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

First Published: March 04, 2013

Last Modified: December 12, 2013

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

Text Part Number: OL-28994-03

CONTENTS

Preface

This preface includes the following sections:

Audience

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

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

Conventions

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

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

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

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

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

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

Warning IMPORTANT SAFETY INSTRUCTIONS

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

SAVE THESE INSTRUCTIONS

New and Changed Information for this Release

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

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

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

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

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

Feature	Description	Where Documented
Modified CIMC port settings.	Support for setting autonegotiate and duplex modes on CIMC dedicated network ports.	Configuring Network-Related Settings, on page 77
Support for single hypervisor (HV) partition configuration.	The SD storage is available to CIMC as a single hypervisor (HV) partition configuration.	Managing the Server, on page 13

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

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

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

Feature	Description	Where Documented
BIOS tokens	Following new tokens were added: • Out-of-Band Mgmt Port • Onboard SCU Storage SW Stack	BIOS Parameters by Server Model, on page 199

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

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

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

Feature	Description	Where Documented
Fan policy	Support for configuring a fan policy for servers through CIMC	Managing the Server, on page 13
DHCP-enhanced registration	Support for modifying the host name of the server	Managing the Server, on page 13
LDAP	Support extended to include RedHat Directory Server, Novell eDirectory, OpenLDAP,Microsoft Active Directory, and Oracle OpenDS.	Managing User Accounts, on page 67
Cisco usNIC	Support for Cisco usNIC for low-latency Open MPI applications using the Cisco VIC 1225 and 1225T adapters	Managing Network Adapters, on page 87

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

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

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

Feature	Description	Where Documented
Enhanced fault reporting	Enhanced fault reporting capabilities in the CIMC UI.	Viewing Faults and Logs, on page 181
Dual SD Card and Cisco Flexible Flash Card	Support for dual SD card configuration and enhanced configuration options with Cisco Flexible Flash cards.	Managing the Server, on page 13
Nvidia GPU information	Support for viewing Nvidia GPU card information	Viewing Server Properties, on page 41
Storage Adapters	Support added for configuration tasks for storage adapters	Managing Network Adapters, on page 87
NTP Configuration	Support for Network Time Protocol	Configuring Network-Related Settings, on page 77

Feature	Description	Where Documented
vNICs	Support for iSCSI boot capability on a vNIC	Managing Network Adapters, on page 87
Virtual Media	Support for configuring network mounted vmedia volumes	Managing Remote Presence, on page 57
Enhanced SNMP features	Enhanced SNMPv3 and SNMP trap configuration is relocated in the user interface.	Configuring Communication Services, on page 149
XML API	Support added for CIMC control by an XML API.	Configuring Communication Services, on page 149

Related Cisco UCS Documentation

Documentation Roadmaps

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

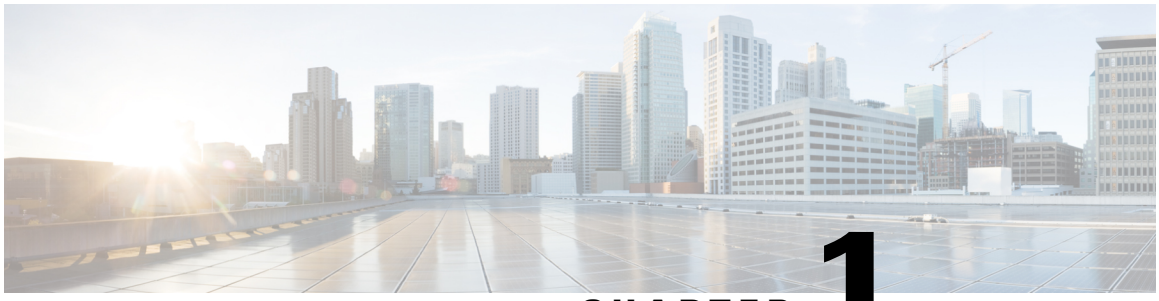
For a complete list of all C-Series documentation, see the *Cisco UCS C-Series Servers Documentation Roadmap* available at the following URL: http://www.cisco.com/go/unifiedcomputing/c-series-doc.

Other Documentation Resources

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

The ISO file is updated after every major documentation release.

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



CHAPTER 1

Overview

This chapter includes the following sections:

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

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

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

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

Overview of the Server Software

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

CIMC Firmware

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

Server OS

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

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

Cisco Integrated Management Controller

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

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

Management Interfaces

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

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

Tasks You Can Perform in CIMC

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

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

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

No Operating System or Application Provisioning or Management

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

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

Overview of the CIMC User Interface

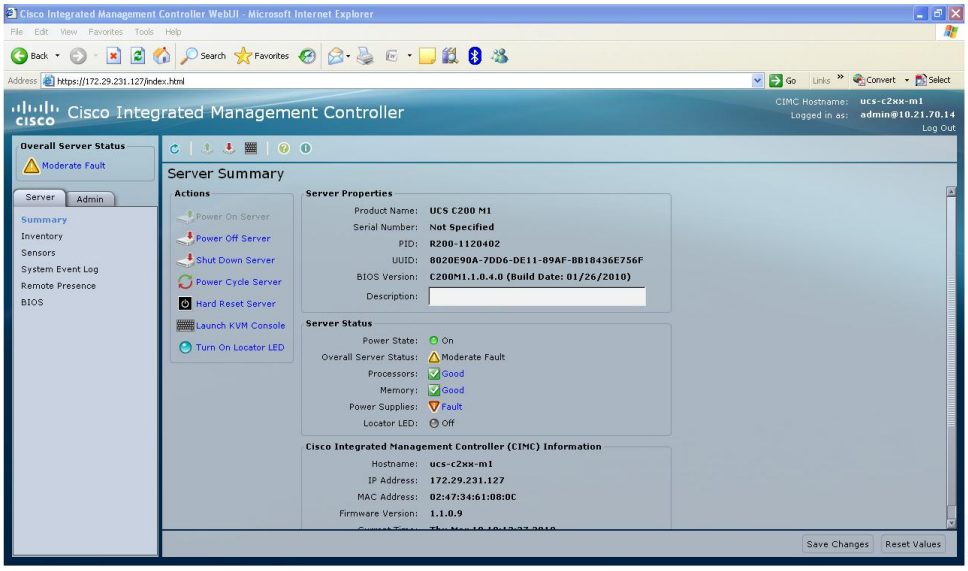
The CIMC user interface is a web-based management interface for Cisco C-Series servers. You can launch the CIMC user interface and manage the server from any remote host that meets the following minimum requirements:

- Java 1.6 or later
- HTTP and HTTPS enabled
- Adobe Flash Player 10 or later

Note In case you lose or forget the password that you use to log in to CIMC, see the password recovery instructions in the Cisco UCS C-Series server installation and service guide for your server. This guide is available from the *Cisco UCS C-Series Servers Documentation Roadmap* at http://www.cisco.com/go/unifiedcomputing/c-series-doc.

CIMC Home Page

When you first log into CIMC GUI, the user interface looks similar to the following illustration:



Navigation and Work Panes

The **Navigation** pane displays on the left side of the CIMC GUI. Clicking links on the **Server**, **Admin**, or **Storage** tabs in the **Navigation** pane displays the associated tabs in the **Work** pane on the right.

The **Navigation** pane has the following areas:

- **Overall Server Status** area
- **Server** tab
- **Admin** tab
- **Storage** tab

Overall Server Status Area

The **Overall Server Status** area is above the **Server** and **Admin** tabs. Click the link in area to refresh the **Server Summary** tab in the **Work** pane.

Note If a different tab is displayed in the **Work** pane, clicking this link redisplays the **Server Summary** tab with updated server information.

Server Tab

Each node in the **Server** tab leads to one or more tabs that display in the **Work** pane. These tabs provides access to the following information:

Server Tab Node Name	Work Pane Tabs Provide Information About...
Summary	Server properties, status, BIOS version, CIMC firmware version, IP address, and MAC address.
Inventory	Installed CPUs, memory cards, power supplies, PCI adapters, Cisco VIC adapters, network adapters, and storage adapters.
Sensors	Power supply, fan, temperature, voltage, current, LEDs, and storage sensor readings.
System Event Log	System event messages.
Remote Presence	KVM, virtual media, and Serial over LAN settings.
BIOS	The installed BIOS firmware version and the server boot order.
Power Policies	Power policy settings.
Fault Summary	Fault sensor readings.

Admin Tab

Each node in the **Admin** tab leads to one or more tabs that display in the **Work** pane. These tabs provides access to the following information:

Admin Tab Node Name	Work Pane Tabs Provide Information About...
User Management	Locally-defined user accounts, Active Directory settings, and current user session information.
Network	NIC, IPv4, VLAN, and LOM properties, along with network security settings.
Communication Services	HTTP, SSH, XML API, IPMI over LAN, and SNMP settings.
Certificate Management	Security certificate information and management.
CIMC Log	CIMC messages.
Event Management	Platform event filters.
Firmware Management	CIMC and BIOS firmware information and management.
Utilities	Technical support data collection, system configuration import and export options, and restore factory defaults settings.

Storage Tab

Each node in the **Storage** tab corresponds to the LSI MegaRAID controllers or Cisco FlexFlash controllers that are installed in theCisco UCS C-Series Rack-Mount Servers. Each node leads to one or more tabs that display in the **Work** pane and provide information about the installed controllers.

Storage Tab Node Name	Work Pane Tabs Provide Information About...
Controller Info	General information about the selected MegaRAID controller or Cisco Flexible Flash controller.
Physical Drive Info	General drive information, identification information, and drive statusl
Virtual Drive Info	General drive information, RAID information, and physical drive information.
Battery Backup Unit	Backup battery information for the selected MegaRAID controller.
Storage Log	Storage messages.

Toolbar

The toolbar displays above the **Work** pane.

Button Name	Description
Refresh	Refreshes the current page.
Power On Server	Powers on the server.
Power Off Server	Powers off the server.
Launch KVM Console	Launches the KVM console.
Help	Displays the online help for the tab displayed in the **Work** pane.
Info	Displays CIMC information.

Cisco Integrated Management Controller Online Help Overview

The GUI for the Cisco Integrated Management Controller (CIMC) software is divided into two main sections, a **Navigation** pane on the left and a **Work** pane on the right.

This help system describes the fields on each CIMC GUI page and in each dialog box.

To access the page help, do one of the following:

- In a particular tab in the CIMC GUI, click the **Help** icon in the toolbar above the **Work** pane.
- In a dialog box, click the **Help** button in that dialog box.

Note 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.

Logging In to CIMC

Before You Begin

If not installed, install Adobe Flash Player 10 or later on your local machine.

Procedure

Step 1 In your web browser, type or select the web link for CIMC.

Step 2 If a security dialog box displays, do the following:

a) (Optional) Check the check box to accept all content from Cisco.

b) Click **Yes** to accept the certificate and continue.

Step 3 In the log in window, enter your username and password.

Tip When logging in for the first time to an unconfigured system, use **admin** as the username and **password** as the password.

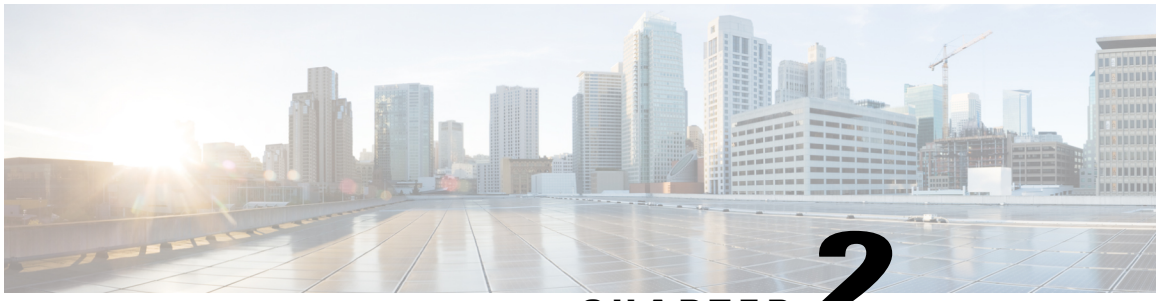
Step 4 Click **Log In**.

Logging Out of CIMC

Procedure

Step 1 In the upper right of CIMC, click **Log Out**.
Logging out returns you to the CIMC log in page.

Step 2 (Optional) Log back in or close your web browser.



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

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

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

- USB flash drive on the network

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

Note When launching the KVM Console from Internet Explorer 6 SP1 on Windows Server 2003, the browser will report that it cannot download a required file. If this occurs, click the browser Tools menu and select Internet Options. Click the Advanced tab and, in the Security section, uncheck the checkbox for "Do not save encrypted pages to disk." Launch the KVM Console again.

Installing an OS Using the KVM Console

Note This procedure describes only the basic installation steps. 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.

Before You Begin

- Locate the OS installation disk or disk image file.
- You must log in as a user with admin privileges to install an OS.

Procedure

Step 1 Load the OS installation disk into your CD/DVD drive, or copy the disk image files to your computer.

Step 2 If CIMC is not open, log in.

Step 3 In the **Navigation** pane, click the **Server** tab.

Step 4 On the **Server** tab, click **Remote Presence**.

Step 5 In the **Remote Presence** pane, click the **Virtual KVM** tab.

Step 6 In the **Actions** area, click **Launch KVM Console**.
The **KVM Console** opens in a separate window.

Step 7 From the KVM console, click the **VM** tab.

Step 8 In the **VM** tab, map the virtual media using either of the following methods:

- Check the **Mapped** check box for the CD/DVD drive containing the OS installation disk.
- Click **Add Image**, navigate to and select the OS installation disk image, click **Open** to mount the disk image, and then check the **Mapped** check box for the mounted disk image.

Note You must keep the **VM** tab open during the OS installation process. Closing the tab unmaps all virtual media.

Step 9 Reboot the server and select the virtual CD/DVD drive as the boot device.

When the server reboots, it begins the installation process from the virtual CD/DVD drive. 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 virtual media boot order to its original setting.

PXE Installation Servers

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

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

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

Installing an OS Using a PXE Installation Server

Before You Begin

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

Procedure

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

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

What to Do Next

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

Booting an Operating System from a USB Port

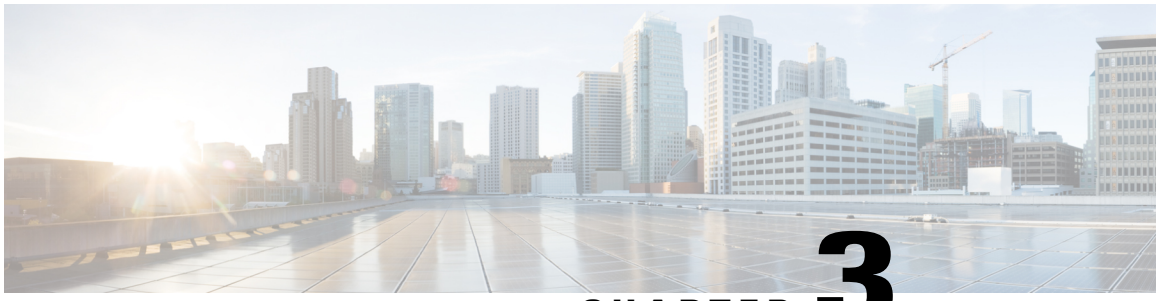
All Cisco UCS C-series servers support booting an operating system from any USB port on the server. However, there are a few guidelines that you must keep in mind, prior to booting an OS from a USB port.

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

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

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

  For information on setting the boot order, see Configuring the Server Boot Order, on page 17 .



CHAPTER 3

Managing the Server

This chapter includes the following sections:

Overview to DHCP User Friendliness

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

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

Viewing Overall Server Status

Procedure

Step 1 In the **Overall Server Status** area of the **Navigation** pane, click the blue health report link to refresh the **Server Summary** pane.

Step 2 (Optional) Review the following information in the **Server Status** area of the **Server Summary** pane:

Note The following list shows all possible status fields. The actual fields displayed depend on the type of C-Series server that you are using.

Name	Description
Power State field	The current power state.
Overall Server Status field	The overall status of the server. This can be one of the following: • **Memory Test In Progress—**The server is performing a self-test of the installed memory. This condition normally occurs during the boot process. • **Good** • **Moderate Fault** • **Severe Fault**
Temperature field	The temperature status. This can be one of the following: • **Good** • **Fault** • **Severe Fault** You can click the link in this field to view more temperature information.
Processors field	The overall status of the processors. This can be one of the following: • **Good** • **Fault** You can click the link in this field to view more information about the processors.

Name	Description
Memory field	The overall status of the memory modules. This can be one of the following: • **Good** • **Fault** • **Severe Fault** You can click the link in this field to view detailed status information.
Power Supplies field	The overall status of the power supplies. This can be one of the following: • **Good** • **Fault** • **Severe Fault** You can click the link in this field to view detailed status information.
Fans field	The overall status of the power supplies. This can be one of the following: • **Good** • **Fault** • **Severe Fault** You can click the link in this field to view detailed status information.
HDD field	The overall status of the hard drives. This can be one of the following: • **Good** • **Fault** You can click the link in this field to view detailed status information.
Locator LED field	Whether the locator LEDs are on or off.
Overall Storage Status field	The overall status of all controllers. This can be one of the following: • **Good** • **Moderate Fault** • **Severe Fault**

Toggling the Locator LED

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Summary**.

Step 3 In the **Actions** area, click **Turn On Locator LED**.
The LED indicator in the **Locator LED** field lights up and the physical locator LED on the server turns on and blinks.

Step 4 In the **Actions** area, click **Turn Off Locator LED**.
The locator LED turns off.

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

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Sensors**.

Step 3 In the **Sensors** pane, click the **Storage** tab.

Step 4 In the **Storage** table, find the hard disk drive (HDD) whose locator LED you want to change.

Step 5 In the **LED Status** column for that HDD, select the desired locator LED state from the drop-down list.
If you select **Turn On**, the LED status indicator in this column lights up and the physical locator LED on the associated HDD turns on and blinks.

Managing the Server Boot Order

Server Boot Order

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

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

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

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

Configuring the Server Boot Order

Before You Begin

You must log in as a user with admin privileges to configure server boot order.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **BIOS**.
The BIOS page appears.

Step 3 In the **Actions** area, click **Configure Boot Order**.
A dialog box with boot order instructions appears.

Step 4 Review the instructions, and then click **OK**.
The **Configure Boot Order** dialog box displays.

Step 5 In the **Configure Boot Order** dialog box, update the following properties:

Name	Description
Device Types table	The server boot options. You can select one or more of the following: • **HDD—**Hard disk drive • **FDD—**Floppy disk drive • **CDROM—**Bootable CD-ROM or DVD • **PXE—**PXE boot • **EFI—**Extensible Firmware Interface **Note** The list of device types is affected by the **Boot Order Rules** BIOS parameter. This parameter is only available on some C-Series servers.
Add >	Moves the selected device type to the **Boot Order** table.
< Remove	Removes the selected device type from the **Boot Order** table.
Boot Order table	Displays the device types from which this server can boot, in the order in which the boot will be attempted.
Up	Moves the selected device type to a higher priority in the **Boot Order** table.
Down	Moves the selected device type to a lower priority in the **Boot Order** table.
Apply button	Saves the changes to the configured boot order or reapplies a previously configured boot order. CIMC sends the configured boot order to the BIOS the next time the server is rebooted.
Cancel button	Closes the dialog box without saving any changes or reapplying the existing configuration. If you select this option, the actual boot order will not be changed the next time the server is rebooted.

Step 6 Click **Apply**.
Additional device types may be appended to the actual boot order, depending on what devices you have connected to your server.

What to Do Next

Reboot the server to boot with your new boot order.

Viewing the Actual Server Boot Order

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

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **BIOS**.
The **BIOS** page appears.

Step 3 In the **Actual Boot Order** area of the **BIOS** page, review the list of boot devices in the order actually used by the BIOS when the server last booted.
If multiple instances of a device type were present during the last boot, you can expand the device type to see those devices.

Resetting the Server

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Summary**.

Step 3 In the **Actions** area, click **Hard Reset Server**.
A dialog box with the message **Hard Reset the Server?** appears.

Step 4 Click **OK**.

Shutting Down the Server

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Summary**.

Step 3 In the **Actions** area, click **Shut Down Server**.
A dialog box with the message **Shut Down the Server?** appears.

Step 4 Click **OK**.

Managing Server Power

Powering On the Server

Note If the server was powered off by any means other than through CIMC, it will not become active immediately when powered on. The server will remain in standby mode until CIMC completes initialization.

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Summary**.

Step 3 In the **Actions** area, click **Power On Server**.
A dialog box with the message **Power on the server?** appears.

Step 4 Click **OK**.

Powering Off the Server

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Summary**.

Step 3 In the **Actions** area, click **Power Off Server**.
A dialog box with the message **Power Off the Server?** appears.

Step 4 Click **OK**.

Power Cycling the Server

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Summary**.

Step 3 In the **Actions** area, click **Power Cycle Server**.
A dialog box with the message **Power Cycle the Server?** appears.

Step 4 Click **OK**.

Configuring Power Policies

Viewing the Power Statistics

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Power Policies**.

Step 3 In the **Power Statistics** area, review the information in the following fields:

Name	Description
Current Consumption field	The power currently being used by the server, in watts.

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

Power Capping Policy

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

Configuring the Power Capping Policy

Note This feature is not available on some servers.

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Power Policies**.

Step 3 In the **Power Configuration** area, update the following properties:

Name	Description
Enable Power Capping check box	If this box is checked, the system monitors how much power is allocated to the server and takes the specified action if the server goes over its maximum allotment.

Name	Description
Peak Power field	The maximum number of watts that can be allocated to this server. If the server requests more power than specified in this field, the system takes the action defined in the **Non-Compliance Action** field. Enter a number of watts within the range defined by the **Minimum Configurable Limit** field and the **Maximum Configurable Limit** field.
Non-Compliance Action drop-down list	The action the system should take if power capping is enabled and the server requests more than its peak power allotment. This can be one of the following: • **Force Power Reduction—**The server is forced to reduce its power consumption by any means necessary. This option is available only on some C-Series servers. • **None—**No action is taken and the server is allowed to use more power than specified in the **Peak Power** field. • **Power Off Host—**The server is shut down. • **Throttle—**Processes running on the server are throttled to bring the total power consumption down.

Step 4 Click **Save Changes**.

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

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Power Policies**.

Step 3 In the **Power Restore Policy** area, update the following fields:

Name	Description
Power Restore Policy drop-down list	The action to be taken when chassis power is restored after an unexpected power loss. This can be one of the following: • **Power Off—**The server remains off until it is manually restarted. • **Power On—**The server is allowed to boot up normally when power is restored. The server can restart immediately or, optionally, after a fixed or random delay. • **Restore Last State—**The server restarts and the system attempts to restore any processes that were running before power was lost.
Power Delay Type drop-down list	If the selected policy is **Power On**, the restart can be delayed with this option. This can be one of the following: • **fixed—**The server restarts after a fixed delay. • **random—**The server restarts after a random delay.
Power Delay Value field	If a fixed delay is selected, once chassis power is restored and the CIMC has finished rebooting, the system waits for the specified number of seconds before restarting the server. Enter an integer between 0 and 240.

Step 4 Click **Save Changes**.

Configuring Fan Policies

Fan Control Policies

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

- Maximum CPU performance

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

- Low power consumption

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

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

Following are the fan policies that you can choose from:

- **Balanced**

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

- **Performance**

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

- **Low Power**

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

- **High Power**

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

- **Maximum Power**

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

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

Configuring the Fan Policy

You can determine the right fan policy based on the server configuration and server components.

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Power Policies**.

Step 3 In the **Fan Policy** area, select a fan policy from the drop-down list. It can be one of the following:

Name	Description
Balanced	This is the default policy. This setting can cool almost any server configuration, but may not be suitable for servers with PCIe cards as these cards overheat easily.
Performance	This setting can be used for server configurations where maximum fan speed is required for high performance. With this setting, the fan speeds run at the same speed or higher speed than that of the fan speed set with the Balanced fan policy.
Low Power	This setting is ideal for minimal configuration servers that do not contain any PCIe cards.
High Power	This setting can be used for server configurations that require fan speeds ranging from 60% to 85%. This policy is ideal for servers that contain PCIe cards that overheat easily and have high temperatures. The minimum fan speed set with this policy varies for each server, but it is approximately in the range of 50 to 85%.
Maximum Power	This setting can be used for server configurations that required extremely high fan speeds ranging from 70% to 100%. This policy is ideal for servers that contain PCIe cards that overheat easily and have very high temperatures. The minimum fan speed set with this policy varies for each server, but it is approximately in the range of 70 to 100%.

Step 4 Click **Save Changes**.

Managing the Flexible Flash Controller

Cisco Flexible Flash

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

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

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

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

Card Management Feature in the Cisco Flexible Flash Controller

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

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

RAID Partition Enumeration

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

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

Scenario	Behavior
Single card	RAID partitions are enumerated if the card is healthy, and if the mode is either **Primary** or **Secondary-active**.

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

Upgrading from Single Card to Dual Card Mirroring with FlexFlash

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

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

  For information on how to complete this task, see

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

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

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

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

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

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

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

Configuring the Flexible Flash Controller Properties

After you upgrade to the latest verison of CIMC or downgrade to a prior version, and reset the configuration, the server will access HV partition only.

Before You Begin

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

Note This task results in the host re-scanning all the virtual drives, and a loss of virtual drive connectivity. We recommend that you configure the Cisco Flexible Flash controller properties before using any virtual drives, or power down the host prior to starting this task

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click **Cisco FlexFlash**.

Step 3 In the **Controller Info** tab, click **Configure Operational Profile**.

Step 4 In the **Operational Profile** dialog box, update the following fields:

Name	Description
Controller field	The system-defined name of the selected Cisco Flexible Flash controller. This name cannot be changed.

Name	Description
Virtual Drives Enabled field	The virtual drives that can be made available to the server as a USB-style drive. A check box against single HV partition is displayed. **Note** In the prior versions, four check boxes against each virtual drive are displayed. If you have created single partition and downgraded to prior version of CIMC, other virtual drives are displayed even though only HV is valid.
RAID Primary Member field	The slot in which the primary RAID member resides.
RAID Secondary Role field	The value must be secondary-active.
I/O Read Error Threshold field	The number of read errors that are permitted while accessing the Cisco Flexible Flash card. If the number of read errors exceeds this threshold on a card, the card is marked unhealthy. To specify a read error threshold, enter an integer between 1 and 255. To specify that the card should never be disabled regardless of the number of errors encountered, enter 0 (zero).
I/O Write Error Threshold field	The number of write errors that are permitted while accessing the Cisco Flexible Flash card. If the number of write errors exceeds this threshold on a card, the card is marked unhealthy. To specify a write error threshold, enter an integer between 1 and 255. To specify that the card should never be disabled regardless of the number of errors encountered, enter 0 (zero).
Clear Errors check box	If checked, the read/write errors are cleared when you click **Save Changes**.

Step 5 Click **Save Changes**.

Booting from the Flexible Flash

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

Note Before you reboot the server, ensure that the virtual drive you select is enabled on the Cisco Flexible Flash card. To verify this, go to the **Storage** tab, select the card, then go to the **Virtual Drive Info** subtab.

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.
Step 2 On the **Server** tab, click **BIOS**.
Step 3 In the **Actions** area, click **Configure Boot Override Priority**.
The **Boot Override Priority** dialog box opens.
Step 4 In the **Boot Override Priority** dialog box, select a virtual drive to boot from.
Step 5 Click **OK**.

Resetting the Flexible Flash Controller

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

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

Before You Begin

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

Procedure

Step 1 On the **Storage Adapters** pane, click **Cisco FlexFlash**.
Step 2 In the **Cisco FlexFlash** pane, click the **Controller Info** tab.
Step 3 In the **Actions** area, click **Reset FlexFlash Controller**.
Step 4 Click **OK** to confirm.

Resetting the Cisco Flexible Flash Card Configuration

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

- The card in the selected slot is marked as primary healthy.

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

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

Before You Begin

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

Procedure

Step 1 On the **Storage Adapters** pane, click **Cisco FlexFlash**.

Step 2 In the **Cisco FlexFlash** pane, click the **Controller Info** tab.

Step 3 In the **Actions** area, click **Reset Partition Defaults**.

Step 4 In the **Reset Partition Defaults** dialog box, update the following fields:

Name	Description
Slot radio button	Select the slot for which you want to mark the card as primary healthy. The card in the other slot, if any, is marked as secondary-active unhealthy.
Reset Partition Defaults button	Resets the configuration of the selected slot.
Cancel button	Closes the dialog box without making any changes.

Step 5 Click **Yes**.

Retaining Configuration of the Cisco Flexible Flash Cards

You can retain the configuration for an FlexFlash that supports firmware version 253 and later card in the following situations:

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

When you retain the configuration, the following situations occur:

- The configuration for the FlexFlash in the selected slot is copied to the other card.
- The card in the selected slot is marked as primary healthy.
- The card in the secondary slot is marked as secondary-active unhealthy.

Before You Begin

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

Procedure

Step 1 On the **Storage Adapters** pane, click **Cisco FlexFlash**.

Step 2 In the **Cisco FlexFlash** pane, click the **Controller Info** tab.

Step 3 In the **Actions** area, click **Synchronize Card Configuration**.

Step 4 In the **Synchronize Card Configuration** dialog box, update the following fields:

Name	Description
Slot radio button	Select the slot for which you want the configuration retained. The configuration is copied from the selected slot to the card in the other slot, and the card in the selected slot is marked as primary healthy.
Synchronize Card Configuration button	Copies the configuration from the selected card only if the selected card is of type SD253 and has single HV configuration.
Cancel button	Closes the dialog box without making any changes.

Step 5 Click **Yes**.

Adding an SD Card and Upgrading the Firmware to 1.5(4) Version

Procedure

Step 1 Insert the empty SD card into SLOT-2 of the server.

Step 2 Upgrade the CIMC software version to release 1.5(4) and reboot CIMC.

Step 3 In the **Navigation** pane, click the **Storage** tab.

Step 4 On the **Storage Adapters** pane, click **Cisco FlexFlash**.

Step 5 In the **Controller Info** tab, determine the state displayed for the **Internal State** field.
The state should be displayed as **WAIT_ON_USER**.

Step 6 Click **Reset FlexFlash Controller**.

Important This option resets the partition enumeration to the host. Before you reset the FlexFlash controller, ensure that the SD card is not used from the host.

When you reset the FlexFlash controller, the card in SLOT-1 is automatically marked as primary healthy, and the empty card in SLOT-2 is marked as secondary active unhealthy card. RAID health is indicated as Degraded. In this situation, all data transactions are written on the healthy card and data mirroring does not occur

Step 7 (Optional) To change the RAID health to healthy, launch Cisco UCS Server Configuration Utility (Cisco UCS SCU) on the host, and click **Hypervisor Sync**.
This option mirrors data from the healthy card to the unhealthy card.

Upgrading an SD Card Firmware to 1.5(4) Version and Adding a New SD Card

Before You Begin

- The size of the empty card that you are adding should match the size of the existing card to successfully create a RAID1 mirror.
- Ensure that the SD card with the valid data in the HyperVisor partition is marked as a primary healthy card. To mark a specific SD card as healthy, you can click **Reset Partition Defaults**. This results in the other card being marked as secondary active unhealthy card.

Procedure

Step 1 Upgrade the CIMC software version to release 1.5(4) and reboot CIMC.

Step 2 In the **Navigation** pane, click the **Storage** tab.

Step 3 On the **Storage Adapters** pane, click **Cisco FlexFlash**.

Step 4 In the **Controller Info** tab, determine the state displayed for the **Internal State** field.
The state should be displayed as **WAIT_ON_USER**.

Step 5 Click **Reset FlexFlash Controller**.

Important This option resets the partition enumeration to the host. Before you reset the FlexFlash controller, ensure that the SD card is not used from the host.

When you reset the FlexFlash controller, the card in SLOT-1 is automatically marked as **primary healthy**, and the empty card in SLOT-2 is marked as **secondary active unhealthy** card. RAID health is indicated as **Degraded**. In this situation, all data transactions are written on the healthy card and data mirroring does not occur

Step 6 On the **Storage Adapters** pane, click **Cisco FlexFlash**.

Step 7 In the **Controller Info** tab, click **Reset Partition Defaults**, and select **SLOT-1** are the primary slot.
The card in SLOT-1 is automatically marked as primary healthy, and the empty card in SLOT-2 is marked as secondary active unhealthy card. RAID health is indicated as Degraded

Step 8 (Optional) To change the RAID health to healthy, launch Cisco UCS Server Configuration Utility (Cisco UCS SCU) on the host, and click **Hypervisor Sync**.
This option mirrors data from the healthy card to the unhealthy card.

Configuring BIOS Settings

Configuring Main BIOS Settings

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **BIOS**.

Step 3 In the **Actions** area, click **Configure BIOS**.

Step 4 In the **Configure BIOS Parameters** dialog box, click the **Main** tab.

Step 5 Specify whether the server should be rebooted after you save your changes.
If you want your changes applied automatically after you click **Save Changes**, check the **Reboot Host Immediately** check box. CIMC immediately reboots the server and applies your changes.

If you want to apply your changes at a later time, clear the **Reboot Host Immediately** check box. CIMC stores the changes and applies them the next time the server reboots.

Note If there are existing BIOS parameter changes pending, CIMC automatically overwrites the stored values with the current settings when you click **Save Changes**.

Step 6 In the **Main** tab, update the BIOS settings fields.
The BIOS parameters available depend on the model of the server that you are using. For descriptions and information about the options for each BIOS setting, see one the following topics:

- Main BIOS Parameters for C22 and C24 Servers , on page 199
- Main BIOS Parameters for C200 and C210 Servers
- Main BIOS Parameters for C250 Servers
- Main BIOS Parameters for C260 Servers , on page 239
- Main BIOS Parameters for C460 Servers , on page 272

Step 7 (Optional) You can reset the parameters or restore the default values using the buttons at the bottom of the **Configure BIOS Parameters** dialog box.
The available options are:

Name	Description
Save Changes button	Saves the settings for the BIOS parameters on all three tabs and closes the dialog box. If the **Reboot Host Immediately** check box is checked, the server is rebooted immediately and the new BIOS settings go into effect. Otherwise the changes are saved until the server is manually rebooted.

Name	Description
Reset Values button	Restores the values for the BIOS parameters on all three tabs to the settings that were in effect when this dialog box was first opened.
Restore Defaults button	Sets the BIOS parameters on all three tabs to their default settings.
Cancel button	Closes the dialog box without making any changes.

Important The buttons in this dialog box affect all BIOS parameters on all available tabs, not just the parameters on the tab that you are viewing.

Step 8 Click **Save Changes**.

Configuring Advanced BIOS Settings

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

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **BIOS**.

Step 3 In the **Actions** area, click **Configure BIOS**.

Step 4 In the **Configure BIOS Parameters** dialog box, click the **Advanced** tab.

Step 5 Specify whether the server should be rebooted after you save your changes.
If you want your changes applied automatically after you click **Save Changes**, check the **Reboot Host Immediately** check box. CIMC immediately reboots the server and applies your changes.

If you want to apply your changes at a later time, clear the **Reboot Host Immediately** check box. CIMC stores the changes and applies them the next time the server reboots.

Note If there are existing BIOS parameter changes pending, CIMC automatically overwrites the stored values with the current settings when you click **Save Changes**.

Step 6 In the **Advanced** tab, update the BIOS settings fields.
The BIOS parameters available depend on the model of the server that you are using. For descriptions and information about the options for each BIOS setting, see one the following topics:

- Advanced BIOS Parameters for C22 and C24 Servers , on page 200
- Advanced BIOS Parameters for C200 and C210 Servers

- Advanced BIOS Parameters for C250 Servers
- Advanced BIOS Parameters for C260 Servers , on page 239
- Advanced BIOS Parameters for C460 Servers , on page 272

Step 7 (Optional) You can reset the parameters or restore the default values using the buttons at the bottom of the **Configure BIOS Parameters** dialog box.
The available options are:

Name	Description
Save Changes button	Saves the settings for the BIOS parameters on all three tabs and closes the dialog box. If the **Reboot Host Immediately** check box is checked, the server is rebooted immediately and the new BIOS settings go into effect. Otherwise the changes are saved until the server is manually rebooted.
Reset Values button	Restores the values for the BIOS parameters on all three tabs to the settings that were in effect when this dialog box was first opened.
Restore Defaults button	Sets the BIOS parameters on all three tabs to their default settings.
Cancel button	Closes the dialog box without making any changes.

Important The buttons in this dialog box affect all BIOS parameters on all available tabs, not just the parameters on the tab that you are viewing.

Step 8 Click **Save Changes**.

Configuring Server Management BIOS Settings

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.
Step 2 On the **Server** tab, click **BIOS**.
Step 3 In the **Actions** area, click **Configure BIOS**.
Step 4 In the **Configure BIOS Parameters** dialog box, click the **Server Management** tab.
Step 5 Specify whether the server should be rebooted after you save your changes.
If you want your changes applied automatically after you click **Save Changes**, check the **Reboot Host Immediately** check box. CIMC immediately reboots the server and applies your changes.

If you want to apply your changes at a later time, clear the **Reboot Host Immediately** check box. CIMC stores the changes and applies them the next time the server reboots.

Note If there are existing BIOS parameter changes pending, CIMC automatically overwrites the stored values with the current settings when you click **Save Changes**.

Step 6 In the **Server Management** tab, update the BIOS settings fields.
The BIOS parameters available depend on the model of the server that you are using. For descriptions and information about the options for each BIOS setting, see one the following topics:

- Server Management BIOS Parameters for C22 and C24 Servers , on page 216
- Server Management BIOS Parameters for C200 and C210 Servers
- Server Management BIOS Parameters for C250 Servers
- Server Management BIOS Parameters for C260 Servers , on page 249
- Server Management BIOS Parameters for C460 Servers , on page 282

Step 7 (Optional) You can reset the parameters or restore the default values using the buttons at the bottom of the **Configure BIOS Parameters** dialog box.
The available options are:

Name	Description
Save Changes button	Saves the settings for the BIOS parameters on all three tabs and closes the dialog box. If the **Reboot Host Immediately** check box is checked, the server is rebooted immediately and the new BIOS settings go into effect. Otherwise the changes are saved until the server is manually rebooted.
Reset Values button	Restores the values for the BIOS parameters on all three tabs to the settings that were in effect when this dialog box was first opened.
Restore Defaults button	Sets the BIOS parameters on all three tabs to their default settings.
Cancel button	Closes the dialog box without making any changes.

