Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide, Release 1.3

First Published: March 11, 2011

Last Modified: October 17, 2011

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-23489-03b

© 2011 Cisco Systems, Inc. All rights reserved.

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

New and Changed Information for this Release

The following table provides an overview of the significant changes to this guide for this current release. The table does not provide an exhaustive list of all changes made to the configuration guides or of the new features in this release. For information about new supported hardware in this release, see the *Release Notes for Cisco UCS C-Series Rack-Mount Servers* available through the Cisco UCS C-Series Servers Documentation Roadmap.

Feature	Description	Where Documented
Cisco Flexible Flash	Some models support an internal Secure Digital (SD) memory card for storage of server software tools and utilities.	Cisco Flexible Flash, on page 24
Power statistics and policies	Power consumption statistics can be viewed in the CIMC GUI and CLI. In addition, you can now define: • The maximum amount of power a server can use • The action the system should take if the server exceeds the specified maximum • The action the system should take if the server unexpectedly loses power	Viewing the Power Statistics, on page 21
Network Interface Virtualization (NIV) mode	If your server has a supported network adapter card, such as the Cisco UCS P81E Virtual Interface Card, this feature enables vNICs to: • Be assigned to a specific channel • Be associated with a port profile • Fail over to another vNIC if there are communication problems	Creating a vNIC, on page 102
BIOS parameters	Some BIOS parameters can now be configured through the CIMC GUI and CLI.	Configuring Main BIOS Settings, on page 27
PCI adapter information available	Details about any PCI adapters installed in the server are now available through the CIMC GUI and CLI.	Viewing PCI Adapter Properties, on page 50
Fault sensor information	Fault sensor information is now available through the CIMC GUI and CLI.	Viewing the Fault Summary, on page 53
SNMP changes	You can define SNMP access and contact information in the CIMC GUI and CLI.	Configuring SNMP Properties, on page 112

Feature	Description	Where Documented
SNMP trap changes	You can send a test SNMP trap message through the CIMC GUI and CLI.	Configuring SNMP Trap Settings, on page 121
Storage inventory	More storage details, including RAID information, are displayed in the CIMC GUI and CLI.	Viewing Storage Properties, on page 49
Expanded memory details	More memory details are displayed in the CIMC GUI and CLI.	Viewing Memory Properties, on page 46

Organization

This document includes the following chapters:

Chapter	Title	Description
Chapter 1	Overview	Describes the Cisco UCS C-Series Rack-Mount Servers and the CIMC GUI.
Chapter 2	Installing the Server OS	Describes how to configure an operating system (OS) on the server.
Chapter 3	Managing the Server	Describes how to configure the boot device order, how to control power to the server, and how to reset the server.
Chapter 4	Viewing Server Properties	Describes how to view the CPU, memory, power supply, storage, and PCI adapter properties of the server.
Chapter 5	Viewing Server Sensors	Describes how to view the power supply, fan, temperature, voltage, current, and storage sensors.
Chapter 6	Managing Remote Presence	Describes how to configure and manage the virtual KVM, virtual media, and the serial over LAN connection.
Chapter 7	Managing User Accounts	Describes how to add or modify user accounts, how to configure Active Directory to authenticate users, and how to manage user sessions.
Chapter 8	Configuring Network-Related Settings	Describes how to configure network interfaces, network settings, and network security.
Chapter 9	Managing Network Adapters	Describes how to create, configure, and manage network adapters.

Chapter	Title	Description
Chapter 10	Configuring Communication Services	Describes how to configure server management communication by HTTP, SSH, IPMI, XML API, and SNMP.
Chapter 11	Managing Certificates	Describes how to generate, upload, and manage server certificates.
Chapter 12	Configuring Platform Event Filters	Describes how to configure and manage platform event filters.
Chapter 13	CIMC Firmware Management	Describes how to obtain, install, and activate firmware images.
Chapter 14	Viewing Logs	Describes how to view, export, and clear CIMC and system event log messages.
Chapter 15	Server Utilities	Describes how to export support data, how to clear or recover the BIOS, how to reset the server configuration to factory defaults, how to back up the configuration, and how to reboot the management interface.

Conventions

This document uses the following conventions:

Convention	Indication
bold font	Commands, keywords, GUI elements, and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
`courier`font	Terminal sessions and information that the system displays appear in `courier` 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.

Convention	Indication
< >	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*.

Tip Means *the following information will help you solve a problem*.

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 Means *reader be warned*. In this situation, you might perform an action that could result in bodily injury.

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.

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to ucs-docfeedback@external.cisco.com. We appreciate your feedback.

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 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 *Release Notes for Cisco Integrated Management Controller*.

Overview of the Server Software

The Cisco UCS C-Series Rack-Mount Server ships with two major software systems installed.

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 main server CPU runs an OS such as Windows or Linux. The server ships with a pre-installed OS, but you can install a different OS using the DVD drive or over the network. You can use CIMC to install the new OS 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:

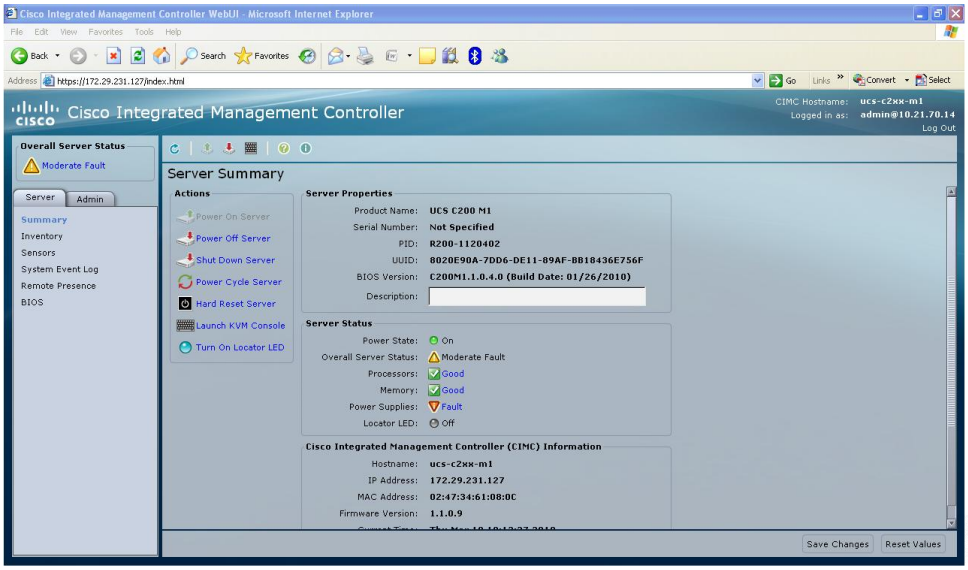
- Java 1.6 or later
- HTTP and HTTPS enabled
- Adobe Flash Player 10 or later

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

Figure 1 shows the CIMC home page.

