Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide, Release 1.2(1)

First Published: September 15, 2010

Last Modified: October 14, 2010

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-23489-02

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

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

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

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

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

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at http://cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

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

© 2010 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface ix

Audience ix

Organization ix

Conventions x

Related Documentation xi

Documentation Feedback xii

Obtaining Documentation and Submitting a Service Request xii

Overview 1

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

Overview of the Server Software 2

Cisco Integrated Management Controller 2

Overview of the CIMC User Interface 3

CIMC Home Page 4

Navigation Pane 4

Work Pane 5

Toolbar 7

Cisco Integrated Management Controller Online Help Overview 8

Logging In to CIMC 8

Logging Out of CIMC 8

Installing the Server OS 11

OS Installation Methods 11

KVM Console 11

Installing an OS Using the KVM Console 12

PXE Installation Servers 12

Installing an OS Using a PXE Installation Server 13

Managing the Server 15

Viewing Overall Server Status 15

Toggling the Locator LED 17

Configuring the Server Boot Order 17
Powering On the Server 18
Powering Off the Server 19
Power Cycling the Server 19
Resetting the Server 20
Shutting Down the Server 20
Viewing Server Properties 21
Viewing CPU Properties 21
Viewing Memory Properties 22
Viewing Power Supply Properties 22
Viewing Storage Properties 23
Viewing Server Sensors 25
Viewing Current Sensors 25
Viewing LED Sensors 26
Viewing Fan Sensors 27
Viewing Power Supply Sensors 27
Viewing Temperature Sensors 29
Viewing Voltage Sensors 30
Managing Remote Presence 31
Configuring Serial Over LAN 31
Configuring Virtual Media 32
KVM Console 32
Configuring the Virtual KVM 33
Disabling the Virtual KVM 34
Enabling the Virtual KVM 34
Managing User Accounts 35
Active Directory 35
Configuring Active Directory in CIMC 35
Configuring the Active Directory Server 36
Configuring Local Users 37
Viewing User Sessions 39
Configuring Network-Related Settings 41
Server NIC Configuration 41
Server NICs 41
Configuring Server NICs 42

Configuring Common Properties 43
Configuring IPv4 44
Connecting to a VLAN 45
Network Security Configuration 45
Network Security 45
Configuring Network Security 45
Managing Network Adapters 47
Overview of the Cisco UCS C-Series Network Adapters 47
Viewing Adapter Properties 48
Configuring Adapter Properties 50
Managing vHBAs 51
Guidelines for Managing vHBAs 51
Viewing vHBA Properties 51
Modifying vHBA Properties 55
vHBA Boot Table 58
Creating a Boot Table Entry 58
Deleting a Boot Table Entry 59
vHBA Persistent Binding 59
Viewing Persistent Bindings 60
Clearing Persistent Bindings 60
Managing vNICs 61
Guidelines for Managing vNICs 61
Viewing vNIC Properties 61
Modifying vNIC Properties 65
Creating a vNIC 68
Deleting a vNIC 69
Backing Up and Restoring the Adapter Configuration 70
Exporting the Adapter Configuration 70
Importing the Adapter Configuration 70
Restoring Adapter Defaults 71
Managing Adapter Firmware 72
Installing Adapter Firmware From a Local File 72
Installing Adapter Firmware From a TFTP Server 72
Activating Adapter Firmware 73
Configuring Communication Services 75