Important The buttons in this dialog box affect all BIOS parameters on all available tabs, not just the parameters on the tab that you are viewing.

Step 8 Click **Save Changes**.

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 and parameters to the customized manufacturing default values.

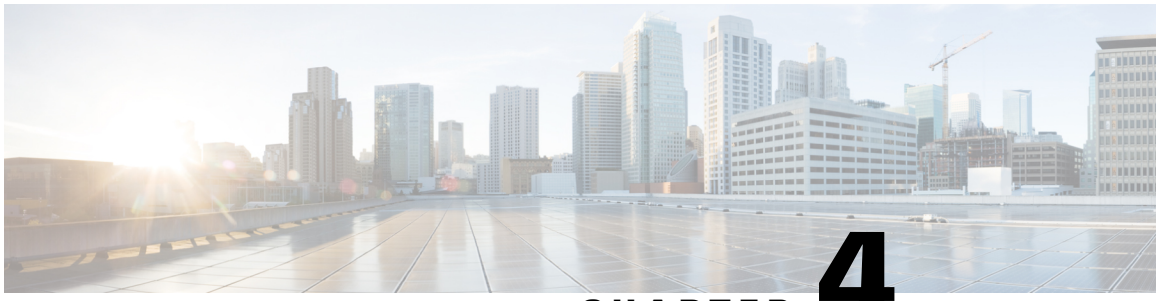
Note This action is only available for some C-Series servers.

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.
Step 2 On the **Server** tab, click **BIOS**.
Step 3 In the **Actions** area, click **Restore Manufacturing Custom Defaults**.
Step 4 Click **OK**.



CHAPTER 4

Viewing Server Properties

This chapter includes the following sections:

Viewing Server Properties

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Summary**.

Step 3 In the **Server Properties** area of the **Server Summary** pane, review the following information:

Name	Description
Product Name field	The model name of the server.
Serial Number field	The serial number for the server.
PID field	The product ID.
UUID field	The UUID assigned to the server.
BIOS Version field	The version of the BIOS running on the server.

Name	Description
Description field	A user-defined description for the server.

Viewing CIMC Information

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Summary**.

Step 3 In the **Cisco Integrated Management Controller (CIMC) Information** area of the **Server Summary** pane, review the following information:

Name	Description
Hostname field	A user-defined hostname for the CIMC. By default, the hostname appears in CXXX-YYYYYY format. Where XXX is the model number and YYYYYY is the serial number of the server.
IP Address field	The IP address for the CIMC.
MAC Address field	The MAC address assigned to the active network interface to the CIMC.
Firmware Version field	The current CIMC firmware version.
Current Time field	The current date and time according to the CIMC clock. **Note** CIMC gets the current date and time from the server BIOS. To change this information, reboot the server and press F2 when prompted to access the BIOS configuration menu. Then change the date or time using the options on the main BIOS configuration tab.

Viewing CPU Properties

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **CPUs** tab.

Step 4 Review the following information for each CPU:

Name	Description
Socket Name field	The socket in which the CPU is installed.
Vendor field	The vendor for the CPU.
Status field	The status of the CPU.
Family field	The family to which this CPU belongs.
Speed field	The CPU speed, in megahertz.
Version field	The CPU version.
Number of Cores field	The number of cores in the CPU.
Signature field	The signature information for the CPU.
Number of Threads field	The maximum number of threads that the CPU can process concurrently.

Viewing Memory Properties

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **Memory** tab.

Step 4 In the **Memory Summary** area, review the following summary information about memory:

Name	Description
Memory Speed field	The memory speed, in megahertz.

Name	Description
Failed Memory field	The amount of memory that is currently failing, in megabytes.
Total Memory field	The total amount of memory available on the server if all DIMMs are fully functional.
Ignored Memory field	The amount of memory currently not available for use, in megabytes.
Effective Memory field	The actual amount of memory currently available to the server.
Number of Ignored DIMMs field	The number of DIMMs that the server cannot access.
Redundant Memory field	The amount of memory used for redundant storage.
Number of Failed DIMMs field	The number of DIMMs that have failed and cannot be used.
Memory RAS Possible field	Details about the RAS memory configuration that the server supports.
Memory Configuration field	The current memory configuration. This can be one of the following: • **Maximum Performance—**The system automatically optimizes the memory performance. • **Mirroring—**The server maintains two identical copies of the data in memory. This option effectively halves the available memory on the server, as one half is automatically reserved for mirrored copy. • **Sparing—**The system reserves some memory for use in the event a DIMM fails. If that happens, the server takes the DIMM offline and replaces it with the reserved memory. This option provides less redundancy than mirroring, but it leaves more of the memory available for programs running on the server. • **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. • **Independent—**All channels are populated with identical memory modules.

Step 5 In the **Memory Details** table, review the following detailed information about each DIMM:

Tip Click a column header to sort the table rows, according to the entries in that column.

Name	Description
Name column	The name of the DIMM slot in which the memory module is installed.
Capacity column	The size of the DIMM.

Name	Description
Channel Speed column	The clock speed of the memory channel, in megahertz.
Channel Type column	The type of memory channel.
Memory Type Detail column	The type of memory used in the device.
Bank Locator column	The location of the DIMM within the memory bank.
Manufacturer column	The vendor ID of the manufacturer. This can be one of the following: • **0x2C00—**Micron Technology, Inc. • **0x5105—**Qimonda AG i. In. • **0x802C—**Micron Technology, Inc. • **0x80AD—**Hynix Semiconductor Inc. • **0x80CE—**Samsung Electronics, Inc. • **0x8551—**Qimonda AG i. In. • **0xAD00—**Hynix Semiconductor Inc. • **0xCE00—**Samsung Electronics, Inc.
Serial Number column	The serial number of the DIMM.
Asset Tag column	The asset tag associated with the DIMM, if any.
Part Number column	The part number for the DIMM assigned by the vendor.
Visibility column	Whether the DIMM is available to the server.
Operability column	Whether the DIMM is currently operating correctly.
Data Width column	The amount of data the DIMM supports, in bits.

Viewing Power Supply Properties

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **Power Supplies** tab.

Step 4 Review the following information for each power supply:

Tip Click a column header to sort the table rows, according to the entries in that column.

Name	Description
Device ID column	The identifier for the power supply unit.
Input column	The input into the power supply, in watts.
Max Output column	The maximum output from the power supply, in watts.
FW Version column	The firmware version for the power supply.
Product ID column	The product identifier for the power supply assigned by the vendor.

Viewing PCI Adapter Properties

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **PCI Adapters** tab.

Step 4 In the **PCI Adapters** area, review the following information for the installed PCI adapters:

Name	Description
Slot ID column	The slot in which the adapter resides.
Product Name column	The name of the adapter.

Name	Description
Vendor ID column	The adapter ID assigned by the vendor.
Sub Vendor ID column	The secondary adapter ID assigned by the vendor.
Device ID column	The device ID assigned by the vendor.
Sub Device ID column	The secondary device ID assigned by the vendor.

Viewing Nvidia GPU Card Information

This information is not available on all Cisco UCS C-series servers.

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **PCI Adapters** tab.

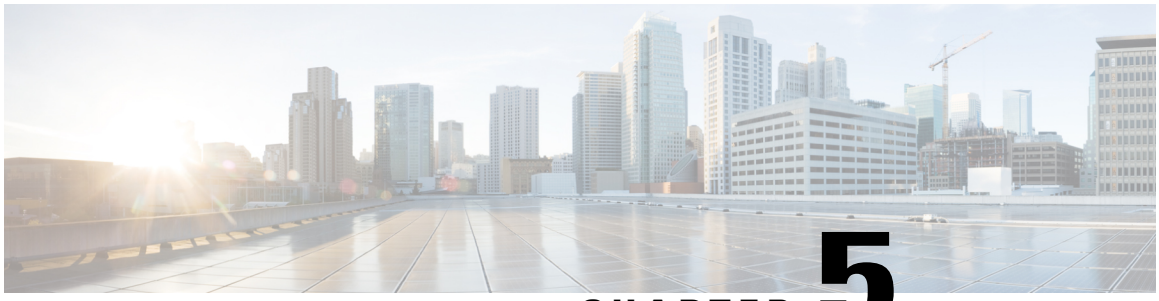
Step 4 In the **PCI Adapters** area, review the following information for the installed PCI adapters:

Name	Description
Slot ID column	The slot in which the adapter resides.
Product Name column	The name of the adapter.
Vendor ID column	The adapter ID assigned by the vendor.
Sub Vendor ID column	The secondary adapter ID assigned by the vendor.
Device ID column	The device ID assigned by the vendor.
Sub Device ID column	The secondary device ID assigned by the vendor.

Step 5 Click the **Slot ID** or the **Product Name** of the Nvidia GPU card.

Step 6 In the **GPU Inventory** dialog box, review the following information for the Nvidia GPU card:

Name	Description
GPU ID	ID of the GPU in the NVidia card.
Temperature	The temperature of the GPU card in Celsius.



CHAPTER 5

Viewing Server Sensors

This chapter includes the following sections:

Viewing Power Supply Sensors

Tip Click a column header to sort the table rows according to the entries in that column.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Sensors**.

Step 3 In the **Sensors** pane, click the **Power Supply** tab.

Step 4 In the **Properties** area, the **Redundancy Status** field displays the status of the power supply redundancy of the server.

Step 5 In the **Discrete Sensors** area, you can view the following statistics for the server:

Name	Description
Sensor Name column	The name of the sensor.

Name	Description
Status column	The status of the sensor. This can be one of the following: • **Unknown** • **Informational** • **Normal** • **Warning** • **Critical** • **Non-Recoverable**
Reading column	The basic state of the sensor.

Step 6 In the **Threshold Sensors** area, you can view the following statistics for the server:

Name	Description
Sensor Name column	The name of the sensor.
Status column	The status of the sensor. This can be one of the following: • **Unknown** • **Informational** • **Normal** • **Warning** • **Critical** • **Non-Recoverable**
Reading column	The current power usage, in watts.
Warning Threshold Min column	The minimum warning threshold.
Warning Threshold Max column	The maximum warning threshold.
Critical Threshold Min column	The minimum critical threshold.
Critical Threshold Max column	The maximum critical threshold.

Viewing Fan Sensors

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Sensors**.

Step 3 In the **Sensors** pane, click the **Fan** tab.

Step 4 View the following fan-related statistics for the server:

Tip Click a column header to sort the table rows according to the entries in that column.

Name	Description
Sensor Name column	The name of the sensor.
Status column	The status of the sensor. This can be one of the following: • **Unknown** • **Informational** • **Normal** • **Warning** • **Critical** • **Non-Recoverable**
Speed column	The fan speed in RPM.
Warning Threshold Min column	The minimum warning threshold.
Warning Threshold Max column	The maximum warning threshold.
Critical Threshold Min column	The minimum critical threshold.
Critical Threshold Max column	The maximum critical threshold.

Viewing Temperature Sensors

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Sensors**.

Step 3 In the **Sensors** pane, click the **Temperature** tab.

Step 4 View the following temperature-related statistics for the server:

Tip Click a column header to sort the table rows according to the entries in that column.

Name	Description
Sensor Name column	The name of the sensor.
Status column	The status of the sensor. This can be one of the following: • **Unknown** • **Informational** • **Normal** • **Warning** • **Critical** • **Non-Recoverable**
Temperature column	The current temperature, in Celsius.
Warning Threshold Min column	The minimum warning threshold.
Warning Threshold Max column	The maximum warning threshold.
Critical Threshold Min column	The minimum critical threshold.
Critical Threshold Max column	The maximum critical threshold.

Viewing Voltage Sensors

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Sensors**.

Step 3 In the **Sensors** pane, click the **Voltage** tab.

Step 4 View the following voltage-related statistics for the server:

Tip Click a column header to sort the table rows according to the entries in that column.

Name	Description
Sensor Name column	The name of the sensor.
Status column	The status of the sensor. This can be one of the following: • **Unknown** • **Informational** • **Normal** • **Warning** • **Critical** • **Non-Recoverable**
Voltage column	The current voltage, in volts.
Warning Threshold Min column	The minimum warning threshold.
Warning Threshold Max column	The maximum warning threshold.
Critical Threshold Min column	The minimum critical threshold.
Critical Threshold Max column	The maximum critical threshold.

Viewing Current Sensors

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Sensors**.

Step 3 In the **Sensors** pane, click the **Current** tab.

Step 4 View the following current-related statistics on the **Current** tab:

Name	Description
Sensor Name column	The name of the sensor.
Status column	The status of the sensor. This can be one of the following: • **Unknown** • **Informational** • **Normal** • **Warning** • **Critical** • **Non-Recoverable**
Current column	The current in amperes.
Warning Threshold Min column	The minimum warning threshold.
Warning Threshold Max column	The maximum warning threshold.
Critical Threshold Min column	The minimum critical threshold.
Critical Threshold Max column	The maximum critical threshold.

Viewing LED Sensors

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Sensors**.

Step 3 In the **Sensors** pane, click the **LEDs** tab.

Step 4 View the following LED-related statistics for the server:

Name	Description
Sensor Name column	The name of the sensor.
LED State column	Whether the LED is on, blinking, or off.
LED Color column	The current color of the LED. For details about what the colors mean, see the hardware installation guide for the type of server you are using.

Viewing Storage Sensors

Procedure

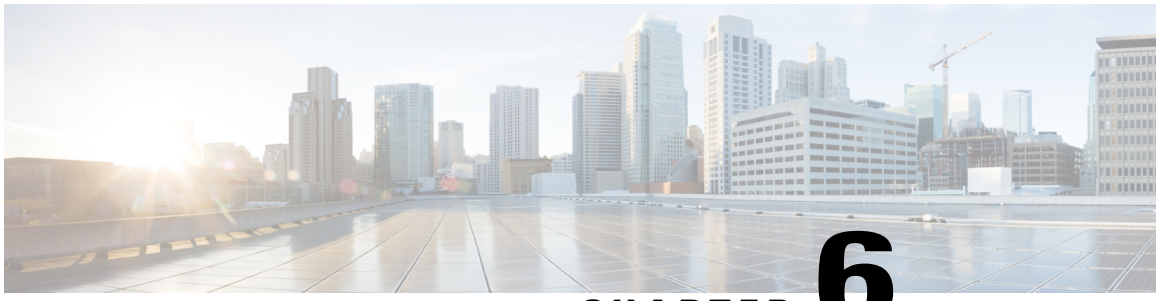
Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Sensors**.

Step 3 In the **Sensors** pane, click the **Storage** tab.

Step 4 View the following storage-related statistics for the server:

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



CHAPTER 6

Managing Remote Presence

This chapter includes the following sections:

Configuring Serial Over LAN

Serial over LAN enables the input and output of the serial port of a managed system to be redirected over IP. Configure and use serial over LAN on your server when you want to reach the host console with CIMC.

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Remote Presence**.

Step 3 In the **Remote Presence** pane, click the **Serial over LAN** tab.

Step 4 In the **Serial over LAN Properties** area, update the following properties:

Name	Description
Enabled check box	If checked, Serial over LAN (SoL) is enabled on this server.

Name	Description
Baud Rate drop-down list	The baud rate the system uses for SoL communication. This can be one of the following: • **9600 bps** • **19.2 kbps** • **38.4 kbps** • **57.6 kbps** • **115.2 kbps**
Com Port drop-down list	The serial port through which the system routes SoL communication. **Note** This field is only available on some C-Series servers. If it is not available, the server always uses COM port 0 for SoL communication. You can select one of the following: • **com0—**SoL communication is routed through COM port 0, an externally accessible serial port that supports either a physical RJ45 connection to an external device or a virtual SoL connection to a network device. If you select this option, the system enables SoL and disables the RJ45 connection, which means that the server can no longer support an external serial device. • **com1—**SoL communication is routed through COM port 1, an internal port accessible only through SoL. If you select this option, you can use SoL on COM port 1 and the physical RJ45 connection on COM port 0. **Note** Changing the Com Port setting disconnects any existing SoL sessions.

Step 5 Click **Save Changes**.

Configuring Virtual Media

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Remote Presence**.

Step 3 In the **Remote Presence** pane, click the **Virtual Media** tab.

Step 4 In the **Virtual Media Properties** area, update the following properties:

Name	Description
Enabled check box	If checked, virtual media is enabled. **Note** If you clear this check box, all virtual media devices are automatically detached from the host.
Active Sessions field	The number of virtual media sessions that are currently running.
Enable Virtual Media Encryption check box	If checked, all virtual media communications are encrypted.
Low Power USB enabled check box	If checked, low power USB is enabled. If the low power USB is enabled, after mapping the ISO and rebooting the host, the virtual drives appear on the boot selection menu. But, while mapping an ISO to a server that has a UCS VIC P81E card and the NIC is in Cisco Card mode, this option must be disabled for the virtual drives to appear on the boot selection menu.

Step 5 Click **Save Changes**.

Creating a CIMC-Mapped vMedia Volume

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Remote Presence**.

Step 3 In the **Remote Presence** pane, click the **Virtual Media** tab.

Step 4 In the **CIMC-Mapped vMedia** area, click **Add New Mapping**.

Step 5 In the **CIMC-Mapped vMedia** dialog box, update the following fields:

Name	Description
Volume field	The identity of the image mounted for mapping.
Mount Type drop-down list	The type of mapping. This can be one of the following: • **NFS—**Network File System. • **CIFS—**Common Internet File System. • **WWW(HTTP/HTTPS)—**HTTP-based or HTTPS-based system.
Remote Share field	The URL of the image to be mapped. The format depends on the selected **Mount Type**: • **NFS—**Use serverip:/share. • **CIFS—**Use //serverip/share. • **WWW(HTTP/HTTPS)—**Use http[s]://serverip/share.
Remote File field	The name and location of the .iso or .img file in the remote share.

Name	Description
Mount Options field	Industry-standard mount options entered in a comma separated list. The options vary depending on the selected **Mount Type**. If you are using **NFS**, leave the field blank or enter one or more of the following: • ro • rw • nolock • noexec • soft • port=VALUE • timeo=VALUE • retry=VALUE If you are using **CIFS**, leave the field blank or enter one or more of the following: • soft • nounix • noserverino • guest • username=VALUE—ignored if guest is entered. • password=VALUE—ignored if guest is entered. If you are using **WWW(HTTP/HTTPS)**, leave the field blank or enter the following: • noauto
User Name field	The username for the specified **Mount Type**, if required.
Password field	The password for the selected username, if required.

Step 6 Click **Save**.

Viewing CIMC-Mapped vMedia Volume Properties

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Remote Presence**.

Step 3 In the **Remote Presence** pane, click the **Virtual Media** tab.

Step 4 In the **CIMC-Mapped vMedia** area, select a row from the **Current Mappings** table.

Step 5 Click **Properties** and review the following information:

Name	Description
Volume field	The identity of the image mounted for mapping.
Mount Type drop-down list	The type of mapping. This can be one of the following: • **NFS—**Network File System. • **CIFS—**Common Internet File System. • **WWW(HTTP/HTTPS)—**HTTP-based or HTTPS- based system.
Remote Share field	The URL of the image to be mapped.
Remote File field	The name and location of the .iso or .img file in the remote share.
Mount Options field	The selected mount options.
User Name field	The username, if any.
Password field	The password for the selected username, if any.

Removing a CIMC-Mapped vMedia Volume

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Remote Presence**.

Step 3 In the **Remote Presence** pane, click the **Virtual Media** tab.

Step 4 In the **CIMC-Mapped vMedia** area, click **Unmap**.

KVM Console

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

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

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

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

Note When launching the KVM Console from Internet Explorer 6 SP1 on Windows Server 2003, the browser will report that it cannot download a required file. If this occurs, click the browser Tools menu and select Internet Options. Click the Advanced tab and, in the Security section, uncheck the checkbox for "Do not save encrypted pages to disk." Launch the KVM Console again.

Configuring the Virtual KVM

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Remote Presence**.

Step 3 In the **Remote Presence** pane, click the **Virtual KVM** tab.

Step 4 On the **Virtual KVM** tab, complete the following fields:

Name	Description
Enabled check box	If checked, the virtual KVM is enabled. **Note** The virtual media viewer is accessed through the KVM. If you disable the KVM console, CIMC also disables access to all virtual media devices attached to the host.
Max Sessions drop-down list	The maximum number of concurrent KVM sessions allowed. You can select any number between 1 and 4.
Active Sessions field	The number of KVM sessions running on the server.
Remote Port field	The port used for KVM communication.
Enable Video Encryption check box	If checked, the server encrypts all video information sent through the KVM.
Enable Local Server Video check box	If checked, the KVM session is also displayed on any monitor attached to the server.

Step 5 Click **Save Changes**.

Enabling the Virtual KVM

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Remote Presence**.

Step 3 In the **Remote Presence** pane, click the **Virtual KVM** tab.

Step 4 On the **Virtual KVM** tab, check the **Enabled** check box.

Step 5 Click **Save Changes**.

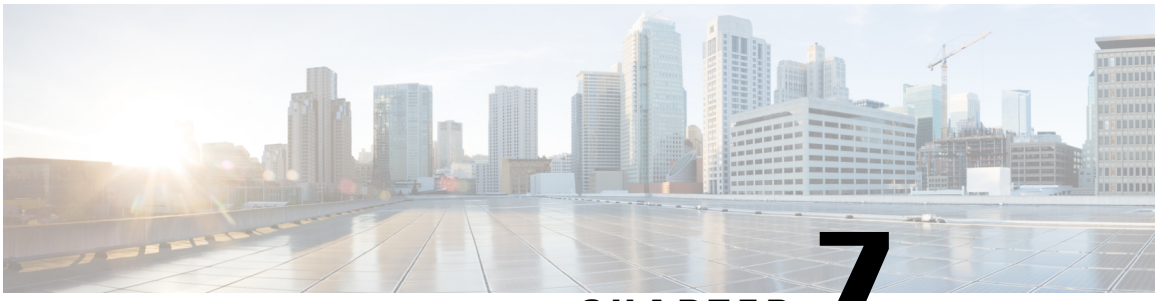
Disabling the Virtual KVM

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.
Step 2 On the **Server** tab, click **Remote Presence**.
Step 3 In the **Remote Presence** pane, click the **Virtual KVM** tab.
Step 4 On the **Virtual KVM** tab, uncheck the **Enabled** check box.
Step 5 Click **Save Changes**.



CHAPTER 7

Managing User Accounts

This chapter includes the following sections:

Configuring Local Users

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **User Management**.

Step 3 In the **User Management** pane, click the **Local User** tab.

Step 4 To configure or modify a local user account, click a row.

Step 5 In the **User Details** dialog box, update the following properties:

Name	Description
ID column	The unique identifier for the user.
Enabled check box	If checked, the user is enabled on the CIMC.
Username column	The username for the user.

Name	Description
Role column	The role assigned to the user. This can be one of the following: • **read-only—**A user with this role can view information but cannot make any changes. • **user—**A user with this role can perform the following tasks: ◦ View all information ◦ Manage the power control options such as power on, power cycle, and power off ◦ Launch the KVM console and virtual media ◦ Clear all logs ◦ Toggle the locator LED • **admin—**A user with this role can perform all actions available through the GUI, CLI, and IPMI.

Step 6 Enter password information.

Step 7 Click **Save Changes**.

LDAP Servers

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

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

By checking the Enable Encryption check box in the **LDAP Settings** area, you can require the server to encrypt data sent to the LDAP server.

Configuring the LDAP Server

The CIMC can be configured to use LDAP for user authentication and authorization. To use LDAP, configure users with an attribute that holds the user role and locale information for the CIMC. You can use an existing LDAP attribute that is mapped to the CIMC user roles and locales or you can modify the LDAP schema to

add a new custom attribute, such as the CiscoAVPair attribute, which has an attribute ID of 1.3.6.1.4.1.9.287247.1.

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

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

The following steps must be performed on the LDAP server.

Procedure

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

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

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

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

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 CIMC:

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

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

What to Do Next

Use the CIMC to configure the LDAP server.

Configuring LDAP Settings and Group Authorization in CIMC

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **User Management**.

Step 3 In the **User Management** pane, click the **LDAP** tab.

Step 4 In the **LDAP Settings** area, update the following properties:

Name	Description
Enable LDAP check box	If checked, user authentication and role authorization is performed first by the LDAP server, followed by user accounts that are not found in the local user database.
Base DN	Base Distinguished Name. This field describes where to load users and groups from. It must be in the dc=domain,dc=com format for Active Directory servers.
Domain	The IPv4 domain that all users must be in. This field is required unless you specify at least one Global Catalog server address.
Enable Encryption	If checked, the server encrypts all information it sends to the LDAP server.
Timeout (0 - 1800) seconds	The number of seconds the CIMC waits until the LDAP search operation times out. If the search operation times out, CIMC tries to connect to the next server listed on this tab, if one is available. **Note** The value you specify for this field could impact the overall time.

Step 5 In the **Configure LDAP Servers** area, update the following properties:

Name	Description
Pre-Configure LDAP Servers radio button	If checked, the Active Directory uses the pre-configured LDAP servers.
LDAP Servers fields	
Server	The IP address of the 6 LDAP servers. If you are using Active Directory for LDAP, then servers 1, 2 and 3 are domain controllers, while servers 4, 5 and 6 are Global Catalogs. If you are not Active Directory for LDAP, then you can configure a maximum of 6 LDAP servers. **Note** You can provide the IP address of the host name as well.
Port	The port numbers for the servers. If you are using Active Directory for LDAP, then for servers 1, 2 and 3, which are domain controllers, the default port number is 389. For servers 4, 5 and 6, which are Global Catalogs, the default port number is 3268. LDAPS communication occurs over the TCP 636 port. LDAPS communication to a global catalog server occurs over TCP 3269 port.
Use DNS to Configure LDAP Servers radio button	If checked, you can use DNS to configure access to the LDAP servers.
DNS Parameters fields	
Source:	Specifies how to obtain the domain name used for the DNS SRV request. It can be one of the following: • **Extracted—**specifies using domain name extracted-domain from the login ID • **Configured—**specifies using the configured-search domain. • **Configured-Extracted—**specifies using the domain name extracted from the login ID than the configured-search domain.

Name	Description
Domain to Search:	A configured domain name that acts as a source for a DNS query. This field is disabled if the source is specified as **Extracted**.
Forest to Search:	A configured forest name that acts as a source for a DNS query. This field is disabled if the source is specified as **Extracted**.

Step 6 In the **Binding Parameters** area, update the following properties:

Name	Description
Method	It can be one of the following: • **Anonymous—**requires NULL username and password. If this option is selected and the LDAP server is configured for Anonymous logins, then the user can gain access. • **Configured Credentials—**requires a known set of credentials to be specified for the initial bind process. If the initial bind process succeeds, then the distinguished name (DN) of the user name is queried and re-used for the re-binding process. If the re-binding process fails, then the user is denied access. • **Login Credentials—**requires the user credentials. If the bind process fails, the user is denied access. By default, the **Login Credentials** option is selected.
Binding DN:	The distinguished name (DN) of the user. This field is editable only if you have selected **Configured Credentials** option as the binding method.
Password:	The password of the user. This field is editable only if you have selected **Configured Credentials** option as the binding method.

Step 7 In the **Search Parameters** area, update the following fields:

Name	Description
Filter Attribute:	This field must match the configured attribute in the schema on the LDAP server. By default, this field displays **sAMAccountName**.
Group Attribute:	This field must match the configured attribute in the schema on the LDAP server. By default, this field displays **memberOf**.
Attribute:	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. The LDAP attribute can use an existing LDAP attribute that is mapped to the CIMC user roles and locales, or can modify the schema such that a new LDAP attribute can be created. For example, **CiscoAvPair**. **Note** If you do not specify this property, the user cannot login. Although the object is located on the LDAP server, it should be an exact match of the attribute that is specified in this field.

Step 8 (Optional) In the **Group Authorization** area, update the following properties:

Name	Description
LDAP Group Authorization check box	If checked, user authentication is also done on the group level for LDAP users that are not found in the local user database. If you check this box, CIMC enables the **Configure Group** button.
Group Name column	The name of the group in the LDAP server database that is authorized to access the server.
Group Domain column	The LDAP server domain the group must reside in.

Name	Description
Role column	The role assigned to all users in this LDAP server group. This can be one of the following: • **read-only—**A user with this role can view information but cannot make any changes. • **user—**A user with this role can perform the following tasks: ◦ View all information ◦ Manage the power control options such as power on, power cycle, and power off ◦ Launch the KVM console and virtual media ◦ Clear all logs ◦ Toggle the locator LED • **admin—**A user with this role can perform all actions available through the GUI, CLI, and IPMI.
Delete column	Deletes an existing LDAP group.

Step 9 Click **Save Changes**.

Viewing User Sessions

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **User Management**.

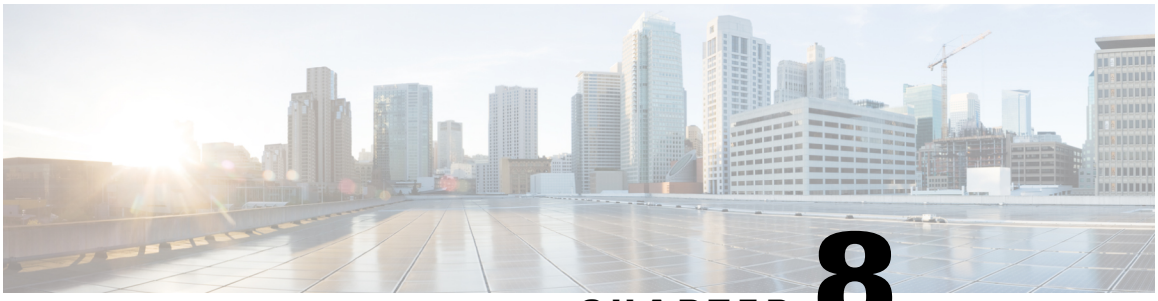
Step 3 In the **User Management** pane, click the **Sessions** tab.

Step 4 View the following information about current user sessions:

Tip Click a column header to sort the table rows, according to the entries in that column.

Name	Description
Session ID column	The unique identifier for the session.
Username column	The username for the user.
IP Address column	The IP address from which the user accessed the server.

Name	Description
Type column	The method by which the user accessed the server.
Action column	If your user account is assigned the **admin** user role, this column displays **Terminate** if you can force the associated user session to end. Otherwise it displays **N/A**. **Note** You cannot terminate your current session from this tab.



CHAPTER 8

Configuring Network-Related Settings

This chapter includes the following sections:

Server NIC Configuration

Server NICs

NIC Mode

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

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

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

NIC Redundancy

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

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

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

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

Configuring Server NICs

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

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.
Step 2 On the **Admin** tab, click **Network**.
Step 3 In the **Network** pane, click the **Network Settings** tab.
Step 4 In the **NIC Properties** area, update the following properties:

Name	Description
NIC Mode drop-down list	Determines the ports that can be used to access the CIMC. This can be one of the following: • **Dedicated—**The management port is used to access the CIMC. • **Shared LOM—**Any LOM (LAN On Motherboard) port can be used to access the CIMC. • **Shared LOM 10G—**Any 10G LOM port can be used to access the CIMC. This option is only available for some adapter cards. • **Cisco Card—**Any port on the adapter card can be used to access the CIMC. The Cisco adapter card has to be installed in a slot with Network Communications Services Interface protocol (NCSI) support. • **Shared LOM Extended—**Any LOM port or adapter card port can be used to access the CIMC. The Cisco adapter card has to be installed in a slot with NCSI support. **Note** If you select any of the shared LOM options, make sure that all host ports belong to the same subnet.
NIC Redundancy drop-down list	The available NIC redundancy options depend on the selected NIC mode and the model of the server that you are using. If you do not see a particular option, then it is not available for the selected mode or server model. This can be one of the following: • **none—**Each port associated with the configured NIC mode operates independently. The ports do not fail over if there is a problem. • **active-active—**If supported, all ports associated with the configured NIC mode operate simultaneously. This increases throughput and provides multiple paths to the CIMC. • **active-standby—**If a port associated with the configured NIC mode fails, traffic will fail over to one of the other ports associated with the NIC mode. **Note** If you select this option, make sure all ports associated with the configured NIC mode are connected to the same subnet to ensure that traffic is secure regardless of which port is used.
MAC Address field	The MAC address of the CIMC network interface selected in the **NIC Mode** field.

Step 5 Click **Save Changes**.

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

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Network**.

Step 3 In the **Network** pane, click the **Network Settings** tab.

Step 4 In the **Hostname** field, enter the name of the host.
By default, the hostname appears in CXXX-YYYYYY format. Where XXX is the model number and YYYYYY is the serial number of the server.

Note If DHCP is enabled, then the DHCP DISCOVER packet sent out will also carry the CIMC hostname in it.

Step 5 Click **Save Changes**.

Configuring IPv4

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Network**.

Step 3 In the **Network** pane, click the **Network Settings** tab.

Step 4 In the **IPv4 Properties** area, update the following properties:

Name	Description
Enable IPv4 check box	If checked, IPv4 is enabled.
Use DHCP check box	If checked, the CIMC uses DHCP.
IP Address field	The IP address for the CIMC.

Name	Description
Subnet Mask field	The subnet mask for the IP address.
Gateway field	The gateway for the IP address.
Obtain DNS Server Addresses from DHCP check box	If checked, the CIMC retrieves the DNS server addresses from DHCP.
Preferred DNS Server field	The IP address of the primary DNS server.
Alternate DNS Server field	The IP address of the secondary DNS server.

Step 5 Click **Save Changes**.

Connecting to a VLAN

Before You Begin

You must be logged in as admin to connect to a VLAN.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Network**.

Step 3 In the **Network** pane, click the **Network Settings** tab.

Step 4 In the **VLAN Properties** area, update the following properties:

Name	Description
Enable VLAN check box	If checked, the CIMC is connected to a virtual LAN. **Note** You can configure a VLAN or a port profile, but you cannot use both. If you want to use a port profile, make sure this check box is not checked.
VLAN ID field	The VLAN ID.
Priority field	The priority of this system on the VLAN.

Step 5 Click **Save Changes**.

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 **Enable VLAN** check box in the **VLAN Properties** area is not checked.

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Network**.

Step 3 In the **Network** pane, click the **Network Settings** tab.

Step 4 In the **Port Profile** area, update the following properties:

Name	Description
Port Profile field	The port profile CIMC should use to configure the management interface, the virtual Ethernet, and the VIF on supported adapter cards such as the Cisco UCS VIC1225 Virtual Interface Card. Enter up to 80 alphanumeric characters. You cannot use spaces or other special characters except for - (hyphen) and _ (underscore). In addition, the port profile name cannot begin with a hyphen. **Note** The port profile must be defined on the switch to which this server is connected.

Step 5 Click **Save Changes**.

Configuring Interface Properties

Overview to Network Interface Configuration

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

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

Configuring Interface Properties

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

Procedure

Step 1 Log in to CIMC Web UI.

Step 2 In the **Navigation** pane, click the **Admin** tab.

Step 3 On the **Admin** tab, click **Network**.

Step 4 In the **Network** pane, click the **Network Settings** tab.

Step 5 In the **NIC Properties** area, select **Dedicated** mode from the **NIC Mode** drop down list.
NIC mode must be in dedicated to set any network configuration like net speed and duplex.

Step 6 In the **Port Properties** area:

- If you check the **Auto Negotiate** check box, the setting for duplex will be ignored by the system. The CIMC retains the speed at which the switch is configured.
- If you uncheck the **Auto Negotiate** check box, you can set duplex. Else, a default speed of 100 Mbps will be applied, and duplex will retain its previous value.

By default, the duplex mode is set to **Full**.

Step 7 Click **Save Changes**.

Network Security Configuration

Network Security

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

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

Configuring Network Security

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

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Network**.

Step 3 In the **Network** pane, click the **Network Security** tab.

Step 4 In the **IP Blocking Properties** area, update the following properties:

Name	Description
Enable IP Blocking check box	Check this box to enable IP blocking.
IP Blocking Fail Count field	The number of times a user can attempt to log in unsuccessfully before the system locks that user out for a specified length of time. The number of unsuccessful login attempts must occur within the time frame specified in the **IP Blocking Fail Window** field. Enter an integer between 3 and 10.
IP Blocking Fail Window field	The length of time, in seconds, in which the unsuccessful login attempts must occur in order for the user to be locked out. Enter an integer between 60 and 120.
IP Blocking Penalty Time field	The number of seconds the user remains locked out if they exceed the maximum number of login attempts within the specified time window. Enter an integer between 300 and 900.

Step 5 Click **Save Changes**.

Network Time Protocol Settings

Network Time Protocol Service Setting

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

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

Configuring Network Time Protocol Settings

Configuring NTP disables the IPMI **Set SEL time** command.

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

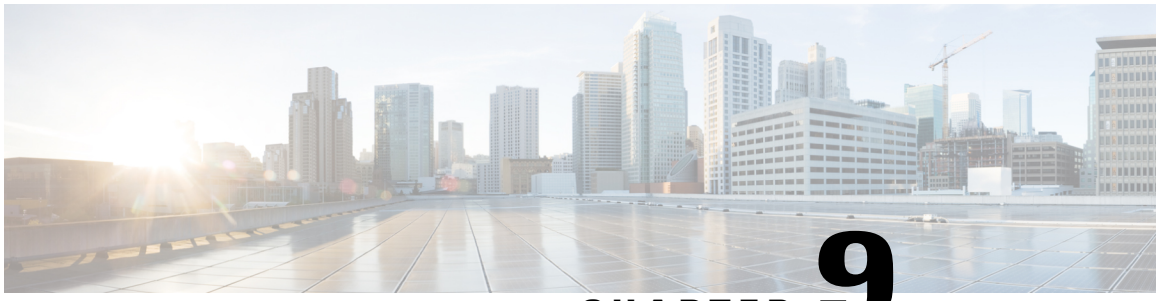
Step 2 On the **Admin** tab, click **Network**.

