the ZIP file containing the Cisco IMC firmware installation files.
The ZIP file is in the *ReleaseNumber*/cisco imc folder and its name follows the format *server-model*-cisco imc-*release*.zip.

For example, 1.4.4a/cisco imc/c240-m3-cisco imc.1.4.4a.zip.

You do not need to extract all of the files contained in this zip file. Instead, you only need to open it so that you can access the Cisco IMC firmware installation BIN file.

d) From the *server-model*-cisco imc-*release*.zip file, extract the full Cisco IMC firmware installation BIN file and save it to your local drive.
The BIN file is in the *server-model*-cisco imc-*release* folder and its name follows the format upd-pkg-*server-model*-cisco imc.full.*release*.bin.

For example, c240-m3-cisco imc.1.4.4a/upd-pkg-c240-m3-cisco imc.full.1.4.4a.bin.

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

# Installing Cisco IMC Firmware from a Remote Server

### 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 the **Activating Installed Cisco IMC Firmware** section.
- Power off the server.

**Note** You must not initiate a Cisco IMC update when another Cisco IMC update is already in progress.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server /server # **scope server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 2** | server /server # **scope bmc** | Enters bmc command mode. |
| **Step 3** | server /server/bmc # **scope firmware** | Enters the firmware command mode. |
| **Step 4** | server /server/bmc/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:<br>• TFTP<br>• FTP<br>• SFTP |

| | Command or Action | Purpose |
|---|---|---|
| | | • SCP<br>• HTTP<br><br>**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.<br><br>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.<br><br>The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to. |
| **Step 5** | server /server/bmc/firmware # **show detail** | (Optional)<br>Displays the progress of the firmware update. |

This example shows how to update the Cisco IMC firmware:

```
server# scope server 1
server /server # scope bmc
server /server/bmc # scope firmware
server /server/bmc/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 /server/bmc/firmware # show detail
Firmware Image Information:
     Update Stage: NONE
    Update Progress: 5
    Current FW Version: 2.0(6.56)
    FW Image 1 Version: 2.0(6.56)
    FW Image 1 State: RUNNING ACTIVATED
    FW Image 2 Version: 2.0(6.55)
    FW Image 2 State: BACKUP INACTIVATED
    Boot-loader Version: 2.0(6.56).36
    Secure Boot: ENABLED

server /server/bmc/firmware #
```

### What to Do Next

Activate the new firmware.

# Activating Installed Cisco IMC Firmware

### Before You Begin

Install the Cisco IMC firmware on the server.

**Important** p

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 /server # **scope server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 2** | server /server # **scope bmc** | Enters bmc command mode. |
| **Step 3** | server /server/bmc # **scope firmware** | Enters the firmware command mode. |
| **Step 4** | Server /server/bmc # **show detail** | Displays the available firmware images and status. |
| **Step 5** | Server /server/bmc # **activate** | Activates the selected image. If no image number is specified, the server activates the currently inactive image. |
| **Step 6** | 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 7** | Log back into the CLI and repeat steps 1–4 to verify the activation. | (Optional) |

This example activates firmware image 2 and then verifies the activation after the BMC reboots:

```
Server# scope server 1
Server/server# scope bmc
Server /server/bmc # scope firmware
Server /server/bmc # show detail
Firmware Image Information:
     Update Stage: NONE
    Update Progress: 100
    Current FW Version: 2.0(6.55)
    FW Image 1 Version: 2.0(6.56)
    FW Image 1 State: BACKUP INACTIVATED
    FW Image 2 Version: 2.0(6.55)
    FW Image 2 State: RUNNING ACTIVATED
    Boot-loader Version: 2.0(6.55).36
    Secure Boot: ENABLED


Server /server/bmc # activate
This operation will activate firmware 2 and reboot the BMC.
Continue?[y|N]y
.
.
```

```
 -- BMC reboot --
.
.
-- Log into CLI as Admin --

Server# scope server 1
Server/server# scope bmc
Server /server/bmc # scope firmware
Server /server/bmc # show detail
Firmware Image Information:
    Update Stage: NONE
    Update Progress: 100
    Current FW Version: 2.0(6.55)
    FW Image 1 Version: 2.0(6.56)
    FW Image 1 State: BACKUP INACTIVATED
    FW Image 2 Version: 2.0(6.55)
    FW Image 2 State: RUNNING ACTIVATED
    Boot-loader Version: 2.0(6.55).36
    Secure Boot: ENABLED
```

# Installing BIOS Firmware from a Remote Server

### 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 the **Activating Installed BIOS Firmware** section.
- Power off the server.

**Note** You must not initiate a BIOS update while another BIOS update is already in progress.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server /server # **scope server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 2** | server /server # **scope bios** | Enters BIOS command mode. |
| **Step 3** | server /server/bios # **update** *protocol IP Address pathrecovery* | 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:<br>• TFTP<br>• FTP<br>• SFTP<br>• SCP<br>• 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.<br>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.<br>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 /server/bios # **show detail** | (Optional)<br>Displays the progress of the firmware update. |

This example updates the BIOS firmware to Cisco IMC software release 2.0(7c):

```
Server# scope server 1
Server /server# scope bios
Server /server/bios# show detail
BIOS:
    BIOS Version: C3X60M3.2.0.7c.0.071620151216
    Backup BIOS Version: C3X60M3.2.0.7c.0.071620151216
    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
Server /server/bios # update ftp 192.0.20.34 //upgrade_bios_files/C3620-BIOS-2-0-7c-0.CAP
 <CR>  Press Enter key
Firmware update has started.
Check the status using "show detail"
Server /bios #
```

# Activating 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 /server # **scope server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 2** | server /server # **scope bios** | Enters BIOS command mode. |
| **Step 3** | Server /server/bios # **activate** | Activates the currently inactive image. |
| **Step 4** | At the prompt, enter y to activate the selected firmware image. | Initiates the activation. |

This example activates firmware and then verifies the activation:

```
Server# scope server 1
Server /server# scope bios
Server /server/bios# show detail
BIOS:
    BIOS Version: C3X60M3.2.0.7c.0.071620151216
    Backup BIOS Version: C3X60M3.2.0.7c.0.071620151216
    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

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

Server# scope server 1
Server /server# scope bios
Server /server/bios# show detail
BIOS:
    BIOS Version: C3X60M3.2.0.7c.0.071620151216
    Backup BIOS Version: C3X60M3.2.0.7c.0.071620151216
    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
```

# Installing CMC Firmware from a Remote Server

**Note** You must not initiate a CMC update while another CMC update is already in progress.

### 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 232.

### 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:<br>• TFTP<br>• FTP<br>• SFTP<br>• SCP<br>• HTTP<br>**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.<br>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.<br>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)<br>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 colusa2_cmc.2.0.7a.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(7a)
    FW Image 1 Version: 2.0(7a)
    FW Image 1 State: RUNNING ACTIVATED
    FW Image 2 Version: 2.0(7a)
    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.

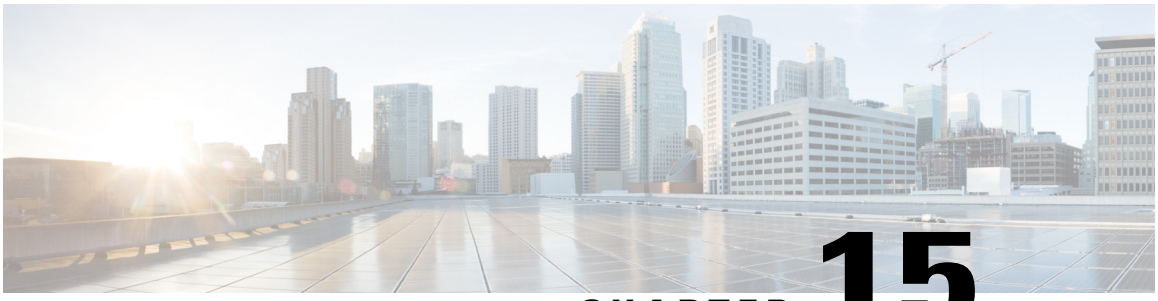
### Procedure

| | 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. |

| | Command or Action | Purpose |
|---|---|---|
| **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
```



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      Distinguished Name (DN)
--------------      ---------     ----------------------------------------
2015-08-18T06:44:02  major        sys/chassis-1/server-2/board/memarray-1/mem-2
2015-08-18T06:43:48  major        sys/chassis-1/server-2/board/memarray-1/mem-1

Description
------------------------------------------------------------
"DDR3_P1_A2_ECC: DIMM 2 is inoperable : Check or replace DIMM"
```

```
"DDR3_P1_A1_ECC: DIMM 1 is inoperable : Check or replace DIMM"
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 Cisco IMC Log

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server # **scope chassis** | Enters chassis command mode. |
| **Step 2** | Server /chassis # **scope log** | Enters log command mode. |
| **Step 3** | Server /chassis/log # **show entries detail** | Displays the CMC trace log details. |

This example displays the CMC trace log details:

```
Server# scope chassis
Server /chassis # scope log
Server /chassis/log # show entries detail
Trace Log:
    Time: 2015 Jul 26 06:35:15
    Severity: Notice
    Source: CMC:dropbear:19566
    Description: PAM password auth succeeded for 'cli' from 10.127.148.234:53791
    Order: 0
Trace Log:
    Time: 2015 Jul 26 06:35:15
    Severity: Notice
    Source: CMC:AUDIT:19566
    Description: Session open (user:admin, ip:10.127.148.234, id:6, type:CLI)
    Order: 1
Trace Log:
    Time: 2015 Jul 26 06:35:15
    Severity: Informational
    Source: CMC:dropbear:19566
    Description: " pam_session_manager(sshd:session): session (6) opened for user admin
from 10.127.148.234 by (uid=0) "
    Order: 2
Trace Log:
    Time: 2015 Jul 26 06:35:15
    Severity: Notice
    Source: CMC:AUDIT:1779
.
.
.