Configuring HTTP 75
Configuring SSH 76
IPMI Over LAN 77
Configuring IPMI over LAN 77
Managing Certificates 79
Managing the Server Certificate 79
Generating a Certificate Signing Request 79
Creating a Self-Signed Certificate 80
Uploading a Server Certificate 82
Configuring Platform Event Filters 85
Platform Event Filters 85
Enabling Platform Event Alerts 85
Disabling Platform Event Alerts 86
Configuring Platform Event Filters 86
Configuring SNMP Trap Settings 87
CIMC Firmware Management 89
Overview of Firmware 89
Obtaining CIMC Firmware from Cisco 90
Installing CIMC Firmware from the TFTP Server 91
Installing CIMC Firmware Through the Browser 92
Activating Installed Firmware 92
Viewing Logs 93
CIMC Log 93
Viewing the CIMC Log 93
Clearing the CIMC Log 94
Sending the CIMC Log to a Remote Server 94
System Event Log 95
Viewing the System Event Log 95
Clearing the System Event Log 95
Server Utilities 97
Exporting Technical Support Data 97
Rebooting CIMC 98
Recovering from a Corrupted BIOS 98
Resetting CIMC to Factory Defaults 99
Backing Up and Importing the CIMC Configuration 99

Backing Up and Importing the CIMC Configuration 99
Backing Up the CIMC Configuration 100
Importing a CIMC Configuration 101

Preface

This preface includes the following sections:

- Audience, page ix
- Organization, page ix
- Conventions, page x
- Related Documentation, page xi
- Documentation Feedback , page xii
- Obtaining Documentation and Submitting a Service Request , page xii

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

Organization

This document includes the following chapters:

Title	Description
Overview	Describes the Cisco UCS C-Series Rack-Mount Servers and the CIMC GUI.
Managing the Server	Describes how to configure the boot device order, how to control power to the server, and how to reset the server.

Title	Description
Viewing Server Properties	Describes how to view the CPU, memory, power supply, and storage properties of the server.
Viewing Server Sensors	Describes how to view the power supply, fan, temperature, current, and voltage sensors.
Managing Remote Presence	Describes how to configure and manage the virtual KVM, virtual media, and the serial over LAN connection.
Managing User Accounts	Describes how to add, delete, and authenticate users, and how to manage user sessions.
Configuring Network-Related Settings	Describes how to configure network interfaces, network settings, and network security.
Managing Network Adapters	Describes how to create, configure, and manage network adapters.
Configuring Communication Services	Describes how to configure server management communication by HTTP, SSH, and IPMI.
Managing Certificates	Describes how to generate, upload, and manage server certificates.
Configuring Platform Event Filters	Describes how to configure and manage platform event filters and SNMP settings.
CIMC Firmware Management	Describes how to obtain, install, and activate firmware images.
Viewing Logs	Describes how to view, export, and clear log messages.
Server Utilities	Describes how to export support data, 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.

Convention	Indication
[ ]	Elements in square brackets are optional.
{x | y | z}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`courier` font	Terminal sessions and information that the system displays appear in `courier` font.
< >	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 Documentation

Documentation for Cisco UCS C-Series Rack-Mount Servers is available at the following URL:

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

Documentation Feedback

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

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

CHAPTER 1

Overview

This chapter includes the following sections:

- Overview of the Cisco UCS C-Series Rack-Mount Servers, page 1
- Overview of the Server Software, page 2
- Cisco Integrated Management Controller, page 2
- Overview of the CIMC User Interface, page 3

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

Following are the Cisco UCS C-Series rack-mount servers:

- Cisco UCS C200 Rack-Mount Server
- Cisco UCS C210 Rack-Mount Server
- Cisco UCS C250 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*.

UCS C200 Rack-Mount Server

The Cisco UCS C200 server is a high-density, two-socket, 1 RU rack-mount server. This server is built for production-level network infrastructure, web services, and mainstream data centers, and branch and remote-office applications.

UCS C210 Rack-Mount Server

The Cisco UCS C210 server is a general-purpose, two-socket, 2 RU rack-mount server. It balances performance, density, and efficiency for storage-intensive workloads. This server is built for applications such as network file and appliances, storage, database, and content-delivery.

UCS C250 Rack-Mount Server

The Cisco UCS C250 server is a high-performance, memory-intensive, two-socket, 2 RU rack-mount server. It increases performance, and it has the capacity for demanding virtualization and large-data-set workloads. The C250 server can also reduce the cost of smaller memory footprints.