Step 3 In the **Network** pane, click the **NTP Settings** tab.

Step 4 In the **NTP Settings** area, update the following properties:

Name	Description
Enable NTP	Check this box to enable the NTP service.
Server 1	The IP/DNS address of one of the four servers that act as an NTP server or the time source server.
Server 2	The IP/DNS address of one of the four servers that act as an NTP server or the time source server.
Server 3	The IP/DNS address of one of the four servers that act as an NTP server or the time source server.
Server 4	The IP/DNS address of one of the four servers that act as an NTP server or the time source server.

Step 5 Click **Save Changes**.



CHAPTER 9

Managing Network Adapters

This chapter includes the following sections:

Overview of the Cisco UCS C-Series Network Adapters

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

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

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

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

Cisco UCS P81E Virtual Interface Card

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

- Allows up to 16 virtual Fibre Channel and 16 virtual Ethernet adapters to be provisioned in virtualized or nonvirtualized environments using just-in-time provisioning, providing tremendous system flexibility and allowing consolidation of multiple physical adapters.
- Delivers uncompromising virtualization support, including hardware-based implementation of Cisco VN-Link technology and pass-through switching.
- Improves system security and manageability by providing visibility and portability of network 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 VIC1225 Virtual Interface Card

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

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

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

Viewing Network Adapter Properties

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **Network Adapters** tab.

Step 4 In the **Network Adapters** area, review the following information:

Name	Description
Slot ID column	The slot in which the adapter is installed.
Product Name column	The product name for the adapter.
Number of Interfaces column	The number of interfaces for the adapter.

Step 5 In the **Adapter Card** area, review the following information:

Name	Description
ID column	The ID for the external ethernet interface.
MAC Address column	The MAC address for the external ethernet interface.

Viewing VIC Adapter 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

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **Cisco VIC Adapters** tab.

Step 4 In the **Adapter Cards** area, click an adapter in the table to display its properties.
The resources of the selected adapter appear in the tabbed menu below the **Adapter Cards** area.

Step 5 In the **Adapter Cards** area, review the following information for the installed adapters:

Name	Description
PCI Slot column	The PCI slot in which the adapter is installed.
Product Name column	The product name for the adapter.
Serial Number column	The serial number for the adapter.
Product ID column	The product ID for the adapter.
Vendor column	The vendor for the adapter.
CIMC Management Enabled column	Whether the adapter is able to manage CIMC. This functionality depends on the type of adapter installed and how it is configured. For details, see the hardware installation guide for the type of server you are using.

Step 6 In the tabbed menu below the **Adapter Cards** area, click the **General** tab.

Step 7 In the **Adapter Card Properties** area, review the following information for the adapter:

Name	Description
PCI Slot field	The PCI slot in which the adapter is installed.
Vendor field	The vendor for the adapter.
Product Name field	The product name for the adapter.
Product ID field	The product ID for the adapter.
Serial Number field	The serial number for the adapter.
Version ID field	The version ID for the adapter.
Hardware Revision field	The hardware revision for the adapter.
CIMC Management Enabled field	If this field displays **yes**, then the adapter is functioning in Cisco Card Mode and passing CIMC management traffic through to the server CIMC.

Name	Description
Configuration Pending field	If this field displays **yes**, the adapter configuration has changed in CIMC but these changes have not been communicated to the host operating system. To activate the changes, an administrator must reboot the adapter.
Description field	The user-defined description for the adapter, if any.
FIP Mode field	Whether FCoE Initialization Protocol (FIP) mode is enabled. FIP mode ensures that the adapter is compatible with current FCoE standards.
VNTAG Mode field	Whether virtual network tag (VNTAG) is enabled. If VNTAG mode is enabled: • vNICs and vHBAs can be assigned to a specific channel • vNICs and vHBAs can be associated with a port profile • vNICs can fail over to another vNIC if there are communication problems
ISCSI Boot Capable field	Whether iSCSI boot is supported on the adapter.
usNIC Capable field	Whether the adapter and the firmware running on the adapter support the usNIC.

Step 8 In the **External Ethernet Interfaces** area, review the following information for the adapter:

Name	Description
ID column	The uplink port ID.
MAC Address column	The MAC address of the uplink port.
Link State column	The current operational state of the uplink port. This can be one of the following: • **Fault** • **Link Up** • **Link Down** • **SFP ID Error** • **SFP Not Installed** • **SFP Security Check Failed** • **Unsupported SFP**

Name	Description
Encap column	The mode in which adapter operates. This can be one of the following: • **CE—**Classical Ethernet mode. • **NIV—**Network Interface Virtualization mode.
Admin Speed column	The data transfer rate for the port. This can be one of the following: • **Auto** • **1 Gpbs** • **10 Gpbs** **Note** This option is only available for some adapter cards.
Operating Speed column	The operating rate for the port. This can be one of the following: • **Auto** • **1 Gpbs** • **10 Gpbs** **Note** This option is only available for some adapter cards.

Step 9 In the **Firmware** area, review the following information for the adapter:

Name	Description
Running Version field	The firmware version that is currently active.
Backup Version field	The alternate firmware version installed on the adapter, if any. The backup version is not currently running. To activate it, administrators can click **Activate Firmware** in the **Actions** area. **Note** When you install new firmware on the adapter, any existing backup version is deleted and the new firmware becomes the backup version. You must manually activate the new firmware if you want the adapter to run the new version.
Startup Version field	The firmware version that will become active the next time the adapter is rebooted.
Bootloader Version field	The bootloader version associated with the adapter card.
Status field	The status of the last firmware activation that was performed on this adapter. **Note** The status is reset each time the adapter is rebooted.

What to Do Next

To view the properties of virtual NICs, VM FEXs, and virtual HBAs, see the following sections:

- Viewing vNIC Properties, on page 108
- Viewing Virtual FEX Properties, on page 128
- Viewing vHBA Properties, on page 94

Viewing Storage Adapter Properties

Before You Begin

- The server must be powered on.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click **Storage Adapters** tab and review the following information:

Name	Description
Controller field	The type of controller.
PCI Slot field	The PCI slot in which the adapter is installed.
Product Name field	The product name for the adapter.
Serial Number field	The serial number for the adapter.
Firmware Package Build field	The installed firmware package for the adapter.
Product ID field	The product ID for the adapter.
Battery Status field	The vendor for the adapter.
Cache Memory Size field	The size of the cache memory, in megabytes.

Name	Description
Health field	The health of the adapter. This can be one of the following: • **Good** • **Moderate Fault** • **Severe Fault** • **N/A**
Details link	Click the **Details** link to view the **Storage** tab.

Managing vHBAs

Guidelines for Managing vHBAs

When managing vHBAs, consider the following guidelines and restrictions:

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

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

- When using the Cisco UCS P81E Virtual Interface Card or Cisco UCS VIC1225 Virtual Interface Card in an FCoE application, you must associate the vHBA with the FCoE VLAN. Follow the instructions in Modifying vHBA Properties, on page 99 to assign the VLAN.
- After making configuration changes, you must reboot the host for settings to take effect.

Viewing vHBA Properties

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.
Step 2 On the **Server** tab, click **Inventory**.
Step 3 In the **Inventory** pane, click the **Cisco VIC Adapters** tab.
Step 4 In the **Adapter Cards** area, select the adapter card.

If the server is powered on, the resources of the selected adapter card appear in the tabbed menu below the **Adapter Cards** area.

Step 5 In the tabbed menu below the **Adapter Cards** area, click the **vHBAs** tab.

Step 6 In the **Host Fibre Channel Interfaces** area, select a vHBA from the table.

Step 7 Click **Properties** to open the **vHBA Properties** dialog box.

Step 8 In the **General** area, review the information in the following fields:

Name	Description
Name field	The name of the virtual HBA. This name cannot be changed after the vHBA has been created.
World Wide Node Name field	The WWNN associated with the vHBA. To let the system generate the WWNN, select **AUTO**. To specify a WWNN, click the second radio button and enter the WWNN in the corresponding field.
World Wide Port Name field	The WWPN associated with the vHBA. To let the system generate the WWPN, select **AUTO**. To specify a WWPN, click the second radio button and enter the WWPN in the corresponding field.
FC SAN Boot check box	If checked, the vHBA can be used to perform a SAN boot.
Enable Persistent LUN Binding check box	If checked, any LUN ID associations are retained in memory until they are manually cleared.
Uplink Port field	The uplink port associated with the vHBA. **Note** This value cannot be changed for the system-defined vHBAs fc0 and fc1.
MAC Address field	The MAC address associated with the vHBA. To let the system generate the MAC address, select **AUTO**. To specify an address, click the second radio button and enter the MAC address in the corresponding field.
Default VLAN field	If there is no default VLAN for this vHBA, click **NONE**. Otherwise, click the second radio button and enter a VLAN ID between 1 and 4094 in the field.
Class of Service drop-down list	The CoS for the vHBA. Select an integer between 0 and 6, with 0 being lowest priority and 6 being the highest priority. **Note** This option cannot be used in VNTAG mode.

Name	Description
Rate Limit field	The data rate limit for traffic on this vHBA, in Mbps. If you want this vHBA to have an unlimited data rate, select **OFF**. Otherwise, click the second radio button and enter an integer between 1 and 10,000. **Note** This option cannot be used in VNTAG mode.
PCIe Device Order field	The order in which this vHBA will be used. To let the system set the order, select **ANY**. To specify an order, select the second radio button and enter an integer between 0 and 17.
EDTOV field	The error detect timeout value (EDTOV), which is the number of milliseconds to wait before the system assumes that an error has occurred. Enter an integer between 1,000 and 100,000. The default is 2,000 milliseconds.
RATOV field	The resource allocation timeout value (RATOV), which is the number of milliseconds to wait before the system assumes that a resource cannot be properly allocated. Enter an integer between 5,000 and 100,000. The default is 10,000 milliseconds.
Max Data Field Size field	The maximum size of the Fibre Channel frame payload bytes that the vHBA supports. Enter an integer between 256 and 2112.
Channel Number field	The channel number that will be assigned to this vHBA. Enter an integer between 1 and 1,000. **Note** VNTAG mode is required for this option.
Port Profile drop-down list	The port profile that should be associated with the vHBA, if any. This field displays the port profiles defined on the switch to which this server is connected. **Note** VNTAG mode is required for this option.

Step 9 In the **Error Recovery** area, review the information in the following fields:

Name	Description
Enable FCP Error Recovery check box	If checked, the system uses FCP Sequence Level Error Recovery protocol (FC-TAPE).

Name	Description
Link Down Timeout field	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. Enter an integer between 0 and 240,000.
Port Down I/O Retries field	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. Enter an integer between 0 and 255.
Port Down Timeout field	The number of milliseconds a remote Fibre Channel port should be offline before informing the SCSI upper layer that the port is unavailable. Enter an integer between 0 and 240,000.

Step 10 In the **Fibre Channel Interrupt** area, review the information in the following fields:

Name	Description
Interrupt Mode drop-down list	The preferred driver interrupt mode. This can be one of the following: • **MSIx—**Message Signaled Interrupts (MSI) with the optional extension. This is the recommended option. • **MSI—**MSI only. • **INTx—**PCI INTx interrupts.

Step 11 In the **Fibre Channel Port** area, review the information in the following fields:

Name	Description
I/O Throttle Count field	The number of I/O operations that can be pending in the vHBA at one time. Enter an integer between 1 and 1,024.
LUNs per Target field	The maximum number of LUNs that the driver will export. This is usually an operating system platform limitation. Enter an integer between 1 and 1,024. The recommended value is 1024.

Step 12 In the **Fibre Channel Port FLOGI** area, review the information in the following fields:

Name	Description
FLOGI Retries field	The number of times that the system tries to log in to the fabric after the first failure. To specify an unlimited number of retries, select the **INFINITE** radio button. Otherwise select the second radio button and enter an integer into the corresponding field.
FLOGI Timeout field	The number of milliseconds that the system waits before it tries to log in again. Enter an integer between 1,000 and 255,000.

Step 13 In the **Fibre Channel Port PLOGI** area, review the information in the following fields:

Name	Description
PLOGI Retries field	The number of times that the system tries to log in to a port after the first failure. Enter an integer between 0 and 255.
PLOGI Timeout field	The number of milliseconds that the system waits before it tries to log in again. Enter an integer between 1,000 and 255,000.

Step 14 In the **SCSI I/O** area, review the information in the following fields:

Name	Description
CDB Transmit Queue Count field	The number of SCSI I/O queue resources the system should allocate. Enter an integer between 1 and 8.
CDB Work Queue Ring Size field	The number of descriptors in each SCSI I/O queue. Enter an integer between 64 and 512.

Step 15 In the **Receive/Transmit Queues** area, review the information in the following fields:

Name	Description
FC Work Queue Ring Size field	The number of descriptors in each transmit queue. Enter an integer between 64 and 128.
FC Receive Queue Ring Size field	The number of descriptors in each receive queue. Enter an integer between 64 and 128.

Modifying vHBA Properties

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **Cisco VIC Adapters** tab.

Step 4 In the **Adapter Cards** area, select the adapter card.
If the server is powered on, the resources of the selected adapter card appear in the tabbed menu below the **Adapter Cards** area.

Step 5 In the tabbed menu below the **Adapter Cards** area, click the **vHBAs** tab.

Step 6 In the **Host Fibre Channel Interfaces** area, select a vHBA from the table.

Step 7 Click **Properties** to open the **vHBA Properties** dialog box.

Step 8 In the **General** area, update the following fields:

Name	Description
Name field	The name of the virtual HBA. This name cannot be changed after the vHBA has been created.
World Wide Node Name field	The WWNN associated with the vHBA. To let the system generate the WWNN, select **AUTO**. To specify a WWNN, click the second radio button and enter the WWNN in the corresponding field.
World Wide Port Name field	The WWPN associated with the vHBA. To let the system generate the WWPN, select **AUTO**. To specify a WWPN, click the second radio button and enter the WWPN in the corresponding field.
FC SAN Boot check box	If checked, the vHBA can be used to perform a SAN boot.
Enable Persistent LUN Binding check box	If checked, any LUN ID associations are retained in memory until they are manually cleared.
Uplink Port field	The uplink port associated with the vHBA. **Note** This value cannot be changed for the system-defined vHBAs fc0 and fc1.
MAC Address field	The MAC address associated with the vHBA. To let the system generate the MAC address, select **AUTO**. To specify an address, click the second radio button and enter the MAC address in the corresponding field.

Name	Description
Default VLAN field	If there is no default VLAN for this vHBA, click **NONE**. Otherwise, click the second radio button and enter a VLAN ID between 1 and 4094 in the field.
Class of Service drop-down list	The CoS for the vHBA. Select an integer between 0 and 6, with 0 being lowest priority and 6 being the highest priority. **Note** This option cannot be used in VNTAG mode.
Rate Limit field	The data rate limit for traffic on this vHBA, in Mbps. If you want this vHBA to have an unlimited data rate, select **OFF**. Otherwise, click the second radio button and enter an integer between 1 and 10,000. **Note** This option cannot be used in VNTAG mode.
PCIe Device Order field	The order in which this vHBA will be used. To let the system set the order, select **ANY**. To specify an order, select the second radio button and enter an integer between 0 and 17.
EDTOV field	The error detect timeout value (EDTOV), which is the number of milliseconds to wait before the system assumes that an error has occurred. Enter an integer between 1,000 and 100,000. The default is 2,000 milliseconds.
RATOV field	The resource allocation timeout value (RATOV), which is the number of milliseconds to wait before the system assumes that a resource cannot be properly allocated. Enter an integer between 5,000 and 100,000. The default is 10,000 milliseconds.
Max Data Field Size field	The maximum size of the Fibre Channel frame payload bytes that the vHBA supports. Enter an integer between 256 and 2112.
Channel Number field	The channel number that will be assigned to this vHBA. Enter an integer between 1 and 1,000. **Note** VNTAG mode is required for this option.

Name	Description
Port Profile drop-down list	The port profile that should be associated with the vHBA, if any. This field displays the port profiles defined on the switch to which this server is connected. **Note** VNTAG mode is required for this option.

Step 9 In the **Error Recovery** area, update the following fields:

Name	Description
Enable FCP Error Recovery check box	If checked, the system uses FCP Sequence Level Error Recovery protocol (FC-TAPE).
Link Down Timeout field	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. Enter an integer between 0 and 240,000.
Port Down I/O Retries field	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. Enter an integer between 0 and 255.
Port Down Timeout field	The number of milliseconds a remote Fibre Channel port should be offline before informing the SCSI upper layer that the port is unavailable. Enter an integer between 0 and 240,000.

Step 10 In the **Fibre Channel Interrupt** area, update the following fields:

Name	Description
Interrupt Mode drop-down list	The preferred driver interrupt mode. This can be one of the following: • **MSIx—**Message Signaled Interrupts (MSI) with the optional extension. This is the recommended option. • **MSI—**MSI only. • **INTx—**PCI INTx interrupts.

Step 11 In the **Fibre Channel Port** area, update the following fields:

Name	Description
I/O Throttle Count field	The number of I/O operations that can be pending in the vHBA at one time. Enter an integer between 1 and 1,024.
LUNs per Target field	The maximum number of LUNs that the driver will export. This is usually an operating system platform limitation. Enter an integer between 1 and 1,024. The recommended value is 1024.

Step 12 In the **Fibre Channel Port FLOGI** area, update the following fields:

Name	Description
FLOGI Retries field	The number of times that the system tries to log in to the fabric after the first failure. To specify an unlimited number of retries, select the **INFINITE** radio button. Otherwise select the second radio button and enter an integer into the corresponding field.
FLOGI Timeout field	The number of milliseconds that the system waits before it tries to log in again. Enter an integer between 1,000 and 255,000.

Step 13 In the **Fibre Channel Port PLOGI** area, update the following fields:

Name	Description
PLOGI Retries field	The number of times that the system tries to log in to a port after the first failure. Enter an integer between 0 and 255.
PLOGI Timeout field	The number of milliseconds that the system waits before it tries to log in again. Enter an integer between 1,000 and 255,000.

Step 14 In the **SCSI I/O** area, update the following fields:

Name	Description
CDB Transmit Queue Count field	The number of SCSI I/O queue resources the system should allocate. Enter an integer between 1 and 8.
CDB Work Queue Ring Size field	The number of descriptors in each SCSI I/O queue. Enter an integer between 64 and 512.

Step 15 In the **Receive/Transmit Queues** area, update the following fields:

Name	Description
FC Work Queue Ring Size field	The number of descriptors in each transmit queue. Enter an integer between 64 and 128.
FC Receive Queue Ring Size field	The number of descriptors in each receive queue. Enter an integer between 64 and 128.

Step 16 Click **Save Changes**.

Creating a vHBA

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

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **Cisco VIC Adapters** tab.

Step 4 In the **Adapter Cards** area, select the adapter card.
If the server is powered on, the resources of the selected adapter card appear in the tabbed menu below the **Adapter Cards** area.

Step 5 In the tabbed menu below the **Adapter Cards** area, click the **vHBAs** tab.

Step 6 In the **Host Fibre Channel Interfaces** area, choose one of these actions:

- To create a vHBA using default configuration settings, click **Add**.
- To create a vHBA using the same configuration settings as an existing vHBA, select that vHBA and click **Clone**.

The **Add vHBA** dialog box appears.

Step 7 In the **Add vHBA** dialog box, enter a name for the vHBA in the **Name** entry box.

Step 8 Click **Add vHBA**.

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 99.

Deleting a vHBA

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **Cisco VIC Adapters** tab.

Step 4 In the **Adapter Cards** area, select the adapter card.
If the server is powered on, the resources of the selected adapter card appear in the tabbed menu below the **Adapter Cards** area.

Step 5 In the tabbed menu below the **Adapter Cards** area, click the **vHBAs** tab.

Step 6 In the **Host Fibre Channel Interfaces** area, select a vHBA from the table.

Note You cannot delete either of the two default vHBAs, **fc0** or **fc1**.

Step 7 Click **Delete** and click **OK** to confirm.

vHBA Boot Table

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

Creating a Boot Table Entry

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **Cisco VIC Adapters** tab.

Step 4 In the **Adapter Cards** area, select the adapter card.
If the server is powered on, the resources of the selected adapter card appear in the tabbed menu below the **Adapter Cards** area.

Step 5 In the tabbed menu below the **Adapter Cards** area, click the **vHBAs** tab.

Step 6 In the **Host Fibre Channel Interfaces** area, select a vHBA from the table.

Step 7 Click **Boot Table** to open the **Boot Table** dialog box for the selected vHBA.

Step 8 In the **Boot Table** dialog box, click **Add** to open the **Add Boot Entry** dialog box.

Step 9 In the **Add Boot Entry** dialog box, update the following fields:

Name	Description
Target WWPN field	The World Wide Port Name (WWPN) that corresponds to the location of the boot image. Enter the WWPN in the format hh:hh:hh:hh:hh:hh:hh:hh.
LUN ID field	The LUN ID that corresponds to the location of the boot image. Enter an ID between 0 and 255.
Add Boot Entry button	Adds the specified location to the boot table.
Reset Values button	Clears the values currently entered in the fields.
Cancel button	Closes the dialog box without saving any changes made while the dialog box was open.

Step 10 Click **Add Boot Entry**.

Deleting a Boot Table Entry

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.
Step 2 On the **Server** tab, click **Inventory**.
Step 3 In the **Inventory** pane, click the **Cisco VIC Adapters** tab.
Step 4 In the **Adapter Cards** area, select the adapter card.
If the server is powered on, the resources of the selected adapter card appear in the tabbed menu below the **Adapter Cards** area.
Step 5 In the tabbed menu below the **Adapter Cards** area, click the **vHBAs** tab.
Step 6 In the **Host Fibre Channel Interfaces** area, select a vHBA from the table.
Step 7 Click **Boot Table** to open the **Boot Table** dialog box for the selected vHBA.
Step 8 In the **Boot Table** dialog box, click the entry to be deleted.
Step 9 Click **Delete** and click **OK** to confirm.

vHBA Persistent Binding

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

Viewing Persistent Bindings

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **Cisco VIC Adapters** tab.

Step 4 In the **Adapter Cards** area, select the adapter card.
If the server is powered on, the resources of the selected adapter card appear in the tabbed menu below the **Adapter Cards** area.

Step 5 In the tabbed menu below the **Adapter Cards** area, click the **vHBAs** tab.

Step 6 In the **Host Fibre Channel Interfaces** area, select a vHBA from the table.

Step 7 Click **Persistent Bindings** to open the **Persistent Bindings** dialog box for the selected vHBA.

Step 8 In the **Persistent Bindings** dialog box for the selected vHBA, review the following information:

Name	Description
Index column	The unique identifier for the binding.
Target WWPN column	The target World Wide Port Name with which the binding is associated.
Host WWPN column	The host World Wide Port Name with which the binding is associated.
Bus ID column	The bus ID with which the binding is associated.
Target ID column	The target ID on the host system with which the binding is associated.
Rebuild Persistent Bindings button	Clears all unused bindings and resets the ones that are in use.
Close button	Closes the dialog box and saves your changes.

Step 9 Click **Close**.

Rebuilding Persistent Bindings

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **Cisco VIC Adapters** tab.

Step 4 In the **Adapter Cards** area, select the adapter card.
If the server is powered on, the resources of the selected adapter card appear in the tabbed menu below the **Adapter Cards** area.

Step 5 In the tabbed menu below the **Adapter Cards** area, click the **vHBAs** tab.

Step 6 In the **Host Fibre Channel Interfaces** area, select a vHBA from the table.

Step 7 Click **Persistent Bindings** to open the **Persistent Bindings** dialog box for the selected vHBA.

Step 8 In the **Persistent Bindings** dialog box for the selected vHBA, click **Rebuild Persistent Bindings**.

Step 9 Click **Close**.

Managing vNICs

Guidelines for Managing vNICs

When managing vNICs, consider the following guidelines and restrictions:

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

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

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

Viewing vNIC Properties

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **Cisco VIC Adapters** tab.

Step 4 In the **Adapter Cards** area, select the adapter card.
If the server is powered on, the resources of the selected adapter card appear in the tabbed menu below the **Adapter Cards** area.

Step 5 In the tabbed menu below the **Adapter Cards** area, click the **vNICs** tab.

Step 6 In the **Host Ethernet Interfaces** area, select a vNIC from the table.

Step 7 Click **Properties** to open the **vNIC Properties** dialog box.

Step 8 In the **General** area, review the information in the following fields:

Name	Description
Name field	The name for the virtual NIC. This name cannot be changed after the vNIC has been created.
MTU field	The maximum transmission unit, or packet size, that this vNIC accepts. Enter an integer between 1500 and 9000.
Uplink Port drop-down list	The uplink port associated with this vNIC. All traffic for this vNIC goes through this uplink port.
MAC Address field	The MAC address associated with the vNIC. To let the adapter select an available MAC address from its internal pool, select **Auto**. To specify an address, click the second radio button and enter the MAC address in the corresponding field.
Class of Service drop-down list	The class of service to associate with traffic from this vNIC. Select an integer between 0 and 6, with 0 being lowest priority and 6 being the highest priority. **Note** This option cannot be used in VNTAG mode.
Trust Host CoS check box	Check this box if you want the vNIC to use the class of service provided by the host operating system.
PCI Order field	The order in which this vNIC will be used. To let the system set the order, select **Any**. To specify an order, select the second radio button and enter an integer between 0 and 17.

Name	Description
Default VLAN field	If there is no default VLAN for this vNIC, click **NONE**. Otherwise, click the second radio button and enter a VLAN ID between 1 and 4094 in the field. **Note** This option cannot be used in VNTAG mode.
VLAN Mode drop-down list	If you want to use VLAN trunking, select **TRUNK**. Otherwise, select **ACCESS**. **Note** This option cannot be used in VNTAG mode.
Rate Limit field	If you want this vNIC to have an unlimited data rate, select OFF. Otherwise, click the second radio button and enter a rate limit in the associated field. Enter an integer between 1 and 10,000 Mbps. **Note** This option cannot be used in VNTAG mode.
Enable PXE Boot check box	Check this box if the vNIC can be used to perform a PXE boot.
Channel Number field	Select the channel number that will be assigned to this vNIC. **Note** VNTAG mode is required for this option.
Port Profile drop-down list	Select the port profile that should be associated with the vNIC. This field displays the port profiles defined on the switch to which this server is connected. **Note** VNTAG mode is required for this option.
Enable Uplink Failover check box	Check this box if traffic on this vNIC should fail over to the secondary interface if there are communication problems. **Note** VNTAG mode is required for this option.
Failback Timeout field	After a vNIC has started using its secondary interface, this setting controls how long the primary interface must be available before the system resumes using the primary interface for the vNIC. Enter a number of seconds between 0 and 600. **Note** VNTAG mode is required for this option.

Step 9 In the **Ethernet Interrupt** area, review the information in the following fields:

Name	Description
Interrupt Count field	The number of interrupt resources to allocate. In general, this value should be equal to the number of completion queue resources. Enter an integer between 1 and 514.
Coalescing Time field	The time to wait between interrupts or the idle period that must be encountered before an interrupt is sent. Enter an integer between 1 and 65535. To turn off interrupt coalescing, enter 0 (zero) in this field.
Coalescing Type drop-down list	This can be one of the following: • **MIN—**The system waits for the time specified in the **Coalescing Time** field before sending another interrupt event. • **IDLE—**The system does not send an interrupt until there is a period of no activity lasting as least as long as the time specified in the **Coalescing Time** field.
Interrupt Mode drop-down list	The preferred driver interrupt mode. This can be one of the following: • **MSI-X—**Message Signaled Interrupts (MSI) with the optional extension. This is the recommended option. • **MSI—**MSI only. • **INTx—**PCI INTx interrupts.

Step 10 In the **Ethernet Receive Queue** area, review the information in the following fields:

Name	Description
Receive Queue Count field	The number of receive queue resources to allocate. Enter an integer between 1 and 256.
Receive Queue Ring Size field	The number of descriptors in each receive queue. Enter an integer between 64 and 4096.

Step 11 In the **Ethernet Transmit Queue** area, review the information in the following fields:

Name	Description
Transmit Queue Count field	The number of transmit queue resources to allocate. Enter an integer between 1 and 256.

Name	Description
Transmit Queue Ring Size field	The number of descriptors in each transmit queue. Enter an integer between 64 and 4096.

Step 12 In the **Completion Queue** area, review the information in the following fields:

Name	Description
Completion Queue Count field	The number of completion queue resources to allocate. In general, the number of completion queue resources you should allocate is equal to the number of transmit queue resources plus the number of receive queue resources. Enter an integer between 1 and 512.
Completion Queue Ring Size field	The number of descriptors in each completion queue. This value cannot be changed.

Step 13 In the **TCP Offload** area, review the information in the following fields:

Name	Description
Enable TCP Segmentation Offload check box	If checked, the CPU sends large TCP packets to the hardware to be segmented. This option may reduce CPU overhead and increase throughput rate. If cleared, the CPU segments large packets. **Note** This option is also known as Large Send Offload (LSO).
Enable TCP Rx Offload Checksum Validation check box	If checked, the CPU sends all packet checksums to the hardware for validation. This option may reduce CPU overhead. If cleared, the CPU validates all packet checksums.
Enable TCP Tx Offload Checksum Generation check box	If checked, the CPU sends all packets to the hardware so that the checksum can be calculated. This option may reduce CPU overhead. If cleared, the CPU calculates all packet checksums.
Enable Large Receive check box	If checked, the hardware reassembles all segmented packets before sending them to the CPU. This option may reduce CPU utilization and increase inbound throughput. If cleared, the CPU processes all large packets.

Step 14 In the **Receive Side Scaling** area, review the information in the following fields:

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

Modifying vNIC Properties

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **Cisco VIC Adapters** tab.

Step 4 In the **Adapter Cards** area, select the adapter card.
If the server is powered on, the resources of the selected adapter card appear in the tabbed menu below the **Adapter Cards** area.

Step 5 In the tabbed menu below the **Adapter Cards** area, click the **vNICs** tab.

Step 6 In the **Host Ethernet Interfaces** area, select a vNIC from the table.

Step 7 Click **Properties** to open the **vNIC Properties** dialog box.

Step 8 In the **General** area, update the following fields:

Name	Description
Name field	The name for the virtual NIC. This name cannot be changed after the vNIC has been created.
MTU field	The maximum transmission unit, or packet size, that this vNIC accepts. Enter an integer between 1500 and 9000.
Uplink Port drop-down list	The uplink port associated with this vNIC. All traffic for this vNIC goes through this uplink port.
MAC Address field	The MAC address associated with the vNIC. To let the adapter select an available MAC address from its internal pool, select **Auto**. To specify an address, click the second radio button and enter the MAC address in the corresponding field.
Class of Service drop-down list	The class of service to associate with traffic from this vNIC. Select an integer between 0 and 6, with 0 being lowest priority and 6 being the highest priority. **Note** This option cannot be used in VNTAG mode.
Trust Host CoS check box	Check this box if you want the vNIC to use the class of service provided by the host operating system.
PCI Order field	The order in which this vNIC will be used. To let the system set the order, select **Any**. To specify an order, select the second radio button and enter an integer between 0 and 17.
Default VLAN field	If there is no default VLAN for this vNIC, click **NONE**. Otherwise, click the second radio button and enter a VLAN ID between 1 and 4094 in the field. **Note** This option cannot be used in VNTAG mode.
VLAN Mode drop-down list	If you want to use VLAN trunking, select **TRUNK**. Otherwise, select **ACCESS**. **Note** This option cannot be used in VNTAG mode.
Rate Limit field	If you want this vNIC to have an unlimited data rate, select OFF. Otherwise, click the second radio button and enter a rate limit in the associated field. Enter an integer between 1 and 10,000 Mbps. **Note** This option cannot be used in VNTAG mode.
Enable PXE Boot check box	Check this box if the vNIC can be used to perform a PXE boot.

Name	Description
Channel Number field	Select the channel number that will be assigned to this vNIC. **Note** VNTAG mode is required for this option.
Port Profile drop-down list	Select the port profile that should be associated with the vNIC. This field displays the port profiles defined on the switch to which this server is connected. **Note** VNTAG mode is required for this option.
Enable Uplink Failover check box	Check this box if traffic on this vNIC should fail over to the secondary interface if there are communication problems. **Note** VNTAG mode is required for this option.
Failback Timeout field	After a vNIC has started using its secondary interface, this setting controls how long the primary interface must be available before the system resumes using the primary interface for the vNIC. Enter a number of seconds between 0 and 600. **Note** VNTAG mode is required for this option.

Step 9 In the **Ethernet Interrupt** area, update the following fields:

Name	Description
Interrupt Count field	The number of interrupt resources to allocate. In general, this value should be equal to the number of completion queue resources. Enter an integer between 1 and 514.
Coalescing Time field	The time to wait between interrupts or the idle period that must be encountered before an interrupt is sent. Enter an integer between 1 and 65535. To turn off interrupt coalescing, enter 0 (zero) in this field.
Coalescing Type drop-down list	This can be one of the following: • **MIN—**The system waits for the time specified in the **Coalescing Time** field before sending another interrupt event. • **IDLE—**The system does not send an interrupt until there is a period of no activity lasting as least as long as the time specified in the **Coalescing Time** field.

Name	Description
Interrupt Mode drop-down list	The preferred driver interrupt mode. This can be one of the following: • **MSI-X—**Message Signaled Interrupts (MSI) with the optional extension. This is the recommended option. • **MSI—**MSI only. • **INTx—**PCI INTx interrupts.

Step 10 In the **Ethernet Receive Queue** area, update the following fields:

Name	Description
Receive Queue Count field	The number of receive queue resources to allocate. Enter an integer between 1 and 256.
Receive Queue Ring Size field	The number of descriptors in each receive queue. Enter an integer between 64 and 4096.

Step 11 In the **Ethernet Transmit Queue** area, update the following fields:

Name	Description
Transmit Queue Count field	The number of transmit queue resources to allocate. Enter an integer between 1 and 256.
Transmit Queue Ring Size field	The number of descriptors in each transmit queue. Enter an integer between 64 and 4096.

Step 12 In the **Completion Queue** area, update the following fields:

Name	Description
Completion Queue Count field	The number of completion queue resources to allocate. In general, the number of completion queue resources you should allocate is equal to the number of transmit queue resources plus the number of receive queue resources. Enter an integer between 1 and 512.
Completion Queue Ring Size field	The number of descriptors in each completion queue. This value cannot be changed.

Step 13 In the **TCP Offload** area, update the following fields:

Name	Description
Enable TCP Segmentation Offload check box	If checked, the CPU sends large TCP packets to the hardware to be segmented. This option may reduce CPU overhead and increase throughput rate. If cleared, the CPU segments large packets. **Note** This option is also known as Large Send Offload (LSO).
Enable TCP Rx Offload Checksum Validation check box	If checked, the CPU sends all packet checksums to the hardware for validation. This option may reduce CPU overhead. If cleared, the CPU validates all packet checksums.
Enable TCP Tx Offload Checksum Generation check box	If checked, the CPU sends all packets to the hardware so that the checksum can be calculated. This option may reduce CPU overhead. If cleared, the CPU calculates all packet checksums.
Enable Large Receive check box	If checked, the hardware reassembles all segmented packets before sending them to the CPU. This option may reduce CPU utilization and increase inbound throughput. If cleared, the CPU processes all large packets.

Step 14 In the **Receive Side Scaling** area, update the following fields:

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

Step 15 Click **Save Changes**.

Creating a vNIC

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

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **Cisco VIC Adapters** tab.

Step 4 In the **Adapter Cards** area, select the adapter card.
If the server is powered on, the resources of the selected adapter card appear in the tabbed menu below the **Adapter Cards** area.

Step 5 In the tabbed menu below the **Adapter Cards** area, click the **vNICs** tab.

Step 6 In the **Host Ethernet Interfaces** area, choose one of these actions:

- To create a vNIC using default configuration settings, click **Add**.
- To create a vNIC using the same configuration settings as an existing vNIC, select that vNIC and click **Clone**.

The **Add vNIC** dialog box appears.

Step 7 In the **Add vNIC** dialog box, enter a name for the vNIC in the **Name** entry box.

Step 8 (Optional) In the **Add vNIC** dialog box, enter a channel number for the vNIC in the **Channel Number** entry box.

Note If NIV is enabled on the adapter, you must assign a channel number for the vNIC when you create it.

Step 9 Click **Add vNIC**.

What to Do Next

If configuration changes are required, configure the new vNIC as described in Modifying vNIC Properties, on page 112.

Deleting a vNIC

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **Cisco VIC Adapters** tab.

Step 4 In the **Adapter Cards** area, select the adapter card.
If the server is powered on, the resources of the selected adapter card appear in the tabbed menu below the **Adapter Cards** area.

Step 5 In the tabbed menu below the **Adapter Cards** area, click the **vNICs** tab.

Step 6 In the **Host Ethernet Interfaces** area, select a vNIC from the table.

Note You cannot delete either of the two default vNICs, **eth0** or **eth1**.

Step 7 Click **Delete** and click **OK** to confirm.

Managing Cisco usNIC

Overview of Cisco usNIC

The Cisco user-space NIC (Cisco usNIC) feature improves the performance of software applications that run on the Cisco UCS servers in your data center by bypassing the kernel when sending and receiving networking packets. The applications interact directly with a Cisco UCS VIC second generation adapter, such as the Cisco UCS VIC-1280, which improves the networking performance of your high-performance computing cluster. To benefit from Cisco usNIC, your applications must use the Message Passing Interface (MPI) instead of sockets or other communication APIs.