Server /chassis/log #
```

# Clearing Trace Logs

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server# **scope chassis** | Enters the chassis command mode. |
| **Step 2** | Server /chassis # **scope log** | Enters the log command mode. |
| **Step 3** | Server /chassis/log # **clear** | Clears the trace log. |

The following example clears the log of trace logs:

```
Server# scope chassis
Server /chassis # scope log
Server /chassis/log # clear

Server /chassis/log #
```

# Configuring the Cisco IMC Log Threshold

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

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server # **scope chassis** | Enters chassis command mode. |
| **Step 2** | Server /chassis # **scope log** | Enters log command mode. |
| **Step 3** | Server /chassis/log # **set local-syslog-severity** *level* | The severity *level* can be one of the following, in decreasing order of severity:<br>• emergency<br>• alert<br>• critical<br>• error<br>• warning<br>• notice<br>• informational<br>• debug<br>**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 /chassis/log # **set remote-syslog-severity** *level* | The severity *level* can be one of the following, in decreasing order of severity:<br>• emergency<br>• alert<br>• critical<br>• error<br>• warning<br>• notice<br>• informational<br>• debug<br>**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. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | Server /chassis/log # **commit** | Commits the transaction to the system configuration. |
| **Step 6** | Server /chassis/log # **show** | (Optional)<br>Displays the configured severity level. |

This example shows how to configure the logging of messages with a minimum severity of Debug for the local syslogs and error for the remote syslog:

```
Server# scope chassis
Server /chassis # scope log
Server /chassis/log # set local-syslog-severity debug
Server /chassis/log # set remote-syslog-severity error
Server /chassis/log *# commit
Server /chassis/log # show
Local Syslog Severity  Remote Syslog Severity
---------------------- ----------------------
debug                  error

Server /chassis/log #
```

# Sending the Cisco IMC Log to a Remote Server

You can configure profiles for one or two remote syslog servers to receive system 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 chassis** | Enters chassis command mode. |
| **Step 2** | Server /chassis # **scope log** | Enters log command mode. |
| **Step 3** | Server /chassis/log # **scope server** {**1** \| **2**} | Selects one of the two remote syslog server profiles and enters the command mode for configuring the profile. |
| **Step 4** | Server /chassis/log/server # **set server-ip** *ipv4 or ipv6 address or domain name* | Specifies the remote syslog server address.<br>**Note** You can set an IPv4 or IPv6 address or a domain name as the remote server address. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | Server /chassis/log/server # **set server-port** *port number* | Sets the destination port number of the remote syslog server. |
| **Step 6** | Server /chassis/log/server # **set enabled** {**yes** \| **no**} | Enables the sending of system log entries to this syslog server. |
| **Step 7** | Server /chassis/log/server # **commit** | Commits the transaction to the system configuration. |
| **Step 8** | Server /chassis/log/server # **exit** | Exits to the log command mode. |
| **Step 9** | Server /chassis/log/server # **showserver** | Exits to the log command mode. |

This example shows how to configure a remote syslog server profile and enable the sending of system log entries:

# 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--
```

# Viewing the System Event Log for Servers

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server# **scope server** {*1* \| *2* } | Enters the server mode for server 1 or 2. |
| **Step 2** | Server /server # **scope sel** | Enters the system event log (SEL) command mode. |
| **Step 3** | Server /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 server 1
Server/server # scope sel
Server /server/sel # show entries
Time                Severity  Description
------------------- --------- ----------------------------------------
2015-08-18 08:46:03 Normal    "BIOS_POST_CMPLT: Presence sensor, Device Inserted / Device
Present was asserted"
2015-08-18 08:46:00 Normal    "System Software event: System Event sensor, OEM System Boot
 Event was asserted"
2010-03-21 00:17:42 Normal    "System Software event: System Event sensor, Timestamp Clock
 Synch (second of pair) was asserted"
2015-08-18 08:44:34 Normal    "System Software event: System Event sensor, Timestamp Clock
 Synch (first of pair) was asserted"
2015-08-18 08:44:00 Normal    "BIOS_POST_CMPLT: Presence sensor, Device Removed / Device
Absent was asserted"
2015-08-18 08:44:00 Normal    "MAIN_POWER_PRS: Presence sensor, Device Inserted / Device
Present was asserted"
2015-08-18 08:43:39 Normal    "MAIN_POWER_PRS: Presence sensor, Device Removed / Device
Absent was asserted"
2015-08-18 08:16:18 Normal    "BIOS_POST_CMPLT: Presence sensor, Device Inserted / Device
Present was asserted"
```

```
2015-08-18 08:16:16 Normal    "System Software event: System Event sensor, OEM System Boot
 Event was asserted"
2010-03-20 23:47:59 Normal    "System Software event: System Event sensor, Timestamp Clock
 Synch (second of pair) was asserted"
2015-08-18 08:14:50 Normal    "System Software event: System Event sensor, Timestamp Clock
 Synch (first of pair) was asserted"
2015-08-18 08:14:20 Normal    "BIOS_POST_CMPLT: Presence sensor, Device Removed / Device
Absent was asserted"
2015-08-18 08:14:20 Normal    "MAIN_POWER_PRS: Presence sensor, Device Inserted / Device
Present was asserted"
2015-08-18 08:13:44 Normal    "MAIN_POWER_PRS: Presence sensor, Device Removed / Device
Absent was asserted"
2015-08-18 08:12:57 Normal    "FRU_RAM SEL_FULLNESS: Event Log sensor for FRU_RAM, Log Area
 Reset/Cleared was asserted"
```

## 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 syslog log.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server # **scope chassis** | Enters chassis command mode. |
| **Step 2** | Server /chassis # **scope log** | Enters log command mode. |
| **Step 3** | Server /chassis/log # **set local-syslog-severity** *level* | The severity *level* can be one of the following, in decreasing order of severity: |

| | Command or Action | Purpose |
|---|---|---|
| | | • emergency<br>• alert<br>• critical<br>• error<br>• warning<br>• notice<br>• informational<br>• debug<br><br>**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 /chassis/log # **set remote-syslog-severity** *level* | The severity *level* can be one of the following, in decreasing order of severity:<br>• emergency<br>• alert<br>• critical<br>• error<br>• warning<br>• notice<br>• informational<br>• debug<br><br>**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 5** | Server /chassis/log # **commit** | Commits the transaction to the system configuration. |
| **Step 6** | Server /chassis/log # **show** | (Optional)<br>Displays the configured severity level. |

This example shows how to configure the logging of messages with a minimum severity of Debug for the local syslogs and error for the remote syslog:

```
Server# scope chassis
Server /chassis # scope log
Server /chassis/log # set local-syslog-severity debug
Server /chassis/log # set remote-syslog-severity error
Server /chassis/log *# commit
Server /chassis/log # show
Local Syslog Severity  Remote Syslog Severity
---------------------- ----------------------
debug                  error

