Cisco UCS C-Series Servers Integrated Management Controller Configuration Guide, Release 1.0(1)

First Published: 11/03/2009

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-21107-01

CONTENTS

Preface

This preface includes the following sections:

Audience

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

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

Organization

This document includes the following parts:

Part	Title	Description
Part 1	Overview	Contains chapters that describe the Cisco UCS C-Series Rack-Mount Servers and the CIMC CLI.

Part	Title	Description
Part 2	Managing the Server	Contains chapters that describe how to configure the boot device order, how to control power to the server, and how to reset the server.
Part 3	Viewing Server Properties	Contains chapters that describe how to view the CPU, memory, power supply, and storage properties of the server.
Part 4	Viewing Server Sensors	Contains chapters that describe how to view the power supply, fan, temperature, and voltage sensors.
Part 5	Managing Remote Presence	Contains chapters that describe how to configure and manage the virtual KVM, virtual media, and the serial over LAN connection.
Part 6	Managing User Accounts	Contains chapters that describe how to add, delete, and authenticate users, and how to manage user sessions.
Part 7	Configuring Network-Related Settings	Contains chapters that describe how to configure network interfaces, network settings, and network security.
Part 8	Configuring Communication Services	Contains chapters that describe how to configure server management communication by HTTP, SSH, and IPMI.
Part 9	Managing Certificates	Contains chapters that describe how to generate, upload, and manage server certificates.
Part 10	Configuring Platform Event Filters	Contains chapters that describe how to configure and manage platform event filters and SNMP settings.
Part 11	CIMC Firmware Management	Contains chapters that describe how to obtain, install, and activate firmware images.
Part 12	Viewing Logs	Contains chapters that describe how to view and clear log messages.
Part 13	Server Utilities	Contains chapters that describe how to export support data, how to reset the server configuration to factory defaults, 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.

Convention	Indication
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{x | y | z}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`courier` font	Terminal sessions and information 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 Unified Computing System (Cisco UCS) is available at the following URL:

http://www.cisco.com

The following are related Cisco UCS documents:

- *Cisco UCS Documentation Roadmap*
- *Cisco UCS C-Series Rack-Mount Servers Configuration Guide*
- *Cisco UCS Manager XML API Programmer's Guide*
- *Cisco UCS Manager Troubleshooting Guide*
- *Cisco UCS Site Preparation Guide*
- *Cisco UCS 6100 Series Fabric Interconnect Hardware Installation Guide*
- *Cisco UCS 5108 Server Chassis Hardware Installation Guide*
- *Regulatory Compliance and Safety Information for Cisco UCS*
- *Release Notes for Cisco UCS*

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

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

- Cisco UCS C200 M1 Rack-Mount Server
- Cisco UCS C210 M1 Rack-Mount Server

UCS C200 M1 Rack-Mount Server

The Cisco UCS C200 M1 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 M1 Rack-Mount Server

The Cisco UCS C210 M1 server is a general-purpose, two-socket, 2 RU rack-mount server. It is designed to balance 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.

Cisco Integrated Management Controller

The Cisco Integrated Management Controller (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

Server Software

CIMC is a separate management module that is built into the motherboard. CIMC has its own ARM-based processor which runs the CIMC software. It is shipped with a running version of the firmware. Users can update CIMC firmware through the **Firmware Update Management** page. You need not worry about installing the initial CIMC firmware.

You do not need to install an OS like Windows or Linux on the server. Servers are shipped pre-installed. You can however, install a different OS on the server using the DVD drive or over the network. You can use CIMC to install the new OS using the KVM console and vMedia.