Figure 1: CIMC Home Page



Navigation Pane

The Navigation pane displays on the left side in the CIMC user interface. Clicking links on the **Server** or **Admin** tabs in the **Navigation** pane displays the selected pages in the **Work** pane on the right side of the CIMC user interface.

The following table describes the elements in the **Navigation** pane:

Element Name	Description
Overall Server Status area	The **Overall Server Status** area is found above the **Server** and **Admin** tabs. Click this area to refresh the **Server Summary** page.
Server tab	The **Server** tab is found in the **Navigation** pane. It contains links to the following pages: • **Summary** • **Inventory** • **Sensors** • **System Event Log** • **Remote Presence** • **BIOS**

	• **Power Policies** • **Faults Summary**
Admin tab	The **Admin** tab is found in the **Navigation** pane. It contains links to the following pages: • **User Management** • **Network** • **Communications Services** • **Certificate Management** • **CIMC Log** • **Event Management** • **Firmware Management** • **Utilities**

Work Pane

The **Work** pane displays on the right side of the UI. Different pages appear in the **Work** pane, depending on what link you click on the **Server** or **Admin** tab.

The following table describes the elements and pages in the **Work** pane.

Page or Element Name	Description
Summary	There are four areas on this page: • **Actions**—Use this area to control server power, reset the server, launch the KVM console, or control the locator LED. • **Server Properties**—Use this area to view the general server properties and assign a server description. • **Server Status**—Use this area to view the overall status of the major server subsystems. • **CIMC Information**—Use this area to view the server management name, network addresses, firmware version, and current date and time.
Inventory	There are six tabs on the page: • **CPUs**—Use this tab to view information about the CPU. • **Memory**—Use this tab to view information about memory. • **Power Supplies**—Use this tab to view information about power supplies.

	• **Network Adapters**—Use this tab to view information about network adapters. • **Storage**—Use this tab to view information about storage. • **PCI Adapters**—Use this tab to view information about PCI adapters.
Sensors	There are seven tabs on the page: • **Power Supply**—Use this tab to view the power supply sensor. • **Fan**—Use this tab to view the fan sensor. • **Temperature**—Use this tab to view the temperature sensor. • **Voltage**—Use this tab to view the voltage sensor. • **Current**—Use this tab to view the current sensor. • **LEDs**—Use this tab to view the state and color of the LEDs. • **Storage**—Use this tab to view the state of the storage devices.
System Event Log	Use this page to view the system event log.
Remote Presence	There are three tabs on the page: • **Virtual KVM**—Use this tab to set vKVM properties. • **Virtual Media**—Use this tab to set virtual media properties. • **Serial over LAN**—Use this tab to set serial over LAN properties.
BIOS	There are three areas on this page: • **Actions**—Use this area to configure the server boot order, recover corrupted BIOS, and clear the BIOS CMOS. • **BIOS Properties**—Use this area to view the running version of the BIOS. • **Boot Order**—Use this area to view the configured and actual boot order.
Power Policies	There are two areas on this page: • **Power Capping**—Use this area to view the power statistics and to configure capping of the server power consumption. • **Power Restore Policy**—Use this area to configure how the server power is restored after an outage.
Fault Summary	There are two areas on this page: • **Discrete Sensors**—Use this area to view the state of discrete sensors.

	• **Threshold Sensors**—Use this area to to view the state of threshold sensors.
User Management	There are three tabs on the page: • **Local Users**—Use this tab to create or modify user accounts. • **Active Directory**—Use this tab to set active directory properties. • **Sessions**—Use this tab to view current user sessions.
Network	There are two tabs on the page: • **Network Settings**—Use this tab to set network properties. • **Network Security**—Use this tab to set up network security.
Communications Services	There are four areas on this page: • **HTTP Properties**—Use this area to set HTTP properties. • **SSH Properties**—Use this area to set SSH properties. • **IPMI over LAN Properties**—Use this area to set IPMI over LAN properties. • **SNMP Properties**—Use this area to set SNMP properties.
Certificate Management	There are two areas on this page: • **Actions**—Use this area to generate and upload a certificate. • **Current Certificate**—Use this area to view the current certificate for the server.
CIMC Log	There are two tabs on the page: • **CIMC Log**—Use this tab to view the CIMC Log. • **Remote Logging**—Use this tab to configure the sending of log messages to remote syslog servers.
Event Management	There are two tabs on the page: • **Platform Event Filters**—Use this tab to set up platform event filters. • **Trap Settings**—Use this tab to set up SNMP traps.
Firmware Management	There are three areas on this page: • **Actions**—Use this area to install CIMC firmware from a client browser or TFTP server, or to activate installed CIMC firmware.

	• **CIMC Firmware**—Use this area to view the status of the running, backup, and boot-loader versions of the firmware. • **Last Firmware Install**—Use this area to view information about the last firmware update.
Utilities	There are three areas on this page: • **Actions**—Use this area to export technical support data, export or import the CIMC configuration, reset the CIMC to factory default, and reboot the CIMC. • **Last Technical Support Data Export**—Use this area to view information about the last technical support data export. • **CIMC Configuration Import/Export**—Use this area to view the action type and its status.

Toolbar

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

Element 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	Launches help.
Info	Displays CIMC information.

Cisco Integrated Management Controller Online Help Overview

The Cisco Integrated Management Controller 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 GUI page and in each dialog box.

To access the page help, do the following:

- In a particular tab in the 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 the available C-Series documentation, see the *Cisco UCS C-Series Servers Documentation Roadmap* at 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

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.

CHAPTER 3

Managing the Server

This chapter includes the following sections:

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:

Name	Description
	• **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.
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**

Name	Description
	• **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.

Toggling the Locator LED

Before You Begin

You must have user privileges for all power control operations including this operation.

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 locator LED turns on and is blinking.

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

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 • **PXE**—PXE boot • **EFI**—Extensible Firmware Interface
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.

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.
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

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.
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, the number of seconds before the server is restarted after chassis power is restored. Enter an integer between 0 and 240.

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 four virtual USB drives. Three are preloaded with Cisco software and the fourth can hold a user-installed hypervisor or other content. The four virtual drives are as follows:

- Cisco UCS Server Configuration Utility (bootable)
- User-installed (may be bootable)
- Cisco drivers (not bootable)
- Cisco Host Upgrade Utility (bootable)

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

Configuring the Flexible Flash Controller Properties

Before You Begin

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

Procedure

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 **Storage** tab.

Step 4 In the **Storage Adapters** table, click the FlexFlash controller.
The properties of the selected FlexFlash controller appear in the tabbed menu below the **Storage Adapters** area.