Server /chassis/log #
```

# Sending the Cisco IMC Log to a Remote Server

You can configure profiles for one or two remote syslog servers to receive system 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 chassis** | Enters chassis command mode. |
| **Step 2** | Server /chassis # **scope log** | Enters log command mode. |
| **Step 3** | Server /chassis/log # **scope server** {**1** \| **2**} | Selects one of the two remote syslog server profiles and enters the command mode for configuring the profile. |
| **Step 4** | Server /chassis/log/server # **set server-ip** *ipv4 or ipv6 address or domain name* | Specifies the remote syslog server address.<br>**Note** You can set an IPv4 or IPv6 address or a domain name as the remote server address. |
| **Step 5** | Server /chassis/log/server # **set server-port** *port number* | Sets the destination port number of the remote syslog server. |
| **Step 6** | Server /chassis/log/server # **set enabled** {**yes** \| **no**} | Enables the sending of system log entries to this syslog server. |
| **Step 7** | Server /chassis/log/server # **commit** | Commits the transaction to the system configuration. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 8** | Server /chassis/log/server # **exit** | Exits to the log command mode. |
| **Step 9** | Server /chassis/log/server # **showserver** | Exits to the log command mode. |

This example shows how to configure a remote syslog server profile and enable the sending of system log entries:

# Sending a Test Cisco IMC Log to a Remote Server

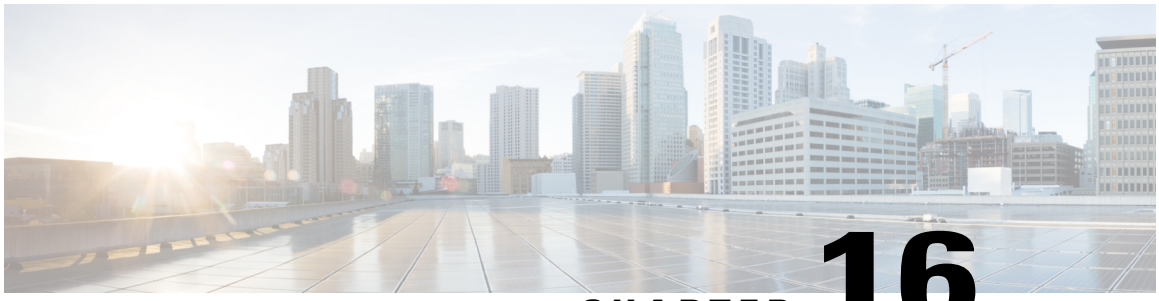
### Before You Begin

- 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 chassis** | Enters chassis command mode. |
| **Step 2** | Server /chassis # **scope log** | Enters log command mode. |
| **Step 3** | Server /chassis/log # **send-test-syslog** | Sends a test log to the remote server. |

This example shows how send a test log to a remote server:



CHAPTER 16

# Server Utilities

This chapter includes the following sections:



## 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 chassis** | Enters chassis command mode. |
| **Step 2** | Server /chassis # **scope tech-support** | Enters the tech-support command mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | Server /chassis/tech-support # **set collect-from** {**all** \| **cmc** \| **peercmc** \| **bmc1** \| **bmc2**} | Specifies the component for which the technical support data has to be exported. |
| **Step 4** | Server /chassis/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 5** | Server /chassis/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.<br>**Tip** To have the system auto-generate the file name, enter the file name as default.tar.gz. |
| **Step 6** | Server /chassis/tech-support # **set remote-protocol** *protocol* | Specifies the protocol to connect to the remote server. It can be of the following types:<br>• TFTP<br>• FTP<br>• SFTP<br>• SCP<br>• HTTP<br>**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.<br>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.<br>The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to. |
| **Step 7** | Server /chassis/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 8** | Server /chassis/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 9** | Server /chassis/tech-support # **commit** | Commits the transaction to the system configuration. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 10** | Server /chassis/tech-support # **start** | Begins the transfer of the data file to the remote server. |
| **Step 11** | Server /chassis/tech-support # **show detail** | (Optional)<br>Displays the progress of the transfer of the data file to the remote server. |
| **Step 12** | Server /chassis/tech-support # **cancel** | (Optional)<br>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 chassis
Server /chassis # scope tech-support
Server /chassis/tech-support # set collect-from all
Server /chassis/tech-support* # set remote-ip 192.0.20.41
Server /chassis/tech-support* # set remote-protocol tftp
Server /chassis/tech-support *# set remote-path /user/user1/default.tar.gz
Server /chassis/tech-support *# commit
Server /chassis/tech-support # start
Tech Support upload started.

Server /chassis/tech-support # show detail

Tech Support:
 Server Address: 192.0.20.41
    Path('default' for auto-naming): default.tar.gz
    Protocol: tftp
    Username:
    Password: ******
    Collect from: all
    Progress(%): 100
    Status: COMPLETED

Server /chassis/tech-support #
```

### 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 server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 2** | Server /server # **scope bmc** | Enters bmc command mode. |
| **Step 3** | Server /server/bmc # **reboot** | The Cisco IMC reboots. |

This example reboots the Cisco IMC:

```
Server# scope server 1
Server /server # scope bmc
Server /server/bmc # 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 server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 2** | Server /server # **scope bios** | Enters the bios command mode. |
| **Step 3** | Server /server/bios # **clear-cmos** | After a prompt to confirm, clears the CMOS memory. |

This example clears the BIOS CMOS memory:

```
Server# scope server 2
Server/server # scope bios
Server /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 /server/bios #
```

# Resetting the BMC to factory Defaults

On rare occasions, such as an issue with the current running firmware, troubleshooting a server may require you to reset the BMC 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 BMC, you are logged off and must log in again. You may also lose connectivity and may need to reconfigure the network settings.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server # **scope server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 2** | Server /server # **scope bmc** | Enters bmc command mode.<br>**Note** Depending on the server number you have chosen, enters the BMC1 or BMC2 mode. |
| **Step 3** | Server /server/bmc # **factory-default** | After a prompt to confirm, the BMC resets to factory defaults. All your BMC configuration is lost and some of the inventory information may not be available until the server is powered on or power cycled. |

This example resets BMC1 to factory defaults:

```
Server# scope server 1
Server /server # scope bmc
Server /server/bmc # factory-default
This operation will reset the Server BMC configuration to factory default.
All your configuration will be lost. Some inventory information may
not be available until the server is powered on or power cycled.
Continue?[y|N] y
```

# Resetting CMCs to Factory Defaults

On rare occasions, such as an issue with the current running firmware, troubleshooting a server may require you to reset the CMCs 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 CMC, you are logged off and must log in again. You may also lose connectivity and may need to reconfigure the network settings.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server# **scope chassis** | Enters the chassis command mode. |
| **Step 2** | Server /chassis # **factory-default** | After a prompt to confirm, the CMCs resets to factory defaults. All your CMC configuration is lost and the network configuration mode is set to **Cisco Card** mode by default. |

The CMCs 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 CMCs to factory defaults:

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

# Exporting and Importing the Cisco IMC and BMC Configuration

## Importing a CMC Configuration

**Important** If any firmware or BIOS updates are in progress, do not import the Cisco IMC 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 # **scope import-export** | Enters the import-export command mode. |
| **Step 3** | Server /chassis/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:<br>• TFTP<br>• FTP<br>• SFTP<br>• SCP<br>• 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.<br>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.<br>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** | 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 chassis
Server /chassis # scope import-export
Server /chassis/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 /chassis/import-export # show detail
Import Export:
    Operation: Import
    Status: COMPLETED
    Error Code: 100 (No Error)
    Diagnostic Message: NONE
Server /chassis/import-export #
```

# Importing BMC Configuration

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

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server # **scope server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 2** | Server /server # **scope bmc** | Enters bmc command mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | Server /server/bmc # **scope import-export** | Enters the import-export command mode. |
| **Step 4** | Server /server/bmc/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:<br>• TFTP<br>• FTP<br>• SFTP<br>• SCP<br>• HTTP<br>**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.<br>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.<br>The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to. |
| **Step 5** | Enter the Username and Password. | Sets the username and password 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 server 2
Server /server# scope bmc
Server /server/bmc # scope import-export
Server /server/bmc/import-export # import-config tftp 192.0.2.34 /ucs/backups/cimc5.xml
Username:pynj
Password:****
Import config started. Please check the status using "show detail".
Server /chassis/import-export # show detail
Import Export:
    Operation: Import
    Status: COMPLETED
    Error Code: 100 (No Error)
    Diagnostic Message: NONE
Server /server/bmc/import-export #
```

# Exporting the BMC Configuration

**Note** For security reasons, this operation does not export user accounts or the server certificate.

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

### Before You Begin

Obtain the backup remote server IP address.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server # **scope server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 2** | Server /server # **scope bmc** | Enters bmc command mode. |
| **Step 3** | Server /server/bmc # **scope import-export** | Enters the import-export command mode. |
| **Step 4** | Server /server/bmc/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:<br>• TFTP<br>• FTP<br>• SFTP<br>• SCP<br>• HTTP<br>**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.<br>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.<br>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 5** | Enter the Username and Password. | 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 server 2
Server /server# scope bmc
Server /server/bmc # scope import-export
Server /server/bmc/import-export # export-config tftp 192.0.2.34 /ucs/backups/cimc5.xml
Username:pynj
Password:****
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 /server/bmc/import-export #
```

# Exporting the CMC Configuration

**Note** For security reasons, this operation does not export user accounts or the server certificate.

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

### Before You Begin

Obtain the backup remote server IP address.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server # **scope chassis** | Enters chassis command mode. |
| **Step 2** | Server /chassis # **scope import-export** | Enters the import-export command mode. |
| **Step 3** | Server /chassis/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:<br>• TFTP |

| | Command or Action | Purpose |
|---|---|---|
| | | • FTP<br>• SFTP<br>• SCP<br>• HTTP<br>**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.<br>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.<br>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** | 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 chassis
Server /chassis # scope import-export
Server /chassis/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 /chassis/import-export # show detail
Import Export:
    Operation: EXPORT
    Status: COMPLETED
    Error Code: 100 (No Error)
    Diagnostic Message: NONE

Server /chassis/import-export #
```

# Generating Non-Maskable Interrupts to the Host

In some situations, the server might hang and not respond to traditional debug mechanisms. By generating a non maskable interrupt (NMI) to the host, you can create and send a crash dump file of the server and use it to debug the server.

Depending on the type of operating system associated with the server, this task might restart the OS.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server # **scope chassis** | Enters chassis command mode. |
| **Step 2** | Server /chassis # **scope server** {**1** \| **2**} | Enters server command mode of server 1 or 2. |
| **Step 3** | Server /chassis/server # **generate-nmi** | Generates the crash dump file for the server.<br>To use this command, the server must be powered on, and you must be logged in as an administrator. |

This example shows how to generate NMI signals to the host:

```
Server # scope chassis
Server /chassis # scope server 2
Server /chassis/server # generate-nmi
This operation will send NMI to host and may cause reboot of OS
OS reboot depends on it's NMI configuration
Do you want to continue? [y|N] y
Server /chassis/server #
```

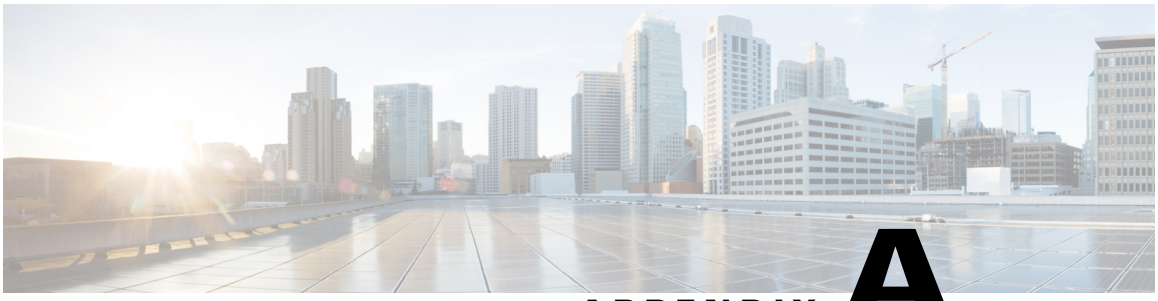
# Adding Cisco IMC Banner

### 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)<br>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 #
```



APPENDIX A

# BIOS Parameters by Server Model

This appendix contains the following sections:



# C3X60 Servers

## Main BIOS Parameters for C3260 Servers

### Main BIOS Parameters

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

# Advanced BIOS Parameters for C3260 Servers

### Processor Configuration Parameters

| Name | Description |
|---|---|
| **Intel Hyper-Threading Technology**<br>**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:<br>• **Disabled—**The processor does not permit hyperthreading.<br>• **Enabled—**The processor allows for the parallel execution of multiple threads.<br>We recommend that you contact your operating system vendor to make sure the operating system supports this feature. |
| **Number of Enabled Cores**<br>**set CoreMultiProcessing** | Allows you to disable one or more of the physical cores on the server. This can be one of the following:<br>• **All—**Enables all physical cores. This also enables Hyper Threading on the associated logical processor cores.<br>• **1** through ***n*—**Specifies the number of physical processor cores that can run on the server. Each physical core has an associated logical core.<br>We recommend that you contact your operating system vendor to make sure the operating system supports this feature. |
| **Execute Disable**<br>**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:<br>• **Disabled—**The processor does not classify memory areas.<br>• **Enabled—**The processor classifies memory areas.<br>We recommend that you contact your operating system vendor to make sure the operating system supports this feature. |

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

| Name | Description |
|---|---|
| **CPU Performance**<br>**set CPUPerformance** | Sets the CPU performance profile for the server. The performance profile consists of the following options:<br>• DCU Streamer Prefetcher<br>• DCU IP Prefetcher<br>• Hardware Prefetcher<br>• Adjacent Cache-Line Prefetch<br>This can be one of the following:<br>• **Enterprise—**All options are enabled.<br>• **High_Throughput—**Only the DCU IP Prefetcher is enabled. The rest of the options are disabled.<br>• **HPC—**All options are enabled. This setting is also known as high performance computing.<br>• **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**<br>**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:<br>• **Disabled—**The hardware prefetcher is not used.<br>• **Enabled—**The processor uses the hardware prefetcher when cache issues are detected. |
| **Adjacent Cache Line Prefetcher**<br>**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:<br>• **Disabled—**The processor only fetches the required line.<br>• **Enabled—** The processor fetches both the required line and its paired line. |

| Name | Description |
|---|---|
| **DCU Streamer Prefetch**<br>**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:<br>• **Disabled—**The processor does not try to anticipate cache read requirements and only fetches explicitly requested lines.<br>• **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**<br>**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:<br>• **Disabled—**The processor does not preload any cache data.<br>• **Enabled—**The DCU IP prefetcher preloads the L1 cache with the data it determines to be the most relevant. |
| **Direct Cache Access Support**<br>**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:<br>• **Disabled—**Data from I/O devices is not placed directly into the processor cache.<br>• **Enabled—**Data from I/O devices is placed directly into the processor cache. |

| Name | Description |
|---|---|
| **Power Technology**<br>**set CPUPowerManagement** | Enables you to configure the CPU power management settings for the following options:<br>• Enhanced Intel Speedstep Technology<br>• Intel Turbo Boost Technology<br>• Processor Power State C6<br>Power Technology can be one of the following:<br>• **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.<br>• **Disabled—**The server does not perform any CPU power management and any settings for the BIOS parameters mentioned above are ignored.<br>• **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**<br>**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:<br>• **Disabled—**The processor never dynamically adjusts its voltage or frequency.<br>• **Enabled—**The processor utilizes Enhanced Intel SpeedStep Technology and enables all supported processor sleep states to further conserve power.<br>We recommend that you contact your operating system vendor to make sure the operating system supports this feature.<br>**Note** **CPUPowerManagement** must be set to **Custom** or the server ignores the setting for this parameter. |

| Name | Description |
|---|---|
| **Intel Turbo Boost Technology**<br>**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:<br>• **Disabled—**The processor does not increase its frequency automatically.<br>• **Enabled—**The processor utilizes Turbo Boost Technology if required.<br>**Note** **CPUPowerManagement** must be set to **Custom** or the server ignores the setting for this parameter. |
| **Processor Power State C6**<br>**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:<br>• **Disabled—**The BIOS does not send the C6 report.<br>• **Enabled—**The BIOS sends the C6 report, allowing the OS to transition the processor to the C6 low power state.<br>**Note** **CPUPowerManagement** must be set to **Custom** or the server ignores the setting for this parameter. |
| **Processor Power State C1 Enhanced**<br>**set ProcessorC1EReport** | Whether the CPU transitions to its minimum frequency when entering the C1 state. This can be one of the following:<br>• **Disabled—**The CPU continues to run at its maximum frequency in C1 state.<br>• **Enabled—**The CPU transitions to its minimum frequency. This option saves the maximum amount of power in C1 state. |
| **Frequency Floor Override**<br>**set CpuFreqFloor** | Whether the CPU is allowed to drop below the maximum non-turbo frequency when idle. This can be one of the following:<br>• **Disabled—** The CPU can drop below the maximum non-turbo frequency when idle. This option decreases power consumption but may reduce system performance.<br>• **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**<br>**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.<br>• **HW_ALL—**The processor hardware is responsible for coordinating the P-state among logical processors with dependencies (all logical processors in a package).<br>• **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.<br>• **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.<br>**Note** **CPUPowerManagement** must be set to **Custom** or the server ignores the setting for this parameter. |
| **Energy Performance**<br>**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:<br>• **Balanced_Energy**<br>• **Balanced_Performance**<br>• **Energy_Efficient**<br>• **Performance** |

### Memory Configuration Parameters

| Name | Description |
|---|---|
| **Select Memory RAS**<br>**set SelectMemoryRAS** | How the memory reliability, availability, and serviceability (RAS) is configured for the server. This can be one of the following:<br>• **Maximum_Performance—**System performance is optimized.<br>• **Mirroring—**System reliability is optimized by using half the system memory as backup.<br>• **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**<br>**set DRAMClockThrottling** | Allows you to tune the system settings between the memory bandwidth and power consumption. This can be one of the following:<br>• **Balanced—** DRAM clock throttling is reduced, providing a balance between performance and power.<br>• **Performance—**DRAM clock throttling is disabled, providing increased memory bandwidth at the cost of additional power.<br>• **Energy_Efficient—**DRAM clock throttling is increased to improve energy efficiency. |
| **NUMA**<br>**set NUMAOptimize** | Whether the BIOS supports Non-Uniform Memory Access (NUMA). This can be one of the following:<br>• **Disabled—**The BIOS does not support NUMA.<br>• **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**<br>**set LvDDRMode** | Whether the system prioritizes low voltage or high frequency memory operations. This can be one of the following:<br>• **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.<br>• **Performance_Mode—**The system prioritizes high frequency operations over low voltage operations. |
| **DRAM Refresh rate**<br>**set DramRefreshRate** | Allows you to set the rate at which the DRAM cells are refreshed. This can be one of the following:<br>• **1x—**DRAM cells are refreshed every 64ms.<br>• **2x—**DRAM cells are refreshed every 32ms.<br>• **3x—**DRAM cells are refreshed every 21ms.<br>• **4x—**DRAM cells are refreshed every 16ms.<br>• **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**<br>**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:<br>• **Auto—**The CPU determines what interleaving is done.<br>• **1_Way—**Some channel interleaving is used.<br>• **2_Way**<br>• **3_Way**<br>• **4_Way—**The maximum amount of channel interleaving is used. |

| Name | Description |
|---|---|
| **Rank Interleaving**<br>**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:<br>• **Auto—**The CPU determines what interleaving is done.<br>• **1_Way—**Some rank interleaving is used.<br>• **2_Way**<br>• **4_Way**<br>• **8_Way—**The maximum amount of rank interleaving is used. |
| **Patrol Scrub**<br>**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:<br>• **Disabled—**The system checks for memory ECC errors only when the CPU reads or writes a memory address.<br>• **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**<br>**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:<br>• **Disabled—** Single bit memory errors are not corrected.<br>• **Enabled—** Single bit memory errors are corrected in memory and the corrected data is set in response to the demand read. |

| Name | Description |
|---|---|
| **Altitude**<br>**set Altitude** | The approximate number of meters above sea level at which the physical server is installed. This can be one of the following:<br>• **Auto—**The CPU determines the physical elevation.<br>• **300_M—**The server is approximately 300 meters above sea level.<br>• **900_M—**The server is approximately 900 meters above sea level.<br>• **1500_M—**The server is approximately 1500 meters above sea level.<br>• **3000_M—**The server is approximately 3000 meters above sea level. |