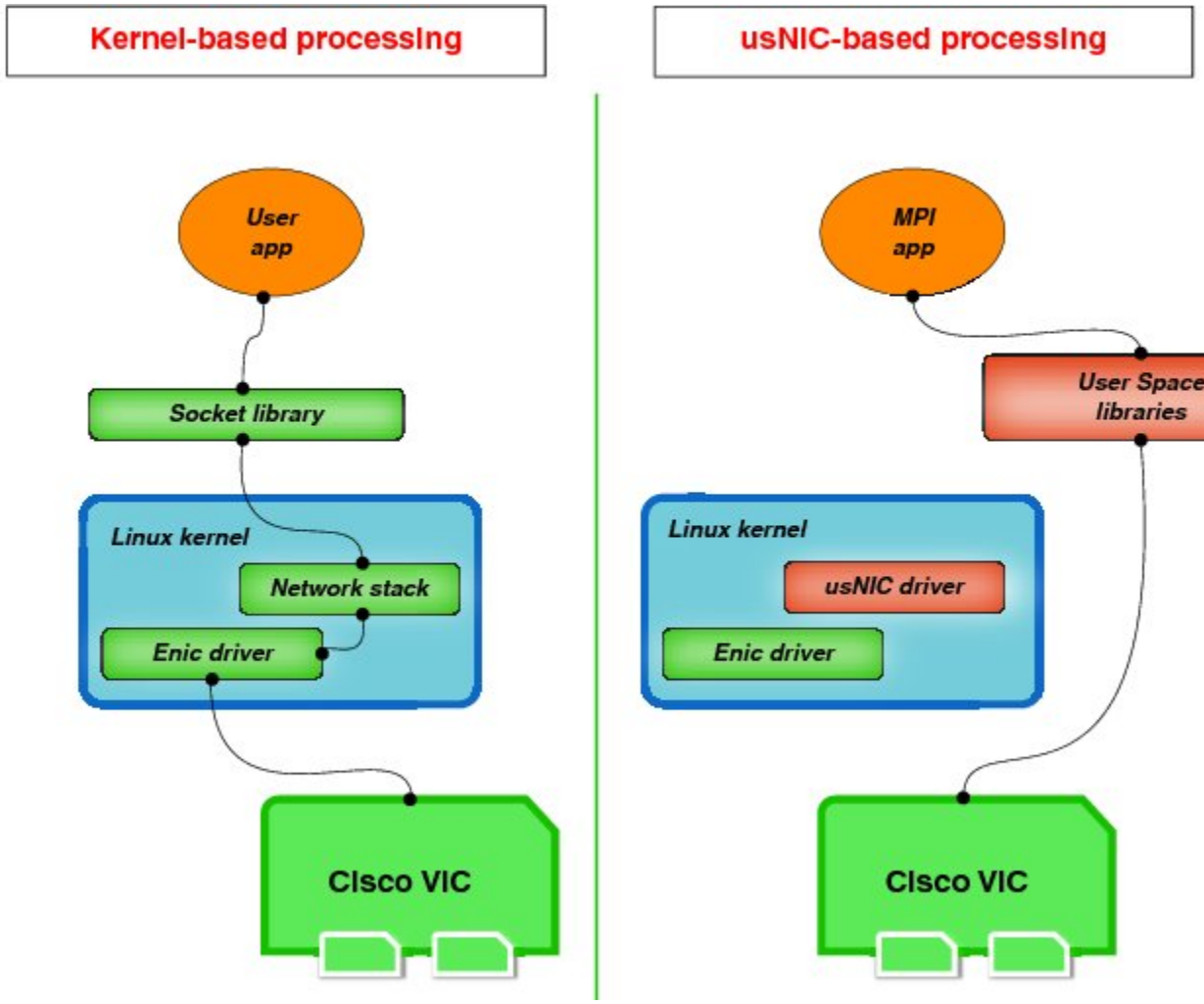
Cisco usNIC offers the following benefits for your MPI applications:

- Provides a low-latency and high-throughput communication transport.
- Employs the standard and application-independent Ethernet protocol.
- Takes advantage of lowlatency forwarding, Unified Fabric, and integrated management support in the following Cisco data center platforms:
  - Cisco UCS server
  - Cisco UCS VIC second generation adapter, such as the Cisco UCS VIC-1280
  - 10GbE network

Standard Ethernet applications use user-space socket libraries, which invoke the networking stack in the Linux kernel. The networking stack then uses the Cisco eNIC driver to communicate with the Cisco VIC hardware.

The following figure shows the contrast between a regular software application and an MPI application that uses usNIC.

Figure 1: Kernel-Based Network Communication versus Cisco usNIC-Based Communication



Configuring Cisco usNIC Using the CIMC GUI

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

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

Before You Begin

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

Procedure

Step 1 Log into the CIMC GUI.
For more information about how to log into CIMC, see the *Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide* available at this URL: http://www.cisco.com/en/US/products/ps10739/products_installation_and_configuration_guides_list.html .

Step 2 In the **Navigation** pane, click the **Server** tab.

Step 3 On the **Server** tab, click **Inventory**.

Step 4 In the **Inventory** pane, click the **Cisco VIC Adapters** tab.

Step 5 In the **Adapter Cards** area, select the adapter card.
If the server is powered on, the resources of the selected adapter card appear in the tabbed menu below the **Adapter Cards** area.

Step 6 In the tabbed menu below the **Adapter Cards** area, click the **vNICs** tab.

Step 7 In the **Host Ethernet Interfaces** area, select a vNIC from the table.

Note For each vNIC that you want to configure as a usNIC, select the vNIC entry from the table and specify its properties as explained in steps 9 through step 18.

Step 8 Click **usNIC** to open the **usNIC Properties** dialog box.

Step 9 In the **usNICs** property, specify the number of Cisco usNICs that you want to create.
Each MPI process that is running on the server requires a dedicated usNIC. You might need to create up to 64 usNICs to sustain 64 MPI processes running simultaneously. We recommend that you create at least as many usNICs, per 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 10 In the **Properties** area, update the following fields:

Field Name	Description
Transmit Queue Count	The number of transmit queue resources to allocate. MPI will use 2 transmit queues per process. Therefore, Cisco recommends that you set this value to 2.
Receive Queue Count	The number of receive queue resources to allocate. MPI will use 2 receive queues per process. Therefore, Cisco recommends that you set this value to 2.
Completion Queue Count	The number of completion queue resources to allocate. In general, the number of completion queue resources you should allocate is equal to the number of transmit queue resources plus the number of receive queue resources. Cisco recommends that you set this value to 4.

Step 11 Click **Apply**.

Step 12 In the **Navigation** pane, click the **Server** tab.

Step 13 On the **Server** tab, click **BIOS**.

Step 14 In the **Actions** area, click **Configure BIOS**.

Step 15 In the **Configure BIOS Parameters** dialog box, click the **Advanced** tab.

Step 16 In the **Processor Configuration** area, set the following properties to Enabled:

- **Intel(R) VT-d**
- **Intel(R) VT-d ATS support**
- **Intel(R) VT-d Coherency Support**

Step 17 Click **Save Changes**.
The changes take effect upon the next server reboot.

Viewing usNIC Properties

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **Cisco VIC Adapters** tab.

Step 4 In the **Adapter Cards** area, select the adapter card.

If the server is powered on, the resources of the selected adapter card appear in the tabbed menu below the **Adapter Cards** area.

Step 5 In the tabbed menu below the **Adapter Cards** area, click the **vNICs** tab.

Step 6 In the **Host Ethernet Interface** area, select the usNIC that is assigned to vNIC, to open the **usNIC properties** dialog box.

Step 7 In the **usNIC** area, review or update the information in the following fields:

Name	Description
Name	The name for the vNIC that is the parent of the usNIC. **Note** This field is read-only.
usNIC field	The number of usNICs assigned to the specific vNIC. Enter an integer between 0 and 225. To assign additional usNICs to a specified vNIC, enter value higher than the existing value. To delete usNICs from a specified vNIC, enter value smaller than the existing value. To delete all the usNICs assigned to a vNIC, enter zero.

Step 8 In the **Properties** area, review or update the information in the following fields:

Name	Description
Transmit Queue Count field	The number of transmit queue resources to allocate. Enter an integer between 1 and 256.
Receive Queue Count field	The number of receive queue resources to allocate. Enter an integer between 1 and 256.
Completion Queue Count field	The number of completion queue resources to allocate. In general, the number of completion queue resources you should allocate is equal to the number of transmit queue resources plus the number of receive queue resources. Enter an integer between 1 and 512.
Transmit Queue Ring Size field	The number of descriptors in each transmit queue. Enter an integer between 64 and 4096.
Receive Queue Ring Size field	The number of descriptors in each receive queue. Enter an integer between 64 and 4096.

Name	Description
Interrupt Count field	The number of interrupt resources to allocate. In general, this value should be equal to the number of completion queue resources. Enter an integer between 1 and 514.
Interrupt Coalescing Type drop-down list	This can be one of the following: • **MIN—**The system waits for the time specified in the **Coalescing Time** field before sending another interrupt event. • **IDLE—**The system does not send an interrupt until there is a period of no activity lasting as least as long as the time specified in the **Coalescing Time** field.
Interrupt Coalescing Timer Time field	The time to wait between interrupts or the idle period that must be encountered before an interrupt is sent. Enter an integer between 1 and 65535. To turn off interrupt coalescing, enter 0 (zero) in this field.
Class of Service field	The class of service to associate with traffic from this usNIC. Select an integer between 0 and 6, with 0 being lowest priority and 6 being the highest priority. **Note** This option cannot be used in VNTAG mode.
TCP Segment Offload check box	If checked, the CPU sends large TCP packets to the hardware to be segmented. This option may reduce CPU overhead and increase throughput rate. If cleared, the CPU segments large packets. **Note** This option is also known as Large Send Offload (LSO).
Large Receive check box	If checked, the hardware reassembles all segmented packets before sending them to the CPU. This option may reduce CPU utilization and increase inbound throughput. If cleared, the CPU processes all large packets.
TCP Tx Checksum check box	If checked, the CPU sends all packets to the hardware so that the checksum can be calculated. This option may reduce CPU overhead. If cleared, the CPU calculates all packet checksums.

Name	Description
TCP Rx Checksum check box	If checked, the CPU sends all packet checksums to the hardware for validation. This option may reduce CPU overhead. If cleared, the CPU validates all packet checksums.

Name	Description
Apply button	Applies changes to all the usNICs associated with the vNIC device.
Reset values button	Restores the values for the usNIC to the settings that were in effect when this dialog box was first opened.
Cancel button	Closes the dialog box without making any changes.

Configuring iSCSI Boot Capability

Configuring iSCSI Boot Capability for vNICs

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

To configure the iSCSI boot capability on a vNIC:

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

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

Configuring iSCSI Boot Capability on a vNIC

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

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the Inventory pane, click the **Cisco VIC Adapters** tab.

Step 4 In the **Adapter Cards** area, select the adapter card.
If the server is powered on, the resources of the selected adapter card appear in the tabbed menu below the **Adapter Cards** area.

Step 5 In the tabbed menu below the **Adapter Cards** area, click the **vNICs** tab.

Step 6 In the **Host Ethernet Interfaces** area, select a vNIC from the table, and click **iSCSI Boot**.

Step 7 In the **General Area**, update the following fields:

Name	Description
Name field	The name of the vNIC.
DHCP Network check box	Whether DHCP Network is enabled for the vNIC. If enabled, the initiator network configuration is obtained from the DHCP server.
DHCP iSCSI check box	Whether DHCP iSCSI is enabled for the vNIC. If enabled and the DHCP ID is set, the initiator IQN and target information are obtained from the DHCP server. **Note** If DHCP iSCSI is enabled without a DHCP ID, only the target information is obtained.
DHCP ID field	The vendor identifier string used by the adapter to obtain the initiator IQN and target information from the DHCP server. Enter a string up to 64 characters.
DHCP Timeout field	The number of seconds to wait before the initiator assumes that the DHCP server is unavailable. Enter an integer between 60 and 300 (default: 60 seconds)
Link Timeout field	The number of seconds to wait before the initiator assumes that the link is unavailable. Enter an integer between 0 and 255 (default: 15 seconds)

Name	Description
LUN Busy Retry Count field	The number of times to retry the connection in case of a failure during iSCSI LUN discovery. Enter an integer between 0 and 255. The default is 15.
IP Version field	The IP version to use during iSCSI boot.

Step 8 In the **Initiator Area**, update the following fields:

Name	Description
Name field	A regular expression that defines the name of the iSCSI initiator. You can enter any alphanumeric string as well as the following special characters: • . (period) • : (colon) • - (dash) **Note** The name is in the IQN format.
IP Address field	The IP address of the iSCSI initiator.
Subnet Mask field	The subnet mask for the iSCSI initiator.
Gateway field	The default gateway.
Primary DNS field	The primary DNS server address.
Secondary DNS field	The secondary DNS server address.
TCP Timeout field	The number of seconds to wait before the initiator assumes that TCP is unavailable. Enter an integer between 0 and 255 (default: 15 seconds)
CHAP Name field	The Challenge-Handshake Authentication Protocol (CHAP) name of the initiator.
CHAP Secret field	The Challenge-Handshake Authentication Protocol (CHAP) shared secret of the initiator.

Step 9 In the **Primary Target Area**, update the following fields:

Name	Description
Name field	The name of the primary target in the IQN format.
IP Address field	The IP address of the target.
TCP Port field	The TCP port associated with the target.
Boot LUN field	The Boot LUN associated with the target.
CHAP Name field	The Challenge-Handshake Authentication Protocol (CHAP) name of the initiator.
CHAP Secret field	The Challenge-Handshake Authentication Protocol (CHAP) shared secret of the initiator.

Step 10 In the **Secondary Target Area**, update the following fields:

Name	Description
Name field	The name of the secondary target in the IQN format.
IP Address field	The IP address of the target.
TCP Port field	The TCP port associated with the target.
Boot LUN field	The Boot LUN associated with the target.
CHAP Name field	The Challenge-Handshake Authentication Protocol (CHAP) name of the initiator.
CHAP Secret field	The Challenge-Handshake Authentication Protocol (CHAP) shared secret of the initiator.

Name	Description
Configure ISCSI button	Configures iSCSI boot on the selected vNIC.
Unconfigure ISCSI button	Removes the configuration from the selected vNIC.
Reset Values button	Restores the values for the vNIC to the settings that were in effect when this dialog box was first opened.
Cancel button	Closes the dialog box without making any changes.

Step 11 Click **Configure ISCSI**.

Removing iSCSI Boot Configuration from a vNIC

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.
Step 2 On the **Server** tab, click **Inventory**.
Step 3 In the Inventory pane, click the **Cisco VIC Adapters** tab.
Step 4 In the **Adapter Cards** area, select the adapter card.
If the server is powered on, the resources of the selected adapter card appear in the tabbed menu below the **Adapter Cards** area.
Step 5 In the tabbed menu below the **Adapter Cards** area, click the **vNICs** tab.
Step 6 In the **Host Ethernet Interfaces** area, select a vNIC from the table, and click **iSCSI Boot**.
Step 7 In the dialog box that appears, click **Unconfigure ISCSI**.

Managing VM FEX

Virtual Machine Fabric Extender

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

Viewing Virtual 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

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **Cisco VIC Adapters** tab.

Step 4 In the **Adapter Cards** area, select the adapter card.
If the server is powered on, the resources of the selected adapter card appear in the tabbed menu below the **Adapter Cards** area.

Step 5 In the tabbed menu below the **Adapter Cards** area, click the **VM FEXs** tab.

Step 6 In the Virtual FEXs area, review the following information:

Name	Description
Properties button	Opens a dialog box that allows you to view the properties for the selected VM FEX.
Name column	The name of the VM FEX.
MTU column	The maximum transmission unit, or packet size, that this VM FEX accepts.
CoS column	If enabled, the VM FEX uses the class of service provided by the host operating system.
VLAN column	The VLAN associated with the VM FEX.
VLAN Mode column	The mode for the associated VLAN.
Uplink Failover column	If VNTAG mode is enabled for the adapter, this column displays whether traffic on this VM FEX will fail over to a secondary interface if the primary interface fails.

Step 7 In the Virtual FEXs area, select a VM FEX from the table.

Step 8 Click **Properties** to open the **VM FEX Properties** dialog box for the selected VM FEX.

Step 9 In the **General Properties** area, review the information in the following fields:

Name	Description
Name field	The name of the VM FEX.
MTU field	The maximum transmission unit, or packet size, that this VM FEX accepts.
Trust Host CoS field	If enabled, the VM FEX uses the class of service provided by the host operating system.
PCI Order field	The order in which this VM FEX will be used, if any.

Name	Description
Default VLAN field	The VLAN associated with the VM FEX.
Rate Limit field	The data rate limit associated with this VM FEX, if any.
PXE Boot field	Whether PXE boot is enabled or disabled for this VM FEX.

Step 10 In the **Ethernet Interrupt** area, review the information in the following fields:

Name	Description
Interrupt Count field	The number of interrupt resources allocated to this VM FEX.
Coalescing Time field	The time CIMC waits between interrupts or the idle period that must be encountered before an interrupt is sent.
Coalescing Type field	This can be one of the following: • **MIN—**The system waits for the time specified in the **Coalescing Time** field before sending another interrupt event. • **IDLE—**The system does not send an interrupt until there is a period of no activity lasting as 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: • **MSIx—**Message Signaled Interrupts (MSI) with the optional extension. • **MSI—**MSI only. • **INTx—**PCI INTx interrupts.

Step 11 In the **Ethernet Receive Queue** area, review the information in the following fields:

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.

Step 12 In the **Ethernet Transmit Queue** area, review the information in the following fields:

Name	Description
Transmit Queue Count field	The number of transmit queue resources allocated to this VM FEX.

Name	Description
Transmit Queue Ring Size field	The number of descriptors in each transmit queue.

Step 13 In the **Completion Queue** area, review the information in the following fields:

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.

Step 14 In the **TCP Offload** area, review the information in the following fields:

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

Step 15 In the **Receive Side Scaling** area, review the information in the following fields:

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

Name	Description
Enable TCP-IPv6 RSS field	If enabled, RSS is enabled for TCP transmissions across IPv6 networks.
Enable IPv6 Extension RSS field	If enabled, RSS is enabled for IPv6 extensions.
Enable TCP-IPv6 Extension RSS field	If enabled, RSS is enabled for TCP transmissions across IPv6 networks.

Managing Storage Adapters

Create Virtual Drive from Unused Physical Drives

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.

Step 3 On the **Work** pane, click the **Virtual Drive Info** tab.

Step 4 In the **Actions** area, click **Create Virtual Drive from Unused Physical Drives**.
The **Create Virtual Drive from Unused Physical Drives** dialog box displays.

Step 5 In the **Create Virtual Drive from Unused Physical Drives** dialog box, select the RAID level for the new virtual drives:
This can be one of the following:

- **Raid 0—**Simple striping.
- **Raid 1—**Simple mirroring.
- **Raid 5—**Striping with parity.
- **Raid 6—**Striping with two parity drives.
- **Raid 10—**Spanned mirroring.
- **Raid 50—**Spanned striping with parity.
- **Raid 60—**Spanned striping with two parity drives.

Step 6 In the **Create Drive Groups** area, choose one or more physical drives to include in the group.

Use the >> button to add the drives to the **Drive Groups** table. Use the << button to remove physical drives from the drive group.

Note The size of the smallest physical drive in the drive group defines the maximum size used for all the physical drives. To ensure maximum use of space for all physical drives, it is recommended that the size of all the drives in the drive group are similar.

Step 7 In the **Virtual Drive Properties** area, update the following properties:

Name	Description
Name field	The name of the new virtual drive you want to create.
Read Policy drop-down list	The read-ahead cache mode. This value cannot be changed.
Cache Policy drop-down list	The cache policy used for buffering reads. This value cannot be changed.
Strip Size drop-down list	The size of each strip, in KB. This value cannot be changed.
Write Policy drop-down list	This can be one of the following • **Write Through—** Data is written through the cache and to the physical drives. Performance is improved, because subsequent reads of that data can be satisfied from the cache. • **Write Back—** Data is stored in the cache, and is only written to the physical drives when space in the cache is needed. Virtual drives requesting this policy fall back to **Write Through** caching when the BBU cannot guarantee the safety of the cache in the event of a power failure. • **Write Back Bad BBU—**With this policy, write caching remains **Write Back** even if the battery backup unit is defective or discharged.
Size field	The size of the virtual drive you want to create. Enter a value and select one of the following units: • MB • GB • TB

Step 8 Click **Create Virtual Drive**.

Create Virtual Drive from an Existing Drive Group

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.

Step 3 On the **Work** pane, click the **Controller Info** tab.

Step 4 In the **Actions** area, click **Create Virtual Drive from an Existing Virtual Drive Group**.
The **Create Virtual Drive from an Existing Virtual Drive Group** dialog box displays.

Step 5 In the **Create Virtual Drive from an Existing Virtual Drive Group** dialog box, select the virtual drive whose drive group you want to use to create a new virtual drive.

Step 6 In the **Virtual Drive Properties** area, update the following properties:

Name	Description
Name field	The name of the new virtual drive you want to create.
Read Policy drop-down list	The read-ahead cache mode. This value cannot be changed.
Cache Policy drop-down list	The cache policy used for buffering reads. This value cannot be changed.
Strip Size drop-down list	The size of each strip, in KB. This value cannot be changed.
Write Policy drop-down list	This can be one of the following • **Write Through—** Data is written through the cache and to the physical drives. Performance is improved, because subsequent reads of that data can be satisfied from the cache. • **Write Back—** Data is stored in the cache, and is only written to the physical drives when space in the cache is needed. Virtual drives requesting this policy fall back to **Write Through** caching when the BBU cannot guarantee the safety of the cache in the event of a power failure. • **Write Back Bad BBU—**With this policy, write caching remains **Write Back** even if the battery backup unit is defective or discharged.

Name	Description
Size field	The size of the virtual drive you want to create. Enter a value and select one of the following units: • MB • GB • TB

Step 7 Click **Create Virtual Drive**.

Clearing Foreign Configuration

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

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.
Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.
Step 3 On the **Work** pane, click the **Controller Info** tab.
Step 4 In the **Actions** area, click **Clear Foreign Config**.
Step 5 Click **OK** to confirm.

Preparing a Drive for Removal

Note You can perform 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

Step 1 In the **Navigation** pane, click the **Storage** tab.
Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.
Step 3 On the **Work** pane, click the **Physical Drive Info** tab.
Step 4 In the **Physical Drives** area, select the drive you want to remove.
Step 5 In the **Actions** area, click **Prepare for Removal**.
Step 6 Click **OK** to confirm.

Undo Preparing a Drive for Removal

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.
Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.
Step 3 On the **Work** pane, click the **Physical Drive Info** tab.
Step 4 In the **Physical Drives** area, select a drive with a status of **Ready to Remove**.
Step 5 In the **Actions** area, click **Undo Prepare for Removal**.
Step 6 Click **OK** to confirm.

Making a Dedicated Hot Spare

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.
Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.
Step 3 On the **Work** pane, click the **Physical Drive Info** tab.
Step 4 In the **Physical Drives** area, select the physical drive you want to make a dedicated hot spare.
Step 5 In the **Actions** area, click **Make Dedicated Hot Spare**.

The **Make Dedicated Hot Spare** dialog box displays.

Step 6 In the **Virtual Drive Details** area, update the following properties:

Name	Description
Virtual Drive Number drop-down list	Select the virtual drive to which you want to dedicate the physical drive as hot spare.
Virtual Drive Name field	The name of the selected virtual drive.
Physical Drive Number field	The number of the physical drive.

Step 7 Click **Make Dedicated Hot Spare** to confirm.

Making a Global Hot Spare

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.
Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.
Step 3 On the **Work** pane, click the **Physical Drive Info** tab.
Step 4 In the **Physical Drives** area, select the physical drive you want to make a global hot spare.
Step 5 In the **Actions** area, click **Make Global Hot Spare**.

Removing a Drive from Hot Spare Pools

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.

Step 3 On the **Work** pane, click the **Physical Drive Info** tab.

Step 4 In the **Physical Drives** area, select the global or dedicated hot spare you want to remove from the hot spare pools.

Step 5 In the **Actions** area, click **Remove From Hot Spare Pools**.

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

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.

Step 3 On the **Work** pane, click the **Virtual Drive Info** tab.

Step 4 In the **Virtual Drives** area, choose the drive that you want to initialize.

Step 5 In the **Actions** area, click **Initialize**.
The **Initialize Virtual Drive** dialog box displays.

Step 6 Choose the type of initialization you want to use for the virtual drive.
This can be one of the following:

- **Fast Initialize—**This option allows you to start writing data to the virtual drive immediately.
- **Full Initialize—**A complete initialization is done on the new configuration. You cannot write data to the new virtual drive until the initialization is complete.

Step 7 Click **Initialize VD** to initialize the drive, or **Cancel** to close the dialog box without making any changes.

Step 8 To view the status of the task running on the drive, in the **Operations** area, click **Refresh**.
The following details are displayed:

Name	Description
Operation	Name of the operation that is in progress on the drive.
Progress in %	Progress of the operation, in percentage complete.

Name	Description
Elapsed Time in secs	The number of seconds that have elapsed since the operation began.

Set as Boot Drive

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.
Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.
Step 3 On the **Work** pane, click the **Virtual Drive Info** tab.
Step 4 In the **Virtual Drives** area, choose the drive from which the controller must boot.
Step 5 In the **Actions** area, click **Set as Boot Drive**.
Step 6 Click **OK** to confirm.

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

Step 1 In the **Navigation** pane, click the **Storage** tab.
Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.
Step 3 On the **Work** pane, click the **Virtual Drive Info** tab.
Step 4 In the **Virtual Drives** area, select the virtual drive you want to delete.
Step 5 In the **Actions** area, click **Delete Virtual Drive**.
Step 6 Click **OK** to confirm.

Enabling Auto Learn Cycle for a Battery Backup Unit

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.
Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.
Step 3 On the **Work** pane, click the **Battery Backup Unit** tab.
Step 4 From the **Actions** pane, click **Enable Auto Learn Mode**.
A dialog prompts you to confirm the task.
Step 5 Click **OK**.

Disabling Auto Learn Cycle for a Battery Backup Unit

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.
Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.
Step 3 On the **Work** pane, click the **Battery Backup Unit** tab.
Step 4 From the **Actions** pane, click **Disable Auto Learn Mode**.
A dialog prompts you to confirm the task.

Step 5 Click **OK**.

Starting Learn Cycles for a Battery Backup Unit

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.
Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.
Step 3 On the **Work** pane, click the **Battery Backup Unit** tab.
Step 4 From the **Actions** pane, click **Start Learn Cycle**.
A dialog prompts you to confirm the task.
Step 5 Click **OK**.

Toggling Locator LED for a Physical Drive

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.
Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.
Step 3 On the **Work** pane, click the **Physical Drive Info** tab.
Step 4 From the **Status** area, select **Turn On** or **Turn Off** radio button for the **Locator LED** field.

Viewing Storage Controller Logs

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Storage** tab.

Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.

Step 3 On the **Work** pane, click **Storage Log** tab and review the following information:

Name	Description
Time column	The date and time the event occurred.
Severity column	The event severity. This can be one of the following: • Emergency • Alert • Critical • Error • Warning • Notice • Informational • Debug
Description column	A description of the event.

Backing Up and Restoring the Adapter Configuration

Exporting the Adapter Configuration

The adapter configuration can be exported as an XML file to a remote server which can be one of the following:

- TFTP
- FTP
- SFTP
- SCP
- HTTP

Before You Begin

Obtain the remote server IP address.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **Cisco VIC Adapters** tab.

Step 4 In the **Adapter Cards** area, select the adapter card.
If the server is powered on, the resources of the selected adapter card appear in the tabbed menu below the **Adapter Cards** area.

Step 5 In the tabbed menu below the **Adapter Cards** area, click the **General** tab.

Step 6 In the **Actions** area of the **General** tab, click **Export Configuration**.
The **Export Adapter Configuration** dialog box opens.

Step 7 In the **Export Adapter Configuration** dialog box, update the following fields:

Name	Description
Export to drop-down list	The remote server type. This can be one of the following: • **TFTP Server** • **FTP Server** • **SFTP Server** • **SCP Server** • **HTTP Server**
Server IP/Hostname field	The IP address or hostname of the server to which the adapter configuration file will be exported. Depending on the setting in the **Export to** drop-down list, the name of the field may vary.
Path and Filename field	The path and filename CIMC should use when exporting the file to the remote server.
Username	The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP.
Password	The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP.

Step 8 Click **Export Configuration**.

Importing the Adapter Configuration

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **Cisco VIC Adapters** tab.

Step 4 In the **Adapter Cards** area, select the adapter card.
If the server is powered on, the resources of the selected adapter card appear in the tabbed menu below the **Adapter Cards** area.

Step 5 In the tabbed menu below the **Adapter Cards** area, click the **General** tab.

Step 6 In the **Actions** area of the **General** tab, click **Import Configuration**.
The **Import Adapter Configuration** dialog box opens.

Step 7 In the **Import Adapter Configuration** dialog box, update the following fields:

Name	Description
Import from drop-down list	The remote server type. This can be one of the following: • **TFTP Server** • **FTP Server** • **SFTP Server** • **SCP Server** • **HTTP Server**
Server IP/Hostname field	The IP address or hostname of the server on which the adapter configuration file resides. Depending on the setting in the **Import from** drop-down list, the name of the field may vary.
Path and Filename field	The path and filename of the configuration file on the remote server.
Username	The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP.
Password	The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP.

Step 8 Click **Import Configuration**.
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.

What to Do Next

Reboot the server to apply the imported configuration.

Restoring Adapter Defaults

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **Cisco VIC Adapters** tab.

Step 4 In the **Adapter Cards** area, select the adapter card.
If the server is powered on, the resources of the selected adapter card appear in the tabbed menu below the **Adapter Cards** area.

Step 5 In the tabbed menu below the **Adapter Cards** area, click the **General** tab.

Step 6 In the **Actions** area of the **General** tab, click **Reset To Defaults** and click **OK** to confirm.

Managing Adapter Firmware

Adapter Firmware

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

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

Installing Adapter Firmware From a Local File

Before You Begin

Store the adapter firmware file in the file system of the managing computer.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **Cisco VIC Adapters** tab.

Step 4 In the **Adapter Cards** area, select the adapter card.
If the server is powered on, the resources of the selected adapter card appear in the tabbed menu below the **Adapter Cards** area.

Step 5 In the tabbed menu below the **Adapter Cards** area, click the **General** tab.

Step 6 In the **Actions** area of the **General** tab, click **Install Firmware** to open the **Install Adapter Firmware** dialog box.

Step 7 In the **Install Adapter Firmware** dialog box, select **Install from local file**, then click **Next**.

Step 8 Click **Browse...** and locate the adapter firmware file.

Step 9 Click **Install Firmware**.

What to Do Next

To activate the new firmware, see *Activating Adapter Firmware*.

Installing Adapter Firmware From a Remote Server

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **Cisco VIC Adapters** tab.

Step 4 In the **Adapter Cards** area, select the adapter card.
If the server is powered on, the resources of the selected adapter card appear in the tabbed menu below the **Adapter Cards** area.

Step 5 In the tabbed menu below the **Adapter Cards** area, click the **General** tab.

Step 6 In the **Actions** area of the **General** tab, click **Install Firmware** to open the **Install Adapter Firmware** dialog box.

Step 7 In the **Install Adapter Firmware** dialog box, select **Install from Remote Server**, then click **Next**.

Step 8 In the **Install Adapter Firmware** dialog box, update the following fields:

Name	Description
Install from drop-down list	The remote server type. This can be one of the following: • **TFTP Server** • **FTP Server** • **SFTP Server** • **SCP Server** • **HTTP Server**
Server IP/Hostname field	The IP address or hostname of the server on which the adapter configuration file resides. Depending on the setting in the **Install from** drop-down list, the name of the field may vary.
Path and Filename field	The path and filename of the configuration file on the remote server.
Username	The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP.
Password	The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP.
Back button	Click this button if you want to specify a local path for the firmware package.
Install Firmware button	Click this button to install the selected firmware package in the adapter's backup memory slot.
Close button	Click this button to close the wizard without making any changes to the firmware versions stored on the server.

Step 9 Click **Install Firmware**.

What to Do Next

To activate the new firmware, see *Activating Adapter Firmware*.

Activating Adapter Firmware

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

Step 3 In the **Inventory** pane, click the **Cisco VIC Adapters** tab.

Step 4 In the **Adapter Cards** area, select the adapter card.
If the server is powered on, the resources of the selected adapter card appear in the tabbed menu below the **Adapter Cards** area.

Step 5 In the tabbed menu below the **Adapter Cards** area, click the **General** tab.

Step 6 In the **Actions** area of the **General** tab, click **Activate Firmware** to open the **Activate Adapter Firmware** dialog box.

Step 7 In the **Activate Adapter Firmware** dialog box, select the image to run the next time the firmware starts up.

Step 8 Click **Activate Adapter Firmware**.

Resetting the Adapter

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Inventory**.

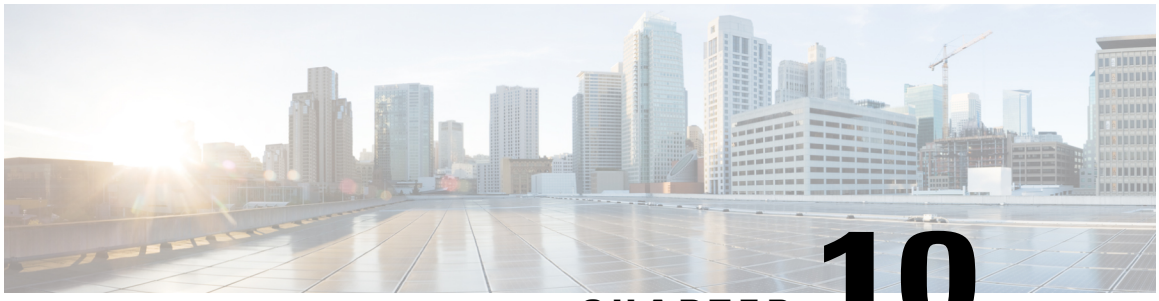
Step 3 In the **Inventory** pane, click the **Cisco VIC Adapters** tab.

Step 4 In the **Adapter Cards** area, select the adapter card.
If the server is powered on, the resources of the selected adapter card appear in the tabbed menu below the **Adapter Cards** area.

Step 5 In the tabbed menu below the **Adapter Cards** area, click the **General** tab.

Step 6 In the **Actions** area of the **General** tab, click **Reset** and click **Yes** to confirm.

Note Resetting the adapter also resets the host.



CHAPTER 10

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 perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Communications Services**.

Step 3 In the **Communications Services** pane, click the **Communication Services** tab.

Step 4 In the **HTTP Properties** area, update the following properties:

Name	Description
HTTP/S Enabled check box	Whether HTTP and HTTPS are enabled on the CIMC.
Redirect HTTP to HTTPS Enabled check box	If enabled, all attempts to communicate via HTTP are redirected to the equivalent HTTPS address. We strongly recommend that you enable this option if you enable HTTP.
HTTP Port field	The port to use for HTTP communication. The default is 80.

Name	Description
HTTPS Port field	The port to use for HTTPS communication. The default is 443
Session Timeout field	The number of seconds to wait between HTTP requests before the CIMC times out and terminates the session. Enter an integer between 60 and 10,800. The default is 1,800 seconds.
Max Sessions field	The maximum number of concurrent HTTP and HTTPS sessions allowed on the CIMC. This value may not be changed.
Active Sessions field	The number of HTTP and HTTPS sessions currently running on the CIMC.

Step 5 Click **Save Changes**.

Configuring SSH

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.
Step 2 On the **Admin** tab, click **Communications Services**.
Step 3 In the **Communications Services** pane, click the **Communication Services** tab.
Step 4 In the **SSH Properties** area, update the following properties:

Name	Description
SSH Enabled check box	Whether SSH is enabled on the CIMC.
SSH Port field	The port to use for secure shell access. The default is 22.
SSH Timeout field	The number of seconds to wait before the system considers an SSH request to have timed out. Enter an integer between 60 and 10,800. The default is 1,800 seconds.
Max Sessions field	The maximum number of concurrent SSH sessions allowed on the CIMC. This value may not be changed.

Name	Description
Active Sessions field	The number of SSH sessions currently running on the CIMC.

Step 5 Click **Save Changes**.

Configuring XML API

XML API for CIMC

The Cisco CIMC XML application programming interface (API) is a programmatic interface to CIMC for a C-Series Rack-Mount Server. The API accepts XML documents through HTTP or HTTPS.

For detailed information about the XML API, see *Cisco UCS Rack-Mount Servers CIMC XML API Programmer's Guide*.

Enabling the XML API

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Communications Services**.

Step 3 In the **Communications Services** pane, click the **Communication Services** tab.

Step 4 In the **XML API Properties** area, update the following properties:

Name	Description
XML API Enabled check box	Whether API access is allowed on this server.
Max Sessions field	The maximum number of concurrent API sessions allowed on the CIMC. This value may not be changed.
Active Sessions field	The number of API sessions currently running on the CIMC.

Step 5 Click **Save Changes**.

Configuring IPMI

IPMI Over LAN

Intelligent Platform Management Interface (IPMI) defines the protocols for interfacing with a service processor embedded in a server platform. This service processor is called a Baseboard Management Controller (BMC) and resides on the server motherboard. The BMC links to a main processor and other on-board elements using a simple serial bus.

During normal operations, IPMI lets a server operating system obtain information about system health and control system hardware. For example, IPMI enables the monitoring of sensors, such as temperature, fan speeds and voltages, for proactive problem detection. If server temperature rises above specified levels, the server operating system can direct the BMC to increase fan speed or reduce processor speed to address the problem.

Configuring IPMI over LAN

Configure IPMI over LAN when you want to manage the CIMC with IPMI messages.

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Communications Services**.

Step 3 In the **Communications Services** pane, click the **Communication Services** tab.

Step 4 In the **IPMI over LAN Properties** area, update the following properties:

Name	Description
Enabled check box	Whether IPMI access is allowed on this server.