Step 5 In the **Storage Card** tabbed menu, click the **Controller Info** tab.

Step 6 In the **Actions** area, click **Configure Operational Profile**.
The **Operational Profile** dialog box opens.

Step 7 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.

Name	Description
	This name cannot be changed.
Virtual Drives Enabled field	The virtual drives that can be made available to the server as a USB-style drive. Check the box next to each virtual drive you want the server to access. The options are: • **SCU**—The server can access the Cisco UCS Server Configuration Utility. • **Drivers**—The server can access the Cisco drivers. • **HV**—The server can access a user-installed hypervisor. • **HUU**—The server can access the Cisco Host Upgrade Utility.
RAID Primary Member field	The slot in which the primary copy of the data resides. **Important** Currently, Cisco Flexible Flash cards are only supported in slot 1. Therefore, this field must be set to slot1.
Error Count Threshold field	The number of read/write errors that are permitted while accessing the Cisco Flexible Flash card. If the number of errors exceeds this threshold, the Cisco Flexible Flash card is disabled and you must reset it manually before CIMC attempts to access it again. To specify a read/write error threshold, enter an integer between 1 and 255. To specify that the card should never be disabled regardless of the number of errors encountered, enter 0 (zero).

Step 8 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 In the **Navigation** pane, click the **Server** tab.

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

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

Step 4 In the **Storage Adapters** table, click the FlexFlash controller.
The properties of the selected FlexFlash controller appear in the tabbed menu below the **Storage Adapters** area.

Step 5 In the **Storage Card** tabbed menu, click the **Controller Info** tab.

Step 6 In the **Actions** area, click **Reset Cisco Flex Flash**.

Step 7 Click **OK** to confirm.

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**.
The **Configure BIOS Parameters** dialog box opens.

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

Step 5 Check or clear the **Reboot Host Immediately** checkbox.
If checked, the server is rebooted immediately after you make changes to the BIOS parameters.

To specify that the server should not reboot automatically, clear this check box. Any parameter changes will take effect the next time the server is rebooted.

Step 6 In the **Main** tab, update the BIOS settings fields.
For descriptions and information about the options for each BIOS setting, see the following topics:

- Main BIOS Settings, on page 29

Step 7 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**.

The **Configure BIOS Parameters** dialog box opens.

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

Step 5 Check or clear the **Reboot Host Immediately** checkbox.
If checked, the server is rebooted immediately after you make changes to the BIOS parameters.

To specify that the server should not reboot automatically, clear this check box. Any parameter changes will take effect the next time the server is rebooted.

Step 6 In the **Advanced** tab, update the BIOS settings fields.
For descriptions and information about the options for each BIOS setting, see the following topics:

- Advanced: Processor BIOS Settings, on page 29
- Advanced: Memory BIOS Settings, on page 35
- Advanced: Mass Storage Controller BIOS Settings, on page 37
- Advanced: Serial Port BIOS Settings, on page 37
- Advanced: USB BIOS Settings, on page 38
- Advanced: PCI BIOS Settings, on page 39

Step 7 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**.
The **Configure BIOS Parameters** dialog box opens.

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

Step 5 Check or clear the **Reboot Host Immediately** checkbox.
If checked, the server is rebooted immediately after you make changes to the BIOS parameters.

To specify that the server should not reboot automatically, clear this check box. Any parameter changes will take effect the next time the server is rebooted.

Step 6 In the **Server Management** tab, update the BIOS settings fields.
For descriptions and information about the options for each BIOS setting, see the following topic:

- Server Management BIOS Settings, on page 40

Step 7 Click **Save Changes**.

Server BIOS Settings

The tables in the following sections list the server BIOS settings that you can view and configure.

Note We recommend that you verify the support for BIOS settings in your server. Depending on your installed hardware, some settings may not be supported.

Main BIOS Settings

Name	Description
Reboot Host Immediately	If checked, the server is rebooted immediately after you click **Save Changes**. To specify that the server should not reboot automatically, clear this check box. Any parameter changes will take effect the next time the server is rebooted.
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.
USB Boot Priority	Whether the BIOS tries to boot from any available USB device before it tries to boot from the server hard drive. This can be one of the following: • **Enabled**—The server attempts to boot from a USB device if one is available. In addition, when a USB device is discovered, it is put at the top of its boot category. • **Disabled**—The server attempts to boot from the server hard drive before it tries USB devices. In addition, when a USB device is discovered, it is put at the bottom of its boot category.

Advanced: Processor BIOS Settings

Name	Description
Intel Turbo Boost Technology	Whether the processor uses Intel Turbo Boost Technology, which allows the processor to automatically increase its

Name	Description
	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.
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	Sets the state of logical processor cores in a package. If you disable this setting, Hyper Threading is also disabled. This can be one of the following: • **All**—Enables multi processing on all logical processor cores. • **1** through *n*—Specifies the number of logical processor cores that can run on the server. To disable multi processing and have only one logical processor core running on the server, select 1. 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 processor sends the C3 report to the operating system. This can be one of the following: • **Disabled**—The processor does not send the C3 report. • **ACPI C2**—The processor sends the C3 report using the ACPI C2 format. • **ACPI C3**—The processor sends the C3 report using the ACPI C3 format.
Processor C6 Report	Whether the processor sends the C6 report to the operating system. This can be one of the following: • **Disabled**—The processor does not send the C6 report. • **Enabled**—The processor sends the C6 report.
Processor C7 Report	Whether the processor sends the C7 report to the operating system. This can be one of the following: • **Disabled**—The processor does not send the C7 report. • **Enabled**—The processor sends the C7 report.

Name	Description
CPU Performance	Sets the CPU performance profile for the server. The performance profile consists of the following options: • Data Reuse Optimization • DCU Streamer Prefetcher • DCU IP Prefetcher • Hardware Prefetcher • Adjacent Cache-Line Prefetch This can be one of the following: • **Enterprise**—Only the DCU IP Prefetcher is enabled. The rest of the options are disabled. • **High Throughput**—All options are enabled. • **HPC**—Data Reuse Optimization is disabled and all other 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. **Note** You must select **Custom** in the **CPU Performance** drop-down list in order to specify this value. For any value other than **Custom**, this option is overridden by the setting in the selected CPU performance profile.
Adjacent Cache-Line Prefetch	Whether the processor uses the Intel Adjacent Cache-Line Prefetch mechanism to fetch data when necessary. This can be one of the following: • **Disabled**—The Adjacent Cache-Line Prefetch mechanism is not used. • **Enabled**— The Adjacent Cache-Line Prefetch mechanism is used when cache issues are detected.