### QPI Configuration Parameters

| Name | Description |
|---|---|
| **QPI Link Frequency Select**<br>**set QPILinkFrequency** | The Intel QuickPath Interconnect (QPI) link frequency, in gigatransfers per second (GT/s). This can be one of the following:<br>• **Auto—**The CPU determines the QPI link frequency.<br>• **6.4_GT/s**<br>• **7.2_GT/s**<br>• **8.0_GT/s** |

### SATA Configuration Parameters

| Name | Description |
|---|---|
| **SATA Mode**<br>**set SataMode** | Mode of operation of Serial Advanced Technology Attachment (SATA) Solid State Drives (SSD).<br>• **Disabled—** All SATA ports is disabled, and drivers are not enumerated.<br>• **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**<br>**set LegacyUSBSupport** | Whether the system supports legacy USB devices. This can be one of the following:<br>• **Disabled—**USB devices are only available to EFI applications.<br>• **Enabled—**Legacy USB support is always available.<br>• **Auto—**Disables legacy USB support if no USB devices are connected. |
| **Port 60/64 Emulation**<br>**set UsbEmul6064** | Whether the system supports 60h/64h emulation for complete USB keyboard legacy support. This can be one of the following:<br>• **Disabled—**60h/64 emulation is not supported.<br>• **Enabled—**60h/64 emulation is supported.<br>You should select this option if you are using a non-USB aware operating system on the server. |
| **All USB Devices**<br>**set AllUsbDevices** | Whether all physical and virtual USB devices are enabled or disabled. This can be one of the following:<br>• **Disabled—**All USB devices are disabled.<br>• **Enabled—**All USB devices are enabled. |
| **USB Port: Rear**<br>**set UsbPortRear** | Whether the rear panel USB devices are enabled or disabled. This can be one of the following:<br>• **Disabled—**Disables the rear panel USB ports. Devices connected to these ports are not detected by the BIOS and operating system.<br>• **Enabled—**Enables the rear panel USB ports. Devices connected to these ports are detected by the BIOS and operating system. |
| **USB Port: Internal**<br>**set UsbPortInt** | Whether the internal USB devices are enabled or disabled. This can be one of the following:<br>• **Disabled—**Disables the internal USB ports. Devices connected to these ports are not detected by the BIOS and operating system.<br>• **Enabled—**Enables the internal USB ports. Devices connected to these ports are detected by the BIOS and operating system. |

| Name | Description |
|---|---|
| **USB Port: KVM**<br>**set UsbPortKVM** | Whether the KVM ports are enabled or disabled. This can be one of the following:<br>• **Disabled—**Disables the KVM keyboard and/or mouse devices. Keyboard and/or mouse will not work in the KVM window.<br>• **Enabled—**Enables the KVM keyboard and/or mouse devices. |
| **USB Port: vMedia**<br>**set UsbPortVMedia** | Whether the virtual media devices are enabled or disabled. This can be one of the following:<br>• **Disabled—**Disables the vMedia devices.<br>• **Enabled—**Enables the vMedia devices. |

### PCI Configuration Parameters

| Name | Description |
|---|---|
| **PCI ROM CLP**<br>**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.<br>• **Enabled—** Enables you to configure execution of different option ROMs such as PxE and iSCSI for an individual ports separately.<br>• **Disabled—**The default option. You cannot choose different option ROMs. A default option ROM is executed during PCI enumeration. |
| **ASPM Support**<br>**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:<br>• **Disabled—**ASPM support is disabled in the BIOS.<br>• **Force L0s—**Force all links to L0 standby (L0s) state.<br>• **Auto—**The CPU determines the power state. |

### Serial Configuration Parameters

| Name | Description |
|---|---|
| **Out-of-Band Mgmt Port**<br>**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:<br>• **Disabled—**Configures the COM port 0 as a general purpose port for use with the Windows Operating System.<br>• **Enabled—**Configures the COM port 0 as a remote management port for Windows Emergency Management services. |
| **Console Redirection**<br>**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:<br>• **Disabled—**No console redirection occurs during POST.<br>• **COM_0—**Enables console redirection on COM port 0 during POST.<br>• **COM_1—**Enables console redirection on COM port 1 during POST. |
| **Terminal Type**<br>**set TerminalType** | What type of character formatting is used for console redirection. This can be one of the following:<br>• **PC-ANSI—**The PC-ANSI terminal font is used.<br>• **VT100—**A supported vt100 video terminal and its character set are used.<br>• **VT100+—**A supported vt100-plus video terminal and its character set are used.<br>• **VT-UTF8—**A video terminal with the UTF-8 character set is used.<br>**Note** This setting must match the setting on the remote terminal application. |

| Name | Description |
|---|---|
| **Bits per second**<br>**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:<br>• **9600—**A 9,600 BAUD rate is used.<br>• **19200—**A 19,200 BAUD rate is used.<br>• **38400—**A 38,400 BAUD rate is used.<br>• **57600—**A 57,600 BAUD rate is used.<br>• **115200—**A 115,200 BAUD rate is used.<br>**Note** This setting must match the setting on the remote terminal application. |
| **Flow Control**<br>**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:<br>• **None—**No flow control is used.<br>• **Hardware_RTS/CTS—**RTS/CTS is used for flow control.<br>**Note** This setting must match the setting on the remote terminal application. |
| **Putty KeyPad**<br>**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:<br>• **VT100—**The function keys generate ESC OP through ESC O[.<br>• **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.<br>• **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.<br>• **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 [{.<br>• **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~.<br>• **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**<br>**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:<br>• **Always_Enable—**BIOS Legacy console redirection is active during the OS boot and run time.<br>• **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**<br>**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:<br>• **Disabled—** CDN support for VIC cards is disabled.<br>• **Enabled—** CDN support is enabled for VIC cards.<br>**Note** CDN support for VIC cards work with Windows 2012 or the latest OS only. |
| **All PCIe Slots OptionROM**<br>**set PcieOptionROMs** | Whether the server can use Option ROM present in the PCIe Cards. This can be one of the following:<br>• **Disabled—**The Option ROM for all PCIe slots are not available.<br>• **Enabled—**The Option ROMs for all the PCIe slots are available.<br>• **UEFI_Only—**The Opiton ROMs for slot ***n*** are available for UEFI only.<br>• **Legacy_Only—**The Option ROM for slot ***n*** are available for legacy only. |
| **PCIe Slot:*n* OptionROM**<br>**set PcieSlot*n*OptionROM** | Whether the server can use the Option ROMs present in the PCIe Cards. This can be one of the following:<br>• **Disabled—**The Option ROM for slot ***n*** is not available.<br>• **Enabled—**The Option ROM for slot ***n*** is available.<br>• **UEFI_Only—**The Option ROM for slot ***n*** is available for UEFI only.<br>• **Legacy_Only—**The Option ROM for slot ***n*** is available for legacy only. |

| Name | Description |
|---|---|
| **PCIe Mezzanine OptionROM**<br>**set PcieMezzOptionROM** | Whether the PCIe mezzanine slot expansion ROM is available to the server. This can be one of the following:<br>• **Disabled—** The Option ROM for slot ***M*** is not available.<br>• **Enabled—** The Option ROM for slot ***M*** is available.<br>• **UEFI_Only—**The Option ROM for slot ***M*** is available for UEFI only.<br>• **Legacy_Only—**The expansion slot for slot ***M*** is available for legacy only. |
| **SIOC1 Link Speed**<br>**Set PcieSlot1LinkSpeed** | System IO Controller 1 (SIOC1) add-on slot 1 link speed.<br>• **GEN1 —** Link speed can reach up to first generation.<br>• **GEN2 —** Link speed can reach up to second generation.<br>• **GEN3—** The default link speed. Link speed can reach up to third generation.<br>• **Disabled —** Slot is disabled, and the card is not enumerated. |
| **SIOC2 Link Speed**<br>**set PcieSlot2LinkSpeed** | System IO Controller 2 (SIOC2) add-on slot 2 link speed.<br>• **GEN1 —** Link speed can reach up to first generation.<br>• **GEN2 —** Link speed can reach up to second generation.<br>• **GEN3—** The default link speed. Link speed can reach up to third generation.<br>• **Disabled —** Slot is disabled, and the card is not enumerated. |
| **Mezz Link Speed**<br>**set PcieSlotMLinkSpeed** | Mezz link speed. This can be one of the following:<br>• **GEN 1—** Link speed can reach up to first generation.<br>• **GEN 2—** Link speed can reach up to second generation.<br>• **GEN 3—**The default link speed. Link speed can reach up to third generation.<br>• **Disabled—**Slot is disabled, and the card is not enumerated. |