UCS C460 Rack-Mount Server

The UCS C460 server is a high-density, 4U rack-mount server. Supporting one to four multi-core processors, it is built for heavy workload applications like data warehousing, ERP, and large-scale virtualization.

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.

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:

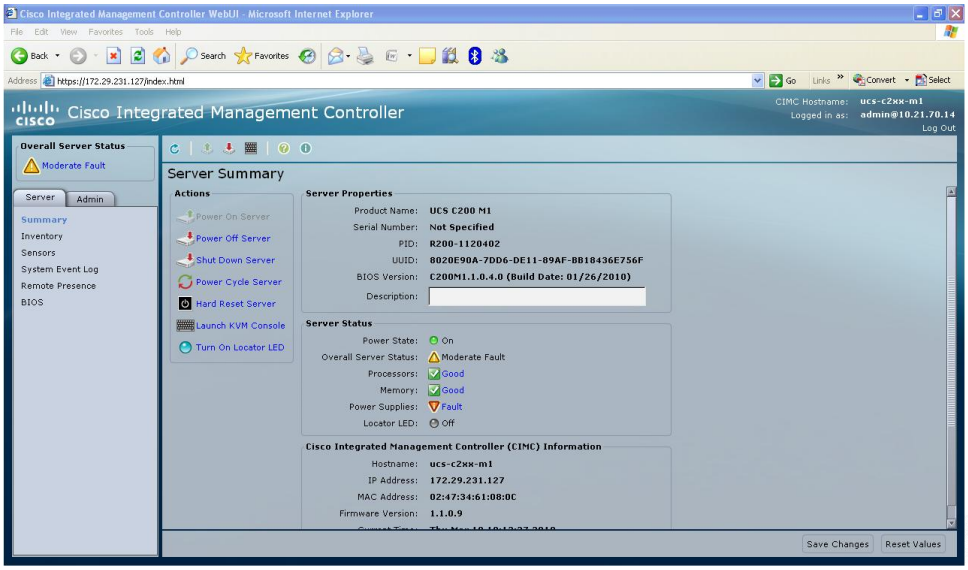
- Java 1.6 or later
- HTTP and HTTPS enabled
- Adobe Flash Player 10 or later

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
Admin tab	The **Admin** tab is found in the **Navigation** pane. It contains links to the following pages: • **Users Management** • **Network** • **Communication 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	On the page, you view server properties, server status, and CIMC information. You also perform actions like powering the server on and off.
Inventory	There are four 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. • **Storage**—Use this tab to view information about storage.
Sensors	There are six 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.
System Event Log	On the page, you can 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.
User Management	There are three tabs on the page: • **Local Users**—Use this tab to create users. • **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 three 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.
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	On this page, you view the CIMC Log.
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 four 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	Launches server 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.

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, page 11
- KVM Console, page 11
- PXE Installation Servers, page 12

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.

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, choose **Tools ➤ Launch Virtual Media** to open the **Virtual Media Session** dialog box.

Step 8 In the **Virtual Media Session** dialog box, 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 **Virtual Media Session** dialog box open during the OS installation process. Closing the dialog box 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, page 15
- Toggling the Locator LED, page 17
- Configuring the Server Boot Order, page 17
- Powering On the Server, page 18
- Powering Off the Server, page 19
- Power Cycling the Server, page 19
- Resetting the Server, page 20
- Shutting Down the Server, page 20

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 Summary** pane:

Name	Description
Power State field	The current power state.
Overall Server Status field	The overall status of the server. This can be: • **Memory Test In Progress**—The server is performing a self-test of the installed memory. This condition normally occurs during the boot process. • **Good**

Name	Description
	• **Moderate Fault** • **Severe Fault**
Processors field	The overall status of the processors. This can be: • **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: • **Good** • **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: • **Good** • **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: • **Good** • **Fault** You can click the link in this field to view detailed status information. **Note** This field is only displayed for some C Series servers.
HDD field	The overall status of the hard drives. This can be: • **Good** • **Fault** You can click the link in this field to view detailed status information. **Note** This field is only displayed for some C Series servers.
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

Name	Description
	• **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.