The following operating systems are supported by the server:

- Windows Server 2003 R2, 32 bit, 64 bit, Windows 7 with Hyper-V, 64 bit, Windows Server 2008 with Hyper-V, Standard and Enterprise Edition, 64 bit
- VMware ESX 3.5 U4, VMware vSphere 4, 4 U1, 4i, 4i U1
- RedHat RHEL 5.3, 64 bit, RHEL 5.4 KVM, 64 bit, RHEL 6 KVM, 64 bit, RedHat Rhat 4.8, 64 bit, and Fedora
- Novell SLES 10 SP3, 64 bit, SLES 11, 64 bit, SLES 11 SP1 XEN, aSLES 11 XEN , 64 bit
- Solaris x86 10.x, 64 bit
- Oracle OVM 2.1.2, 2.2
- Oracle Enterprise Linux
- XenServer Citrix

Note Use specific product installation documentation when installing an operating system.

CIMC GUI

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

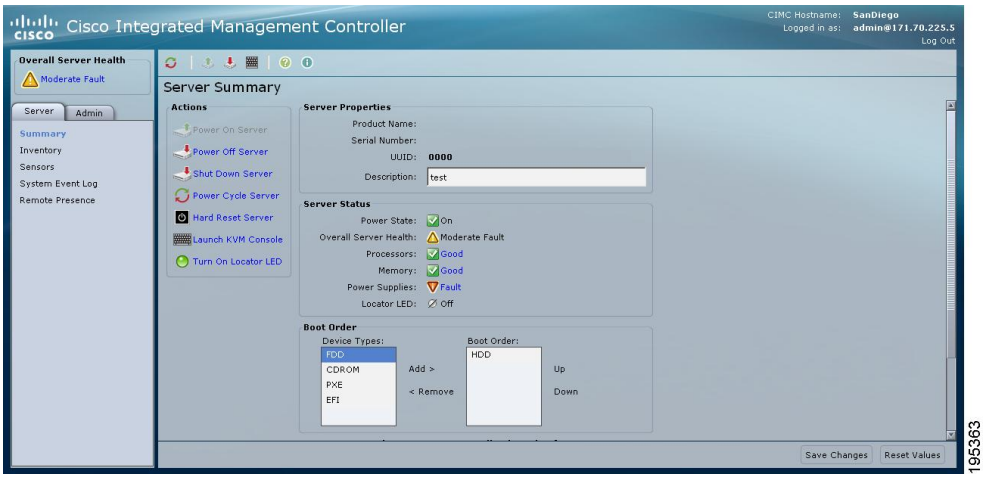
- Java 1.6 or higher
- HTTP and HTTPS enabled
- Adobe Flash Player 10 or higher

Note In case you lose or forget the password that you use to log into CIMC, see the Cisco UCS C-Series server installation and service guide for your platform for password recovery instructions.

CIMC Elements

Figure 1 shows the CIMC GUI.

Figure 1: CIMC GUI



Navigation Pane

The Navigation pane displays on the left side of the CIMC GUI. 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 GUI.

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

Element Name	Description
Overall Server Health area	The **Overall Server Health** 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**
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, dependant 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 four tabs on the page: • **Power Supply Sensors**—Use this tab to view the power supply sensor. • **Fan Sensors**—Use this tab to view the fan sensor. • **Temperature Sensors**—Use this tab to view the temperature sensor. • **Voltage Sensors**—Use this tab to view the voltage sensor.
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.
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 Image 1**—Use this area to view version and status information for firmware image 1. • **CIMC Firmware Image 2**—Use this area to view version and status information for firmware image 2.

	• **Last Firmware Update**—Use this area to view information about the last firmware update.
Utilities	There are two areas on this page: • **Actions**—Use this area to export technical support data, 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.

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 GUI Online Help Overview

The Cisco Integrated Management Controller GUI 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.

For details about the tasks you can perform using this GUI, see the *Cisco CIMC GUI Configuration Guide*.

Logging In to CIMC

Before You Begin

If not installed, install Adobe Flash Player 10 or higher 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

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:

- PXE installation server
- KVM console

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 on your computer
- CD/DVD or floppy drive on the network
- Disk image files 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.
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 methods.