# Server Management BIOS Parameters for C3260 Servers

### Server Management BIOS Parameters

| Name | Description |
|---|---|
| **FRB-2 Timer**<br>**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:<br>• **Disabled—**The FRB2 timer is not used.<br>• **Enabled—**The FRB2 timer is started during POST and used to recover the system if necessary. |
| **OS Watchdog Timer**<br>**set OSBootWatchdogTimer** | Whether the BIOS programs the watchdog timer with a specified timeout value. This can be one of the following:<br>• **Disabled—**The watchdog timer is not used to track how long the server takes to boot.<br>• **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**<br>**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:<br>• **5_Minutes—**The OS watchdog timer expires 5 minutes after it begins to boot.<br>• **10_Minutes—**The OS watchdog timer expires 10 minutes after it begins to boot.<br>• **15_Minutes—**The OS watchdog timer expires 15 minutes after it begins to boot.<br>• **20_Minutes—**The OS watchdog timer expires 20 minutes after it begins to boot.<br>**Note** This option is only applicable if you enable the OS Boot Watchdog Timer. |

| Name | Description |
|---|---|
| **OS Watchdog Timer Policy**<br>**set OSBootWatchdogTimerPolicy** | What action the system takes if the watchdog timer expires. This can be one of the following:<br>• **Do_Nothing—**The server takes no action if the watchdog timer expires during OS boot.<br>• **Power_Down—**The server is powered off if the watchdog timer expires during OS boot.<br>• **Reset—**The server is reset if the watchdog timer expires during OS boot.<br>**Note** This option is only applicable if you enable the OS Boot Watchdog Timer. |

# Main BIOS Parameters for C3X60 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. |
| **TPM Support** | 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:<br>• **Disabled—**The server does not use the TPM.<br>• **Enabled—**The server uses the TPM.<br>**Note** We recommend that you contact your operating system vendor to make sure the operating system supports this feature. |

# Advanced BIOS Parameters for C3X60 M4 Servers

### Processor Configuration Parameters

| Name | Description |
|---|---|
| **Intel Hyper-Threading Technology**<br>**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:<br>• **Disabled—**The processor does not permit hyperthreading.<br>• **Enabled—**The processor allows for the parallel execution of multiple threads.<br>We recommend that you contact your operating system vendor to make sure the operating system supports this feature. |
| **Number of Enabled Cores**<br>**set CoreMultiProcessing** | Allows you to disable one or more of the physical cores on the server. This can be one of the following:<br>• **All—**Enables all physical cores. This also enables Hyper Threading on the associated logical processor cores.<br>• **1** through ***n*—**Specifies the number of physical processor cores that can run on the server. Each physical core has an associated logical core.<br>We recommend that you contact your operating system vendor to make sure the operating system supports this feature. |
| **Execute Disable**<br>**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:<br>• **Disabled—**The processor does not classify memory areas.<br>• **Enabled—**The processor classifies memory areas.<br>We recommend that you contact your operating system vendor to make sure the operating system supports this feature. |

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

| Name | Description |
|---|---|
| **CPU Performance**<br>**set CPUPerformance** | Sets the CPU performance profile for the server. The performance profile consists of the following options:<br>• DCU Streamer Prefetcher<br>• DCU IP Prefetcher<br>• Hardware Prefetcher<br>• Adjacent Cache-Line Prefetch<br>This can be one of the following:<br>• **Enterprise—**All options are enabled.<br>• **High_Throughput—**Only the DCU IP Prefetcher is enabled. The rest of the options are disabled.<br>• **HPC—**All options are enabled. This setting is also known as high performance computing.<br>• **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**<br>**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:<br>• **Disabled—**The hardware prefetcher is not used.<br>• **Enabled—**The processor uses the hardware prefetcher when cache issues are detected. |
| **Adjacent Cache Line Prefetcher**<br>**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:<br>• **Disabled—**The processor only fetches the required line.<br>• **Enabled—** The processor fetches both the required line and its paired line. |

| Name | Description |
|---|---|
| **DCU Streamer Prefetch**<br>**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:<br>• **Disabled—**The processor does not try to anticipate cache read requirements and only fetches explicitly requested lines.<br>• **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**<br>**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:<br>• **Disabled—**The processor does not preload any cache data.<br>• **Enabled—**The DCU IP prefetcher preloads the L1 cache with the data it determines to be the most relevant. |
| **Direct Cache Access Support**<br>**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:<br>• **Disabled—**Data from I/O devices is not placed directly into the processor cache.<br>• **Enabled—**Data from I/O devices is placed directly into the processor cache. |

| Name | Description |
|---|---|
| **Power Technology**<br>**set CPUPowerManagement** | Enables you to configure the CPU power management settings for the following options:<br>• Enhanced Intel Speedstep Technology<br>• Intel Turbo Boost Technology<br>• Processor Power State C6<br>Power Technology can be one of the following:<br>• **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.<br>• **Disabled—**The server does not perform any CPU power management and any settings for the BIOS parameters mentioned above are ignored.<br>• **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**<br>**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:<br>• **Disabled—**The processor never dynamically adjusts its voltage or frequency.<br>• **Enabled—**The processor utilizes Enhanced Intel SpeedStep Technology and enables all supported processor sleep states to further conserve power.<br>We recommend that you contact your operating system vendor to make sure the operating system supports this feature.<br>**Note** **CPUPowerManagement** must be set to **Custom** or the server ignores the setting for this parameter. |

| Name | Description |
|---|---|
| **Intel Turbo Boost Technology**<br>**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:<br>• **Disabled—**The processor does not increase its frequency automatically.<br>• **Enabled—**The processor utilizes Turbo Boost Technology if required.<br>**Note** **CPUPowerManagement** must be set to **Custom** or the server ignores the setting for this parameter. |
| **Processor C3 Report**<br>**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:<br>• **Disabled—**BIOS does not send C3 report.<br>• **Enabled—**BIOS sends the C3 report, allowing the OS to transition the processor to the C3 low power state.<br>**Note** **CPUPowerManagement** must be set to **Custom** or the server ignores the setting for this parameter. |
| **Processor C6 Report**<br>**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:<br>• **Disabled—**The BIOS does not send the C6 report.<br>• **Enabled—**The BIOS sends the C6 report, allowing the OS to transition the processor to the C6 low power state.<br>**Note** **CPUPowerManagement** must be set to **Custom** or the server ignores the setting for this parameter. |
| **Processor Power State C1 Enhanced**<br>**set ProcessorC1EReport** | Whether the CPU transitions to its minimum frequency when entering the C1 state. This can be one of the following:<br>• **Disabled—**The CPU continues to run at its maximum frequency in C1 state.<br>• **Enabled—**The CPU transitions to its minimum frequency. This option saves the maximum amount of power in C1 state. |

| Name | Description |
|---|---|
| **P-STATE Coordination**<br>**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.<br>• **HW_ALL—**The processor hardware is responsible for coordinating the P-state among logical processors with dependencies (all logical processors in a package).<br>• **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.<br>• **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.<br>**Note** **CPUPowerManagement** must be set to **Custom** or the server ignores the setting for this parameter. |
| **Energy Performance Tuning**<br>**set PwrPerfTuning** | Allows you to choose BIOS or Operating System for energy performance bias tuning. This can be one of the following:<br>• **OS—** Chooses OS for energy performance tuning.<br>• **BIOS—** Chooses BIOS for energy performance tuning. |
| **Energy Performance**<br>**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:<br>• **Balanced_Energy**<br>• **Balanced_Performance**<br>• **Energy_Efficient**<br>• **Performance** |

| Name | Description |
|---|---|
| **Package C State Limit**<br>**set PackageCStateLimit** | The amount of power available to the server components when they are idle. This can be one of the following:<br>• **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.<br>• **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.<br>• **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.<br>• **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.<br>• **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.<br>• **No_Limit—**The server may enter any available C state. |
| **Extended APIC**<br>**set LocalX2Apic** | Allows you to enable or disable extended APIC support. This can be one of the following:<br>• **XAPIC—**Enables APIC support.<br>• **X2APIC—**Enables APIC and also enables Intel VT-d and Interrupt Remapping . |
| **Workload Configuration**<br>**set WorkLdConfig** | Allows you to set a parameter to optimize workload characterization. This can be one of the following:<br>• **Balanced—** Chooses balanced option for optimization.<br>• **I/O Sensitive—** Chooses I/O sensitive option for optimization.<br>**Note** We recommend you to set the workload configuration to **Balanced**. |