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**.

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**.

CHAPTER 4

Viewing Server Properties

This chapter includes the following sections:

- Viewing CPU Properties, page 21
- Viewing Memory Properties, page 22
- Viewing Power Supply Properties, page 22
- Viewing Storage Properties, page 23

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.
Version field	The CPU version.
Number of Cores field	The number of cores in the CPU.
Signature field	The signature information for the CPU.
Number of Threads field	The maximum number of threads that the CPU can process concurrently.

Viewing Memory Properties

Procedure

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

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

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

Step 4 Review the following information about memory:

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.

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.

Name	Description
FW Version column	The firmware version for the power supply.
Model column	The model number for the power supply.

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 Review the following information about storage:

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 HDD sensor.
Status column	The current sensor reading.

CHAPTER 5

Viewing Server Sensors

This chapter includes the following sections:

- Viewing Current Sensors, page 25
- Viewing LED Sensors, page 26
- Viewing Fan Sensors, page 27
- Viewing Power Supply Sensors, page 27
- Viewing Temperature Sensors, page 29
- Viewing Voltage Sensors, page 30

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: • **Unknown** • **Informational** • **Normal** • **Warning**

Name	Description
	• **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.

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: • **Unknown** • **Informational** • **Normal** • **Warning** • **Critical** • **Non-Recoverable**
Speed column	The fan speed in RPM.
Warning Threshold Min column	The minimum warning threshold.
Warning Threshold Max column	The maximum warning threshold.
Critical Threshold Min column	The minimum critical threshold.
Critical Threshold Max column	The maximum critical threshold.

Viewing 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 **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: • **Unknown** • **Informational** • **Normal** • **Warning** • **Critical** • **Non-Recoverable**
Reading column	The current power supply usage, in watts.
Warning Threshold Min column	The minimum warning threshold.
Warning Threshold Max column	The maximum warning threshold.
Critical Threshold Min column	The minimum critical threshold.
Critical Threshold Max column	The maximum critical threshold.

Step 6 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: • **Unknown** • **Informational** • **Normal** • **Warning** • **Critical**

Name	Description
	• **Non-Recoverable**
Reading column	This can be: • **absent** • **present**

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: • **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.

Name	Description
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: • **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.

CHAPTER 6

Managing Remote Presence

This chapter includes the following sections:

- Configuring Serial Over LAN, page 31
- Configuring Virtual Media, page 32
- KVM Console, page 32
- Configuring the Virtual KVM, page 33

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.

Configuring the Virtual KVM

Before You Begin

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

Procedure

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

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

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

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

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

Step 5 Click **Save Changes**.

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, page 35
- Configuring Local Users, page 37
- Viewing User Sessions, page 39

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, all user authentication and role authorization is performed by Active Directory, and the CIMC ignores the local database. If the CIMC cannot connect to Active Directory, it reverts to the local 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 local users.

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 a local user, 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 has admin privileges, 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, page 41
- Configuring Common Properties, page 43
- Configuring IPv4, page 44
- Connecting to a VLAN, page 45
- Network Security Configuration, page 45

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, page 47
- Viewing Adapter Properties, page 48
- Configuring Adapter Properties, page 50
- Managing vHBAs, page 51
- Managing vNICs, page 61
- Backing Up and Restoring the Adapter Configuration, page 70
- Managing Adapter Firmware, page 72

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 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 **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, 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.

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** • **Link Down** • **Unsupported Transceiver**

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, 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 **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.

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 Modifying vHBA Properties, page 55 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 **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.
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.

Name	Description
	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.