Name	Description
	Note You must select **Custom** in the **CPU Performance** drop-down list in order to specify this value. For any value other than **Custom**, this option is overridden by the setting in the selected CPU performance profile.
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.
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.
C1E	Whether the CPU transitions to its minimum frequency when entering the C1 state. This can be one of the following:

Name	Description
	• **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.

Advanced: Memory BIOS Settings

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**—System reliability is enhanced with a degree of memory redundancy while making more memory available to the operating system than mirroring.
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.
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.
Sparing Mode	The sparing mode used by the CIMC. This can be one of the following:

Name	Description
	• **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.
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 set to **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.

Name	Description
	• **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.

Advanced: Mass Storage Controller BIOS Settings

Name	Description
Onboard SATA Controller	Whether the processor uses its built-in SATA controller. This can be one of the following: • **Disabled**—The server does not use the onboard SATA controller. • **Enabled**—The processor uses the built-in SATA controller.
SATA Mode	The mode in which the SATA controller runs. This can be one of the following: • **AHCI**—The controller enables the Advanced Host Controller Interface (AHCI) and disables RAID. • **Compatibility**—The controller disables both AHCI and RAID and runs in IDE emulation mode. • **Enhanced**—The controller enables both AHCI and RAID. • **S/W RAID**—The controller enables RAID and disables the AHCI.

Advanced: Serial Port BIOS Settings

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.
Serial A Address	If serial port A is enabled, select the hex address that it should use. This can be one of the following: • **3F8** • **2F8** • **3E8** • **2E8**

Name	Description
Serial B Enable	Whether serial port B is enabled or disabled. This can be one of the following: • **Disabled**—The serial port is disabled. • **Enabled**—The serial port is enabled.
Serial B Address	If serial port B is enabled, select the hex address that it should use. This can be one of the following: • **3F8** • **2F8** • **3E8** • **2E8**

Advanced: USB BIOS Settings

Name	Description
USB Controller	Whether the processor uses its built-in USB controller. This can be one of the following: • **Disabled**—The server does not use the built-in USB controller. • **Enabled**—The processor uses the built-in USB controller.
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.
USB Performance Mode	Whether the server uses USB 2.0 or USB 1.1 mode. This can be one of the following: • **High Performance**—The server enables the EHCI (USB 2.0) controllers so that all USB devices function in USB 2.0 mode. This option maximizes USB device performance but requires additional power. • **Lower Idle Power**—The server disables the EHCI (USB 2.0) controllers so that all USB devices function in USB 1.1 mode. This option requires less power but decreases USB device performance.

Advanced: PCI BIOS Settings

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 Gbit NIC 1	Whether the first onboard Network Interface Card (NIC) is enabled or disabled on the server. This can be one of the following: • **Disabled**—NIC 1 is not available. • **Enabled**—NIC 1 is available.
Onboard Gbit NIC 2	Whether the second onboard NIC is enabled or disabled on the server. This can be one of the following: • **Disabled**—NIC 2 is not available. • **Enabled**—NIC 2 is available.
Onboard Gbit NIC 1 ROM	Whether the system loads the embedded PXE option ROM for the first onboard NIC. This can be one of the following: • **Disabled**—PXE option ROM is not available for NIC 1. • **Enabled**—PXE option ROM is available for NIC 1.
Onboard Gbit NIC 2 ROM	Whether the system loads the embedded PXE option ROM for the second onboard NIC. This can be one of the following: • **Disabled**—PXE option ROM is not available for NIC 2. • **Enabled**—PXE option ROM is available for NIC 2.
Onboard Gbit NIC 3 ROM	Whether the system loads the embedded PXE option ROM for the third onboard NIC. This can be one of the following: • **Disabled**—PXE option ROM is not available for NIC 3. • **Enabled**—PXE option ROM is available for NIC 3.

Name	Description
Onboard Gbit NIC 4 ROM	Whether the system loads the embedded PXE option ROM for the fourth onboard NIC. This can be one of the following: • **Disabled**—PXE option ROM is not available for NIC 4. • **Enabled**—PXE option ROM is available for NIC 4.
PCIe Option ROMs	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.
PCIe Slot *n* ROM	Whether the PCIe expansion slot designated by ***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.
PCIe Mezzanine Slot ROM	Whether the PCIe mezzanine slot expansion ROM is available to the server. This can be one of the following: • **Disabled**—The mezzanine slot is not available. • **Enabled**—The mezzanine slot is available.
Active Video	How the server displays video. This can be one of the following: • **Auto**—The server uses an external graphics adapter for display if one is available. • **Onboard Device**—The server always uses its internal graphics adapter even if an external graphics adapter is available.

Server Management BIOS Settings

Name	Description
Reboot Host Immediately	If checked, the server is rebooted immediately after you click **Save Changes**. To specify that the server should not reboot automatically, clear this check box. Any parameter changes will take effect the next time the server is rebooted.
Boot Option Retry	Whether the BIOS retries NON-EFI based boot options without waiting for user input. This can be one of the following:

Name	Description
	• **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.
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.
FRB2 Enable	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.
PlugNPlay BMC Detection	Whether the system automatically detects the BMC in ACPI-compliant operating systems. This can be one of the following: • **Disabled**—The system never automatically detects the BMC. • **Enabled**—The system automatically detects the BMC whenever possible.
ACPI1.0 Support	Whether the BIOS publishes the ACPI 1.0 version of FADT in the Root System Description table. This version may be required for compatibility with OS versions that only support ACPI 1.0. This can be one of the following:

Name	Description
	• **Disabled**—ACPI 1.0 version is not published. • **Enabled**—ACPI 1.0 version is published.
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 serial port A for console redirection during POST. This option is valid for blade servers and rack-mount servers. **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.
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.

Name	Description
	• **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.
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. If the operating system does not complete booting before the timer expires, the CIMC resets the system and an error is logged. 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 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:

Name	Description
	• **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.

Common Controls

The buttons described in the following table are available in all **Configure BIOS Parameters** tabs.

Name	Description
Save Changes button	Saves the settings for the BIOS parameters on all three tabs and closed the wizard. 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.

CHAPTER 4

Viewing Server Properties

This chapter includes the following sections:

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.

Name	Description
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.
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 what memory configuration the server supports. This can be one of the following: • **Memory configuration can support mirroring** • **Memory configuration can support sparing** • **Memory configuration can support either mirroring or sparing** • **Memory configuration cannot support RAS**

Name	Description
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.

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.
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.

Name	Description
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 Storage 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 **Storage** tab.

Step 4 In the **Storage Adapters** area, review the information about the available adapter cards.
This area contains a table listing all MegaRAID and Cisco Flexible Flash controllers on the server that can be managed through CIMC. To view details about a particular storage device, select it in the table and view the information in the tabs below.

If a particular storage device does not appear on this tab it cannot be managed through CIMC. To view the status of an unsupported device, see the documentation for that device.