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 Health

Procedure

Step 1 In the **Overall Server Health** area of the **Navigation** pane, click the blue health report link.

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

Name	Description
Power State field	The current power state.
Overall Server Health field	The overall health of the server. This can be: • **Good** • **Moderate Fault** • **Severe Fault** • **Powered Off**

Name	Description
Processors field	The overall health of the processors. This can be: • **Good** • **Fault** • **Powered Off** You can click the link in this field to view more information about the processors.
Memory field	The overall health of the memory modules. This can be: • **Good** • **Fault** • **Powered Off** You can click the link in this field to view detailed status information.
Power Supplies field	The overall health of the power supplies. This can be: • **Good** • **Fault** • **Powered Off** You can click the link in this field to view detailed status information.
Locator LED field	Whether the locator LEDs are on or off.

Toggling the Locator LED

Before You Begin

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

Procedure

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

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

Step 3 In the **Actions** area, click **Turn On Locator LED**.
The locator LED turns on and is blinking.

Step 4 In the **Actions** area, click **Turn Off Locator LED**.

The locator LED turns off.

Resetting the Server Boot Order

Before You Begin

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

Procedure

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

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

Step 3 In the **Boot Order** area, update the following properties:

Name	Description
Device Types table	The server boot options. You can select one or more of the following: • **FDD**—Floppy disk drive • **CDROM**—Bootable CD-ROM • **PXE**—PXE boot • **HDD**—Hard disk drive • **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.

Step 4 Click **Save Changes**.

Powering On the Server

Note If the server was powered off other than through the CIMC, the server will not become active immediately when powered on. In this case, the server will enter standby mode until the CIMC completes initialization.

Before You Begin

You must log in as a user with user privileges to power on the server.

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 as a user with user privileges to power off the server.

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 as a user with user privileges to power cycle the server.

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 as a user with use privileges to reset the server.

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 as a user with user privileges to shut down the server.

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

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.
Serial Number field	The serial number for the CPU.
Vendor field	The vendor for the CPU.
Version field	The CPU version.
Number of Cores field	The number of cores in the CPU.
Signature field	The CPU signature.
Max Speed field	The maximum CPU speed.

Name	Description
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, in megabytes.
Speed column	The clock speed of the memory module, in megahertz.
Type column	The memory type.

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.

Name	Description
Input column	The input into the power supply, in watts.
Max Output column	The maximum output from the power supply, in watts.
FW Version column	The firmware version for the power supply.

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 storage device.
Status column	The status of the storage device. This can be: • **absent** • **present**

CHAPTER 5

Viewing Server Sensors

This chapter includes the following sections:

Viewing Power Supply Sensors

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

Procedure

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

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

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

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

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 Sensors** 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 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 Sensors** 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.
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 Sensors** 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:

Managing the Virtual KVM

Enabling the Virtual KVM

Before You Begin

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

Procedure

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

Disabling the Virtual KVM

Before You Begin

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

Procedure

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

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 field	The maximum number of concurrent KVM sessions allowed. Enter an integer 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.

Name	Description
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**.

Launching the KVM Console

Before You Begin

You must log in as a user with user privileges to launch the KVM console.

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

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.

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

Step 5 Click **Save Changes**.

Configuring Serial Over LAN

Configure serial over LAN when you want to reach the host console with the 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 field	The baud rate the system uses for Serial over LAN communication.

Step 5 Click **Save Changes**.

CHAPTER 7

Managing User Accounts

This chapter includes the following sections:

Configuring Local Users

Before You Begin

You must log in as a user with admin privileges to configure 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 in 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.
User Name column	The user name 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.

Name	Description
	• **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**.

Configuring Active Directory

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

Properties	Value
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 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, all user authentication and role authorization is performed by Active Directory and CIMC ignores the local user database. **Note** If the CIMC cannot establish a connection to Active Directory, it automatically reverts back to using 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**.