Name	Description
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.

Name	Description
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 **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.
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.

Name	Description
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. 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 **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 **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 **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.
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 **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 **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.

Name	Description
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.
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.

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:

Name	Description
	• **MIN**—The system waits for the time specified in the **Coalescing Time** field before sending another interrupt event. • **IDLE**—The system does not send an interrupt until there is a period of no activity lasting as least as long as the time specified in the **Coalescing Time** field.
Interrupt Mode drop-down list	The preferred driver interrupt mode. This can be one of the following: • **MSI-X**—Message Signaled Interrupts (MSI) with the optional extension. This is the recommended option. • **MSI**—MSI only. • **INTx**—PCI INTx interrupts.

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

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

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

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

Name	Description
	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.

Name	Description
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 **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.

Name	Description
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.
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.

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. • **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.

Name	Description
	• **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).

Name	Description
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 **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 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 **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 **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 **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 **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 **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 **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.
Cancel button	Click this button to cancel the firmware installation process. No changes are made 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 **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, page 75
- Configuring SSH, page 76
- IPMI Over LAN, page 77
- Configuring IPMI over LAN, page 77

Configuring HTTP

Before You Begin

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

Procedure

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

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

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 **Communication 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 user role that must be assigned to users accessing the system though IPMI. This can be: • **read-only**—This user can view information but cannot make any changes. • **user**—This user can perform some functions through IPMI but cannot perform administrative tasks. • **admin**—This user can perform all actions available through IPMI. **Note** The value of this field must match exactly the role assigned to the user attempting to log in. For example, if this field is set to **read-only** and a user with the admin role attempts to log in through IPMI, that login attempt fails.
Encryption Key field	The IPMI encryption key to use for IPMI communications.

Step 4 Click **Save Changes**.

CHAPTER 11

Managing Certificates

This chapter includes the following sections:

- Managing the Server Certificate, page 79
- Generating a Certificate Signing Request, page 79
- Creating a Self-Signed Certificate, page 80
- Uploading a Server Certificate, page 82

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, page 85
- Enabling Platform Event Alerts, page 85
- Disabling Platform Event Alerts, page 86
- Configuring Platform Event Filters, page 86
- Configuring SNMP Trap Settings, page 87

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.
Event column	The name of the event filter.

Name	Description
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, page 85
- Configuring SNMP Trap Settings, page 87

Configuring SNMP Trap Settings

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 **Event Management**.

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

Step 4 In the **SNMP Community** area, enter the name of the SNMP community to which trap information should be sent.

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

Name	Description
ID column	The trap destination ID. This value cannot be modified.

Name	Description
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.

Step 6 Click **Save Changes**.

CHAPTER 13

CIMC Firmware Management

This chapter includes the following sections:

- Overview of Firmware, page 89
- Obtaining CIMC Firmware from Cisco, page 90
- Installing CIMC Firmware from the TFTP Server, page 91
- Installing CIMC Firmware Through the Browser, page 92
- Activating Installed Firmware, page 92

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 Installing CIMC Firmware Through the Browser, page 92 or Installing CIMC Firmware from the TFTP Server, page 91, 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 Installing CIMC Firmware Through the Browser, page 92 or Installing CIMC Firmware from the TFTP Server, page 91, 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, page 93
- System Event Log, page 95

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.

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.

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.

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, page 97
- Rebooting CIMC, page 98
- Recovering from a Corrupted BIOS, page 98
- Resetting CIMC to Factory Defaults, page 99
- Backing Up and Importing the CIMC Configuration, page 99

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.

Backing Up and Importing the CIMC Configuration

Backing Up and Importing the CIMC Configuration

When you 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 backup 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 a backup 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 a backup or import operation, consider these guidelines:

- You can perform a backup or an import while the system is up and running. While a backup 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 a backup and an import simultaneously.

Backing Up 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.