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

Step 5 In the **Storage Adapters** area, click a row to view the detailed properties of that adapter.
The properties of the selected storage adapter appear in the tabbed menu below the **Storage Adapters** area.

Step 6 Select the **Controller Info** tab and review the information.
If a MegaRAID controller is selected in the **Storage Adapters** table, this tab shows the following information.

- Firmware versions
- PCI information
- Manufacturing information
- Running and startup firmware image information
- Virtual and physical drive counts
- General settings
- Capabilities
- Hardware configuration
- Error counters

If a Cisco Flexible Flash controller is selected in the **Storage Adapters** table, this tab shows the following information.

Area Name	Description
Actions Area	This area contains the following actions: • **Reset Cisco Flex Flash**—Allows you to reset the selected Cisco Flexible Flash controller • **Configure Operational Profile**—Opens a dialog box that allows you to configure the selected Cisco Flexible Flash controller

Area Name	Description
General Area	This area displays basic information about the controller, its status and internal state, and the firmware that it is running.
Physical Drive Count Area	This area displays the number of physical drives. For more information, go to the **Physical Drive Info** tab.
Virtual Drive Count Area	This area displays the number of virtual drives. For more information, go to the **Virtual Drive Info** tab.

Step 7 Select the **Physical Drive Info** tab and review the information.
This tab shows the following information for the controller selected in the **Storage Adapters** table.

- General drive information
- Identification information
- Drive status

Step 8 Select the **Virtual Drive Info** tab and review the information.
This tab shows the following information for the controller selected in the **Storage Adapters** table.

- General drive information
- RAID information
- Physical drive information

Step 9 Select the **Battery Backup Unit** tab and review the information.
This tab shows information about the backup battery on the controller selected in the **Storage Adapters** table.

Note This tab does not apply if you select a Cisco Flexible Flash controller in the **Storage Adapters** table.

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.
Vendor ID column	The adapter ID assigned by the vendor.
Device ID column	The device ID assigned by the vendor.

CHAPTER 5

Viewing Server Sensors

This chapter includes the following sections:

Viewing the Fault Summary

Procedure

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

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

Step 3 In the **Discrete Sensors** area, review the following information:

Name	Description
Sensor Name column	The name of the sensor.
Status column	The status of the sensor. This can be one of the following: • **Critical** • **Non-Recoverable** • **Warning**

Name	Description
Reading column	This can be one of the following: • **absent** • **present**

Step 4 In the **Threshold Sensors** area, review the following information:

Name	Description
Sensor Name column	The name of the sensor.
Status column	The status of the sensor. This can be one of the following: • **Critical** • **Non-Recoverable** • **Warning**
Reading column	The value reported by the sensor.
Units column	The units in which the sensor data is reported.
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 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.
Status column	The status of the sensor. This can be one of the following: • **Unknown** • **Informational** • **Normal** • **Warning** • **Critical** • **Non-Recoverable**
Reading column	This can be: • **absent** • **present**

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.

Name	Description
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.

Name	Description
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 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	The status of the device. This can be: • **Absent** • **Degraded** • **N/A** • **Online** • **Present**

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 is enabled on this server.
Baud Rate drop-down list	The baud rate the system uses for Serial over LAN communication. You can select one of the following: • 9600 bps • 19.2 kbps

Name	Description
	• 38.4 kbps • 57.6 kbps • 115.2 kbps

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 currently running.
Enable Virtual Media Encryption check box	If checked, all virtual media communications are encrypted.

Step 5 Click **Save Changes**.

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.

Name	Description
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**.

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**.

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**.

CHAPTER 7

Managing User Accounts

This chapter includes the following sections:

Active Directory

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 Active Directory.

When Active Directory is enabled in the CIMC, user authentication and role authorization is performed by Active Directory for user accounts not found in the local user database.

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

Configuring Active Directory in CIMC

Before You Begin

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

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 **Active Directory** tab.

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

Name	Description
Enabled check box	If checked, user authentication and role authorization is performed by Active Directory for user accounts not found in the local user database.
Server IP Address field	The Active Directory server IP address.
Timeout field	The number of seconds the CIMC waits until it assumes the connection to Active Directory cannot be established.
Enable Encryption check box	If checked, the server encrypts all information it sends to Active Directory.
Domain field	The domain that all users must be in.
Attributes field	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 must have the following attribute ID: 1.3.6.1.4.1.9.287247.1 **Note** If you do not specify this property, user access is restricted to read-only.

Step 5 Click **Save Changes**.

Configuring the Active Directory Server

The CIMC can be configured to use Active Directory for user authentication and authorization. To use Active Directory, 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 Active Directory 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. For more information about altering the Active Directory schema, see the article at http://technet.microsoft.com/en-us/library/bb727064.aspx.

The following steps are to be performed on the Active Directory server.

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.

Procedure

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

Step 2 Using the Active Directory 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 Active Directory 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 Active Directory.

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

Step 6 Enter password information.

Step 7 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.
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

Two NIC modes are available for connection to the CIMC. In one mode, you can also choose an active-active or active-standby redundancy mode, depending on your platform.

NIC Mode

The **NIC Mode** drop-down list in the **NIC Properties** area determines which ports can reach the CIMC. The following mode options are available, depending on your platform:

- Cisco Card—A connection to the CIMC is available through an installed adapter card.
- Dedicated—A connection to the CIMC is available through the management Ethernet port or ports.
- Shared LOM—A connection to the CIMC is available only through the LAN On Motherboard (LOM) Ethernet host ports. In some platforms, a 10 Gigabit Ethernet LOM option is available.

Note In shared LOM mode, all host ports must belong to the same subnet.

- Shipping (if supported)—A connection to the CIMC is available through the management Ethernet port or ports using a limited factory default configuration.

Note Shipping mode is intended only for your initial connection to the CIMC. Configure another mode for operation.

NIC Redundancy

The **NIC Redundancy** drop-down list in the **NIC Properties** area determines how NIC redundancy is handled:

- None—Redundancy is not available.
- Active-Active—All Ethernet ports operate simultaneously. This mode provides multiple paths to the CIMC.
- Active-Standby—One port fails over to the other.

The available redundancy modes vary depending on the selected network mode and your platform. For the available modes, see the 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.

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	The NIC mode. This can be: • **Dedicated**—The management port is used to access the CIMC. • **Shared LOM**—The LOM (LAN On Motherboard) ports are used to access the CIMC. • **Shared LOM 10G**—The 10G LOM ports are used to access the CIMC. • **Cisco Card**—The ports on the adapter card are used to access the CIMC. This option is only available for some adapter cards. • **Shipping**—The out-of-the-box defaults will be used for all options. This option is only available for some C-Series servers.