### Memory Configuration Parameters

| Name | Description |
|---|---|
| **Select Memory RAS**<br>**set SelectMemoryRAS** | How the memory reliability, availability, and serviceability (RAS) is configured for the server. This can be one of the following:<br>• **Maximum_Performance—**System performance is optimized.<br>• **Mirroring—**System reliability is optimized by using half the system memory as backup.<br>• **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**<br>**set NUMAOptimize** | Whether the BIOS supports Non-Uniform Memory Access (NUMA). This can be one of the following:<br>• **Disabled—**The BIOS does not support NUMA.<br>• **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**<br>**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:<br>• **Auto—**The CPU determines what interleaving is done.<br>• **1_Way—**Some channel interleaving is used.<br>• **2_Way**<br>• **3_Way**<br>• **4_Way—**The maximum amount of channel interleaving is used. |

| Name | Description |
|---|---|
| **Rank Interleaving**<br>**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:<br>• **Auto—**The CPU determines what interleaving is done.<br>• **1_Way—**Some rank interleaving is used.<br>• **2_Way**<br>• **4_Way**<br>• **8_Way—**The maximum amount of rank interleaving is used. |
| **Patrol Scrub**<br>**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:<br>• **Disabled—**The system checks for memory ECC errors only when the CPU reads or writes a memory address.<br>• **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**<br>**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:<br>• **Disabled—** Single bit memory errors are not corrected.<br>• **Enabled—** Single bit memory errors are corrected in memory and the corrected data is set in response to the demand read. |

| Name | Description |
|---|---|
| **Altitude**<br>**set Altitude** | The approximate number of meters above sea level at which the physical server is installed. This can be one of the following:<br>• **Auto—**The CPU determines the physical elevation.<br>• **300_M—**The server is approximately 300 meters above sea level.<br>• **900_M—**The server is approximately 900 meters above sea level.<br>• **1500_M—**The server is approximately 1500 meters above sea level.<br>• **3000_M—**The server is approximately 3000 meters above sea level. |

### QPI Configuration Parameters

| Name | Description |
|---|---|
| **QPI Link Frequency Select**<br>**set QPILinkFrequency** | The Intel QuickPath Interconnect (QPI) link frequency, in gigatransfers per second (GT/s). This can be one of the following:<br>• **Auto—**The CPU determines the QPI link frequency.<br>• **6.4_GT/s**<br>• **7.2_GT/s**<br>• **8.0_GT/s** |
| **QPI Snoop Mode**<br>**set QpiSnoopMode** | The Intel QuickPath Interconnect (QPI) snoop mode. This can be one of the following:<br>• **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.<br>• **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.<br>• **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. |

### USB Configuration Parameters

| Name | Description |
|---|---|
| **Legacy USB Support**<br>**set LegacyUSBSupport** | Whether the system supports legacy USB devices. This can be one of the following:<br>• **Disabled—**USB devices are only available to EFI applications.<br>• **Enabled—**Legacy USB support is always available.<br>• **Auto—**Disables legacy USB support if no USB devices are connected. |
| **Port 60/64 Emulation**<br>**set UsbEmul6064** | Whether the system supports 60h/64h emulation for complete USB keyboard legacy support. This can be one of the following:<br>• **Disabled—**60h/64 emulation is not supported.<br>• **Enabled—**60h/64 emulation is supported.<br>You should select this option if you are using a non-USB aware operating system on the server. |
| **xHCI Mode**<br>**set PchUsb30Mode** | Whether the xHCI controller legacy support is enabled or disabled. This can be one of the following:<br>• **Disabled—**Disables the xHCI controller legacy support.<br>• **Enabled—**Enables the xHCI controller legacy support. |

### PCI Configuration Parameters

| Name | Description |
|---|---|
| **Memory Mapped I/O Above 4GB**<br>**set MemoryMappedIOAbove4GB** | Whether to enable or disable MMIO above 4GB or not. This can be one of the following:<br>• **Disabled—**The server does not map I/O of 64-bit PCI devices to 4GB or greater address space.<br>• **Enabled—**The server maps I/O of 64-bit PCI devices to 4GB or greater address space.<br>**Note** PCI devices that are 64-bit compliant but use a legacy option ROM may not function correctly with this setting enabled. |

| Name | Description |
|---|---|
| **Sriov**<br>**set SrIov** | Whether SR-IOV (Single Root I/O Virtualization) is enabled or disabled on the server. This can be one of the following:<br>• **Disabled—**SR-IOV is disabled.<br>• **Enabled—**SR-IOV is enabled. |

### Serial Configuration Parameters

| Name | Description |
|---|---|
| **Out-of-Band Mgmt Port**<br>**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:<br>• **Disabled—**Configures the COM port 0 as a general purpose port for use with the Windows Operating System.<br>• **Enabled—**Configures the COM port 0 as a remote management port for Windows Emergency Management services. |
| **Console Redirection**<br>**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:<br>• **Disabled—**No console redirection occurs during POST.<br>• **COM_0—**Enables console redirection on COM port 0 during POST.<br>• **COM_1—**Enables console redirection on COM port 1 during POST. |
| **Terminal Type**<br>**set TerminalType** | What type of character formatting is used for console redirection. This can be one of the following:<br>• **PC-ANSI—**The PC-ANSI terminal font is used.<br>• **VT100—**A supported vt100 video terminal and its character set are used.<br>• **VT100+—**A supported vt100-plus video terminal and its character set are used.<br>• **VT-UTF8—**A video terminal with the UTF-8 character set is used.<br>**Note** This setting must match the setting on the remote terminal application. |

| Name | Description |
|---|---|
| **Bits per second**<br>**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:<br>• **9600—**A 9,600 BAUD rate is used.<br>• **19200—**A 19,200 BAUD rate is used.<br>• **38400—**A 38,400 BAUD rate is used.<br>• **57600—**A 57,600 BAUD rate is used.<br>• **115200—**A 115,200 BAUD rate is used.<br>**Note** This setting must match the setting on the remote terminal application. |
| **Flow Control**<br>**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:<br>• **None—**No flow control is used.<br>• **Hardware_RTS/CTS—**RTS/CTS is used for flow control.<br>**Note** This setting must match the setting on the remote terminal application. |
| **Putty KeyPad**<br>**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:<br>• **VT100—**The function keys generate ESC OP through ESC O[.<br>• **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.<br>• **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.<br>• **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 [{.<br>• **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~.<br>• **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**<br>**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:<br>• **Always_Enable—**BIOS Legacy console redirection is active during the OS boot and run time.<br>• **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**<br>**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:<br>• **Disabled—** CDN support for VIC cards is disabled.<br>• **Enabled—** CDN support is enabled for VIC cards.<br>**Note** CDN support for VIC cards work with Windows 2012 or the latest OS only. |
| **PCI ROM CLP**<br>**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.<br>• **Enabled—** Enables you to configure execution of different option ROMs such as PxE and iSCSI for an individual ports separately.<br>• **Disabled—**The default option. You cannot choose different option ROMs. A default option ROM is executed during PCI enumeration. |
| **All PCIe Slots OptionROM**<br>**set PcieOptionROMs** | Whether the server can use Option ROM present in the PCIe Cards. This can be one of the following:<br>• **Disabled—**The Option ROM for slot ***n*** is not available.<br>• **Enabled—**The Option ROM for slot ***n*** is available.<br>• **UEFI_Only—**The Option ROM for slot ***n*** is available for UEFI only.<br>• **Legacy_Only—**The Option ROM for slot ***n*** is available for legacy only. |

| Name | Description |
|---|---|
| **SBNVMe1 OptionROM**<br>**set SBNVMe1OptionROM** | Whether the server can use Option ROM present in SBNVMe1 controller. This can be one of the following:<br>• **Disabled—**The Option ROM for SBNVMe1 controllers is not available.<br>• **Enabled—**The Option ROMs for SBNVMe1 controller is available.<br>• **UEFI_Only—**The Option ROMs for slot are available for UEFI only.<br>• **Legacy_Only—**The Option ROM for slot are available for legacy only. |
| **SIOC1 OptionROM**<br>**set SIOC1OptionROM** | Whether the server can use Option ROM present in System IO Controller 1 (SIOC1). This can be one of the following:<br>• **Disabled—**The Option ROM for System IO Controller 1 (SIOC1) is not available.<br>• **Enabled—**The Option ROMs for System IO Controller 1 (SIOC1) is available.<br>• **UEFI_Only—**The Option ROMs for slot are available for UEFI only.<br>• **Legacy_Only—**The Option ROM for slot are available for legacy only. |
| **SIOC2 OptionROM set SIOC2OptionROM**<br>**set SIOC2OptionROM** | Whether the server can use Option ROM present in System IO Controller 2 (SIOC2). This can be one of the following:<br>• **Disabled—**The Option ROM for System IO Controller 2 (SIOC2) is not available.<br>• **Enabled—**The Option ROMs for System IO Controller 2 (SIOC2) is available.<br>• **UEFI_Only—**The Option ROMs for slot are available for UEFI only.<br>• **Legacy_Only—**The Option ROM for slot are available for legacy only. |