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: • **TFTP Server IP Address**—The IP address of the TFTP server to which the configuration file will be exported.

Name	Description
	• **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

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

A

Active Directory 35, 36
adapter
  activating firmware 73
  configuring properties 50
  exporting the configuration 70
  importing the configuration 70
  installing firmware from local file 72
  installing firmware from TFTP server 72
  restoring default configuration 71
  viewing properties 48
adapters
  overview 47

B

backing up
  CIMC configuration 99, 100
boot order, configuring 17
boot table
  creating entry 58
  deleting entry 59
  description 58

C

certificate management
  new certificates 79
  uploading a certificate 82
certificates 79
CIMC
  clearing log 94
  firmware
    about 89
    activating 92
    installing from TFTP server 91
    installing through browser 92
    obtaining from Cisco 90
  rebooting 98
CIMC *(continued)*
  resetting to factory defaults 99
  sending log 94
  viewing log 93
CIMC GUI 3, 4
CIMC overview 2
common properties 43
communication services properties
  HTTP properties 75
  IPMI over LAN properties 77
  SSH properties 76
configuration
  backing up 99, 100
  importing 101
CPU properties 21
current sensors 25

D

disabling KVM 34

E

enabling KVM 33, 34
encrypting virtual media 32
event filters, platform
  about 85
  configuring 86
event log, system
  clearing 95
  viewing 95
events
  platform
    disabling alerts 86
    enabling alerts 85
exporting
  CIMC configuration 99, 100

F

fan sensors 27
FIP mode 50
firmware
  about 89
  activating 92
  installing from TFTP server 91
  installing through browser 92
  obtaining from Cisco 90
floppy disk emulation 32

H

HTTP properties 75

I

importing
  CIMC configuration 101
IP blocking 45
IPMI over LAN 77
IPMI over LAN properties 77
IPv4 properties 44

K

KVM
  configuring 33
  disabling 34
  enabling 33, 34
KVM console 11, 32

L

LED sensors 26
local users 37
locator LED 17
logging in 8
logging out 8

M

memory properties 22

N

navigation pane 4
network properties
  common properties 43
  IPv4 properties 44
  NIC properties 42
  VLAN properties 45
network security 45
NIC properties 42

O

operating system installation 12
OS installation
  KVM console 12
  methods 11
  PXE 13

P

persistent binding
  clearing 60
  description 59
  viewing 60
platform event filters
  about 85
  configuring 86
platform events
  disabling alerts 86
  enabling alerts 85
power cycling the server 19
power supply properties 22
power supply sensors 27
powering off the server 19
powering on the server 18
PXE installation 12

R

recovering from a corrupted bios 98
remote presence
  serial over LAN 31
  virtual KVM 33, 34
  virtual media 32
resetting the server 20

S

self-signed certificate 80
sensors
current 25
fan 27
LED 26
power supply 27
temperature 29
voltage 30
serial over LAN 31
server health 15
server management
configuring the boot order 17
locator LED 17
power cycling the server 19
powering off the server 19
powering on the server 18
resetting the server 20
server health 15
shutting down the server 20
server NICs 41
server overview 1
server software 2
shutting down the server 20
SNMP traps 87
SSH properties 76
storage properties 23
syslog
sending CIMC log 94
system event log
clearing 95
viewing 95

T

technical support data, exporting 97
temperature sensors 29
toolbar 7

U

uploading a server certificate 82
user management
Active Directory 35
local users 37
user sessions 39
user sessions 39

V

vHBA
boot table 58
clearing persistent binding 60
creating boot table entry 58
deleting boot table entry 59
guidelines for managing 51
modifying properties 55
persistent binding 59
viewing persistent binding 60
viewing properties 51
virtual KVM 33, 34
virtual media 32
VLAN properties 45
vNIC
creating 68
deleting 69
guidelines for managing 61
modifying properties 65
viewing properties 61
voltage sensors 30

W

work pane 5