Name	Description
NIC Redundancy drop-down list	The NIC redundancy options depend on the mode chosen in the **NIC Mode** drop-down list 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. The available options are: • **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.

Note The available NIC mode options may vary depending on your platform.

If you select Shared LOM, make sure that all host ports belong to the same subnet.

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.
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.
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.
VLAN ID field	The VLAN ID.
Priority field	The priority of this system on the VLAN.

Step 5 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**.

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. Following are the available adapters:

- Cisco UCS P81E Virtual Interface Card

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 2 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.

Viewing Network Adapter Properties

Before You Begin

- The server must be powered on, or the properties will not display.
- A Cisco UCS P81E Virtual Interface Card 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 **Network 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.
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.
NIV Mode field	Whether Network Interface Virtualization (NIV) is enabled. If NIV mode is enabled, vNICs: • Can be assigned to a specific channel • Can be associated with a port profile • Can fail over to another vNIC if there are communication problems

Step 8 In the **Uplinks** 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: • **Link Up**

Name	Description
	• **Link Down** • **Unsupported Transceiver**
Encap column	The attribute added to the virtual network tag (VNTag) to support Network Interface Virtualization (NIV).

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.
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 and virtual HBAs, see *Viewing vNIC Properties* and *Viewing vHBA Properties*.

Configuring Adapter Properties

Before You Begin

- You must log in with admin privileges to perform this task.
- A Cisco UCS P81E Virtual Interface Card 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 **Network 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 **Set Adapter Properties**.
The **Modify Adapter Properties** dialog box opens.

Step 7 In the **Modify Adapter Properties** dialog box, update the following fields:

Name	Description
Description field	A user-defined description for the adapter. You can enter between 1 and 63 characters.
Enable FIP Mode check box	If checked, then FCoE Initialization Protocol (FIP) mode is enabled. FIP mode ensures that the adapter is compatible with current FCoE standards. **Note** We recommend that you use this option only when explicitly directed to do so by a technical support representative.
Enable NIV Mode check box	If checked, then Network Interface Virtualization (NIV) mode is enabled. If NIV mode is enabled, vNICs: • Can be assigned to a specific channel • Can be associated with a port profile • Can fail over to another vNIC if there are communication problems

Step 8 Click **Save Changes**.

Managing vHBAs

Guidelines for Managing vHBAs

When managing vHBAs, consider the following guidelines and restrictions:

- The Cisco UCS P81E Virtual Interface Card provides two vHBAs (fc0 and fc1). You cannot create additional vHBAs on this adapter card.

- When using the Cisco UCS P81E Virtual Interface Card in an FCoE application, you must associate the vHBA with the FCoE VLAN. Follow the instructions in to assign the VLAN.
- You must reset the adapter card after making configuration changes.

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 **Network 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 **Virtual HBAs** 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 system-assigned name of the virtual HBA.
World Wide Node Name field	The WWNN associated with the vHBA.
World Wide Port Name field	The WWPN associated with the vHBA.
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 field	The uplink port associated with the vHBA.
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 in the field. The ID can be an integer between 1 and 4094.
Class of Service drop-down list	Select an integer between 0 and 6, with 0 being lowest priority and 6 being the highest priority.

Name	Description
Rate Limit field	If you want this vHBA to have an unlimited data rate, select **OFF**. Otherwise, click the second radio button and enter a rate limit in the associated field. You can enter an integer between 1 and 10,000 Mbps.
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 99.
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.

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).
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: • **MSI-X**—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 1024.
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 1024. 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 **Network 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 **Virtual HBAs** 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 system-assigned name of the virtual HBA.
World Wide Node Name field	The WWNN associated with the vHBA.
World Wide Port Name field	The WWPN associated with the vHBA.

Name	Description
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 field	The uplink port associated with the vHBA.
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 in the field. The ID can be an integer between 1 and 4094.
Class of Service drop-down list	Select an integer between 0 and 6, with 0 being lowest priority and 6 being the highest priority.
Rate Limit field	If you want this vHBA to have an unlimited data rate, select **OFF**. Otherwise, click the second radio button and enter a rate limit in the associated field. You can enter an integer between 1 and 10,000 Mbps.
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 99.
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.

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: • **MSI-X**—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 1024.
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 1024. 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.

Name	Description
	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**.

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 **Network 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 **Virtual HBAs** 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 **Network 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 **Virtual HBAs** 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 **Network 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 **Virtual HBAs** 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.

Name	Description
Target WWPN column	The target World Wide Port Name with which the binding is associated.
Target LUN column	The target LUN ID with which the binding is associated.
Host LUN column	The target LUN ID on the host system with which the binding is associated.
Clear Persistent Bindings button	Clears all current bindings.
Close button	Closes the dialog box and saves your changes.

Step 9 Click **Close**.

Clearing 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 **Network 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 **Virtual HBAs** 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 **Clear 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 provides two default vNICs (eth0 and eth1). You can create up to 16 additional vNICs on this adapter card.

- You must reset the adapter card after making configuration changes.

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 **Network 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 **Virtual Ethernet Interface Cards** 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	A user-defined name for the virtual NIC. Once you create the vNIC, this name cannot be changed.
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.
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 99.

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 in the field. The ID can be an integer between 1 and 4094.
VLAN Mode drop-down list	If you want to use VLAN trunking, select **TRUNK**. Otherwise, select **ACCESS**.
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. You can enter an integer between 1 and 10,000 Mbps.
Enable PXE Boot check box	Check this box if the vNIC can be used to perform a PXE boot.
Channel Number field	If NIV mode is enabled for the adapter, select the channel number that will be assigned to this vNIC.
Port Profile drop-down list	If NIV mode is enabled for the adapter, select the port profile that should be associated with the vNIC. **Note** This field displays the port profiles defined on the switch to which this server is connected.
Enable Uplink Failover check box	If NIV mode is enabled for the adapter, check this box if traffic on this vNIC should fail over to the secondary interface if there are communication problems.
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.

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 a value 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.

Name	Description
	• **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.
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	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 **Network 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 **Virtual Ethernet Interface Cards** 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	A user-defined name for the virtual NIC. Once you create the vNIC, this name cannot be changed.
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.
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 99.

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 in the field. The ID can be an integer between 1 and 4094.
VLAN Mode drop-down list	If you want to use VLAN trunking, select **TRUNK**. Otherwise, select **ACCESS**.
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. You can enter an integer between 1 and 10,000 Mbps.
Enable PXE Boot check box	Check this box if the vNIC can be used to perform a PXE boot.
Channel Number field	If NIV mode is enabled for the adapter, select the channel number that will be assigned to this vNIC.
Port Profile drop-down list	If NIV mode is enabled for the adapter, select the port profile that should be associated with the vNIC. **Note** This field displays the port profiles defined on the switch to which this server is connected.
Enable Uplink Failover check box	If NIV mode is enabled for the adapter, check this box if traffic on this vNIC should fail over to the secondary interface if there are communication problems.
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.