| Name | Description |
|---|---|
| **SBMezz1 OptionROM**<br>**set SBMezz1OptionROM** | Whether the server can use Option ROM present in SBMezz1 controller. This can be one of the following:<br>• **Disabled—**The Option ROM for SBMezz1 controllers is not available.<br>• **Enabled—**The Option ROMs for SBMezz1 controller is available.<br>• **UEFI_Only—**The Option ROMs for slot are available for UEFI only.<br>• **Legacy_Only—**The Option ROM for slot are available for legacy only. |
| **IOESlot1 OptionROM**<br>**set IOESlot1OptionROM** | Whether option ROM is enabled on the IOE slot 1. This can be one of the following:<br>• **Disabled—** Option ROM is disabled.<br>• **Enabled—** Default value. Option ROM is enabled.<br>• **UEFI Only—** slot 1 option ROM is available for UEFI only.<br>• **Legacy Only—** slot 1 option ROM is available for legacy only. |
| **IOEMezz1 OptionROM**<br>**set IOEMezz1OptionROM** | Whether option ROM is enabled on the IOE Mezz1. This can be one of the following:<br>• **Disabled—** Option ROM is disabled.<br>• **Enabled—** Default value. Option ROM is enabled.<br>• **UEFI Only—** Mezz1 option ROM is available for UEFI only.<br>• **Legacy Only—** Mezz1 option ROM is available for legacy only. |
| **IOESlot2 OptionROM**<br>**set IOESlot2OptionROM** | Whether option ROM is enabled on the IOE slot 2. This can be one of the following:<br>• **Disabled—** Option ROM is disabled.<br>• **Enabled—** Default value. Option ROM is enabled.<br>• **UEFI Only—** slot 2 option ROM is available for UEFI only.<br>• **Legacy Only—** slot 2 option ROM is available for legacy only. |

| Name | Description |
|---|---|
| **IOENVMe1 OptionROM**<br>**set IOENVMe1OptionROM** | Whether option ROM is enabled on the IOE NVMe1. This can be one of the following:<br>• **Disabled—** Option ROM is disabled.<br>• **Enabled—** Default value. Option ROM is enabled.<br>• **UEFI Only—** Mezz1 option ROM is available for UEFI only.<br>• **Legacy Only—** Mezz1 option ROM is available for legacy only. |
| **IOENVMe2 OptionROM**<br>**set IOENVMe2OptionROM** | Whether option ROM is enabled on the IOE NVMe2. This can be one of the following:<br>• **Disabled—** Option ROM is disabled.<br>• **Enabled—** Default value. Option ROM is enabled.<br>• **UEFI Only—** Mezz1 option ROM is available for UEFI only.<br>• **Legacy Only—** Mezz1 option ROM is available for legacy only. |
| **SBNVMe1 Link Speed**<br>**Set SBNVMe1LinkSpeed** | SBNVMe1 add-on slot 1 link speed.<br>• **Auto—**Link speed is automatically assigned.<br>• **GEN1—** Link speed can reach up to first generation.<br>• **GEN2—**The default link speed. Link speed can reach up to second generation.<br>• **GEN3—** Link speed can reach up to third generation.<br>• **Disabled—**Slot is disabled, and the card is not enumerated. |
| **SIOC1 Link Speed**<br>**Set PcieSlot1LinkSpeed** | System IO Controller 1 (SIOC1) add-on slot 1 link speed.<br>• **GEN1 —** Link speed can reach up to first generation.<br>• **GEN2 —** Link speed can reach up to second generation.<br>• **GEN3—** The default link speed. Link speed can reach up to third generation.<br>• **Disabled —** Slot is disabled, and the card is not enumerated. |

| Name | Description |
|---|---|
| **SIOC2 Link Speed**<br>**set PcieSlot2LinkSpeed** | System IO Controller 2 (SIOC2) add-on slot 2 link speed.<br>• **GEN1 —** Link speed can reach up to first generation.<br>• **GEN2 —** Link speed can reach up to second generation.<br>• **GEN3—** The default link speed. Link speed can reach up to third generation.<br>• **Disabled —** Slot is disabled, and the card is not enumerated. |
| **SBMezz1 Link Speed**<br>**Set SBMezz1LinkSpeed** | SBMezz1 add-on slot 1 link speed.<br>• **Auto—**Link speed is automatically assigned.<br>• **GEN1—** Link speed can reach up to first generation.<br>• **GEN2—**The default link speed. Link speed can reach up to second generation.<br>• **GEN3—** Link speed can reach up to third generation.<br>• **Disabled—**Slot is disabled, and the card is not enumerated. |
| **IOESlot1 Link Speed**<br>**set IOESlot1LinkSpeed** | Slot 1 link speed. This can be one of the following:<br>• **Auto—** Default value. Slot is enabled.<br>• **GEN 1—** Link speed can reach up to first generation.<br>• **GEN 2—** Link speed can reach up to second generation.<br>• **GEN 3—** Link speed can reach up to third generation.<br>• **Disabled—**Slot is disabled, and the card is not enumerated. |
| **IOEMezz1 Link Speed**<br>**set IOEMezz1LinkSpeed** | Mezz1 link speed. This can be one of the following:<br>• **Auto—** Default value. Slot is enabled.<br>• **GEN 1—** Link speed can reach up to first generation.<br>• **GEN 2—** Link speed can reach up to second generation.<br>• **GEN 3—** Link speed can reach up to third generation.<br>• **Disabled—**Slot is disabled, and the card is not enumerated. |

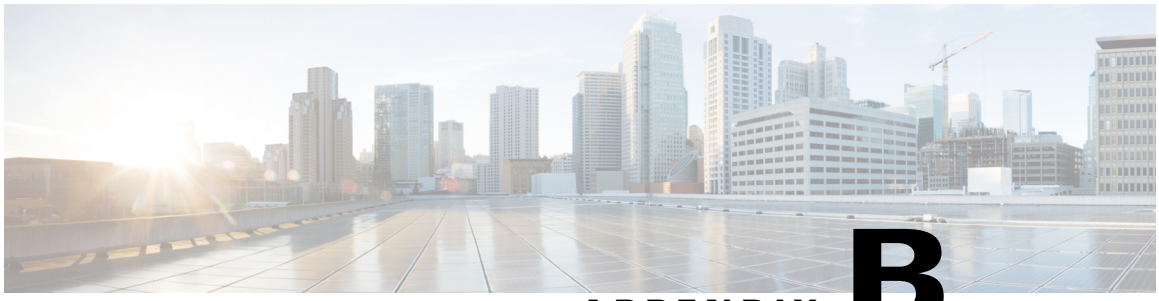
| Name | Description |
|---|---|
| **IOESlot2 Link Speed**<br>**set IOESlot2LinkSpeed** | Slot 2 link speed. This can be one of the following:<br>• **Auto—** Default value. Slot is enabled.<br>• **GEN 1—** Link speed can reach up to first generation.<br>• **GEN 2—** Link speed can reach up to second generation.<br>• **GEN 3—** Link speed can reach up to third generation.<br>• **Disabled—**Slot is disabled, and the card is not enumerated. |
| **IOENVMe1 Link Speed**<br>**set IOENVMe1LinkSpeed** | NVMe1 link speed. This can be one of the following:<br>• **Auto—** Default value. Slot is enabled.<br>• **GEN 1—** Link speed can reach up to first generation.<br>• **GEN 2—** Link speed can reach up to second generation.<br>• **GEN 3—** Link speed can reach up to third generation.<br>• **Disabled—**Slot is disabled, and the card is not enumerated. |
| **IOENVMe2 Link Speed**<br>**set IOENVMe2LinkSpeed** | NVMe2 link speed. This can be one of the following:<br>• **Auto—** Default value. Slot is enabled.<br>• **GEN 1—** Link speed can reach up to first generation.<br>• **GEN 2—** Link speed can reach up to second generation.<br>• **GEN 3—** Link speed can reach up to third generation.<br>• **Disabled—**Slot is disabled, and the card is not enumerated. |

# Server Management BIOS Parameters for C3X60 M4 Servers

### Server Management BIOS Parameters

| Name | Description |
|---|---|
| **FRB-2 Timer**<br>**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:<br>• **Disabled—**The FRB2 timer is not used.<br>• **Enabled—**The FRB2 timer is started during POST and used to recover the system if necessary. |

| Name | Description |
|---|---|
| **OS Watchdog Timer**<br>**set OSBootWatchdogTimer** | Whether the BIOS programs the watchdog timer with a specified timeout value. This can be one of the following:<br>• **Disabled—**The watchdog timer is not used to track how long the server takes to boot.<br>• **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**<br>**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:<br>• **5_Minutes—**The OS watchdog timer expires 5 minutes after it begins to boot.<br>• **10_Minutes—**The OS watchdog timer expires 10 minutes after it begins to boot.<br>• **15_Minutes—**The OS watchdog timer expires 15 minutes after it begins to boot.<br>• **20_Minutes—**The OS watchdog timer expires 20 minutes after it begins to boot.<br>**Note** This option is only applicable if you enable the OS Boot Watchdog Timer. |
| **OS Watchdog Timer Policy**<br>**set OSBootWatchdogTimerPolicy** | What action the system takes if the watchdog timer expires. This can be one of the following:<br>• **Do_Nothing—**The server takes no action if the watchdog timer expires during OS boot.<br>• **Power_Down—**The server is powered off if the watchdog timer expires during OS boot.<br>• **Reset—**The server is reset if the watchdog timer expires during OS boot.<br>**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 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 Name Comparison for Multiple Interfaces

| 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 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 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 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

## D



## E



## F



## G



## H



## I



## K

## L



## M



## N



## O



## P



## R



## S

## T



## U



## V

## X



## Y



## Z