Name	Description
Privilege Level Limit drop-down list	The highest privilege level that can be assigned to an IPMI session on this server. This can be one of the following: • **read-only—**IPMI users can view information but cannot make any changes. If you select this option, IPMI users with the "Administrator", "Operator", or "User" user roles can only create read-only IPMI sessions, regardless of their other IPMI privileges. • **user—**IPMI users can perform some functions but cannot perform administrative tasks. If you select this option, IPMI users with the "Administrator" or "Operator" user role can create user and read-only sessions on this server. • **admin—**IPMI users can perform all available actions. If you select this option, IPMI users with the "Administrator" user role can create admin, user, and read-only sessions on this server.
Encryption Key field	The IPMI encryption key to use for IPMI communications.

Step 5 Click **Save Changes**.

Configuring SNMP

SNMP

The Cisco UCS C-Series Rack-Mount Servers support the Simple Network Management Protocol (SNMP) for viewing server configuration and status and for sending fault and alert information by SNMP traps. For information on Management Information Base (MIB) files supported by CIMC, see the *MIB Quick Reference for Cisco UCS* at this URL: http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/mib/reference/UCS_MIBRef.html.

Configuring SNMP Properties

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Communications Services**.

Step 3 In the **Communications Services** pane, click the **SNMP** tab.

Step 4 In the **SNMP Properties** area, update the following properties:

Name	Description
SNMP Enabled check box	Whether this server sends SNMP traps to the designated host. **Note** After you check this check box, you need to click **Save Changes** before you can configure SNMP users or traps.
SNMP Port field	The port the server uses to communicate with the SNMP host. This value cannot be changed.
Access Community String field	The default SNMP v1 or v2c community name or SNMP v3 username CIMC includes on any trap messages it sends to the SNMP host. Enter a string up to 18 characters.
SNMP Community Access drop-down list	This can be one of the following: • **Disabled —** This option blocks access to the information in the inventory tables. • **Limited —** This option provides partial access to read the information in the inventory tables. • **Full —** This option provides full access to read the information in the inventory tables.
Trap Community String field	The name of the SNMP community group to which trap information should be sent. Enter a string up to 18 characters.
System Contact field	The system contact person responsible for the SNMP implementation. Enter a string up to 64 characters, such as an email address or a name and telephone number.
System Location field	The location of the host on which the SNMP agent (server) runs. Enter a string up to 64 characters.

Step 5 Click **Save Changes**.

What to Do Next

Configure SNMP trap settings as described in Configuring SNMP Trap Settings, on page 155.

Configuring SNMP Trap Settings

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Communications Services**.

Step 3 In the **Communications Services** pane, click the **SNMP** tab.

Step 4 Click on **Trap Destinations** tab.

Step 5 In the **Trap Destinations** area, you can perform one of the following:

- Select an existing user from the table and click **Modify**.
- Click **Add** to create a new user.

Note If the fields are not highlighted, select **Enabled**.

Step 6 In the **Trap Details** dialog box, complete the following fields:

Name	Description
ID field	The trap destination ID. This value cannot be modified.
Enabled check box	If checked, then this trap is active on the server.
SNMP Version drop-down list	The SNMP version and model used for the trap. This can be one of the following: • **V1** • **V2** • **V3**
Trap Type radio button	If you select **V2** for the version, this is the type of trap to send. This can be one of the following: • **Trap**: If this option is chosen, the trap will be sent to the destination but you do not receive any notifications. • **Inform**: When this option is chosen, you will receive a notification when a trap is received at the destination.

Name	Description
User drop-down list	The drop-down list displays all available users, select a user from the list.
Destination IP field	The IP address to which SNMP trap information is sent.

Step 7 Click **Save Changes**.

Step 8 If you want to delete a trap destination, select the row and click **Delete**.
Click **OK** in the delete confirmation prompt.

Sending a Test SNMP Trap Message

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Communications Services**.

Step 3 Click the **SNMP** tab, and then click on the **Trap Destinations** tab.

Step 4 In the **Trap Destinations** area, select the row of the desired SNMP trap destination.

Step 5 Click **Send SNMP Test Trap**.
An SNMP test trap message is sent to the trap destination.

Note The trap must be configured and enabled in order to send a test message.

Managing SNMPv3 Users

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Communications Services**.

Step 3 In the **Communications Services** pane, click the **SNMP** tab.

Step 4 In the **SNMPV3 Users** area, update the following properties:

Name	Description
Add button	Click an available row in the table then click this button to add a new SNMP user.
Modify button	Select the user you want to change in the table then click this button to modify the selected SNMP user.
Delete button	Select the user you want to delete in the table then click this button to delete the selected SNMP user.
ID column	The system-assigned identifier for the SNMP user.
Name column	The SNMP user name.
Auth Type column	The user authentication type.
Privacy Type column	The user privacy type.

Step 5 Click **Save Changes**.

Configuring SNMPv3 Users

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Communications Services**.

Step 3 In the **Communications Services** pane, click the **SNMP** tab.

Step 4 In the **Users** area, perform one of the following actions:

- Select an existing user from the table and click **Modify**.
- Select a row in the **Users** area and click **Add** to create a new user.

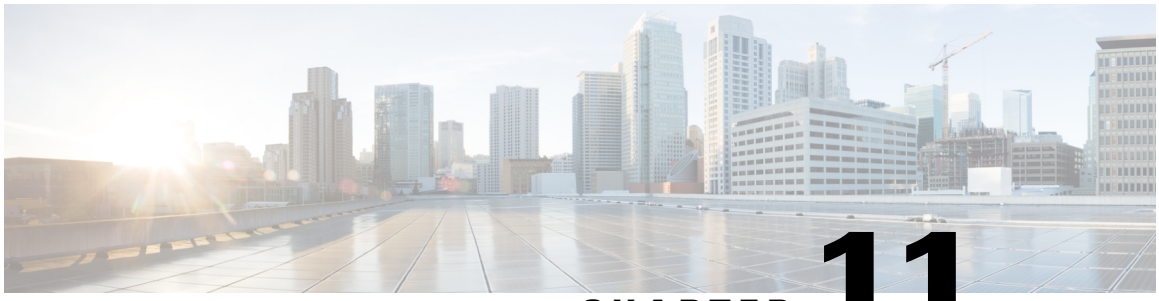
Step 5 In the **SNMP User Details** dialog box, update the following properties:

Name	Description
ID field	The unique identifier for the user. This field cannot be changed.
Name field	The SNMP username. Enter between 1 and 31 characters or spaces. **Note** CIMC automatically trims leading or trailing spaces.
Security Level drop-down list	The security level for this user. This can be one of the following: • **no auth, no priv—**The user does not require an authorization or privacy password. • **auth, no priv—**The user requires an authorization password but not a privacy password. If you select this option, CIMC enables the Auth fields described below. • **auth, priv—**The user requires both an authorization password and a privacy password. If you select this option, CIMC enables the Auth and Privacy fields.
Auth Type radio button	The authorization type. This can be one of the following: • **MD5** • **SHA**
Auth Password field	The authorization password for this SNMP user. Enter between 8 and 64 characters or spaces. **Note** CIMC automatically trims leading or trailing spaces.
Confirm Auth Password field	The authorization password again for confirmation purposes.
Privacy Type radio button	The privacy type. This can be one of the following: • **DES** • **AES**
Privacy Password field	The privacy password for this SNMP user. Enter between 8 and 64 characters or spaces. **Note** CIMC automatically trims leading or trailing spaces.

Name	Description
Confirm Privacy Password field	The authorization password again for confirmation purposes.

Step 6 Click **Save Changes**.

Step 7 If you want to delete a user, select the user and click **Delete**.
Click **OK** in the delete confirmation prompt.



CHAPTER 11

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 CIMC to replace the current server certificate. The server certificate may be signed either by a public Certificate Authority (CA), such as Verisign, or by your own certificate authority.

Procedure

Step 1 Generate the CSR from the CIMC.

Step 2 Submit the CSR file to a certificate authority that will issue and sign your certificate. If your organization generates its own self-signed certificates, you can use the CSR file to generate a self-signed certificate.

Step 3 Upload the new certificate to the CIMC.

Note The uploaded certificate must be created from a CSR generated by the CIMC. Do not upload a certificate that was not created by this method.

Generating a Certificate Signing Request

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Certificate Management**.

Step 3 In the **Actions** area, click the **Generate New Certificate Signing Request** link.
The **Generate New Certificate Signing Request** dialog box appears.

Step 4 In the **Generate New Certificate Signing Request** dialog box, update the following properties:

Name	Description
Common Name field	The fully qualified name of the CIMC. By default the CN of the servers appears in CXXX-YYYYYY format. Where XXX is the model number and YYYYYY is the serial number of the server. When you upgrade to latest version, CN is retained as is.
Organization Name field	The organization requesting the certificate.
Organization Unit field	The organizational unit.
Locality field	The city or town in which the company requesting the certificate is headquartered.
State Name field	The state or province in which the company requesting the certificate is headquartered.
Country Code drop-down list	The country in which the company resides.
Email field	The email contact at the company.

Step 5 Click **Generate CSR**.
The **Opening csr.txt** dialog box appears.

Step 6 Perform any one of the following steps to manage the CSR file, csr.txt:

a) Click **Open With** to view csr.txt.

b) Click **Save File** and then click **OK** to save csr.txt to your local machine.

What to Do Next

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.

Creating a Self-Signed Certificate

As an alternative to using a public Certificate Authority (CA) to generate and sign a server certificate, you can operate your own CA and sign your own certificates. This section shows commands for creating a CA and generating a server certificate using the OpenSSL certificate server running on Linux. For detailed information about OpenSSL, see http://www.openssl.org.

Note These commands are to be entered on a Linux server with the OpenSSL package, not in the CIMC CLI.

Before You Begin

Obtain and install a certificate server software package on a server within your organization.

Procedure

	Command or Action	Purpose
Step 1	**openssl genrsa -out** *CA_keyfilename keysize* **Example:** `# openssl genrsa -out ca.key 1024`	This command generates an RSA private key that will be used by the CA. **Note** To allow the CA to access the key without user input, do not use the -des3 option for this command. The specified file name contains an RSA key of the specified key size.
Step 2	**openssl req -new -x509 -days** *numdays* **-key** *CA_keyfilename* **-out** *CA_certfilename* **Example:** `# openssl req -new -x509 -days 365 -key ca.key -out ca.crt`	This command generates a new self-signed certificate for the CA using the specified key. The certificate is valid for the specified period. The command prompts the user for additional certificate information. The certificate server is an active CA.
Step 3	**echo "nsCertType = server" > openssl.conf** **Example:** `# echo "nsCertType = server" > openssl.conf`	This command adds a line to the OpenSSL configuration file to designate the certificate as a server-only certificate. This designation is a defense against a man-in-the-middle attack, in which an authorized client attempts to impersonate the server. The OpenSSL configuration file openssl.conf contains the statement "nsCertType = server".
Step 4	**openssl x509 -req -days** *numdays* **-in** *CSR_filename* **-CA** *CA_certfilename* **-set_serial 04 -CAkey** *CA_keyfilename* **-out** *server_certfilename* **-extfile openssl.conf** **Example:** `# openssl x509 -req -days 365 -in csr.txt -CA ca.crt -set_serial 04 -CAkey ca.key -out myserver05.crt -extfile openssl.conf`	This command directs the CA to use your CSR file to generate a server certificate. Your server certificate is contained in the output file.

This example shows how to create a CA and to generate a server certificate signed by the new CA. These commands are entered on a Linux server running OpenSSL.

```
# /usr/bin/openssl genrsa -out ca.key 1024
Generating RSA private key, 1024 bit long modulus
.............++++++
.....++++++
e is 65537 (0x10001)
# /usr/bin/openssl req -new -x509 -days 365 -key ca.key -out ca.crt
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:US
State or Province Name (full name) [Berkshire]:California
Locality Name (eg, city) [Newbury]:San Jose
Organization Name (eg, company) [My Company Ltd]:Example Incorporated
Organizational Unit Name (eg, section) []:Unit A
Common Name (eg, your name or your server's hostname) []:example.com
Email Address []:admin@example.com
# echo "nsCertType = server" > openssl.conf
# /usr/bin/openssl x509 -req -days 365 -in csr.txt -CA ca.crt -set_serial 01 -CAkey ca.key -out server.crt
-extfile openssl.conf
Signature ok
subject=/C=US/ST=California/L=San Jose/O=Example Inc./OU=Unit
A/CN=example.com/emailAddress=john@example.com
Getting CA Private Key
#
```

What to Do Next

Upload the new certificate to the CIMC.

Uploading a Server Certificate

Before You Begin

You must log in as a user with admin privileges to upload a certificate.

The certificate file to be uploaded must reside on a locally accessible file system.

Note You must first generate a CSR using the CIMC Certificate Management menu, and you must use that CSR to obtain the certificate for uploading. Do not upload a certificate that was not obtained by this method.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

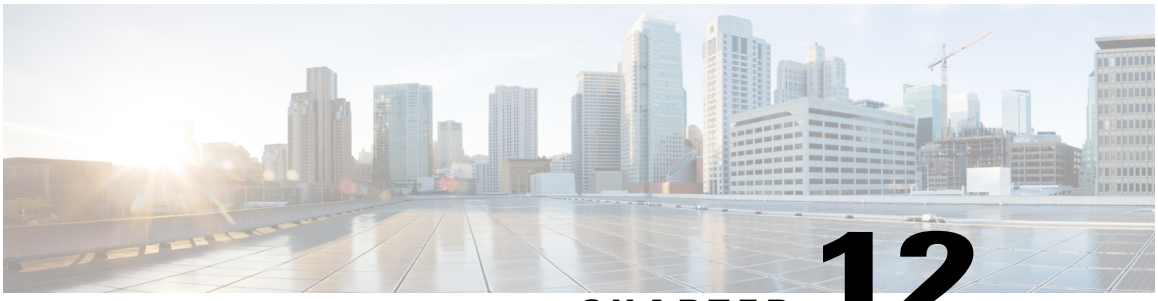
Step 2 On the **Admin** tab, click **Certificate Management**.

Step 3 In the **Actions** area, click **Upload Server Certificate**.
The **Upload Certificate** dialog box appears.

Step 4 In the **Upload Certificate** dialog box, update the following properties:

Name	Description
File field	The certificate file you want to upload.
Browse button	Opens a dialog box that allows you to navigate to the appropriate certificate file.

Step 5 Click **Upload Certificate**.



CHAPTER 12

Configuring Platform Event Filters

This chapter includes the following sections:

Platform Event Filters

A platform event filter (PEF) can trigger an action and generate an alert when a critical hardware-related event occurs. For each PEF, you can choose the action to be taken (or take no action) when a platform event occurs. You can also choose to generate and send an alert when a platform event occurs. Alerts are sent as an SNMP trap, so you must configure an SNMP trap destination before the alerts can be sent.

You can globally enable or disable the generation of platform event alerts. When disabled, alerts are not sent even if PEFs are configured to send them.

Enabling Platform Event Alerts

Before You Begin

You must log in as a user with admin privileges to enable platform event alerts.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.
Step 2 On the **Admin** tab, click **Event Management**.
Step 3 In the **Event Management** pane, click the **Platform Event Filters** tab.
Step 4 In the **Platform Event Properties** area, check the **Enable Platform Event Filters** check box.
Step 5 Click **Save Changes**.

Disabling Platform Event Alerts

Before You Begin

You must log in as a user with admin privileges to disable platform event alerts.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.
Step 2 On the **Admin** tab, click **Event Management**.
Step 3 In the **Event Management** pane, click the **Platform Event Filters** tab.
Step 4 In the **Platform Event Properties** area, uncheck the **Enable Platform Event Filters** check box.
Step 5 Click **Save Changes**.

Configuring Platform Event Filters

Before You Begin

You must log in as a user with admin privileges to configure platform event filters.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.
Step 2 On the **Admin** tab, click **Event Management**.
Step 3 In the **Event Management** pane, click the **Platform Event Filters** tab.
Step 4 In the **Platform Event Filters** area, complete the following fields for each event:

Name	Description
ID column	The unique filter ID.

Name	Description
Event column	The name of the event filter.
Action column	For each filter, select the desired action from the scrolling list box. This can be one of the following: • **None—**No action is taken. • **Reboot—**The server is rebooted. • **Power Cycle—**The server is power cycled. • **Power Off—**The server is powered off.
Send Alert column	For each filter that you want to send an alert, check the associated check box in this column. **Note** In order to send an alert, the filter trap settings must be configured properly and the **Enable Platform Event Filters** check box must also be checked.

Step 5 Click **Save Changes**.

What to Do Next

If you configure any PEFs to send an alert, complete the following task:

- Configuring SNMP Trap Settings, on page 155

Configuring Event Trap Destination

Before You Begin

You must log in as a user with admin privileges to configure platform event filters.

Procedure

	Command or Action	Purpose
Step 1	In the **Navigation** pane, click the **Admin** tab.	
Step 2	On the **Admin** tab, click **Event Management**.	
Step 3	In the **Event Management** pane, click the **Event Trap Destination Settings** tab.	
Step 4	In the **Event Trap Destination** area, select a row and complete the following in the **Destination Settings** dialog box:	**Name** — **Description** **ID** column — The unique filter ID.

	Command or Action	Purpose
		<table><tr><th>Name</th><th>Description</th></tr><tr><td>**Enabled** check box</td><td>If this field is checked, alerts will be sent for the specified filter ID.</td></tr><tr><td>**Destination IP Address** column</td><td>The IP address to which platform event information is sent.</td></tr></table>
Step 5	Click **Save Changes**.	
Step 6	Click **Send Event** to send the platform event to the set destination.	

Interpreting Platform Event Traps

A CIMC platform event alert contains an enterprise object identifier (OID) in the form `1.3.6.1.4.1.3183.1.1.0.event`. The first ten fields of the OID represent the following information: `iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).wired_for_management(3183).PET(1).version(1).version(0)`, indicating an IPMI platform event trap (PET) version 1.0 message. The last field is an event number, indicating the specific condition or alert being notified.

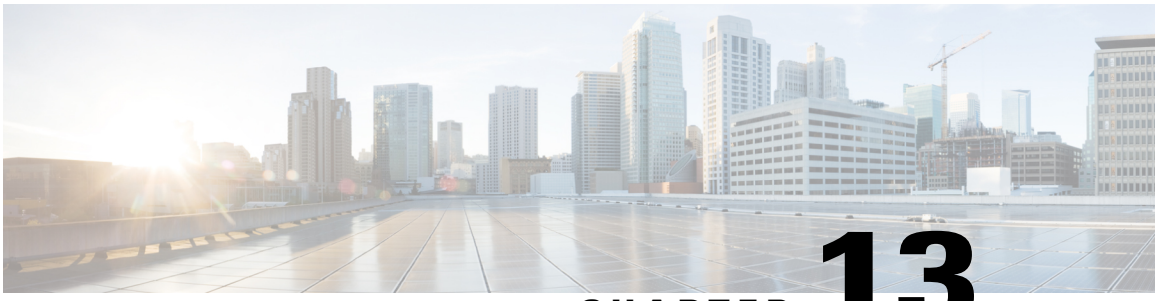
Platform Event Trap Descriptions

The following table provides a description of the event being notified in a platform event trap message, based on the event number in the trap OID.

Event Number [Note 1]		Platform Event Description
0	0h	Test Trap
65799	010107h	Temperature Warning
65801	010109h	Temperature Critical
131330	020102h	Under Voltage, Critical
131337	020109h	Voltage Critical
196871	030107h	Current Warning
262402	040102h	Fan Critical
459776	070400h	Processor related (IOH-Thermalert/Caterr sensor) – predictive failure deasserted

Event Number [Note 1]		Platform Event Description
459777	070401h	Processor related (IOH-Thermalert/Caterr sensor) – predictive failure asserted
460032	070500h	Processor Power Warning – limit not exceeded
460033	070501h	Processor Power Warning – limit exceeded
524533	0800F5h	Power Supply Critical
524551	080107h	Power Supply Warning
525313	080401h	Discrete Power Supply Warning
527105	080B01h	Power Supply Redundancy Lost
527106	080B02h	Power Supply Redundancy Restored
552704	086F00h	Power Supply Inserted
552705	086F01h	Power Supply Failure
552707	086F03h	Power Supply AC Lost
786433	0C0001h	Correctable ECC Memory Errors, Release 1.3(1) and later releases, filter set to accept all reading types [Note 4]
786439	0C0007h	DDR3_INFO sensor LED - RED bit asserted (Probable ECC error on a DIMM), Generic Sensor [Notes 2,3]
786689	0C0101h	Correctable ECC Memory Errors, Release 1.3(1) and later releases
818945	0C7F01h	Correctable ECC Memory Errors, Release 1.2(x) and earlier releases
818951	0C7F07h	DDR3_INFO sensor LED - RED bit asserted (Probable ECC error on a DIMM), 1.2(x) and earlier releases [Note 3]
851968	0D0000h	HDD sensor indicates no fault, Generic Sensor [Note 2]
851972	0D0004h	HDD sensor indicates a fault, Generic Sensor [Note 2]
854016	0D0800h	HDD Absent, Generic Sensor [Note 2]
854017	0D0801h	HDD Present, Generic Sensor [Note 2]
880384	0D6F00h	HDD Present, no fault indicated
880385	0D6F01h	HDD Fault
880512	0D6F80h	HDD Not Present
880513	0D6F81h	HDD is deasserted but not in a fault state
884480	0D7F00h	Drive Slot LED Off
884481	0D7F01h	Drive Slot LED On
884482	0D7F02h	Drive Slot LED fast blink
884483	0D7F03h	Drive Slot LED slow blink

Event Number [Note 1]		Platform Event Description
884484	0D7F04h	Drive Slot LED green
884485	0D7F05h	Drive Slot LED amber
884486	0D7F01h	Drive Slot LED blue
884487	0D7F01h	Drive Slot LED read
884488	0D7F08h	Drive Slot Online
884489	0D7F09h	Drive Slot Degraded
Note 1: Basic information about the event number format can be found in the *IPMI Platform Event Trap Format Specification v1.0* at this URL: ftp://download.intel.com/design/servers/ipmi/pet100.pdf.		
Note 2: Some platforms and releases use generic sensor implementations, while some use Cisco proprietary sensor implementations.		
Note 3: In Release 1.3(1) and later releases, the ECC sensor no longer activates the LED.		
Note 4: When the event filter is set to accept all reading types, bits 15:8 of the hex event number are masked to 0. For example, event number 786689 (0C0101h) becomes 786433 (0C0001h).		



CHAPTER 13

CIMC Firmware Management

This chapter includes the following sections:

Overview of Firmware

C-Series servers use Cisco-certified firmware specific to the C-Series server model that you are using. You can download new releases of the firmware for all supported server models from Cisco.com.

Caution When you install new BIOS firmware, it must be from the same software release as the CIMC firmware running on the server. Do not install new BIOS firmware until after you have activated the matching CIMC firmware or the server will not boot.

To avoid potential problems, we strongly recommend that you use the Cisco Host Upgrade Utility (HUU), which upgrades the BIOS, CIMC, and other firmware to compatible levels. For detailed information about this utility, see the *Cisco Host Upgrade Utility Guide* for the version of the HUU that goes with the CIMC software release that you want to install. The HUU guides are available at the following URL: http://www.cisco.com/en/US/products/ps10493/products_user_guide_list.html.

If you elect to update the firmware manually, you must update the CIMC firmware first. The CIMC firmware update process is divided into the following stages to minimize the amount of time the server will be offline:

- Installation. During this stage, CIMC installs the selected CIMC firmware in the non-active, or backup, slot on the server.

- Activation. During this stage, CIMC sets the non-active firmware version as active and reboots the server, causing a disruption in service. When the server reboots, the firmware in the new active slot becomes the running version.

After you activate the CIMC firmware, you can update the BIOS firmware. The server must be powered off during the entire BIOS update process, so the process is not divided into stages. Instead, you only need to issue a single command and CIMC installs and updates the BIOS firmware as quickly as possible. Once the CIMC finishes rebooting, the server can be powered on and returned to service.

Note You can either upgrade an older firmware version to a newer one, or downgrade a newer firmware version to an older one.

Obtaining Firmware from Cisco

Procedure

Step 1 Navigate to http://www.cisco.com/.

Step 2 If you are not already logged in, click **Log In** at the top right-hand edge of the page and log in using your Cisco.com credentials.

Step 3 In the menu bar at the top, click **Support**.

Step 4 Click **All Downloads** in the roll down menu.

Step 5 If your server model is listed in the **Recently Used Products** list, click the server name. Otherwise, do the following:

a) In the left-hand box, click **Products**.
b) In the center box, click **Unified Computing and Servers**.
c) In the right-hand box, click **Cisco UCS C-Series Rack-Mount Standalone Server Software**.
d) In the right-hand box, click the server model whose software you want to download.

Step 6 Click the **Unified Computing System (UCS) Server Firmware** link.

Step 7 (Optional) Select a prior release from the menu bar on the left-hand side of the page.

Step 8 Click the **Download** button associated with the Cisco Host Upgrade Utility ISO for the selected release.

Step 9 Click **Accept License Agreement**.

Step 10 Save the ISO file to a local drive.
We recommend you upgrade the CIMC and BIOS firmware on your server using this ISO file, which contains the Cisco Host Upgrade Utility. For detailed information about this utility, see the *Cisco Host Upgrade Utility Guide* for the version of the HUU that goes with the CIMC software release that you want to install. The HUU guides are available at the following URL: http://www.cisco.com/en/US/products/ps10493/products_user_guide_list.html.

Step 11 (Optional) If you plan to upgrade the CIMC and BIOS firmware manually, do the following:

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

For example, C240M3_1.4.4A.ZIP.

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

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

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

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

For example, 1.4.4a/cimc/c240-m3-cimc.1.4.4a.zip.

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

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

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

Step 12 (Optional) If you plan to install the firmware from a remote server, copy the BIOS installation CAP file and the CIMC installation BIN file to the remote server you want to use.
The remote server can be one of the following:

- TFTP
- FTP
- SFTP
- SCP
- HTTP

The server must have read permission for the destination folder on the remote server.

What to Do Next

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

Installing CIMC Firmware from a Remote Server

Before You Begin

- Log in to the CIMC GUI 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 174.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Firmware Management**.

Step 3 In the **Actions** area, click **Install CIMC Firmware from Remote Server**.

Step 4 In the **Install CIMC Firmware** dialog box, complete the following fields:

Name	Description
Install CIMC Firmware from drop-down list	The remote server type. This can be one of the following: • **TFTP Server** • **FTP Server** • **SFTP Server** • **SCP Server** • **HTTP Server**
Server IP/Hostname field	The IP address or hostname of the server on which the CIMC firmware installation file resides. Depending on the setting in the **Install CIMC Firmware from** drop-down list, the name of the field may vary.
Image Path and Filename field	The path and filename of the CIMC firmware installation file on the remote server.
Username	The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP.
Password	The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP.

Step 5 Click **Install Firmware**.

What to Do Next

Activate the CIMC firmware.

Installing CIMC Firmware Through the Browser

Before You Begin

- Log in to the CIMC GUI 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 174.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Firmware Management**.

Step 3 In the **Actions** area, click **Install CIMC Firmware through Browser Client**.

Step 4 In the **Install Firmware** dialog box, click **Browse** and use the **Choose File** dialog box to select the .bin file you want to install.

Step 5 Click **Install Firmware**.

What to Do Next

Activate the CIMC firmware.

Activating Installed CIMC Firmware

Before You Begin

Install the CIMC firmware on the server.

Important While the activation is in progress, do not:

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

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Firmware Management**.

Step 3 In the **Actions** area, click **Activate CIMC Firmware**.

The **Activate Firmware** dialog box appears.

Step 4 In the **Activate Firmware** dialog box, choose the firmware image to activate.

Step 5 Click **Activate Firmware**.

Installing BIOS Firmware from a Remote Server

Note This procedure is not available on some servers. For other BIOS installation methods, see the *Cisco UCS C-Series Rack-Mount Server BIOS Upgrade Guide* available at the following URL: http://www.cisco.com/en/US/docs/unified_computing/ucs/c/sw/bios/b_Upgrading_BIOS_Firmware.html.

Before You Begin

- Log in to the CIMC GUI as a user with admin privileges.
- Activate the CIMC firmware that goes with the BIOS version you want to install, as described in Activating Installed CIMC Firmware, on page 177.
- Power off the server.

Caution When you install new BIOS firmware, it must be from the same software release as the CIMC firmware running on the server. Do not install new BIOS firmware until after you have activated the matching CIMC firmware or the server will not boot.

To avoid potential problems, we strongly recommend that you use the Cisco Host Upgrade Utility (HUU), which upgrades the BIOS, CIMC, and other firmware to compatible levels. For detailed information about this utility, see the *Cisco Host Upgrade Utility Guide* for the version of the HUU that goes with the CIMC software release that you want to install. The HUU guides are available at the following URL: http://www.cisco.com/en/US/products/ps10493/products_user_guide_list.html.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Summary**.

Step 3 In the **Server Status** area, verify that the **Power State** field says "Off". If it says "On", click **Power Off Server** in the **Actions** area and wait for the server to power off before continuing.

Step 4 In the **Navigation** pane, click the **Admin** tab.

Step 5 On the **Admin** tab, click **Firmware Management**.

Step 6 In the **CIMC Firmware** area, make sure the firmware version shown in the **Running Version** field matches the BIOS firmware version you are installing.

Important If the CIMC firmware version does not match, activate the CIMC firmware before continuing with this procedure or the server will not boot. For details, see Activating Installed CIMC Firmware, on page 177.

Step 7 In the **Actions** area, click **Install BIOS Firmware from Remote Server**.

Step 8 In the **Install BIOS Firmware** dialog box, complete the following fields:

Name	Description
Install BIOS Firmware from drop-down list	The remote server type. This can be one of the following: • **TFTP Server** • **FTP Server** • **SFTP Server** • **SCP Server** • **HTTP Server**
Server IP/Hostname field	The IP address or hostname of the server on which the BIOS firmware installation file resides. Depending on the setting in the **Install BIOS Firmware from** drop-down list, the name of the field may vary.
Image Path and Filename field	The path and filename of the BIOS firmware installation file on the remote server.
Username	The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP.
Password	The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP.

Step 9 Click **Install Firmware**.

Step 10 Watch the messages in the **Status** field in the **Last BIOS Firmware Install** area until the status changes to "Completed Successfully".

Step 11 Power on the server to complete the BIOS upgrade.

Installing BIOS Firmware Through the Browser

Note This procedure is not available on some servers. For other BIOS installation methods, see the *Cisco UCS C-Series Rack-Mount Server BIOS Upgrade Guide* available at the following URL: http://www.cisco.com/en/US/docs/unified_computing/ucs/c/sw/bios/b_Upgrading_BIOS_Firmware.html.

Before You Begin

- Log in to the CIMC GUI as a user with admin privileges.

- Activate the CIMC firmware that goes with the BIOS version you want to install, as described in Activating Installed CIMC Firmware, on page 177.
- Power off the server.

Caution When you install new BIOS firmware, it must be from the same software release as the CIMC firmware running on the server. Do not install new BIOS firmware until after you have activated the matching CIMC firmware or the server will not boot.

To avoid potential problems, we strongly recommend that you use the Cisco Host Upgrade Utility (HUU), which upgrades the BIOS, CIMC, and other firmware to compatible levels. For detailed information about this utility, see the *Cisco Host Upgrade Utility Guide* for the version of the HUU that goes with the CIMC software release that you want to install. The HUU guides are available at the following URL: http://www.cisco.com/en/US/products/ps10493/products_user_guide_list.html.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Summary**.

Step 3 In the **Server Status** area, verify that the **Power State** field says "Off". If it says "On", click **Power Off Server** in the **Actions** area and wait for the server to power off before continuing.

Step 4 In the **Navigation** pane, click the **Admin** tab.

Step 5 On the **Admin** tab, click **Firmware Management**.

Step 6 In the **CIMC Firmware** area, make sure the firmware version shown in the **Running Version** field matches the BIOS firmware version you are installing.

Important If the CIMC firmware version does not match, activate the CIMC firmware before continuing with this procedure or the server will not boot. For details, see Activating Installed CIMC Firmware, on page 177.

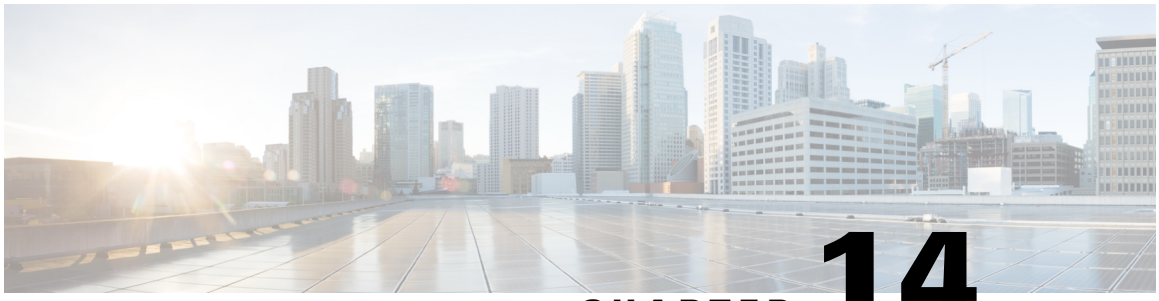
Step 7 In the **Actions** area, click **Install BIOS Firmware through Browser Client**.

Step 8 In the **Install BIOS Firmware** dialog box, click **Browse** and use the **Choose File** dialog box to select the CAP file you want to install.

Step 9 Click **Install Firmware**.

Step 10 Watch the messages in the **Status** field in the **Last BIOS Firmware Install** area until the status changes to "Completed Successfully".

Step 11 Power on the server to complete the BIOS upgrade.



CHAPTER 14

Viewing Faults and Logs

This chapter includes the following sections:

Faults Summary

Viewing the Fault Summary

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Faults and Logs**.

Step 3 In the **Faults Summary** tab, review the following information:

Name	Description
Time	The time when the fault occurred.
Severity	This can be one of the following: • **Cleared** - A fault or condition was cleared. • **Critical** • **Info** • **Major** • **Minor** • **Warning**

Name	Description
Code	The unique identifier assigned to the fault.
DN	The distinguished name (DN) is a hierarchical representation of the device endpoint and its instance on the server.
Probable Cause	The unique identifier associated with the event that caused the fault.
Description	More information about the fault. It also includes a proposed solution.

CIMC Log

Viewing the CIMC Log

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Faults and Logs**.

Step 3 In the **Faults and Logs** window, click **CIMC Log**.

Step 4 Review the following information for each CIMC event in the log.

Name	Description
Time column	The date and time the event occurred.

Name	Description
Severity column	The event severity. This can be one of the following: • **Emergency** • **Alert** • **Critical** • **Error** • **Warning** • **Notice** • **Informational** • **Debug**
Source column	The software module that logged the event.
Description column	A description of the event.
Clear Log button	Clears all events from the log file. **Note** This option is only available if your user ID is assigned the **admin** or **user** user role.

Step 5 From the **Entries Per Page** drop-down list, select the number of CIMC events to display on each page.

Step 6 Click **<Newer** and **Older>** to move backward and forward through the pages of CIMC events, or click **<<Newest** to move to the top of the list.
By default, the newest CIMC events are displayed at the top if the list.

Clearing the CIMC Log

Before You Begin

You must log in as a user with user privileges to clear the CIMC log.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Faults and Logs**.

Step 3 In the **Faults and Logs** pane, click **CIMC Log**.

Step 4 In the **CIMC Log** pane, click **Clear Log**.

Step 5 In the dialog box that appears, click **OK**.

Configuring the CIMC Log Threshold

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

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Faults and Logs**.

Step 3 In the **Faults and Logs** pane, click the **Logging Controls** tab.

Step 4 In the **Local Logging** area, use the **Minimum Severity to Report** drop-down list to specify the lowest level of messages that will be included in the CIMC log.
You can select one of the following, in decreasing order of severity:

- **Emergency**
- **Alert**
- **Critical**
- **Error**
- **Warning**
- **Notice**
- **Informational**
- **Debug**

Note CIMC does not log any messages with a severity below the selected severity. For example, if you select **Error**, then the CIMC log will contain all messages with the severity Emergency, Alert, Critical, or Error. It will not show Warning, Notice, Informational, or Debug messages.

Sending the CIMC Log to a Remote Server

You can configure profiles for one or two remote syslog servers to receive CIMC log entries.

Before You Begin

- The remote syslog server must be configured to receive logs from a remote host.
- The remote syslog server must be configured to receive all types of logs, including authentication-related logs.
- The remote syslog server's firewall must be configured to allow syslog messages to reach the syslog server.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Faults and Logs**.

Step 3 In the **Faults and Logs** pane, click the **Logging Controls** tab.

Step 4 In either of the **Remote Syslog Server** areas, complete the following fields:

Name	Description
Enabled check box	If checked, CIMC sends log messages to the Syslog server named in the **IP Address** field.
IP Address field	The IP address of the Syslog server on which the CIMC log should be stored.

Step 5 (Optional) In the **Minimum Severity to Report** drop-down list, specify the lowest level of messages that will be included in the remote logs.
You can select one of the following, in decreasing order of severity:

- **Emergency**
- **Alert**
- **Critical**
- **Error**
- **Warning**
- **Notice**
- **Informational**
- **Debug**

Note CIMC does not remotely log any messages with a severity below the selected severity. For example, if you select **Error**, then the CIMC remote log will contain all messages with the severity Emergency, Alert, Critical, or Error. It will not show Warning, Notice, Informational, or Debug messages.

Step 6 Click **Save Changes**.

System Event Log

Viewing the System Event Log

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Faults and Logs**.

Step 3 In the **Faults and Logs** window, click **System Event Log**.

Step 4 Above the log table, view the percentage bar, which indicates how full the log buffer is.