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 a value 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.

Name	Description
	• **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, 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	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 **Network 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 **Virtual Ethernet Interface Cards** 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*.

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 **Network 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 **Virtual Ethernet Interface Cards** area, select a vNIC from the table.

Step 7 In the **Virtual Ethernet Interface Cards** area, select a vNIC from the table.

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

Step 8 Click **Delete** and click **OK** to confirm.

Backing Up and Restoring the Adapter Configuration

Exporting the Adapter Configuration

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

Before You Begin

Obtain the TFTP 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 **Network 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
TFTP Server IP Address field	The IP address of the TFTP server to which the adapter configuration file will be exported.
Path and Filename field	The path and filename CIMC should use when exporting the file to the TFTP server.

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 **Network 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
TFTP Server IP Address field	The IP address of the TFTP server on which the adapter configuration file resides.
Path and Filename field	The path and filename of the configuration file on the TFTP server.

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 **Network 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

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 **Network 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 TFTP 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 **Network 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 TFTP server**, then click **Next**.

Step 8 In the **Install Adapter Firmware** dialog box, update the following fields:

Name	Description
TFTP Server IP Address field	The IP address of the TFTP server on which the adapter configuration file resides.
Path and Filename field	The path and filename of the configuration file on the TFTP server.
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 **Network 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**.

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 **HTTP Properties** area, update the following properties:

Name	Description
HTTP/S Enabled check box	Whether HTTP and HTTPS are enabled on the CIMC.
HTTP Port field	The port to use for HTTP communication. The default is 80.
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.

Name	Description
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 4 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 **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.
Active Sessions field	The number of SSH sessions currently running on the CIMC.

Step 4 Click **Save Changes**.

Configuring IPMI

IPMI Over LAN

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 configure IPMI over LAN.

Procedure

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

Step 2 On the **Admin** tab, click **Communications Services**.

Step 3 In the **IPMI over LAN Properties** area, update the following properties:

Name	Description
Enabled check box	Whether IPMI access is allowed on this server.
Privilege Level Limit drop-down list	The highest privilege level that can be assigned to an IPMI session on this server. This can be: • **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.

Name	Description
Encryption Key field	The IPMI encryption key to use for IPMI communications.

Step 4 Click **Save Changes**.

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
Enabled check box	Whether this server sends SNMP traps to the designated host.
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.
System Contact field	The system contact person responsible for the SNMP implementation. Enter a string up to 254 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 254 characters.

Step 5 Click **Save Changes**.

What to Do Next

Configure SNMP trap settings as described in Configuring SNMP Trap Settings, on page 121.

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 hostname of the CIMC.
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 Alerts** area, check the **Enable Platform Event Alerts** 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 Alerts** area, uncheck the **Enable Platform Event Alerts** 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 tasks:

- Enabling Platform Event Alerts, on page 119
- Configuring SNMP Trap Settings, on page 121

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 In the **Common Trap Destination Settings** area, complete the following fields:

Name	Description
Trap Community String field	The name of the SNMP community group to which trap information should be sent.

Name	Description
SNMP Version drop-down list	The SNMP version and model used for the trap. This can be one of the following: • **V1** • **V2** • **V3**
Type field	If you select **V2** for the version, this is the type of trap to send. This can be one of the following: • **Trap** • **Inform**

Step 5 In the **Trap Destinations** area, complete the following fields:

Name	Description
ID column	The trap destination ID. This value cannot be modified.
Enabled column	For each SNMP trap destination that you want to use, check the associated check box in this column.
Trap Destination IP Address column	The IP address to which SNMP trap information is sent.

Tip To change the settings for a trap or to send a test trap message, administrators can click the trap row in the table.

Step 6 Click **Save Changes**.

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 **Event Management**.

Step 3 In the **Event Management** pane, click the **Trap Settings** tab.

Step 4 In the **Trap Destinations** area, click the row of the desired SNMP trap destination.

The **Traps Details** dialog box opens.

Step 5 Click **Send SNMP trap**.
An SNMPv1 test trap message is sent to the trap destination.

Note The trap must be configured and enabled in order to send a test message.

Interpreting Platform Event Traps

A CIMC platform event alert sent as an SNMP trap 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	Platform Event Description
0	Test Trap
131330	Under Voltage
131337	Voltage Critical
196871	Current Warning
262402	Fan Critical
459776	Processor related (IOH-Thermalert/Caterr sensor) predictive failure deasserted
459777	Processor related (IOH-Thermalert/Caterr sensor) predictive failure asserted
460032	Power Warning
460033	Power Warning
524533	Power Supply Critical
524551	Power Supply Warning
525313	Discrete Power Supply Warning
527105	Power Supply Redundancy Lost
527106	Power Supply Redundancy Restored
552704	Power Supply Inserted
552705	PSU Failure
552707	Power Supply AC Lost

Event Number	Platform Event Description
65799	Temperature Warning
65801	Temperature Critical
786433	Memory Warning
786439	DDR3_INFO sensor LED - RED bit asserted (Probable ECC error on a DIMM)
818945	Memory Warning
818951	DDR3_INFO sensor LED - RED bit asserted (Probable ECC error on a DIMM)
851968	Related to HDD sensor
851972	Related to HDD sensor
854016	HDD Absent
854017	HDD Present
880384	HDD Present, no fault indicated
880385	HDD Fault
880512	HDD Not Present
880513	HDD is deasserted but not in a fault state
884480	Drive Present
884481	Drive Slot Warning
884485	Drive in Critical Array
884488	Drive Rebuild/Remap Aborted
884489	Drive Slot Warning

CHAPTER 13

CIMC Firmware Management

This chapter includes the following sections:

Overview of Firmware

C-Series servers use firmware downloaded from cisco.com. This firmware is certified by Cisco to upgrade firmware on a C-Series server.

The firmware you download is packaged in a .zip file. After you have downloaded a firmware .zip from Cisco, you can use it to update the firmware on your server. Cisco also provides release notes with each image, which you can obtain from the same website from which you obtained the image.

Warning Do not use the .zip file to reimage your server.

You use a .bin file to reimage. You must extract the proper .bin upgrade file from this .zip file. You can extract this .bin to a TFTP server or your local machine. As you see in or , you can reimage using an TFTP server or a browser on your local machine.

Note When you update the firmware, you can either upgrade an older firmware version to a newer one, or downgrade a newer firmware version to an older one.