Step 5 Review the following information for each system event in the log:

Name	Description
Time column	The date and time the event occurred.
Severity column	The severity field includes both text and a color-coded icon. For the icon, green indicates normal operation, yellow is informational, and warning, critical, and non-recoverable errors are shown in shades of red.
Description column	A description of the event.
Clear Log button	Clears all events from the log file. **Note** This option is only available if your user ID is assigned the **admin** or **user** user role.

Step 6 From the **Entries Per Page** drop-down list, select the number of system events to display on each page.

Step 7 Click **<Newer** and **Older>** to move backward and forward through the pages of system events, or click **<<Newest** to move to the top of the list.
By default, the newest system events are displayed at the top if the list.

Clearing the System Event Log

Before You Begin

You must log in as a user with user privileges to clear the system event log.

Procedure

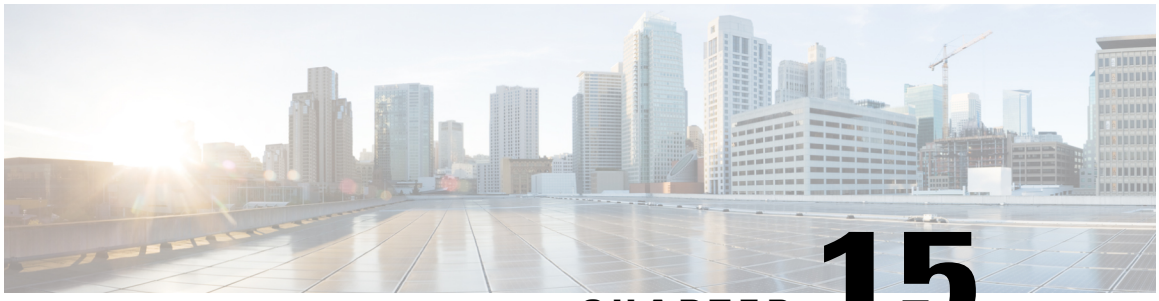
Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Faults and Logs**.

Step 3 In the **Faults and Logs** window, click **System Event Log**.

Step 4 In the **System Event Log** pane, click **Clear Log**.

Step 5 In the dialog box that appears, click **OK**.



CHAPTER 15

Server Utilities

This chapter includes the following sections:

Exporting Technical Support Data

Exporting Technical Support Data to a Remote Server

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.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Utilities**.

Step 3 In the **Actions** area of the **Utilities** pane, click **Export Technical Support Data to Remote Server**.

Step 4 In the **Export Technical Support Data** dialog box, complete the following fields:

Name	Description
Export Technical Support Data to drop-down list	The remote server type. This can be one of the following: • **TFTP Server** • **FTP Server** • **SFTP Server** • **SCP Server** • **HTTP Server**
Server IP/Hostname field	The IP address or hostname of the server on which the support data file should be stored. Depending on the setting in the **Export Technical Support Data to** drop-down list, the name of the field may vary.
Path and Filename field	The path and filename CIMC should use when exporting the file to the remote server. **Note** If the server includes one of the supported network adapter cards, such as the Cisco UCS P81E Virtual Interface Card, the data file also includes technical support data from the adapter card.
Username	The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP.
Password	The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP.

Step 5 Click **Export**.

What to Do Next

Provide the generated report file to Cisco TAC.

Downloading Technical Support Data to a Local File

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.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Utilities**.

Step 3 In the **Actions** area of the **Utilities** pane, click **Generate Technical Support Data for Local Download**.

Step 4 In the **Download Technical Support Data to Local File** dialog box, complete the following fields:

Name	Description
Generate Technical Support Data radio button	CIMC displays this radio button when there is no technical support data file to download. Click **Generate** to create the data file. When data collection is complete, click **Download Technical Support Data to Local File** in the **Actions** area to download the file.
Regenerate Technical Support Data radio button	CIMC displays this radio button when a technical support data file is available to download. To replace the existing support data file with a new one, select this option and click **Regenerate**. When data collection is complete, click **Download Technical Support Data to Local File** in the **Actions** area to download the file.
Download to local file radio button	CIMC enables this radio button when a technical support data file is available to download. To download the existing file, select this option and click **Download**. **Note** If the server includes one of the supported network adapter cards, such as the Cisco UCS P81E Virtual Interface Card, the data file also includes technical support data from the adapter card.

What to Do Next

Provide the generated report file to Cisco TAC.

Rebooting CIMC

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

Note If you reboot the CIMC while the server is performing power-on self test (POST) or is operating in the Extensible Firmware Interface (EFI) shell, the server will be powered down until the CIMC reboot is complete.

Before You Begin

You must log in as a user with admin privileges to reboot the CIMC.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.
Step 2 On the **Admin** tab, click **Utilities**.
Step 3 In the **Actions** area of the **Utilities** pane, click **Reboot CIMC**.
Step 4 Click **OK**.

Recovering from a Corrupted BIOS

Note This procedure is not available in some server models.

In addition to this procedure, there are three other methods for recovering from a corrupted BIOS:

- Use the Cisco Host Upgrade Utility (HUU). This is the recommended method.
- Use the CIMC CLI interface.
- If your server model supports it, use the BIOS recovery function of the hardware jumper on the server motherboard. For instructions, see the Cisco UCS Server Installation and Service Guide for your server model.

Before You Begin

- You must be logged in as admin to recover corrupt BIOS.
- Have the BIOS recovery ISO image ready. You will find the BIOS recovery ISO image under the **Recovery** folder of the firmware distribution package.
- Schedule some down time for the server because it will be powered cycled at the end of the recovery procedure.

Procedure

Step 1 In the **Navigation** pane, click the **Server** tab.
Step 2 On the server tab, click **BIOS**.

The BIOS page appears.

Step 3 In the **Actions** area, click **Recover Corrupt BIOS**.
The **Recover Corrupt BIOS** wizard appears.

Step 4 Use the **Recover Corrupt BIOS** wizard to recover your corrupt BIOS.

Resetting CIMC to Factory Defaults

On rare occasions, such as an issue with the current running firmware, troubleshooting a server may require you to reset the CIMC to the factory default. When this happens, all user-configurable settings are reset.

This procedure is not part of the normal server maintenance. After you reset the CIMC, you are logged off and must log in again. You may also lose connectivity and may need to reconfigure the network settings.

When you upgrade from version 1.5(1) to version 1.5(2), the hostname in the CIMC interface is retained as is. However, after upgrading to version 1.5(2), if you do a factory reset, the hostname changes to CXXX-YYYYYY format, where XXX is the model number and YYYYYY is the serial number of the server.

When you downgrade from version 1.5(2) to version 1.5(1), the hostname is retained as is. However, if you do a factory reset, the hostname changes to ucs-cxx-mx format.

Before You Begin

You must log in as a user with admin privileges to reset the CIMC to factory defaults.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Utilities**.

Step 3 In the **Actions** area of the **Utilities** pane, click **Reset CIMC to Factory Default Configuration**.

Step 4 Click **OK**.
A reboot of CIMC while the host is performing BIOS POST (Power on Self Test) or is in EFI shell will turn off the host for a short amount of time. CIMC will power on when it is ready.

Exporting and Importing the CIMC Configuration

Exporting and Importing the CIMC Configuration

To perform a backup of the CIMC configuration, you take a snapshot of the system configuration and export the resulting CIMC configuration file to a location on your network. The export operation saves information from the management plane only; it does not back up data on the servers. Sensitive configuration information such as user accounts and the server certificate are not exported.

You can restore an exported CIMC configuration file to the same system or you can import it to another CIMC system, provided that the software version of the importing system is the same as or is configuration-compatible with the software version of the exporting system. When you import a configuration file to another system as a configuration template, you must modify system-specific settings such as IP addresses and host names. An import operation modifies information on the management plane only.

The CIMC configuration file is an XML text file whose structure and elements correspond to the CIMC command modes.

When performing an export or import operation, consider these guidelines:

- You can perform an export or an import while the system is up and running. While an export operation has no impact on the server or network traffic, some modifications caused by an import operation, such as IP address changes, can disrupt traffic or cause a server reboot.
- You cannot execute an export and an import simultaneously.

Exporting the CIMC Configuration

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

Before You Begin

Obtain the backup remote server IP address.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Utilities**.

Step 3 In the **Actions** area of the **Utilities** pane, click **Export CIMC Configuration**.

Step 4 In the **Export CIMC Configuration** dialog box, complete the following fields:

Name	Description
Export to a local file radio button	Select this option and click **Export** to save the XML configuration file to a drive that is local to the computer running the CIMC GUI. When you select this option, CIMC GUI displays a **File Download** dialog box that lets you navigate to the location to which the configuration file should be saved.
Export to Remote server radio button	Select this option to save the XML configuration file to a remote server. When you select this option, CIMC GUI displays the remote server fields.

Name	Description
Export to drop-down list	The remote server type. This can be one of the following: • **TFTP Server** • **FTP Server** • **SFTP Server** • **SCP Server** • **HTTP Server**
Server IP/Hostname field	The IP address or hostname of the server to which the configuration file will be exported. Depending on the setting in the **Export to** drop-down list, the name of the field may vary.
Path and Filename field	The path and filename CIMC should use when exporting the file to the remote server.
Username	The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP.
Password	The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP.

Step 5 Click **Export**.

Importing a CIMC Configuration

Before You Begin

If you want to restore the SNMP configuration information when you import the configuration file, make sure that SNMP is disabled on this server before you do the import. If SNMP is enabled when you perform the import, CIMC does not overwrite the current values with those saved in the configuration file.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.
Step 2 On the **Admin** tab, click **Utilities**.
Step 3 In the **Actions** area of the **Utilities** pane, click **Import CIMC Configuration**.
Step 4 In the **Import CIMC Configuration** dialog box, complete the following fields:

Name	Description
Import from a local file radio button	Select this option and click **Import** to navigate to the XML configuration file stored on a drive that is local to the computer running the CIMC GUI. When you select this option, CIMC GUI displays a **Browse** button that lets you navigate to the file you want to import.
Import from Remote server radio button	Select this option to import the XML configuration file from a remote server. When you select this option, CIMC GUI displays the remote server fields.
Import from drop-down list	The remote server type. This can be one of the following: • **TFTP Server** • **FTP Server** • **SFTP Server** • **SCP Server** • **HTTP Server**
Server IP/Hostname field	The IP address or hostname of the server on which the configuration file resides. Depending on the setting in the **Import from** drop-down list, the name of the field may vary.
Path and Filename field	The path and filename of the configuration file on the remote server.
Username	The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP.
Password	The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP.

Step 5 Click **Import**.

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.

Before You Begin

- You must log in as a user with admin privileges.
- The server must be powered on.

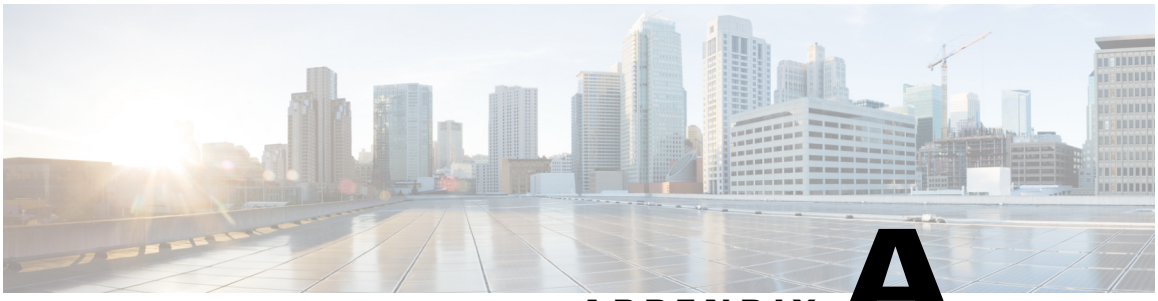
Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Utilities**.

Step 3 In the **Actions** area of the **Utilities** pane, click **Generate NMI to host**.
This action sends an NMI signal to the host, which might restart the OS.

Step 4 Click **OK**.



APPENDIX A

BIOS Parameters by Server Model

This appendix contains the following sections:

C22 and C24 Servers

Main BIOS Parameters for C22 and C24 Servers

Name	Description
TPM Support	TPM (Trusted Platform Module) is a microchip designed to provide basic security-related functions primarily involving encryption keys. This option allows you to control the TPM Security Device support for the system. It can be one of the following: • **Disabled**—The server does not use the TPM. • **Enabled**—The server uses the TPM. **Note** We recommend that you contact your operating system vendor to make sure the operating system supports this feature.

Advanced BIOS Parameters for C22 and C24 Servers

Processor Configuration Parameters

Name	Description
Intel Hyper-Threading Technology	Whether the processor uses Intel Hyper-Threading Technology, which allows multithreaded software applications to execute threads in parallel within each processor. This can be one of the following: • **Disabled—**The processor does not permit hyperthreading. • **Enabled—**The processor allows for the parallel execution of multiple threads. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.
Number of Enabled Cores	Allows you to disable one or more of the physical cores on the server. This can be one of the following: • **All—**Enables all physical cores. This also enables Hyper Threading on the associated logical processor cores. • **1** through ***n*—**Specifies the number of physical processor cores that can run on the server. Each physical core has an associated logical core. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.
Execute Disable	Classifies memory areas on the server to specify where application code can execute. As a result of this classification, the processor disables code execution if a malicious worm attempts to insert code in the buffer. This setting helps to prevent damage, worm propagation, and certain classes of malicious buffer overflow attacks. This can be one of the following: • **Disabled—**The processor does not classify memory areas. • **Enabled—**The processor classifies memory areas. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.

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

Name	Description
CPU Performance	Sets the CPU performance profile for the server. The performance profile consists of the following options: • DCU Streamer Prefetcher • DCU IP Prefetcher • Hardware Prefetcher • Adjacent Cache-Line Prefetch This can be one of the following: • **Enterprise—**All options are enabled. • **High Throughput—**Only the DCU IP Prefetcher is enabled. The rest of the options are disabled. • **HPC—**All options are enabled. This setting is also known as high performance computing. • **Custom—**All performance profile options can be configured from the BIOS setup on the server. In addition, the Hardware Prefetcher and Adjacent Cache-Line Prefetch options can be configured in the fields below.
Hardware Prefetcher	Whether the processor allows the Intel hardware prefetcher to fetch streams of data and instruction from memory into the unified second-level cache when necessary. This can be one of the following: • **Disabled—**The hardware prefetcher is not used. • **Enabled—**The processor uses the hardware prefetcher when cache issues are detected.
Adjacent Cache Line Prefetcher	Whether the processor fetches cache lines in even/odd pairs instead of fetching just the required line. This can be one of the following: • **Disabled—**The processor only fetches the required line. • **Enabled—** The processor fetches both the required line and its paired line.

Name	Description
DCU Streamer Prefetch	Whether the processor uses the DCU IP Prefetch mechanism to analyze historical cache access patterns and preload the most relevant lines in the L1 cache. This can be one of the following: • **Disabled—**The processor does not try to anticipate cache read requirements and only fetches explicitly requested lines. • **Enabled—**The DCU prefetcher analyzes the cache read pattern and prefetches the next line in the cache if it determines that it may be needed.
DCU IP Prefetcher	Whether the processor uses the DCU IP Prefetch mechanism to analyze historical cache access patterns and preload the most relevant lines in the L1 cache. This can be one of the following: • **Disabled—**The processor does not preload any cache data. • **Enabled—**The DCU IP prefetcher preloads the L1 cache with the data it determines to be the most relevant.
Direct Cache Access Support	Allows processors to increase I/O performance by placing data from I/O devices directly into the processor cache. This setting helps to reduce cache misses. This can be one of the following: • **Disabled—**Data from I/O devices is not placed directly into the processor cache. • **Enabled—**Data from I/O devices is placed directly into the processor cache.

Name	Description
Power Technology	Enables you to configure the CPU power management settings for the following options: • Enhanced Intel Speedstep Technology • Intel Turbo Boost Technology • Processor Power State C6 Power Technology can be one of the following: • **Custom—**The server uses the individual settings for the BIOS parameters mentioned above. You must select this option if you want to change any of these BIOS parameters. • **Disabled—**The server does not perform any CPU power management and any settings for the BIOS parameters mentioned above are ignored. • **Energy Efficient—**The server determines the best settings for the BIOS parameters mentioned above and ignores the individual settings for these parameters.
Enhanced Intel Speedstep Technology	Whether the processor uses Enhanced Intel SpeedStep Technology, which allows the system to dynamically adjust processor voltage and core frequency. This technology can result in decreased average power consumption and decreased average heat production. This can be one of the following: • **Disabled—**The processor never dynamically adjusts its voltage or frequency. • **Enabled—**The processor utilizes Enhanced Intel SpeedStep Technology and enables all supported processor sleep states to further conserve power. We recommend that you contact your operating system vendor to make sure the operating system supports this feature. **Note** **Power Technology** must be set to **Custom** or the server ignores the setting for this parameter.

Name	Description
Intel Turbo Boost Technology	Whether the processor uses Intel Turbo Boost Technology, which allows the processor to automatically increase its frequency if it is running below power, temperature, or voltage specifications. This can be one of the following: • **Disabled—**The processor does not increase its frequency automatically. • **Enabled—**The processor utilizes Turbo Boost Technology if required. **Note** **Power Technology** must be set to **Custom** or the server ignores the setting for this parameter.
Processor Power State C6	Whether the BIOS sends the C6 report to the operating system. When the OS receives the report, it can transition the processor into the lower C6 power state to decrease energy usage while maintaining optimal processor performance. This can be one of the following: • **Disabled—**The BIOS does not send the C6 report. • **Enabled—**The BIOS sends the C6 report, allowing the OS to transition the processor to the C6 low power state. **Note** **Power Technology** must be set to **Custom** or the server ignores the setting for this parameter.
Processor Power State C1 Enhanced	Whether the CPU transitions to its minimum frequency when entering the C1 state. This can be one of the following: • **Disabled—**The CPU continues to run at its maximum frequency in C1 state. • **Enabled—**The CPU transitions to its minimum frequency. This option saves the maximum amount of power in C1 state.
Frequency Floor Override	Whether the CPU is allowed to drop below the maximum non-turbo frequency when idle. This can be one of the following: • **Disabled—** The CPU can drop below the maximum non-turbo frequency when idle. This option decreases power consumption but may reduce system performance. • **Enabled—** The CPU cannot drop below the maximum non-turbo frequency when idle. This option improves system performance but may increase power consumption.

Name	Description
P-STATE Coordination	Allows you to define how BIOS communicates the P-state support model to the operating system. There are 3 models as defined by the Advanced Configuration and Power Interface (ACPI) specification. • **HW_ALL—**The processor hardware is responsible for coordinating the P-state among logical processors with dependencies (all logical processors in a package). • **SW_ALL—**The OS Power Manager (OSPM) is responsible for coordinating the P-state among logical processors with dependencies (all logical processors in a physical package), and must initiate the transition on all of the logical processors. • **SW_ANY—**The OS Power Manager (OSPM) is responsible for coordinating the P-state among logical processors with dependencies (all logical processors in a package), and may initiate the transition on any of the logical processors in the domain. **Note** **Power Technology** must be set to **Custom** or the server ignores the setting for this parameter.
Energy Performance	Allows you to determine whether system performance or energy efficiency is more important on this server. This can be one of the following: • **Balanced Energy** • **Balanced Performance** • **Energy Efficient** • **Performance**

Memory Configuration Parameters

Name	Description
Select Memory RAS	How the memory reliability, availability, and serviceability (RAS) is configured for the server. This can be one of the following: • **Maximum Performance—**System performance is optimized. • **Mirroring—**System reliability is optimized by using half the system memory as backup. • **Lockstep—**If the DIMM pairs in the server have an identical type, size, and organization and are populated across the SMI channels, you can enable lockstep mode to minimize memory access latency and provide better performance. This option offers better system performance than Mirroring and better reliability than Maximum Performance but lower reliability than Mirroring and lower system performance than Maximum Performance.
DRAM Clock Throttling	Allows you to tune the system settings between the memory bandwidth and power consumption. This can be one of the following: • **Balanced—** DRAM clock throttling is reduced, providing a balance between performance and power. • **Performance—**DRAM clock throttling is disabled, providing increased memory bandwidth at the cost of additional power. • **Energy Efficient—**DRAM clock throttling is increased to improve energy efficiency.
NUMA	Whether the BIOS supports NUMA. This can be one of the following: • **Disabled—**The BIOS does not support NUMA. • **Enabled—**The BIOS includes the ACPI tables that are required for NUMA-aware operating systems. If you enable this option, the system must disable Inter-Socket Memory interleaving on some platforms.

Name	Description
Low Voltage DDR Mode	Whether the system prioritizes low voltage or high frequency memory operations. This can be one of the following: • **Power Saving Mode—**The system prioritizes low voltage memory operations over high frequency memory operations. This mode may lower memory frequency in order to keep the voltage low. • **Performance Mode—**The system prioritizes high frequency operations over low voltage operations.
DRAM Refresh rate	Allows you to set the rate at which the DRAM cells are refreshed. This can be one of the following: • **1x—**DRAM cells are refreshed every 64ms. • **2x—**DRAM cells are refreshed every 32ms. • **3x—**DRAM cells are refreshed every 21ms. • **4x—**DRAM cells are refreshed every 16ms. • **Auto—**DRAM cells refresh rate is automatically chosen by the BIOS based on the system configuration. This is the recommended setting for this parameter.
Channel Interleaving	Whether the CPU divides memory blocks and spreads contiguous portions of data across interleaved channels to enable simultaneous read operations. This can be one of the following: • **Auto—**The CPU determines what interleaving is done. • **1 Way—**Some channel interleaving is used. • **2 Way** • **3 Way** • **4 Way—**The maximum amount of channel interleaving is used.

Name	Description
Rank Interleaving	Whether the CPU interleaves physical ranks of memory so that one rank can be accessed while another is being refreshed. This can be one of the following: • **Auto—**The CPU determines what interleaving is done. • **1 Way—**Some rank interleaving is used. • **2 Way** • **4 Way** • **8 Way—**The maximum amount of rank interleaving is used.
Patrol Scrub	Whether the system actively searches for, and corrects, single bit memory errors even in unused portions of the memory on the server. This can be one of the following: • **Disabled—**The system checks for memory ECC errors only when the CPU reads or writes a memory address. • **Enabled—**The system periodically reads and writes memory searching for ECC errors. If any errors are found, the system attempts to fix them. This option may correct single bit errors before they become multi-bit errors, but it may adversely affect performance when the patrol scrub is running.
Demand Scrub	Whether the system corrects single bit memory errors encountered when the CPU or I/O makes a demand read. This can be one of the following: • **Disabled—** Single bit memory errors are not corrected. • **Enabled—** Single bit memory errors are corrected in memory and the corrected data is set in response to the demand read.

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

QPI Configuration Parameters

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

Onboard Storage Parameters

Name	Description
Onboard SCU Storage Support	Whether the onboard software RAID controller is available to the server. This can be one of the following: • **Disabled—**The software RAID controller is not available. • **Enabled—**The software RAID controller is available.

USB Configuration Parameters

Name	Description
Legacy USB Support	Whether the system supports legacy USB devices. This can be one of the following: • **Disabled—**USB devices are only available to EFI applications. • **Enabled—**Legacy USB support is always available. • **Auto—**Disables legacy USB support if no USB devices are connected.
Port 60/64 Emulation	Whether the system supports 60h/64h emulation for complete USB keyboard legacy support. This can be one of the following: • **Disabled—**60h/64 emulation is not supported. • **Enabled—**60h/64 emulation is supported. You should select this option if you are using a non-USB aware operating system on the server.
All USB Devices	Whether all physical and virtual USB devices are enabled or disabled. This can be one of the following: • **Disabled—**All USB devices are disabled. • **Enabled—**All USB devices are enabled.
USB Port: Rear	Whether the rear panel USB devices are enabled or disabled. This can be one of the following: • **Disabled—**Disables the rear panel USB ports. Devices connected to these ports are not detected by the BIOS and operating system. • **Enabled—**Enables the rear panel USB ports. Devices connected to these ports are detected by the BIOS and operating system.
USB Port: Front	Whether the front panel USB devices are enabled or disabled. This can be one of the following: • **Disabled—**Disables the front panel USB ports. Devices connected to these ports are not detected by the BIOS and operating system. • **Enabled—**Enables the front panel USB ports. Devices connected to these ports are detected by the BIOS and operating system.

Name	Description
USB Port: Internal	Whether the internal USB devices are enabled or disabled. This can be one of the following: • **Disabled—**Disables the internal USB ports. Devices connected to these ports are not detected by the BIOS and operating system. • **Enabled—**Enables the internal USB ports. Devices connected to these ports are detected by the BIOS and operating system.
USB Port: KVM	Whether the KVM ports are enabled or disabled. This can be one of the following: • **Disabled—**Disables the KVM keyboard and/or mouse devices. Keyboard and/or mouse will not work in the KVM window. • **Enabled—**Enables the KVM keyboard and/or mouse devices.
USB Port: VMedia	Whether the virtual media devices are enabled or disabled. This can be one of the following: • **Disabled—**Disables the vMedia devices. • **Enabled—**Enables the vMedia devices.

PCI Configuration Parameters

Name	Description
MMIO Above 4GB	Whether to enable or disable memory mapped I/O of 64-bit PCI devices to 4GB or greater address space. Legacy option ROMs are not able to access addresses above 4GB. PCI devices that are 64-bit compliant but use a legacy option ROM may not function correctly with this setting enabled. This can be one of the following: • **Disabled—**The server does not map I/O of 64-bit PCI devices to 4GB or greater address space. • **Enabled—**The server maps I/O of 64-bit PCI devices to 4GB or greater address space.
ASPM Support	Allows you to set the level of ASPM (Active Power State Management) support in the BIOS. This can be one of the following: • **Disabled—**ASPM support is disabled in the BIOS. • **Force L0s—**Force all links to L0 standby (L0s) state. • **Auto—**The CPU determines the power state.

Name	Description
VGA Priority	Allows you to set the priority for VGA graphics devices if multiple VGA devices are found in the system. This can be one of the following: • **Onboard—**Priority is given to the onboard VGA device. BIOS post screen and OS boot are driven through the onboard VGA port. • **Offboard—**Priority is given to the PCIE Graphics adapter. BIOS post screen and OS boot are driven through the external graphics adapter port. • **Onboard VGA Disabled—**Priority is given to the PCIE Graphics adapter, and the onboard VGA device is disabled. **Note** The vKVM does not function when the onboard VGA is disabled.

Serial Configuration Parameters

Name	Description
Console Redirection	Allows a serial port to be used for console redirection during POST and BIOS booting. After the BIOS has booted and the operating system is responsible for the server, console redirection is irrelevant and has no effect. This can be one of the following: • **Disabled—**No console redirection occurs during POST. • **Enabled—**Enables console redirection on serial port A during POST.
Terminal Type	What type of character formatting is used for console redirection. This can be one of the following: • **PC-ANSI—**The PC-ANSI terminal font is used. • **VT100—**A supported vt100 video terminal and its character set are used. • **VT100+—**A supported vt100-plus video terminal and its character set are used. • **VT-UTF8—**A video terminal with the UTF-8 character set is used. **Note** This setting must match the setting on the remote terminal application.

Name	Description
Bits per second	What BAUD rate is used for the serial port transmission speed. If you disable Console Redirection, this option is not available. This can be one of the following: • **9600—**A 9,600 BAUD rate is used. • **19200—**A 19,200 BAUD rate is used. • **38400—**A 38,400 BAUD rate is used. • **57600—**A 57,600 BAUD rate is used. • **115200—**A 115,200 BAUD rate is used. **Note** This setting must match the setting on the remote terminal application.
Flow Control	Whether a handshake protocol is used for flow control. Request to Send / Clear to Send (RTS/CTS) helps to reduce frame collisions that can be introduced by a hidden terminal problem. This can be one of the following: • **None—**No flow control is used. • **Hardware RTS/CTS—**RTS/CTS is used for flow control. **Note** This setting must match the setting on the remote terminal application.
Putty KeyPad	Allows you to change the action of the PuTTY function keys and the top row of the numeric keypad. This can be one of the following: • **VT100—**The function keys generate ESC OP through ESC O[. • **LINUX—**Mimics the Linux virtual console. Function keys F6 to F12 behave like the default mode, but F1 to F5 generate ESC [[A through ESC [[E. • **XTERMR6—**Function keys F5 to F12 behave like the default mode. Function keys F1 to F4 generate **ESC OP** through ESC OS, which are the sequences produced by the top row of the keypad on Digital terminals. • **SCO—**The function keys F1 to F12 generate ESC [M through ESC [X. The function and shift keys generate ESC [Y through ESC [j. The control and function keys generate ESC [k through ESC [v. The shift, control and function keys generate ESC [w through ESC [{. • **ESCN—**The default mode. The function keys match the general behavior of Digital terminals. The function keys generate sequences such as ESC [11~ and ESC [12~. • **VT400—**The function keys behave like the default mode. The top row of the numeric keypad generates ESC OP through ESC OS.

Name	Description
Redirection After BIOS POST	Whether BIOS console redirection should be active after BIOS POST is complete and control given to the OS bootloader. This can be one of the following: • **Always Enable—**BIOS Legacy console redirection is active during the OS boot and run time. • **Bootloader—**BIOS Legacy console redirection is disabled before giving control to the OS boot loader.
Out-of-Band Mgmt Port	Allows you to configure the COM port 0 that can be used for Windows Emergency Management services. ACPI SPCR table is reported based on this setup option. This can be one of the following: • **Disabled—**Configures the COM port 0 as a general purpose port for use with the Windows Operating System. • **Enabled—**Configures the COM port 0 as a remote management port for Windows Emergency Management services.

LOM and PCIe Slots Configuration Parameters

Name	Description
All Onboard LOM Ports	Whether all LOM ports are enabled or disabled. This can be one of the following: • **Disabled—**All LOM ports are disabled. • **Enabled—**All LOM ports are enabled.
LOM Port *n* OptionROM	Whether Option ROM is available on the LOM port designated by ***n***. This can be one of the following: • **Disabled—**Option ROM is not available on LOM port ***n***. • **Enabled—**Option ROM is available on LOM port ***n***. • **UEFI Only—**The expansion slot ***n*** is available for UEFI only. • **Legacy Only—**The expansion slot ***n*** is available for legacy only.

Name	Description
All PCIe Slots OptionROM	Whether the server can use the PCIe Option ROM expansion slots. This can be one of the following: • **Disabled—**PCIe Option ROMs are not available. • **Enabled—**PCIe Option ROMs are available. • **UEFI Only—**The expansion slot ***n*** is available for UEFI only. • **Legacy Only—**The expansion slot ***n*** is available for legacy only.
PCIe Slot:*n* OptionROM	Whether PCIe expansion slot ***n*** is available to the server. This can be one of the following: • **Disabled—**The expansion slot ***n*** is not available. • **Enabled—**The expansion slot ***n*** is available. • **UEFI Only—**The expansion slot ***n*** is available for UEFI only. • **Legacy Only—**The expansion slot ***n*** is available for legacy only.
PCIe Slot:*n* Link Speed	This option allows you to restrict the maximum speed of an adapter card installed in PCIe slot ***n***. This can be one of the following: • **GEN1—**2.5GT/s (gigatransfers per second) is the maximum speed allowed. • **GEN2—**5GT/s is the maximum speed allowed. • **GEN3—**8GT/s is the maximum speed allowed. • **Disabled—**The maximum speed is not restricted. For example, if you have a 3rd generation adapter card in PCIe slot 2 that you want to run at a maximum of 5GT/s instead of the 8GT/s that card supports, set the PCIe Slot 2 Link Speed to **GEN2**. The system then ignores the card's supported maximum speed of 8GT/s and forces it to run at a maximum of 5 GT/s.

Server Management BIOS Parameters for C22 and C24 Servers

Name	Description
FRB-2 Timer	Whether the FRB2 timer is used by CIMC to recover the system if it hangs during POST. This can be one of the following: • **Disabled—**The FRB2 timer is not used. • **Enabled—**The FRB2 timer is started during POST and used to recover the system if necessary.

Name	Description
OS Watchdog Timer	Whether the BIOS programs the watchdog timer with a specified timeout value. This can be one of the following: • **Disabled—**The watchdog timer is not used to track how long the server takes to boot. • **Enabled—**The watchdog timer tracks how long the server takes to boot. If the server does not boot within the length of time specified in the **OS Boot Watchdog Timer Timeout** field, the CIMC logs an error and takes the action specified in the **OS Boot Watchdog Policy** field.
OS Watchdog Timer Timeout	What timeout value the BIOS uses to configure the watchdog timer. This can be one of the following: • **5 Minutes—**The watchdog timer expires 5 minutes after the OS begins to boot. • **10 Minutes—**The watchdog timer expires 10 minutes after the OS begins to boot. • **15 Minutes—**The watchdog timer expires 15 minutes after the OS begins to boot. • **20 Minutes—**The watchdog timer expires 20 minutes after the OS begins to boot. **Note** This option is only applicable if you enable the OS Boot Watchdog Timer.
OS Watchdog Timer Policy	What action the system takes if the watchdog timer expires. This can be one of the following: • **Do Nothing—**The server takes no action if the watchdog timer expires during OS boot. • **Power Down—**The server is powered off if the watchdog timer expires during OS boot. • **Reset—**The server is reset if the watchdog timer expires during OS boot. **Note** This option is only applicable if you enable the OS Boot Watchdog Timer.

Name	Description
Boot Order Rules	How the server changes the boot order list defined through the CIMC GUI or CLI when there are no devices of a particular device type available or when the user defines a different boot order using the server's BIOS Setup Utility. The supported device types are: • **HDD—**Hard disk drive • **FDD—**Floppy disk drive • **CDROM—**Bootable CD-ROM or DVD • **PXE—**PXE boot • **EFI—**Extensible Firmware Interface The Boot Order Rules option can be one of the following: • **Strict—**When no devices of a particular type are available, the system creates a placeholder for that device type in the boot order list. When a device of that type becomes available, it is added to the boot order in the previously defined position. If the user defines a boot order through the server's BIOS Setup Utility, that boot order is given priority over the boot order configured through the CIMC GUI or CLI. All device types defined through CIMC that are not present in the boot order defined through the BIOS Setup Utility are removed from the boot order list. • **Loose—**When no devices of a particular type are available, the system removes that device type from the boot order. When a device of that type becomes available, the system adds it to the end of the boot order list. If the boot order is configured through the server's BIOS Setup Utility, that boot order is given priority over the boot order configured through the CIMC GUI or CLI. All device types defined through CIMC that are not present in the boot order defined through the BIOS Setup Utility are moved to the end of the boot order list.

C220 and C240 Servers

Main BIOS Parameters for C220 and C240 Servers

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

Advanced BIOS Parameters for C220 and C240 Servers

Processor Configuration Parameters

Name	Description
Intel Hyper-Threading Technology	Whether the processor uses Intel Hyper-Threading Technology, which allows multithreaded software applications to execute threads in parallel within each processor. This can be one of the following: • **Disabled—**The processor does not permit hyperthreading. • **Enabled—**The processor allows for the parallel execution of multiple threads. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.

Name	Description
Number of Enabled Cores	Allows you to disable one or more of the physical cores on the server. This can be one of the following: • **All—**Enables all physical cores. This also enables Hyper Threading on the associated logical processor cores. • **1** through ***n*—**Specifies the number of physical processor cores that can run on the server. Each physical core has an associated logical core. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.
Execute Disable	Classifies memory areas on the server to specify where application code can execute. As a result of this classification, the processor disables code execution if a malicious worm attempts to insert code in the buffer. This setting helps to prevent damage, worm propagation, and certain classes of malicious buffer overflow attacks. This can be one of the following: • **Disabled—**The processor does not classify memory areas. • **Enabled—**The processor classifies memory areas. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.
Intel VT	Whether the processor uses Intel Virtualization Technology (VT), which allows a platform to run multiple operating systems and applications in independent partitions. This can be one of the following: • **Disabled—**The processor does not permit virtualization. • **Enabled—**The processor allows multiple operating systems in independent partitions. **Note** If you change this option, you must power cycle the server before the setting takes effect.
Intel VT-d	Whether the processor uses Intel Virtualization Technology for Directed I/O (VT-d). This can be one of the following: • **Disabled—**The processor does not use virtualization technology. • **Enabled—**The processor uses virtualization technology.

Name	Description
Intel VT-d Coherency Support	Whether the processor supports Intel VT-d Coherency. This can be one of the following: • **Disabled—**The processor does not support coherency. • **Enabled—**The processor uses VT-d Coherency as required.
Intel VT-d ATS Support	Whether the processor supports Intel VT-d Address Translation Services (ATS). This can be one of the following: • **Disabled—**The processor does not support ATS. • **Enabled—**The processor uses VT-d ATS as required.
CPU Performance	Sets the CPU performance profile for the server. The performance profile consists of the following options: • DCU Streamer Prefetcher • DCU IP Prefetcher • Hardware Prefetcher • Adjacent Cache-Line Prefetch This can be one of the following: • **Enterprise—**All options are enabled. • **High Throughput—**Only the DCU IP Prefetcher is enabled. The rest of the options are disabled. • **HPC—**All options are enabled. This setting is also known as high performance computing. • **Custom—**All performance profile options can be configured from the BIOS setup on the server. In addition, the Hardware Prefetcher and Adjacent Cache-Line Prefetch options can be configured in the fields below.
Hardware Prefetcher	Whether the processor allows the Intel hardware prefetcher to fetch streams of data and instruction from memory into the unified second-level cache when necessary. This can be one of the following: • **Disabled—**The hardware prefetcher is not used. • **Enabled—**The processor uses the hardware prefetcher when cache issues are detected.

Name	Description
Adjacent Cache Line Prefetcher	Whether the processor fetches cache lines in even/odd pairs instead of fetching just the required line. This can be one of the following: • **Disabled—**The processor only fetches the required line. • **Enabled—** The processor fetches both the required line and its paired line.
DCU Streamer Prefetch	Whether the processor uses the DCU IP Prefetch mechanism to analyze historical cache access patterns and preload the most relevant lines in the L1 cache. This can be one of the following: • **Disabled—**The processor does not try to anticipate cache read requirements and only fetches explicitly requested lines. • **Enabled—**The DCU prefetcher analyzes the cache read pattern and prefetches the next line in the cache if it determines that it may be needed.
DCU IP Prefetcher	Whether the processor uses the DCU IP Prefetch mechanism to analyze historical cache access patterns and preload the most relevant lines in the L1 cache. This can be one of the following: • **Disabled—**The processor does not preload any cache data. • **Enabled—**The DCU IP prefetcher preloads the L1 cache with the data it determines to be the most relevant.
Direct Cache Access Support	Allows processors to increase I/O performance by placing data from I/O devices directly into the processor cache. This setting helps to reduce cache misses. This can be one of the following: • **Disabled—**Data from I/O devices is not placed directly into the processor cache. • **Enabled—**Data from I/O devices is placed directly into the processor cache.

Name	Description
Power Technology	Enables you to configure the CPU power management settings for the following options: • Enhanced Intel Speedstep Technology • Intel Turbo Boost Technology • Processor Power State C6 Power Technology can be one of the following: • **Custom**—The server uses the individual settings for the BIOS parameters mentioned above. You must select this option if you want to change any of these BIOS parameters. • **Disabled**—The server does not perform any CPU power management and any settings for the BIOS parameters mentioned above are ignored. • **Energy Efficient**—The server determines the best settings for the BIOS parameters mentioned above and ignores the individual settings for these parameters.
Enhanced Intel Speedstep Technology	Whether the processor uses Enhanced Intel SpeedStep Technology, which allows the system to dynamically adjust processor voltage and core frequency. This technology can result in decreased average power consumption and decreased average heat production. This can be one of the following: • **Disabled**—The processor never dynamically adjusts its voltage or frequency. • **Enabled**—The processor utilizes Enhanced Intel SpeedStep Technology and enables all supported processor sleep states to further conserve power. We recommend that you contact your operating system vendor to make sure the operating system supports this feature. **Note** **Power Technology** must be set to **Custom** or the server ignores the setting for this parameter.

Name	Description
Intel Turbo Boost Technology	Whether the processor uses Intel Turbo Boost Technology, which allows the processor to automatically increase its frequency if it is running below power, temperature, or voltage specifications. This can be one of the following: • **Disabled—**The processor does not increase its frequency automatically. • **Enabled—**The processor utilizes Turbo Boost Technology if required. **Note** **Power Technology** must be set to **Custom** or the server ignores the setting for this parameter.
Processor Power State C6	Whether the BIOS sends the C6 report to the operating system. When the OS receives the report, it can transition the processor into the lower C6 power state to decrease energy usage while maintaining optimal processor performance. This can be one of the following: • **Disabled—**The BIOS does not send the C6 report. • **Enabled—**The BIOS sends the C6 report, allowing the OS to transition the processor to the C6 low power state. **Note** **Power Technology** must be set to **Custom** or the server ignores the setting for this parameter.
Processor Power State C1 Enhanced	Whether the CPU transitions to its minimum frequency when entering the C1 state. This can be one of the following: • **Disabled—**The CPU continues to run at its maximum frequency in C1 state. • **Enabled—**The CPU transitions to its minimum frequency. This option saves the maximum amount of power in C1 state.
Frequency Floor Override	Whether the CPU is allowed to drop below the maximum non-turbo frequency when idle. This can be one of the following: • **Disabled—** The CPU can drop below the maximum non-turbo frequency when idle. This option decreases power consumption but may reduce system performance. • **Enabled—** The CPU cannot drop below the maximum non-turbo frequency when idle. This option improves system performance but may increase power consumption.

Name	Description
P-STATE Coordination	Allows you to define how BIOS communicates the P-state support model to the operating system. There are 3 models as defined by the Advanced Configuration and Power Interface (ACPI) specification. • **HW_ALL**—The processor hardware is responsible for coordinating the P-state among logical processors with dependencies (all logical processors in a package). • **SW_ALL**—The OS Power Manager (OSPM) is responsible for coordinating the P-state among logical processors with dependencies (all logical processors in a physical package), and must initiate the transition on all of the logical processors. • **SW_ANY**—The OS Power Manager (OSPM) is responsible for coordinating the P-state among logical processors with dependencies (all logical processors in a package), and may initiate the transition on any of the logical processors in the domain. **Note** **Power Technology** must be set to **Custom** or the server ignores the setting for this parameter.
Energy Performance	Allows you to determine whether system performance or energy efficiency is more important on this server. This can be one of the following: • **Balanced Energy** • **Balanced Performance** • **Energy Efficient** • **Performance**

Memory Configuration Parameters

Name	Description
Select Memory RAS	How the memory reliability, availability, and serviceability (RAS) is configured for the server. This can be one of the following: • **Maximum Performance—**System performance is optimized. • **Mirroring—**System reliability is optimized by using half the system memory as backup. • **Lockstep—**If the DIMM pairs in the server have an identical type, size, and organization and are populated across the SMI channels, you can enable lockstep mode to minimize memory access latency and provide better performance. This option offers better system performance than Mirroring and better reliability than Maximum Performance but lower reliability than Mirroring and lower system performance than Maximum Performance.
DRAM Clock Throttling	Allows you to tune the system settings between the memory bandwidth and power consumption. This can be one of the following: • **Balanced—** DRAM clock throttling is reduced, providing a balance between performance and power. • **Performance—**DRAM clock throttling is disabled, providing increased memory bandwidth at the cost of additional power. • **Energy Efficient—**DRAM clock throttling is increased to improve energy efficiency.
NUMA	Whether the BIOS supports NUMA. This can be one of the following: • **Disabled—**The BIOS does not support NUMA. • **Enabled—**The BIOS includes the ACPI tables that are required for NUMA-aware operating systems. If you enable this option, the system must disable Inter-Socket Memory interleaving on some platforms.

Name	Description
Low Voltage DDR Mode	Whether the system prioritizes low voltage or high frequency memory operations. This can be one of the following: • **Power Saving Mode—**The system prioritizes low voltage memory operations over high frequency memory operations. This mode may lower memory frequency in order to keep the voltage low. • **Performance Mode—**The system prioritizes high frequency operations over low voltage operations.
DRAM Refresh rate	Allows you to set the rate at which the DRAM cells are refreshed. This can be one of the following: • **1x—**DRAM cells are refreshed every 64ms. • **2x—**DRAM cells are refreshed every 32ms. • **3x—**DRAM cells are refreshed every 21ms. • **4x—**DRAM cells are refreshed every 16ms. • **Auto—**DRAM cells refresh rate is automatically chosen by the BIOS based on the system configuration. This is the recommended setting for this parameter.
Channel Interleaving	Whether the CPU divides memory blocks and spreads contiguous portions of data across interleaved channels to enable simultaneous read operations. This can be one of the following: • **Auto—**The CPU determines what interleaving is done. • **1 Way—**Some channel interleaving is used. • **2 Way** • **3 Way** • **4 Way—**The maximum amount of channel interleaving is used.

Name	Description
Rank Interleaving	Whether the CPU interleaves physical ranks of memory so that one rank can be accessed while another is being refreshed. This can be one of the following: • **Auto—**The CPU determines what interleaving is done. • **1 Way—**Some rank interleaving is used. • **2 Way** • **4 Way** • **8 Way—**The maximum amount of rank interleaving is used.
Patrol Scrub	Whether the system actively searches for, and corrects, single bit memory errors even in unused portions of the memory on the server. This can be one of the following: • **Disabled—**The system checks for memory ECC errors only when the CPU reads or writes a memory address. • **Enabled—**The system periodically reads and writes memory searching for ECC errors. If any errors are found, the system attempts to fix them. This option may correct single bit errors before they become multi-bit errors, but it may adversely affect performance when the patrol scrub is running.
Demand Scrub	Whether the system corrects single bit memory errors encountered when the CPU or I/O makes a demand read. This can be one of the following: • **Disabled—** Single bit memory errors are not corrected. • **Enabled—** Single bit memory errors are corrected in memory and the corrected data is set in response to the demand read.

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

QPI Configuration Parameters

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

Onboard Storage Parameters

Name	Description
Onboard SCU Storage Support	Whether the onboard software RAID controller is available to the server. This can be one of the following: • **Disabled—**The software RAID controller is not available. • **Enabled—**The software RAID controller is available.

Name	Description
Onboard SCU Storage SW Stack	Allows you to choose a pre-boot software stack for an onboard SCU storage controller. This can be one of the following: • **Intel RSTe(1)** • **LSI SW RAID (0)** **Note** This configuration parameter is valid only for the C220 servers.

USB Configuration Parameters

Name	Description
Legacy USB Support	Whether the system supports legacy USB devices. This can be one of the following: • **Disabled—**USB devices are only available to EFI applications. • **Enabled—**Legacy USB support is always available. • **Auto—**Disables legacy USB support if no USB devices are connected.
Port 60/64 Emulation	Whether the system supports 60h/64h emulation for complete USB keyboard legacy support. This can be one of the following: • **Disabled—**60h/64 emulation is not supported. • **Enabled—**60h/64 emulation is supported. You should select this option if you are using a non-USB aware operating system on the server.
All USB Devices	Whether all physical and virtual USB devices are enabled or disabled. This can be one of the following: • **Disabled—**All USB devices are disabled. • **Enabled—**All USB devices are enabled.
USB Port: Rear	Whether the rear panel USB devices are enabled or disabled. This can be one of the following: • **Disabled—**Disables the rear panel USB ports. Devices connected to these ports are not detected by the BIOS and operating system. • **Enabled—**Enables the rear panel USB ports. Devices connected to these ports are detected by the BIOS and operating system.

Name	Description
USB Port: Front	Whether the front panel USB devices are enabled or disabled. This can be one of the following: • **Disabled—**Disables the front panel USB ports. Devices connected to these ports are not detected by the BIOS and operating system. • **Enabled—**Enables the front panel USB ports. Devices connected to these ports are detected by the BIOS and operating system.
USB Port: Internal	Whether the internal USB devices are enabled or disabled. This can be one of the following: • **Disabled—**Disables the internal USB ports. Devices connected to these ports are not detected by the BIOS and operating system. • **Enabled—**Enables the internal USB ports. Devices connected to these ports are detected by the BIOS and operating system.
USB Port: KVM	Whether the KVM ports are enabled or disabled. This can be one of the following: • **Disabled—**Disables the KVM keyboard and/or mouse devices. Keyboard and/or mouse will not work in the KVM window. • **Enabled—**Enables the KVM keyboard and/or mouse devices.
USB Port: VMedia	Whether the virtual media devices are enabled or disabled. This can be one of the following: • **Disabled—**Disables the vMedia devices. • **Enabled—**Enables the vMedia devices.
USB Port: SD Card	Whether the SD card drives are enabled or disabled. This can be one of the following: • **Disabled—**Disables the SD card drives. The SD card drives are not detected by the BIOS and operating system. • **Enabled—**Enables the SD card drives.

PCI Configuration Parameters

Name	Description
Memory Mapped I/O Above 4GB	Whether to enable or disable memory mapped I/O of 64-bit PCI devices to 4GB or greater address space. Legacy option ROMs are not able to access addresses above 4GB. PCI devices that are 64-bit compliant but use a legacy option ROM may not function correctly with this setting enabled. This can be one of the following: • **Disabled—**The server does not map I/O of 64-bit PCI devices to 4GB or greater address space. • **Enabled—**The server maps I/O of 64-bit PCI devices to 4GB or greater address space.
ASPM Support	Allows you to set the level of ASPM (Active Power State Management) support in the BIOS. This can be one of the following: • **Disabled—**ASPM support is disabled in the BIOS. • **Force L0s—**Force all links to L0 standby (L0s) state. • **Auto—**The CPU determines the power state.
VGA Priority	Allows you to set the priority for VGA graphics devices if multiple VGA devices are found in the system. This can be one of the following: • **Onboard—**Priority is given to the onboard VGA device. BIOS post screen and OS boot are driven through the onboard VGA port. • **Offboard—**Priority is given to the PCIE Graphics adapter. BIOS post screen and OS boot are driven through the external graphics adapter port. • **Onboard VGA Disabled—**Priority is given to the PCIE Graphics adapter, and the onboard VGA device is disabled. **Note** The vKVM does not function when the onboard VGA is disabled.

Serial Configuration Parameters

Name	Description
Console Redirection	Allows a serial port to be used for console redirection during POST and BIOS booting. After the BIOS has booted and the operating system is responsible for the server, console redirection is irrelevant and has no effect. This can be one of the following: • **Disabled—**No console redirection occurs during POST. • **COM 0—**Enables console redirection on COM port 0 during POST. • **COM 1—**Enables console redirection on COM port 1 during POST.
Terminal Type	What type of character formatting is used for console redirection. This can be one of the following: • **PC-ANSI—**The PC-ANSI terminal font is used. • **VT100—**A supported vt100 video terminal and its character set are used. • **VT100+—**A supported vt100-plus video terminal and its character set are used. • **VT-UTF8—**A video terminal with the UTF-8 character set is used. **Note** This setting must match the setting on the remote terminal application.
Bits per second	What BAUD rate is used for the serial port transmission speed. If you disable Console Redirection, this option is not available. This can be one of the following: • **9600—**A 9,600 BAUD rate is used. • **19200—**A 19,200 BAUD rate is used. • **38400—**A 38,400 BAUD rate is used. • **57600—**A 57,600 BAUD rate is used. • **115200—**A 115,200 BAUD rate is used. **Note** This setting must match the setting on the remote terminal application.

Name	Description
Flow Control	Whether a handshake protocol is used for flow control. Request to Send / Clear to Send (RTS/CTS) helps to reduce frame collisions that can be introduced by a hidden terminal problem. This can be one of the following: • **None—**No flow control is used. • **Hardware RTS/CTS—**RTS/CTS is used for flow control. **Note** This setting must match the setting on the remote terminal application.
Putty KeyPad	Allows you to change the action of the PuTTY function keys and the top row of the numeric keypad. This can be one of the following: • **VT100—**The function keys generate ESC OP through ESC O[. • **LINUX—**Mimics the Linux virtual console. Function keys F6 to F12 behave like the default mode, but F1 to F5 generate ESC [[A through ESC [[E. • **XTERMR6—**Function keys F5 to F12 behave like the default mode. Function keys F1 to F4 generate **ESC OP** through ESC OS, which are the sequences produced by the top row of the keypad on Digital terminals. • **SCO—**The function keys F1 to F12 generate ESC [M through ESC [X. The function and shift keys generate ESC [Y through ESC [j. The control and function keys generate ESC [k through ESC [v. The shift, control and function keys generate ESC [w through ESC [{. • **ESCN—**The default mode. The function keys match the general behavior of Digital terminals. The function keys generate sequences such as ESC [11~ and ESC [12~. • **VT400—**The function keys behave like the default mode. The top row of the numeric keypad generates ESC OP through ESC OS.
Redirection After BIOS POST	Whether BIOS console redirection should be active after BIOS POST is complete and control given to the OS bootloader. This can be one of the following: • **Always Enable—**BIOS Legacy console redirection is active during the OS boot and run time. • **Bootloader—**BIOS Legacy console redirection is disabled before giving control to the OS boot loader.

Name	Description
Out-of-Band Mgmt Port	Allows you to configure the COM port 0 that can be used for Windows Emergency Management services. ACPI SPCR table is reported based on this setup option. This can be one of the following: • **Disabled—**Configures the COM port 0 as a general purpose port for use with the Windows Operating System. • **Enabled—**Configures the COM port 0 as a remote management port for Windows Emergency Management services.

LOM and PCIe Slots Configuration Parameters

Name	Description
All Onboard LOM Ports	Whether all LOM ports are enabled or disabled. This can be one of the following: • **Disabled—**All LOM ports are disabled. • **Enabled—**All LOM ports are enabled.
LOM Port *n* OptionROM	Whether Option ROM is available on the LOM port designated by ***n***. This can be one of the following: • **Disabled—**The expansion slot ***n*** is not available. • **Enabled—**The expansion slot ***n*** is available. • **UEFI Only—**The expansion slot ***n*** is available for UEFI only. • **Legacy Only—**The expansion slot ***n*** is available for legacy only.
All PCIe Slots OptionROM	Whether the server can use the PCIe Option ROM expansion slots. This can be one of the following: • **Disabled—**The expansion slot ***n*** is not available. • **Enabled—**The expansion slot ***n*** is available. • **UEFI Only—**The expansion slot ***n*** is available for UEFI only. • **Legacy Only—**The expansion slot ***n*** is available for legacy only.

Name	Description
PCIe Slot:*n* OptionROM	Whether PCIe expansion slot ***n*** is available to the server. This can be one of the following: • **Disabled—**The expansion slot ***n*** is not available. • **Enabled—**The expansion slot ***n*** is available. • **UEFI Only—**The expansion slot ***n*** is available for UEFI only. • **Legacy Only—**The expansion slot ***n*** is available for legacy only.
PCIe Mezzanine OptionROM	Whether the PCIe mezzanine slot expansion ROM is available to the server. This can be one of the following: • **Disabled—**The expansion slot ***n*** is not available. • **Enabled—**The expansion slot ***n*** is available. • **UEFI Only—**The expansion slot ***n*** is available for UEFI only. • **Legacy Only—**The expansion slot ***n*** is available for legacy only.
PCIe Slot:*n* Link Speed	This option allows you to restrict the maximum speed of an adapter card installed in PCIe slot ***n***. This can be one of the following: • **GEN1—**2.5GT/s (gigatransfers per second) is the maximum speed allowed. • **GEN2—**5GT/s is the maximum speed allowed. • **GEN3—**8GT/s is the maximum speed allowed. • **Disabled—**The maximum speed is not restricted. For example, if you have a 3rd generation adapter card in PCIe slot 2 that you want to run at a maximum of 5GT/s instead of the 8GT/s that card supports, set the PCIe Slot 2 Link Speed to **GEN2**. The system then ignores the card's supported maximum speed of 8GT/s and forces it to run at a maximum of 5 GT/s.

Server Management BIOS Parameters for C220 and C240 Servers

Name	Description
FRB-2 Timer	Whether the FRB2 timer is used by CIMC to recover the system if it hangs during POST. This can be one of the following: • **Disabled—**The FRB2 timer is not used. • **Enabled—**The FRB2 timer is started during POST and used to recover the system if necessary.

Name	Description
OS Watchdog Timer	Whether the BIOS programs the watchdog timer with a specified timeout value. This can be one of the following: • **Disabled—**The watchdog timer is not used to track how long the server takes to boot. • **Enabled—**The watchdog timer tracks how long the server takes to boot. If the server does not boot within the length of time specified in the **OS Boot Watchdog Timer Timeout** field, the CIMC logs an error and takes the action specified in the **OS Boot Watchdog Policy** field.
OS Watchdog Timer Timeout	What timeout value the BIOS uses to configure the watchdog timer. This can be one of the following: • **5 Minutes—**The watchdog timer expires 5 minutes after the OS begins to boot. • **10 Minutes—**The watchdog timer expires 10 minutes after the OS begins to boot. • **15 Minutes—**The watchdog timer expires 15 minutes after the OS begins to boot. • **20 Minutes—**The watchdog timer expires 20 minutes after the OS begins to boot. **Note** This option is only applicable if you enable the OS Boot Watchdog Timer.
OS Watchdog Timer Policy	What action the system takes if the watchdog timer expires. This can be one of the following: • **Do Nothing—**The server takes no action if the watchdog timer expires during OS boot. • **Power Down—**The server is powered off if the watchdog timer expires during OS boot. • **Reset—**The server is reset if the watchdog timer expires during OS boot. **Note** This option is only applicable if you enable the OS Boot Watchdog Timer.

Name	Description
Boot Order Rules	How the server changes the boot order list defined through the CIMC GUI or CLI when there are no devices of a particular device type available or when the user defines a different boot order using the server's BIOS Setup Utility. The supported device types are: • **HDD—**Hard disk drive • **FDD—**Floppy disk drive • **CDROM—**Bootable CD-ROM or DVD • **PXE—**PXE boot • **EFI—**Extensible Firmware Interface The Boot Order Rules option can be one of the following: • **Strict—**When no devices of a particular type are available, the system creates a placeholder for that device type in the boot order list. When a device of that type becomes available, it is added to the boot order in the previously defined position. If the user defines a boot order through the server's BIOS Setup Utility, that boot order is given priority over the boot order configured through the CIMC GUI or CLI. All device types defined through CIMC that are not present in the boot order defined through the BIOS Setup Utility are removed from the boot order list. • **Loose—**When no devices of a particular type are available, the system removes that device type from the boot order. When a device of that type becomes available, the system adds it to the end of the boot order list. If the boot order is configured through the server's BIOS Setup Utility, that boot order is given priority over the boot order configured through the CIMC GUI or CLI. All device types defined through CIMC that are not present in the boot order defined through the BIOS Setup Utility are moved to the end of the boot order list.

C260 Servers

Main BIOS Parameters for C260 Servers

Name	Description
POST Error Pause	What happens when the server encounters a critical error during POST. This can be one of the following: • **Enabled—**The BIOS pauses the attempt to boot the server and opens the Error Manager when a critical error occurs during POST. • **Disabled—**The BIOS continues to attempt to boot the server.
Boot Option Retry	Whether the BIOS retries NON-EFI based boot options without waiting for user input. This can be one of the following: • **Enabled—**Continually retries NON-EFI based boot options without waiting for user input. • **Disabled—**Waits for user input before retrying NON-EFI based boot options.

Advanced BIOS Parameters for C260 Servers

Processor Configuration Parameters

Name	Description
Intel Turbo Boost Technology	Whether the processor uses Intel Turbo Boost Technology, which allows the processor to automatically increase its frequency if it is running below power, temperature, or voltage specifications. This can be one of the following: • **Disabled—**The processor does not increase its frequency automatically. • **Enabled—**The processor utilizes Turbo Boost Technology if required.

Name	Description
Enhanced Intel Speedstep Technology	Whether the processor uses Enhanced Intel SpeedStep Technology, which allows the system to dynamically adjust processor voltage and core frequency. This technology can result in decreased average power consumption and decreased average heat production. This can be one of the following: • **Disabled—**The processor never dynamically adjusts its voltage or frequency. • **Enabled—**The processor utilizes Enhanced Intel SpeedStep Technology and enables all supported processor sleep states to further conserve power. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.
Intel Hyper-Threading Technology	Whether the processor uses Intel Hyper-Threading Technology, which allows multithreaded software applications to execute threads in parallel within each processor. This can be one of the following: • **Disabled—**The processor does not permit hyperthreading. • **Enabled—**The processor allows for the parallel execution of multiple threads. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.
Number of Enabled Cores	Allows you to disable one or more of the physical cores on the server. This can be one of the following: • **All—**Enables all physical cores. This also enables Hyper Threading on the associated logical processor cores. • **1** through ***n*—**Specifies the number of physical processor cores that can run on the server. Each physical core has an associated logical core. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.

Name	Description
Execute Disable	Classifies memory areas on the server to specify where application code can execute. As a result of this classification, the processor disables code execution if a malicious worm attempts to insert code in the buffer. This setting helps to prevent damage, worm propagation, and certain classes of malicious buffer overflow attacks. This can be one of the following: • **Disabled—**The processor does not classify memory areas. • **Enabled—**The processor classifies memory areas. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.
Intel Virtualization Technology	Whether the processor uses Intel Virtualization Technology (VT), which allows a platform to run multiple operating systems and applications in independent partitions. This can be one of the following: • **Disabled—**The processor does not permit virtualization. • **Enabled—**The processor allows multiple operating systems in independent partitions. **Note** If you change this option, you must power cycle the server before the setting takes effect.
Intel VT for Directed IO	Whether the processor uses Intel Virtualization Technology for Directed I/O (VT-d). This can be one of the following: • **Disabled—**The processor does not use virtualization technology. • **Enabled—**The processor uses virtualization technology.
Intel VT-d Interrupt Remapping	Whether the processor supports Intel VT-d Interrupt Remapping. This can be one of the following: • **Disabled—**The processor does not support remapping. • **Enabled—**The processor uses VT-d Interrupt Remapping as required.
Intel VT-d Coherency Support	Whether the processor supports Intel VT-d Coherency. This can be one of the following: • **Disabled—**The processor does not support coherency. • **Enabled—**The processor uses VT-d Coherency as required.

Name	Description
Intel VT-d Address Translation Services	Whether the processor supports Intel VT-d Address Translation Services (ATS). This can be one of the following: • **Disabled—**The processor does not support ATS. • **Enabled—**The processor uses VT-d ATS as required.
Intel VT-d PassThrough DMA	Whether the processor supports Intel VT-d Pass-through DMA. This can be one of the following: • **Disabled—**The processor does not support pass-through DMA. • **Enabled—**The processor uses VT-d Pass-through DMA as required.
Direct Cache Access	Allows processors to increase I/O performance by placing data from I/O devices directly into the processor cache. This setting helps to reduce cache misses. This can be one of the following: • **Disabled—**Data from I/O devices is not placed directly into the processor cache. • **Enabled—**Data from I/O devices is placed directly into the processor cache.
Processor C3 Report	Whether the BIOS sends the C3 report to the operating system. When the OS receives the report, it can transition the processor into the lower C3 power state to decrease energy usage while maintaining optimal processor performance. This can be one of the following: • **Disabled—**The BIOS does not send the C3 report. • **ACPI C2—**The BIOS sends the C3 report using the ACPI C2 format, allowing the OS to transition the processor to the C3 low power state. • **ACPI C3—**The BIOS sends the C3 report using the ACPI C3 format, allowing the OS to transition the processor to the C3 low power state.

Name	Description
Processor C6 Report	Whether the BIOS sends the C6 report to the operating system. When the OS receives the report, it can transition the processor into the lower C6 power state to decrease energy usage while maintaining optimal processor performance. This can be one of the following: • **Disabled—**The BIOS does not send the C6 report. • **Enabled—**The BIOS sends the C6 report, allowing the OS to transition the processor to the C6 low power state.
Package C State Limit	The amount of power available to the server components when they are idle. This can be one of the following: • **C0 state—**The server provides all server components with full power at all times. This option maintains the highest level of performance and requires the greatest amount of power. • **C1 state—**When the CPU is idle, the system slightly reduces the power consumption. This option requires less power than C0 and allows the server to return quickly to high performance mode. • **C3 state—**When the CPU is idle, the system reduces the power consumption further than with the C1 option. This requires less power than C1 or C0, but it takes the server slightly longer to return to high performance mode. • **C6 state—**When the CPU is idle, the system reduces the power consumption further than with the C3 option. This option saves more power than C0, C1, or C3, but there may be performance issues until the server returns to full power. • **C7 state—**When the CPU is idle, the server makes a minimal amount of power available to the components. This option saves the maximum amount of power but it also requires the longest time for the server to return to high performance mode. • **No Limit—**The server may enter any available C state. **Note** This option is used only if **CPU C State** is enabled.

Name	Description
CPU C State	Whether the system can enter a power savings mode during idle periods. This can be one of the following: • **Disabled—**The system remains in high performance state even when idle. • **Enabled—**The system can reduce power to system components such as the DIMMs and CPUs. The amount of power reduction is specified in the **Package C State Limit** field.
C1E	Whether the CPU transitions to its minimum frequency when entering the C1 state. This can be one of the following: • **Disabled—**The CPU continues to run at its maximum frequency in C1 state. • **Enabled—**The CPU transitions to its minimum frequency. This option saves the maximum amount of power in C1 state. **Note** This option is used only if **CPU C State** is enabled.

Memory Configuration Parameters

Name	Description
Select Memory RAS	How the memory reliability, availability, and serviceability (RAS) is configured for the server. This can be one of the following: • **Maximum Performance—**System performance is optimized. • **Mirroring—**System reliability is optimized by using half the system memory as backup. • **Sparing—**The system reserves some memory for use in the event a DIMM fails. If that happens, the server takes the DIMM offline and replaces it with the reserved memory. This option provides less redundancy than mirroring, but it leaves more of the memory available for programs running on the server.

Name	Description
NUMA Optimized	Whether the BIOS supports NUMA. This can be one of the following: • **Disabled—**The BIOS does not support NUMA. • **Enabled—**The BIOS includes the ACPI tables that are required for NUMA-aware operating systems. If you enable this option, the system must disable Inter-Socket Memory interleaving on some platforms.
Sparing Mode	The sparing mode used by the CIMC. This can be one of the following: • **Rank Sparing—**The spared memory is allocated at the rank level. • **DIMM Sparing—**The spared memory is allocated at the DIMM level. **Note** This option is used only if **Select Memory RAS** is set to **Sparing**.
Mirroring Mode	Mirroring is supported across Integrated Memory Controllers (IMCs) where one memory riser is mirrored with another. This can be one of the following: • **Intersocket—**Each IMC is mirrored across two sockets. • **Intrasocket—**One IMC is mirrored with another IMC in the same socket. **Note** This option is used only if **Select Memory RAS** is set to **Mirroring**.
DRAM Refresh rate	Allows you to set the rate at which the DRAM cells are refreshed. This can be one of the following: • **1x—**DRAM cells are refreshed every 64ms. • **2x—**DRAM cells are refreshed every 32ms. • **3x—**DRAM cells are refreshed every 21ms. • **4x—**DRAM cells are refreshed every 16ms. • **Auto—**DRAM cells refresh rate is automatically chosen by the BIOS based on the system configuration. This is the recommended setting for this parameter.

Name	Description
Patrol Scrub	Whether the system actively searches for, and corrects, single bit memory errors even in unused portions of the memory on the server. This can be one of the following: • **Disabled—**The system checks for memory ECC errors only when the CPU reads or writes a memory address. • **Enabled—**The system periodically reads and writes memory searching for ECC errors. If any errors are found, the system attempts to fix them. This option may correct single bit errors before they become multi-bit errors, but it may adversely affect performance when the patrol scrub is running.
Patrol Scrub Interval	Controls the time interval between each patrol scrub memory access. A lower interval scrubs the memory more often but requires more memory bandwidth. Select a value between 5 and 23. The default value is 8. **Note** This option is used only if **Patrol Scrub** is enabled.
CKE Low Policy	Controls the DIMM power savings mode policy. This can be one of the following: • **Disabled—**DIMMs do not enter power saving mode. • **Slow—**DIMMs can enter power saving mode, but the requirements are higher. Therefore, DIMMs enter power saving mode less frequently. • **Fast—**DIMMs enter power saving mode as often as possible. • **Auto—**The BIOS controls when a DIMM enters power saving mode based on the DIMM configuration.

Serial Port Configuration Parameters

Name	Description
Serial A Enable	Whether serial port A is enabled or disabled. This can be one of the following: • **Disabled—**The serial port is disabled. • **Enabled—**The serial port is enabled.

USB Configuration Parameters

Name	Description
Make Device Non-Bootable	Whether the server can boot from a USB device. This can be one of the following: • **Disabled—**The server can boot from a USB device. • **Enabled—**The server cannot boot from a USB device.

PCI Configuration Parameters

Name	Description
Memory Mapped I/O Above 4GB	Whether to enable or disable memory mapped I/O of 64-bit PCI devices to 4GB or greater address space. Legacy option ROMs are not able to access addresses above 4GB. PCI devices that are 64-bit compliant but use a legacy option ROM may not function correctly with this setting enabled. This can be one of the following: • **Disabled—**The server does not map I/O of 64-bit PCI devices to 4GB or greater address space. • **Enabled—**The server maps I/O of 64-bit PCI devices to 4GB or greater address space.
Onboard NIC *n* ROM	Whether the system loads the embedded PXE option ROM for the onboard NIC designated by ***n***. This can be one of the following: • **Disabled—**PXE option ROM is not available for NIC ***n***. • **Enabled—**PXE option ROM is available for NIC ***n***.
PCIe OptionROMs	Whether the server can use the PCIe Option ROM expansion slots. This can be one of the following: • **Disabled—**PCIe Option ROMs are not available. • **Enabled—**PCIe Option ROMs are available. • **UEFI Only—**The expansion slot ***n*** is available for UEFI only. • **Legacy Only—**The expansion slot ***n*** is available for legacy only.

Name	Description
PCIe Slot *n* ROM	Whether PCIe expansion slot ***n*** is available to the server. This can be one of the following: • **Disabled—**The expansion slot ***n*** is not available. • **Enabled—**The expansion slot ***n*** is available. • **UEFI Only—**The expansion slot ***n*** is available for UEFI only. • **Legacy Only—**The expansion slot ***n*** is available for legacy only.
Onboard Gbit LOM	Whether Gbit LOM is enabled or disabled on the server. This can be one of the following: • **Disabled—**Gbit LOM is not available. • **Enabled—**10Git LOM is available.
Onboard 10Gbit LOM	Whether 10Gbit LOM is enabled or disabled on the server. This can be one of the following: • **Disabled—**10GBit LOM is not available. • **Enabled—**10GBit LOM is available.
Sriov	Whether SR-IOV (Single Root I/O Virtualization) is enabled or disabled on the server. This can be one of the following: • **Disabled—**SR-IOV is disabled. • **Enabled—**SR-IOV is enabled.

Name	Description
IOH Resource Allocation	Enables you to distribute 64KB of 16-bit IO resources between IOH0 and IOH1 as per system requirement. This can be one of the following: • **IOH0 24k IOH1 40k—** Allocates 24KB of 16-bit IO resources to IOH0 and 40KB of 16-bit IO resources to IOH1. • **IOH0 32k IOH1 32k—** Allocates 32KB of 16-bit IO resources to IOH0 and 32KB of 16-bit IO resources to IOH1. • **IOH0 40k IOH1 24k—** Allocates 40KB of 16-bit IO resources to IOH0 and 24KB of 16-bit IO resources to IOH1. • **IOH0 48k IOH1 16k—** Allocates 48KB of 16-bit IO resources to IOH0 and 16KB of 16-bit IO resources to IOH1. • **IOH0 56k IOH1 8k—** Allocates 56KB of 16-bit IO resources to IOH0 and 8KB of 16-bit IO resources to IOH1.

Server Management BIOS Parameters for C260 Servers

Name	Description
Assert NMI on SERR	Whether the BIOS generates a non-maskable interrupt (NMI) and logs an error when a system error (SERR) occurs. This can be one of the following: • **Disabled—**The BIOS does not generate an NMI or log an error when a SERR occurs. • **Enabled—**The BIOS generates an NMI and logs an error when a SERR occurs. You must enable this setting if you want to enable **Assert NMI on PERR**.
Assert NMI on PERR	Whether the BIOS generates a non-maskable interrupt (NMI) and logs an error when a processor bus parity error (PERR) occurs. This can be one of the following: • **Disabled—**The BIOS does not generate an NMI or log an error when a PERR occurs. • **Enabled—**The BIOS generates an NMI and logs an error when a PERR occurs. You must enable **Assert NMI on SERR** to use this setting.

Name	Description
Console Redirection	Allows a serial port to be used for console redirection during POST and BIOS booting. After the BIOS has booted and the operating system is responsible for the server, console redirection is irrelevant and has no effect. This can be one of the following: • **Disabled—**No console redirection occurs during POST. • **Serial Port A—**Enables console redirection on serial port A during POST. **Note** If you enable this option, you also disable the display of the Quiet Boot logo screen during POST.
Flow Control	Whether a handshake protocol is used for flow control. Request to Send / Clear to Send (RTS/CTS) helps to reduce frame collisions that can be introduced by a hidden terminal problem. This can be one of the following: • **None—**No flow control is used. • **RTS-CTS—**RTS/CTS is used for flow control. **Note** This setting must match the setting on the remote terminal application.
Baud Rate	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: • **9.6k—**A 9600 BAUD rate is used. • **19.2k—**A 19200 BAUD rate is used. • **38.4k—**A 38400 BAUD rate is used. • **57.6k—**A 57600 BAUD rate is used. • **115.2k—**A 115200 BAUD rate is used. **Note** This setting must match the setting on the remote terminal application.

Name	Description
Terminal Type	What type of character formatting is used for console redirection. This can be one of the following: • **PC-ANSI—**The PC-ANSI terminal font is used. • **VT100—**A supported vt100 video terminal and its character set are used. • **VT100-PLUS—**A supported vt100-plus video terminal and its character set are used. • **VT-UTF8—**A video terminal with the UTF-8 character set is used. **Note** This setting must match the setting on the remote terminal application.
OS Boot Watchdog Timer Timeout	What timeout value the BIOS uses to configure the watchdog timer. This can be one of the following: • **5 Minutes—**The watchdog timer expires 5 minutes after the OS begins to boot. • **10 Minutes—**The watchdog timer expires 10 minutes after the OS begins to boot. • **15 Minutes—**The watchdog timer expires 15 minutes after the OS begins to boot. • **20 Minutes—**The watchdog timer expires 20 minutes after the OS begins to boot. **Note** This option is only applicable if you enable the OS Boot Watchdog Timer.
OS Boot Watchdog Policy	What action the system takes if the watchdog timer expires. This can be one of the following: • **Power Off—**The server is powered off if the watchdog timer expires during OS boot. • **Reset—**The server is reset if the watchdog timer expires during OS boot. **Note** This option is only applicable if you enable the OS Boot Watchdog Timer.

Name	Description
Legacy OS Redirection	Whether redirection from a legacy operating system, such as DOS, is enabled on the serial port. This can be one of the following: • **Disabled—**The serial port enabled for console redirection is hidden from the legacy operating system. • **Enabled—**The serial port enabled for console redirection is visible to the legacy operating system.
OS Boot Watchdog Timer	Whether the BIOS programs the watchdog timer with a specified timeout value. This can be one of the following: • **Disabled—**The watchdog timer is not used to track how long the server takes to boot. • **Enabled—**The watchdog timer tracks how long the server takes to boot. If the server does not boot within the length of time specified in the **OS Boot Watchdog Timer Timeout** field, the CIMC logs an error and takes the action specified in the **OS Boot Watchdog Policy** field.