The CIMC separates the firmware update process into stages to ensure that you can install the firmware to a component while the server is running without affecting its uptime. Because you do not need to reboot the server until after you activate, you can perform that task overnight or during other maintenance periods. When you update firmware, the following stages occur:

Install

During this stage, the CIMC transfers the selected firmware version to the server. The install process always overwrites the firmware in the non-active slot on the server. You can install the firmware using either of the following methods:

- Through a browser client—This method allows you to browse for a firmware image on your computer and install it on the server.
- From a TFTP server—This method allows you to install a firmware image residing on a TFTP server.

Activate

During this stage, the CIMC sets the non-active firmware version as active and reboots the server. When the server reboots, the non-active slot becomes the active slot, and the active slot becomes the non-active slot. The firmware in the new active slot becomes the running version.

Obtaining CIMC Firmware from Cisco

Procedure

Step 1 Navigate to cisco.com.

Step 2 Click **Support** on the top toolbar, and then select Software Download from the drop-down menu.

Step 3 Click the **Unified Computing** link in the lower left corner, and then log in.

Step 4 Expand the **Cisco C-Series Rack-Mount Servers** node to display links to each model of the Cisco C-Series Rack-Mount Servers.

Step 5 Click the appropriate link for your server model.

Step 6 Click the **Unified Computing System (UCS) Integrated Management Controller Firmware** link, and then click the appropriate release version link.

Step 7 Click **Download Now**.
The **Download Cart** dialog box appears.

Step 8 Review the information in the **Download Cart** dialog box, and then click **Proceed with Download**.
The **Software Download Rules** page appears.

Step 9 Review the download rules, and click **Agree**.
A dialog box listing your download appears. The **Select Location** dialog box also appears. This dialog box has the focus.

Step 10 Select a location in the **Select Location** dialog box, and then click **Open**.
The download begins.

Step 11 Click **Close** when the download is finished.
The file that you downloaded is a .zip file.

Warning Do not use the .zip file to reimage your server.

You use a .bin file to reimage. You must extract the proper .bin upgrade file from this .zip file. You can extract this .bin to an TFTP server or your local machine. As you see in or , you can reimage using an TFTP server or a browser on your local machine.

The name of the proper .bin you extract file depends on the model server you are reimaging. Following are examples of 1.0.2 firmware update files:

- C200 and C210—upd-pkg-c200-m1-cimc.full.1.0.2.bin
- C250—upd-pkg-c250-m1-cimc.full.1.0.2.bin

What to Do Next

Install the CIMC firmware on the server.

Installing CIMC Firmware from the TFTP Server

Before You Begin

- You must log in as a user with admin privileges to install CIMC firmware through the browser.
- Obtain the CIMC .zip firmware file from Cisco.
- Unzip the proper .bin upgrade file on your TFTP server.

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 TFTP Server**.

Step 4 In the **Install Firmware** dialog box, complete the following fields:

Name	Description
TFTP Server IP Address field	The IP address of the TFTP server on which the firmware image resides.
Image Path and Filename field	The firmware image filename on the server. When you enter this name, include the relative path for the image file from the top of the TFTP tree to the file location.

Step 5 Click **Install Firmware**.

What to Do Next

Activate the CIMC firmware.

Installing CIMC Firmware Through the Browser

Before You Begin

- You must log in as a user with admin privileges to install CIMC firmware through the browser.
- Obtain the CIMC .zip firmware file from Cisco.
- Unzip the proper .bin upgrade file to your local machine.

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 Firmware

Before You Begin

- You must log in as a user with admin privileges to activate firmware.
- Install CIMC firmware on the server.

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**.

CHAPTER 14

Viewing Logs

This chapter includes the following sections:

CIMC Log

Viewing the CIMC Log

Procedure

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

Step 2 On the **Admin** tab, click **CIMC Log**.

Step 3 Review the following information for each CIMC event in the log.

Name	Description
Timestamp column	The date and time the event occurred.
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 4 From the **Entries Per Page** drop-down list, select the number of CIMC events to display on each page.

Step 5 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 **Admin** tab.
Step 2 On the **Admin** tab, click **CIMC Log**.
Step 3 In the **CIMC Log** pane, click **Clear Log**.
Step 4 In the dialog box that appears, click **OK**.

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 **Admin** tab.
Step 2 On the **Admin** tab, click **CIMC Log**.
Step 3 In the **CIMC Log** pane, click the **Remote Logging** tab.
Step 4 In either of the **Remote Syslog Server** dialog boxes, 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 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 **System Event Log**.

Step 3 Review the following information for each system event in the log:

Name	Description
Timestamp column	The date and time the event occurred.
Severity column	The event severity. This can be: • **Unknown** • **Informational** • **Normal** • **Warning** • **Critical** • **Non-Recoverable**
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 4 From the **Entries Per Page** drop-down list, select the number of system events to display on each page.

Step 5 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 **System Event Log**.
Step 3 In the **System Event Log** pane, click **Clear Log**.
Step 4 In the dialog box that appears, click **OK**.

CHAPTER 15

Server Utilities

This chapter includes the following sections:

Exporting Technical Support Data

Perform this task when requested by the Cisco Technical Assistance Center (TAC). This utility creates a summary report containing configuration information, logs and diagnostic data that will help TAC in troubleshooting and resolving a technical issue.

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**.

Step 4 In the **Export Technical Support Data** dialog box, complete the following fields:

Name	Description
TFTP Server IP Address field	The IP address of the TFTP server on which the support data file should be stored.
Path and Filename field	The name of the file in which the support data should be stored on the server. When you enter this name, include the relative path for the file from the top of the TFTP tree to the desired location.

Name	Description
	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.

Step 5 Click **Export**.

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

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.

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 TFTP server IP address.

If you want the option to restore the SNMP configuration information when you import the configuration file, make sure that SNMP is enabled on this server before you create the configuration file. If SNMP is disabled when you export the configuration, CIMC will not apply the SNMP values when the file is imported.

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 **Browse** dialog box that lets you navigate to the location to which the configuration file should be saved.
Export to TFTP server radio button	Select this option to save the XML configuration file to a TFTP server. When you select this option, CIMC GUI displays the following fields:

Name	Description
	• **TFTP Server IP Address**—The IP address of the TFTP server to which the configuration file will be exported. • **Path and Filename**—The path and filename CIMC should use when exporting the file to the TFTP server.

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 the **File** field and a **Browse** button that lets you navigate to the file you want to import.
Import from TFTP server radio button	Select this option to import the XML configuration file from a TFTP server. When you select this option, CIMC GUI displays the following fields: • **TFTP Server IP Address**—The IP address of the TFTP server on which the configuration file resides. • **Path and Filename**—The path and filename of the configuration file on the TFTP server.

Step 5 Click **Import**.

INDEX

F

H

I

K

L

M

N

O

P

R

S

T

U

V