C420 Servers

Main BIOS Parameters for C420 Servers

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

Advanced BIOS Parameters for C420 Servers

Processor Configuration Parameters

Name	Description
Intel Hyper-Threading Technology	Whether the processor uses Intel Hyper-Threading Technology, which allows multithreaded software applications to execute threads in parallel within each processor. This can be one of the following: • **Disabled—**The processor does not permit hyperthreading. • **Enabled—**The processor allows for the parallel execution of multiple threads. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.
Number of Enabled Cores	Allows you to disable one or more of the physical cores on the server. This can be one of the following: • **All—**Enables all physical cores. This also enables Hyper Threading on the associated logical processor cores. • **1** through ***n*—**Specifies the number of physical processor cores that can run on the server. Each physical core has an associated logical core. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.
Execute Disable	Classifies memory areas on the server to specify where application code can execute. As a result of this classification, the processor disables code execution if a malicious worm attempts to insert code in the buffer. This setting helps to prevent damage, worm propagation, and certain classes of malicious buffer overflow attacks. This can be one of the following: • **Disabled—**The processor does not classify memory areas. • **Enabled—**The processor classifies memory areas. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.

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

Name	Description
CPU Performance	Sets the CPU performance profile for the server. The performance profile consists of the following options: • DCU Streamer Prefetcher • DCU IP Prefetcher • Hardware Prefetcher • Adjacent Cache-Line Prefetch This can be one of the following: • **Enterprise—**All options are enabled. • **High Throughput—**Only the DCU IP Prefetcher is enabled. The rest of the options are disabled. • **HPC—**All options are enabled. This setting is also known as high performance computing. • **Custom—**All performance profile options can be configured from the BIOS setup on the server. In addition, the Hardware Prefetcher and Adjacent Cache-Line Prefetch options can be configured in the fields below.
Hardware Prefetcher	Whether the processor allows the Intel hardware prefetcher to fetch streams of data and instruction from memory into the unified second-level cache when necessary. This can be one of the following: • **Disabled—**The hardware prefetcher is not used. • **Enabled—**The processor uses the hardware prefetcher when cache issues are detected.
Adjacent Cache Line Prefetcher	Whether the processor fetches cache lines in even/odd pairs instead of fetching just the required line. This can be one of the following: • **Disabled—**The processor only fetches the required line. • **Enabled—** The processor fetches both the required line and its paired line.

Name	Description
DCU Streamer Prefetch	Whether the processor uses the DCU IP Prefetch mechanism to analyze historical cache access patterns and preload the most relevant lines in the L1 cache. This can be one of the following: • **Disabled—**The processor does not try to anticipate cache read requirements and only fetches explicitly requested lines. • **Enabled—**The DCU prefetcher analyzes the cache read pattern and prefetches the next line in the cache if it determines that it may be needed.
DCU IP Prefetcher	Whether the processor uses the DCU IP Prefetch mechanism to analyze historical cache access patterns and preload the most relevant lines in the L1 cache. This can be one of the following: • **Disabled—**The processor does not preload any cache data. • **Enabled—**The DCU IP prefetcher preloads the L1 cache with the data it determines to be the most relevant.
Direct Cache Access Support	Allows processors to increase I/O performance by placing data from I/O devices directly into the processor cache. This setting helps to reduce cache misses. This can be one of the following: • **Disabled—**Data from I/O devices is not placed directly into the processor cache. • **Enabled—**Data from I/O devices is placed directly into the processor cache.

Name	Description
Power Technology	Enables you to configure the CPU power management settings for the following options: • Enhanced Intel Speedstep Technology • Intel Turbo Boost Technology • Processor Power State C6 Power Technology can be one of the following: • **Custom—**The server uses the individual settings for the BIOS parameters mentioned above. You must select this option if you want to change any of these BIOS parameters. • **Disabled—**The server does not perform any CPU power management and any settings for the BIOS parameters mentioned above are ignored. • **Energy Efficient—**The server determines the best settings for the BIOS parameters mentioned above and ignores the individual settings for these parameters.
Enhanced Intel Speedstep Technology	Whether the processor uses Enhanced Intel SpeedStep Technology, which allows the system to dynamically adjust processor voltage and core frequency. This technology can result in decreased average power consumption and decreased average heat production. This can be one of the following: • **Disabled—**The processor never dynamically adjusts its voltage or frequency. • **Enabled—**The processor utilizes Enhanced Intel SpeedStep Technology and enables all supported processor sleep states to further conserve power. We recommend that you contact your operating system vendor to make sure the operating system supports this feature. **Note** **Power Technology** must be set to **Custom** or the server ignores the setting for this parameter.

Name	Description
Intel Turbo Boost Technology	Whether the processor uses Intel Turbo Boost Technology, which allows the processor to automatically increase its frequency if it is running below power, temperature, or voltage specifications. This can be one of the following: • **Disabled—**The processor does not increase its frequency automatically. • **Enabled—**The processor utilizes Turbo Boost Technology if required. **Note** **Power Technology** must be set to **Custom** or the server ignores the setting for this parameter.
Processor Power State C6	Whether the BIOS sends the C6 report to the operating system. When the OS receives the report, it can transition the processor into the lower C6 power state to decrease energy usage while maintaining optimal processor performance. This can be one of the following: • **Disabled—**The BIOS does not send the C6 report. • **Enabled—**The BIOS sends the C6 report, allowing the OS to transition the processor to the C6 low power state. **Note** **Power Technology** must be set to **Custom** or the server ignores the setting for this parameter.
Processor Power State C1 Enhanced	Whether the CPU transitions to its minimum frequency when entering the C1 state. This can be one of the following: • **Disabled—**The CPU continues to run at its maximum frequency in C1 state. • **Enabled—**The CPU transitions to its minimum frequency. This option saves the maximum amount of power in C1 state.
Frequency Floor Override	Whether the CPU is allowed to drop below the maximum non-turbo frequency when idle. This can be one of the following: • **Disabled—** The CPU can drop below the maximum non-turbo frequency when idle. This option decreases power consumption but may reduce system performance. • **Enabled—** The CPU cannot drop below the maximum non-turbo frequency when idle. This option improves system performance but may increase power consumption.

Name	Description
P-STATE Coordination	Allows you to define how BIOS communicates the P-state support model to the operating system. There are 3 models as defined by the Advanced Configuration and Power Interface (ACPI) specification. • **HW_ALL**—The processor hardware is responsible for coordinating the P-state among logical processors with dependencies (all logical processors in a package). • **SW_ALL**—The OS Power Manager (OSPM) is responsible for coordinating the P-state among logical processors with dependencies (all logical processors in a physical package), and must initiate the transition on all of the logical processors. • **SW_ANY**—The OS Power Manager (OSPM) is responsible for coordinating the P-state among logical processors with dependencies (all logical processors in a package), and may initiate the transition on any of the logical processors in the domain. **Note** **Power Technology** must be set to **Custom** or the server ignores the setting for this parameter.
Energy Performance	Allows you to determine whether system performance or energy efficiency is more important on this server. This can be one of the following: • **Balanced Energy** • **Balanced Performance** • **Energy Efficient** • **Performance**

Memory Configuration Parameters

Name	Description
Select Memory RAS	How the memory reliability, availability, and serviceability (RAS) is configured for the server. This can be one of the following: • **Maximum Performance—**System performance is optimized. • **Mirroring—**System reliability is optimized by using half the system memory as backup. • **Lockstep—**If the DIMM pairs in the server have an identical type, size, and organization and are populated across the SMI channels, you can enable lockstep mode to minimize memory access latency and provide better performance. This option offers better system performance than Mirroring and better reliability than Maximum Performance but lower reliability than Mirroring and lower system performance than Maximum Performance.
DRAM Clock Throttling	Allows you to tune the system settings between the memory bandwidth and power consumption. This can be one of the following: • **Balanced—** DRAM clock throttling is reduced, providing a balance between performance and power. • **Performance—**DRAM clock throttling is disabled, providing increased memory bandwidth at the cost of additional power. • **Energy Efficient—**DRAM clock throttling is increased to improve energy efficiency.
NUMA	Whether the BIOS supports NUMA. This can be one of the following: • **Disabled—**The BIOS does not support NUMA. • **Enabled—**The BIOS includes the ACPI tables that are required for NUMA-aware operating systems. If you enable this option, the system must disable Inter-Socket Memory interleaving on some platforms.

Name	Description
Low Voltage DDR Mode	Whether the system prioritizes low voltage or high frequency memory operations. This can be one of the following: • **Power Saving Mode—**The system prioritizes low voltage memory operations over high frequency memory operations. This mode may lower memory frequency in order to keep the voltage low. • **Performance Mode—**The system prioritizes high frequency operations over low voltage operations.
DRAM Refresh rate	Allows you to set the rate at which the DRAM cells are refreshed. This can be one of the following: • **1x—**DRAM cells are refreshed every 64ms. • **2x—**DRAM cells are refreshed every 32ms. • **3x—**DRAM cells are refreshed every 21ms. • **4x—**DRAM cells are refreshed every 16ms. • **Auto—**DRAM cells refresh rate is automatically chosen by the BIOS based on the system configuration. This is the recommended setting for this parameter.
Channel Interleaving	Whether the CPU divides memory blocks and spreads contiguous portions of data across interleaved channels to enable simultaneous read operations. This can be one of the following: • **Auto—**The CPU determines what interleaving is done. • **1 Way—**Some channel interleaving is used. • **2 Way** • **3 Way** • **4 Way—**The maximum amount of channel interleaving is used.

Name	Description
Rank Interleaving	Whether the CPU interleaves physical ranks of memory so that one rank can be accessed while another is being refreshed. This can be one of the following: • **Auto—**The CPU determines what interleaving is done. • **1 Way—**Some rank interleaving is used. • **2 Way** • **4 Way** • **8 Way—**The maximum amount of rank interleaving is used.
Patrol Scrub	Whether the system actively searches for, and corrects, single bit memory errors even in unused portions of the memory on the server. This can be one of the following: • **Disabled—**The system checks for memory ECC errors only when the CPU reads or writes a memory address. • **Enabled—**The system periodically reads and writes memory searching for ECC errors. If any errors are found, the system attempts to fix them. This option may correct single bit errors before they become multi-bit errors, but it may adversely affect performance when the patrol scrub is running.
Demand Scrub	Whether the system corrects single bit memory errors encountered when the CPU or I/O makes a demand read. This can be one of the following: • **Disabled—** Single bit memory errors are not corrected. • **Enabled—** Single bit memory errors are corrected in memory and the corrected data is set in response to the demand read.

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

QPI Configuration Parameters

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

USB Configuration Parameters

Name	Description
Legacy USB Support	Whether the system supports legacy USB devices. This can be one of the following: • **Disabled—**USB devices are only available to EFI applications. • **Enabled—**Legacy USB support is always available. • **Auto—**Disables legacy USB support if no USB devices are connected.

Name	Description
All USB Devices	Whether all physical and virtual USB devices are enabled or disabled. This can be one of the following: • **Disabled—**All USB devices are disabled. • **Enabled—**All USB devices are enabled.
USB Port: Rear	Whether the rear panel USB devices are enabled or disabled. This can be one of the following: • **Disabled—**Disables the rear panel USB ports. Devices connected to these ports are not detected by the BIOS and operating system. • **Enabled—**Enables the rear panel USB ports. Devices connected to these ports are detected by the BIOS and operating system.
USB Port: Front	Whether the front panel USB devices are enabled or disabled. This can be one of the following: • **Disabled—**Disables the front panel USB ports. Devices connected to these ports are not detected by the BIOS and operating system. • **Enabled—**Enables the front panel USB ports. Devices connected to these ports are detected by the BIOS and operating system.
USB Port: Internal	Whether the internal USB devices are enabled or disabled. This can be one of the following: • **Disabled—**Disables the internal USB ports. Devices connected to these ports are not detected by the BIOS and operating system. • **Enabled—**Enables the internal USB ports. Devices connected to these ports are detected by the BIOS and operating system.
USB Port: KVM	Whether the KVM ports are enabled or disabled. This can be one of the following: • **Disabled—**Disables the KVM keyboard and/or mouse devices. Keyboard and/or mouse will not work in the KVM window. • **Enabled—**Enables the KVM keyboard and/or mouse devices.
USB Port: VMedia	Whether the virtual media devices are enabled or disabled. This can be one of the following: • **Disabled—**Disables the vMedia devices. • **Enabled—**Enables the vMedia devices.

Name	Description
USB Port: SD Card	Whether the SD card drives are enabled or disabled. This can be one of the following: • **Disabled—**Disables the SD card drives. The SD card drives are not detected by the BIOS and operating system. • **Enabled—**Enables the SD card drives.

PCI Configuration Parameters

Name	Description
MMIO Above 4GB	Whether to enable or disable memory mapped I/O of 64-bit PCI devices to 4GB or greater address space. Legacy option ROMs are not able to access addresses above 4GB. PCI devices that are 64-bit compliant but use a legacy option ROM may not function correctly with this setting enabled. This can be one of the following: • **Disabled—**The server does not map I/O of 64-bit PCI devices to 4GB or greater address space. • **Enabled—**The server maps I/O of 64-bit PCI devices to 4GB or greater address space.
ASPM Support	Allows you to set the level of ASPM (Active Power State Management) support in the BIOS. This can be one of the following: • **Disabled—**ASPM support is disabled in the BIOS. • **Force L0s—**Force all links to L0 standby (L0s) state. • **Auto—**The CPU determines the power state.

Name	Description
VGA Priority	Allows you to set the priority for VGA graphics devices if multiple VGA devices are found in the system. This can be one of the following: • **Onboard—**Priority is given to the onboard VGA device. BIOS post screen and OS boot are driven through the onboard VGA port. • **Offboard—**Priority is given to the PCIE Graphics adapter. BIOS post screen and OS boot are driven through the external graphics adapter port. • **Onboard VGA Disabled—**Priority is given to the PCIE Graphics adapter, and the onboard VGA device is disabled. **Note** The vKVM does not function when the onboard VGA is disabled.

Serial Configuration Parameters

Name	Description
Console Redirection	Allows a serial port to be used for console redirection during POST and BIOS booting. After the BIOS has booted and the operating system is responsible for the server, console redirection is irrelevant and has no effect. This can be one of the following: • **Disabled—**No console redirection occurs during POST. • **Enabled—**Enables console redirection on serial port A during POST.
Terminal Type	What type of character formatting is used for console redirection. This can be one of the following: • **PC-ANSI—**The PC-ANSI terminal font is used. • **VT100—**A supported vt100 video terminal and its character set are used. • **VT100+—**A supported vt100-plus video terminal and its character set are used. • **VT-UTF8—**A video terminal with the UTF-8 character set is used. **Note** This setting must match the setting on the remote terminal application.

Name	Description
Bits per second	What BAUD rate is used for the serial port transmission speed. If you disable Console Redirection, this option is not available. This can be one of the following: • **9600—**A 9,600 BAUD rate is used. • **19200—**A 19,200 BAUD rate is used. • **38400—**A 38,400 BAUD rate is used. • **57600—**A 57,600 BAUD rate is used. • **115200—**A 115,200 BAUD rate is used. **Note** This setting must match the setting on the remote terminal application.
Flow Control	Whether a handshake protocol is used for flow control. Request to Send / Clear to Send (RTS/CTS) helps to reduce frame collisions that can be introduced by a hidden terminal problem. This can be one of the following: • **None—**No flow control is used. • **Hardware RTS/CTS—**RTS/CTS is used for flow control. **Note** This setting must match the setting on the remote terminal application.
Putty KeyPad	Allows you to change the action of the PuTTY function keys and the top row of the numeric keypad. This can be one of the following: • **VT100—**The function keys generate ESC OP through ESC O[. • **LINUX—**Mimics the Linux virtual console. Function keys F6 to F12 behave like the default mode, but F1 to F5 generate ESC [[A through ESC [[E. • **XTERMR6—**Function keys F5 to F12 behave like the default mode. Function keys F1 to F4 generate **ESC OP** through ESC OS, which are the sequences produced by the top row of the keypad on Digital terminals. • **SCO—**The function keys F1 to F12 generate ESC [M through ESC [X. The function and shift keys generate ESC [Y through ESC [j. The control and function keys generate ESC [k through ESC [v. The shift, control and function keys generate ESC [w through ESC [{. • **ESCN—**The default mode. The function keys match the general behavior of Digital terminals. The function keys generate sequences such as ESC [11~ and ESC [12~. • **VT400—**The function keys behave like the default mode. The top row of the numeric keypad generates ESC OP through ESC OS.

Name	Description
Redirection After BIOS POST	Whether BIOS console redirection should be active after BIOS POST is complete and control given to the OS bootloader. This can be one of the following: • **Always Enable—**BIOS Legacy console redirection is active during the OS boot and run time. • **Bootloader—**BIOS Legacy console redirection is disabled before giving control to the OS boot loader.

LOM and PCIe Slots Configuration Parameters

Name	Description
All Onboard LOM Ports	Whether all LOM ports are enabled or disabled. This can be one of the following: • **Disabled—**All LOM ports are disabled. • **Enabled—**All LOM ports are enabled.
LOM Port *n* OptionROM	Whether Option ROM is available on the LOM port designated by ***n***. This can be one of the following: • **Disabled—**Option ROM is not available on LOM port ***n***. • **Enabled—**Option ROM is available on LOM port ***n***. • **UEFI Only—**The expansion slot ***n*** is available for UEFI only. • **Legacy Only—**The expansion slot ***n*** is available for legacy only.
All PCIe Slots OptionROM	Whether the server can use the PCIe Option ROM expansion slots. This can be one of the following: • **Disabled—**PCIe Option ROMs are not available. • **Enabled—**PCIe Option ROMs are available. • **UEFI Only—**The expansion slot ***n*** is available for UEFI only. • **Legacy Only—**The expansion slot ***n*** is available for legacy only.

Name	Description
PCIe Slot:*n* OptionROM	Whether PCIe expansion slot ***n*** is available to the server. This can be one of the following: • **Disabled—**The expansion slot ***n*** is not available. • **Enabled—**The expansion slot ***n*** is available. • **UEFI Only—**The expansion slot ***n*** is available for UEFI only. • **Legacy Only—**The expansion slot ***n*** is available for legacy only.
PCIe Slot:*n* Link Speed	This option allows you to restrict the maximum speed of an adapter card installed in PCIe slot ***n***. This can be one of the following: • **GEN1—**2.5GT/s (gigatransfers per second) is the maximum speed allowed. • **GEN2—**5GT/s is the maximum speed allowed. • **GEN3—**8GT/s is the maximum speed allowed. • **Disabled—**The maximum speed is not restricted. For example, if you have a 3rd generation adapter card in PCIe slot 2 that you want to run at a maximum of 5GT/s instead of the 8GT/s that card supports, set the PCIe Slot 2 Link Speed to **GEN2**. The system then ignores the card's supported maximum speed of 8GT/s and forces it to run at a maximum of 5 GT/s.

Server Management BIOS Parameters for C420 Servers

Name	Description
FRB-2 Timer	Whether the FRB2 timer is used by CIMC to recover the system if it hangs during POST. This can be one of the following: • **Disabled—**The FRB2 timer is not used. • **Enabled—**The FRB2 timer is started during POST and used to recover the system if necessary.

Name	Description
OS Watchdog Timer	Whether the BIOS programs the watchdog timer with a specified timeout value. This can be one of the following: • **Disabled—**The watchdog timer is not used to track how long the server takes to boot. • **Enabled—**The watchdog timer tracks how long the server takes to boot. If the server does not boot within the length of time specified in the **OS Boot Watchdog Timer Timeout** field, the CIMC logs an error and takes the action specified in the **OS Boot Watchdog Policy** field.
OS Watchdog Timer Timeout	What timeout value the BIOS uses to configure the watchdog timer. This can be one of the following: • **5 Minutes—**The watchdog timer expires 5 minutes after the OS begins to boot. • **10 Minutes—**The watchdog timer expires 10 minutes after the OS begins to boot. • **15 Minutes—**The watchdog timer expires 15 minutes after the OS begins to boot. • **20 Minutes—**The watchdog timer expires 20 minutes after the OS begins to boot. **Note** This option is only applicable if you enable the OS Boot Watchdog Timer.
OS Watchdog Timer Policy	What action the system takes if the watchdog timer expires. This can be one of the following: • **Do Nothing—**The server takes no action if the watchdog timer expires during OS boot. • **Power Down—**The server is powered off if the watchdog timer expires during OS boot. • **Reset—**The server is reset if the watchdog timer expires during OS boot. **Note** This option is only applicable if you enable the OS Boot Watchdog Timer.

Name	Description
Boot Order Rules	How the server changes the boot order list defined through the CIMC GUI or CLI when there are no devices of a particular device type available or when the user defines a different boot order using the server's BIOS Setup Utility. The supported device types are: • **HDD—**Hard disk drive • **FDD—**Floppy disk drive • **CDROM—**Bootable CD-ROM or DVD • **PXE—**PXE boot • **EFI—**Extensible Firmware Interface The Boot Order Rules option can be one of the following: • **Strict—**When no devices of a particular type are available, the system creates a placeholder for that device type in the boot order list. When a device of that type becomes available, it is added to the boot order in the previously defined position. If the user defines a boot order through the server's BIOS Setup Utility, that boot order is given priority over the boot order configured through the CIMC GUI or CLI. All device types defined through CIMC that are not present in the boot order defined through the BIOS Setup Utility are removed from the boot order list. • **Loose—**When no devices of a particular type are available, the system removes that device type from the boot order. When a device of that type becomes available, the system adds it to the end of the boot order list. If the boot order is configured through the server's BIOS Setup Utility, that boot order is given priority over the boot order configured through the CIMC GUI or CLI. All device types defined through CIMC that are not present in the boot order defined through the BIOS Setup Utility are moved to the end of the boot order list.

C460 Servers

Main BIOS Parameters for C460 Servers

Name	Description
POST Error Pause	What happens when the server encounters a critical error during POST. This can be one of the following: • **Enabled—**The BIOS pauses the attempt to boot the server and opens the Error Manager when a critical error occurs during POST. • **Disabled—**The BIOS continues to attempt to boot the server.
Boot Option Retry	Whether the BIOS retries NON-EFI based boot options without waiting for user input. This can be one of the following: • **Enabled—**Continually retries NON-EFI based boot options without waiting for user input. • **Disabled—**Waits for user input before retrying NON-EFI based boot options.

Advanced BIOS Parameters for C460 Servers

Processor Configuration Parameters

Name	Description
Intel Turbo Boost Technology	Whether the processor uses Intel Turbo Boost Technology, which allows the processor to automatically increase its frequency if it is running below power, temperature, or voltage specifications. This can be one of the following: • **Disabled—**The processor does not increase its frequency automatically. • **Enabled—**The processor utilizes Turbo Boost Technology if required.

Name	Description
Enhanced Intel Speedstep Technology	Whether the processor uses Enhanced Intel SpeedStep Technology, which allows the system to dynamically adjust processor voltage and core frequency. This technology can result in decreased average power consumption and decreased average heat production. This can be one of the following: • **Disabled—**The processor never dynamically adjusts its voltage or frequency. • **Enabled—**The processor utilizes Enhanced Intel SpeedStep Technology and enables all supported processor sleep states to further conserve power. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.
Intel Hyper-Threading Technology	Whether the processor uses Intel Hyper-Threading Technology, which allows multithreaded software applications to execute threads in parallel within each processor. This can be one of the following: • **Disabled—**The processor does not permit hyperthreading. • **Enabled—**The processor allows for the parallel execution of multiple threads. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.
Number of Enabled Cores	Allows you to disable one or more of the physical cores on the server. This can be one of the following: • **All—**Enables all physical cores. This also enables Hyper Threading on the associated logical processor cores. • **1** through ***n*—**Specifies the number of physical processor cores that can run on the server. Each physical core has an associated logical core. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.

Name	Description
Execute Disable	Classifies memory areas on the server to specify where application code can execute. As a result of this classification, the processor disables code execution if a malicious worm attempts to insert code in the buffer. This setting helps to prevent damage, worm propagation, and certain classes of malicious buffer overflow attacks. This can be one of the following: • **Disabled—**The processor does not classify memory areas. • **Enabled—**The processor classifies memory areas. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.
Intel Virtualization Technology	Whether the processor uses Intel Virtualization Technology (VT), which allows a platform to run multiple operating systems and applications in independent partitions. This can be one of the following: • **Disabled—**The processor does not permit virtualization. • **Enabled—**The processor allows multiple operating systems in independent partitions. **Note** If you change this option, you must power cycle the server before the setting takes effect.
Intel VT for Directed IO	Whether the processor uses Intel Virtualization Technology for Directed I/O (VT-d). This can be one of the following: • **Disabled—**The processor does not use virtualization technology. • **Enabled—**The processor uses virtualization technology.
Intel VT-d Interrupt Remapping	Whether the processor supports Intel VT-d Interrupt Remapping. This can be one of the following: • **Disabled—**The processor does not support remapping. • **Enabled—**The processor uses VT-d Interrupt Remapping as required.
Intel VT-d Coherency Support	Whether the processor supports Intel VT-d Coherency. This can be one of the following: • **Disabled—**The processor does not support coherency. • **Enabled—**The processor uses VT-d Coherency as required.

Name	Description
Intel VT-d Address Translation Services	Whether the processor supports Intel VT-d Address Translation Services (ATS). This can be one of the following: • **Disabled—**The processor does not support ATS. • **Enabled—**The processor uses VT-d ATS as required.
Intel VT-d PassThrough DMA	Whether the processor supports Intel VT-d Pass-through DMA. This can be one of the following: • **Disabled—**The processor does not support pass-through DMA. • **Enabled—**The processor uses VT-d Pass-through DMA as required.
Direct Cache Access	Allows processors to increase I/O performance by placing data from I/O devices directly into the processor cache. This setting helps to reduce cache misses. This can be one of the following: • **Disabled—**Data from I/O devices is not placed directly into the processor cache. • **Enabled—**Data from I/O devices is placed directly into the processor cache.
Processor C3 Report	Whether the BIOS sends the C3 report to the operating system. When the OS receives the report, it can transition the processor into the lower C3 power state to decrease energy usage while maintaining optimal processor performance. This can be one of the following: • **Disabled—**The BIOS does not send the C3 report. • **ACPI C2—**The BIOS sends the C3 report using the ACPI C2 format, allowing the OS to transition the processor to the C3 low power state. • **ACPI C3—**The BIOS sends the C3 report using the ACPI C3 format, allowing the OS to transition the processor to the C3 low power state.

Name	Description
Processor C6 Report	Whether the BIOS sends the C6 report to the operating system. When the OS receives the report, it can transition the processor into the lower C6 power state to decrease energy usage while maintaining optimal processor performance. This can be one of the following: • **Disabled—**The BIOS does not send the C6 report. • **Enabled—**The BIOS sends the C6 report, allowing the OS to transition the processor to the C6 low power state.
Package C State Limit	The amount of power available to the server components when they are idle. This can be one of the following: • **C0 state—**The server provides all server components with full power at all times. This option maintains the highest level of performance and requires the greatest amount of power. • **C1 state—**When the CPU is idle, the system slightly reduces the power consumption. This option requires less power than C0 and allows the server to return quickly to high performance mode. • **C3 state—**When the CPU is idle, the system reduces the power consumption further than with the C1 option. This requires less power than C1 or C0, but it takes the server slightly longer to return to high performance mode. • **C6 state—**When the CPU is idle, the system reduces the power consumption further than with the C3 option. This option saves more power than C0, C1, or C3, but there may be performance issues until the server returns to full power. • **C7 state—**When the CPU is idle, the server makes a minimal amount of power available to the components. This option saves the maximum amount of power but it also requires the longest time for the server to return to high performance mode. • **No Limit—**The server may enter any available C state. **Note** This option is used only if **CPU C State** is enabled.

Name	Description
CPU C State	Whether the system can enter a power savings mode during idle periods. This can be one of the following: • **Disabled—**The system remains in high performance state even when idle. • **Enabled—**The system can reduce power to system components such as the DIMMs and CPUs. The amount of power reduction is specified in the **Package C State Limit** field.
C1E	Whether the CPU transitions to its minimum frequency when entering the C1 state. This can be one of the following: • **Disabled—**The CPU continues to run at its maximum frequency in C1 state. • **Enabled—**The CPU transitions to its minimum frequency. This option saves the maximum amount of power in C1 state. **Note** This option is used only if **CPU C State** is enabled.

Memory Configuration Parameters

Name	Description
Select Memory RAS	How the memory reliability, availability, and serviceability (RAS) is configured for the server. This can be one of the following: • **Maximum Performance—**System performance is optimized. • **Mirroring—**System reliability is optimized by using half the system memory as backup. • **Sparing—**The system reserves some memory for use in the event a DIMM fails. If that happens, the server takes the DIMM offline and replaces it with the reserved memory. This option provides less redundancy than mirroring, but it leaves more of the memory available for programs running on the server.

Name	Description
NUMA Optimized	Whether the BIOS supports NUMA. This can be one of the following: • **Disabled—**The BIOS does not support NUMA. • **Enabled—**The BIOS includes the ACPI tables that are required for NUMA-aware operating systems. If you enable this option, the system must disable Inter-Socket Memory interleaving on some platforms.
Sparing Mode	The sparing mode used by the CIMC. This can be one of the following: • **Rank Sparing—**The spared memory is allocated at the rank level. • **DIMM Sparing—**The spared memory is allocated at the DIMM level. **Note** This option is used only if **Select Memory RAS** is set to **Sparing**.
Mirroring Mode	Mirroring is supported across Integrated Memory Controllers (IMCs) where one memory riser is mirrored with another. This can be one of the following: • **Intersocket—**Each IMC is mirrored across two sockets. • **Intrasocket—**One IMC is mirrored with another IMC in the same socket. **Note** This option is used only if **Select Memory RAS** is set to **Mirroring**.
Patrol Scrub	Whether the system actively searches for, and corrects, single bit memory errors even in unused portions of the memory on the server. This can be one of the following: • **Disabled—**The system checks for memory ECC errors only when the CPU reads or writes a memory address. • **Enabled—**The system periodically reads and writes memory searching for ECC errors. If any errors are found, the system attempts to fix them. This option may correct single bit errors before they become multi-bit errors, but it may adversely affect performance when the patrol scrub is running.

Name	Description
Patrol Scrub Interval	Controls the time interval between each patrol scrub memory access. A lower interval scrubs the memory more often but requires more memory bandwidth. Select a value between 5 and 23. The default value is 8. **Note** This option is used only if **Patrol Scrub** is enabled.
CKE Low Policy	Controls the DIMM power savings mode policy. This can be one of the following: • **Disabled—**DIMMs do not enter power saving mode. • **Slow—**DIMMs can enter power saving mode, but the requirements are higher. Therefore, DIMMs enter power saving mode less frequently. • **Fast—**DIMMs enter power saving mode as often as possible. • **Auto—**The BIOS controls when a DIMM enters power saving mode based on the DIMM configuration.

Serial Port Configuration Parameters

Name	Description
Serial A Enable	Whether serial port A is enabled or disabled. This can be one of the following: • **Disabled—**The serial port is disabled. • **Enabled—**The serial port is enabled.

USB Configuration Parameters

Name	Description
Make Device Non-Bootable	Whether the server can boot from a USB device. This can be one of the following: • **Disabled—**The server can boot from a USB device. • **Enabled—**The server cannot boot from a USB device.

PCI Configuration Parameters

Name	Description
Memory Mapped I/O Above 4GB	Whether to enable or disable memory mapped I/O of 64-bit PCI devices to 4GB or greater address space. Legacy option ROMs are not able to access addresses above 4GB. PCI devices that are 64-bit compliant but use a legacy option ROM may not function correctly with this setting enabled. This can be one of the following: • **Disabled—**The server does not map I/O of 64-bit PCI devices to 4GB or greater address space. • **Enabled—**The server maps I/O of 64-bit PCI devices to 4GB or greater address space.
Onboard NIC *n* ROM	Whether the system loads the embedded PXE option ROM for the onboard NIC designated by ***n***. This can be one of the following: • **Disabled—**PXE option ROM is not available for NIC ***n***. • **Enabled—**PXE option ROM is available for NIC ***n***.
PCIe OptionROMs	Whether the server can use the PCIe Option ROM expansion slots. This can be one of the following: • **Disabled—**PCIe Option ROMs are not available. • **Enabled—**PCIe Option ROMs are available. • **UEFI Only—**The expansion slot ***n*** is available for UEFI only. • **Legacy Only—**The expansion slot ***n*** is available for legacy only.
PCIe Slot *n* ROM	Whether PCIe expansion slot ***n*** is available to the server. This can be one of the following: • **Disabled—**The expansion slot ***n*** is not available. • **Enabled—**The expansion slot ***n*** is available. • **UEFI Only—**The expansion slot ***n*** is available for UEFI only. • **Legacy Only—**The expansion slot ***n*** is available for legacy only.

Name	Description
Onboard Gbit LOM	Whether Gbit LOM is enabled or disabled on the server. This can be one of the following: • **Disabled—**Gbit LOM is not available. • **Enabled—**10Git LOM is available.
Onboard 10Gbit LOM	Whether 10Gbit LOM is enabled or disabled on the server. This can be one of the following: • **Disabled—**10GBit LOM is not available. • **Enabled—**10GBit LOM is available.
Sriov	Whether SR-IOV (Single Root I/O Virtualization) is enabled or disabled on the server. This can be one of the following: • **Disabled—**SR-IOV is disabled. • **Enabled—**SR-IOV is enabled.
IOH Resource Allocation	Enables you to distribute 64KB of 16-bit IO resources between IOH0 and IOH1 as per system requirement. This can be one of the following: • **IOH0 24k IOH1 40k—** Allocates 24KB of 16-bit IO resources to IOH0 and 40KB of 16-bit IO resources to IOH1. • **IOH0 32k IOH1 32k—** Allocates 32KB of 16-bit IO resources to IOH0 and 32KB of 16-bit IO resources to IOH1. • **IOH0 40k IOH1 24k—** Allocates 40KB of 16-bit IO resources to IOH0 and 24KB of 16-bit IO resources to IOH1. • **IOH0 48k IOH1 16k—** Allocates 48KB of 16-bit IO resources to IOH0 and 16KB of 16-bit IO resources to IOH1. • **IOH0 56k IOH1 8k—** Allocates 56KB of 16-bit IO resources to IOH0 and 8KB of 16-bit IO resources to IOH1.

Server Management BIOS Parameters for C460 Servers

Name	Description
Assert NMI on SERR	Whether the BIOS generates a non-maskable interrupt (NMI) and logs an error when a system error (SERR) occurs. This can be one of the following: • **Disabled—**The BIOS does not generate an NMI or log an error when a SERR occurs. • **Enabled—**The BIOS generates an NMI and logs an error when a SERR occurs. You must enable this setting if you want to enable **Assert NMI on PERR**.
Assert NMI on PERR	Whether the BIOS generates a non-maskable interrupt (NMI) and logs an error when a processor bus parity error (PERR) occurs. This can be one of the following: • **Disabled—**The BIOS does not generate an NMI or log an error when a PERR occurs. • **Enabled—**The BIOS generates an NMI and logs an error when a PERR occurs. You must enable **Assert NMI on SERR** to use this setting.
Console Redirection	Allows a serial port to be used for console redirection during POST and BIOS booting. After the BIOS has booted and the operating system is responsible for the server, console redirection is irrelevant and has no effect. This can be one of the following: • **Disabled—**No console redirection occurs during POST. • **Serial Port A—**Enables console redirection on serial port A during POST. **Note** If you enable this option, you also disable the display of the Quiet Boot logo screen during POST.
Flow Control	Whether a handshake protocol is used for flow control. Request to Send / Clear to Send (RTS/CTS) helps to reduce frame collisions that can be introduced by a hidden terminal problem. This can be one of the following: • **None—**No flow control is used. • **RTS-CTS—**RTS/CTS is used for flow control. **Note** This setting must match the setting on the remote terminal application.

Name	Description
Baud Rate	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: • **9.6k—**A 9600 BAUD rate is used. • **19.2k—**A 19200 BAUD rate is used. • **38.4k—**A 38400 BAUD rate is used. • **57.6k—**A 57600 BAUD rate is used. • **115.2k—**A 115200 BAUD rate is used. **Note** This setting must match the setting on the remote terminal application.
Terminal Type	What type of character formatting is used for console redirection. This can be one of the following: • **PC-ANSI—**The PC-ANSI terminal font is used. • **VT100—**A supported vt100 video terminal and its character set are used. • **VT100-PLUS—**A supported vt100-plus video terminal and its character set are used. • **VT-UTF8—**A video terminal with the UTF-8 character set is used. **Note** This setting must match the setting on the remote terminal application.
OS Boot Watchdog Timer Timeout	What timeout value the BIOS uses to configure the watchdog timer. This can be one of the following: • **5 Minutes—**The watchdog timer expires 5 minutes after the OS begins to boot. • **10 Minutes—**The watchdog timer expires 10 minutes after the OS begins to boot. • **15 Minutes—**The watchdog timer expires 15 minutes after the OS begins to boot. • **20 Minutes—**The watchdog timer expires 20 minutes after the OS begins to boot. **Note** This option is only applicable if you enable the OS Boot Watchdog Timer.

Name	Description
OS Boot Watchdog Policy	What action the system takes if the watchdog timer expires. This can be one of the following: • **Power Off—**The server is powered off if the watchdog timer expires during OS boot. • **Reset—**The server is reset if the watchdog timer expires during OS boot. **Note** This option is only applicable if you enable the OS Boot Watchdog Timer.
Legacy OS Redirection	Whether redirection from a legacy operating system, such as DOS, is enabled on the serial port. This can be one of the following: • **Disabled—**The serial port enabled for console redirection is hidden from the legacy operating system. • **Enabled—**The serial port enabled for console redirection is visible to the legacy operating system.
OS Boot Watchdog Timer	Whether the BIOS programs the watchdog timer with a specified timeout value. This can be one of the following: • **Disabled—**The watchdog timer is not used to track how long the server takes to boot. • **Enabled—**The watchdog timer tracks how long the server takes to boot. If the server does not boot within the length of time specified in the **OS Boot Watchdog Timer Timeout** field, the CIMC logs an error and takes the action specified in the **OS Boot Watchdog Policy** field.

INDEX

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W

X