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 user name for the user.
IP Address column	The IP address from which the user accessed the server.

Name	Description
Type column	The method by which the user accessed the server.
Action column	If your user account 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

Server NICs

You can configure NIC mode and NIC redundancy for the server NICs using the CIMC.

The **NIC Mode** drop-down list in the **NIC Properties** area determines which port you want to use to reach the CIMC:

- Dedicated—CIMC port
- Shared—Host ports 1 and 2

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

- None—No redundancy
- Teaming—Use both ports simultaneously
- Failover—Fail one port over to another

Note Teaming provides a throughput improvement by utilizing both host ports simultaneously.

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.
NIC Redundancy drop-down list	The NIC redundancy for systems in which the NIC mode is **Shared LOM**. This can be: • **None**—The NICs operate independently and do not failover if there is a problem. • **active-active**—If supported, both NICs are utilized simultaneously. This increases throughput and provides multiple paths to the BMC. **Note** If you select this option for a server that does not support active-active redundancy, the system displays an error message when you save your changes. • **active-standby**—If one NIC fails, traffic fails over to the other NIC. **Note** If you select this option, make sure that both NICs are connected to the same subnet to ensure that the traffic is secure regardless of which NIC is used.
MAC Address field	The MAC address for this server.

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.

Name	Description
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

Configuring Communication Services

This chapter includes the following sections:

Configuring HTTP

Before You Begin

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

Procedure

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
HTTP Timeout field	The number of seconds to wait between HTTP requests before the CIMC times out and terminates the session. Enter an integer between 60 and 10,800. The default is 1,800 seconds.
Max Sessions field	The maximum number of concurrent HTTP and HTTPS sessions allowed on the CIMC.

Name	Description
	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 300 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 Configuration

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 IMPI over LAN

Configure IMPI 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 IMPI 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 IMPI 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: ◦ 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

Name	Description
	• **admin**—This user can perform all actions available through the GUI, CLI, and 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 will fail.
Encryption Key field	The IMPI encryption key to use for IMPI communications.

Step 4 Click **Save Changes**.

CHAPTER 10

Managing Certificates

This chapter includes the following sections:

Managing the Server Certificate

You can generate a certificate signing request (CSR) to obtain a new certificate, and you can upload the new certificate to the CIMC to replace the current server certificate. The server certificate may be signed either by a public Certificate Authority (CA), such as Verisign, or by your own certificate authority.

Procedure

	Command or Action	Purpose
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`	This command directs the CA to use your CSR file to generate a server certificate. Your server certificate is contained in the output file.

	Command or Action	Purpose
	`-CAkey ca.key -out myserver05.crt -extfile openssl.conf`	

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 11

Configuring Platform Event Filters

This chapter includes the following sections:

Platform Event Filters

A platform event filter (PEF) can trigger an action and generate an alert when a critical hardware-related event occurs. For each PEF, you can choose the action to be taken (or take no action) when a platform event occurs. You can also choose to generate and send an alert when a platform event occurs. Alerts are sent as an SNMP trap, so you must configure an SNMP trap destination before the alerts can be sent.

You can globally enable or disable the generation of platform event alerts. When disabled, alerts are not sent even if PEFs are configured to send them.

Enabling Platform Event Alerts

Before You Begin

You must log in as a user with admin privileges to enable platform event alerts.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.
Step 2 On the **Admin** tab, click **Event Management**.
Step 3 In the **Event Management** pane, click the **Platform Event Filters** tab.
Step 4 In the **Platform Event Alerts** area, check the **Enable Platform Event Alerts** check box.
Step 5 Click **Save Changes**.

Disabling Platform Event Alerts

Before You Begin

You must log in as a user with admin privileges to disable platform event alerts.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.
Step 2 On the **Admin** tab, click **Event Management**.
Step 3 In the **Event Management** pane, click the **Platform Event Filters** tab.
Step 4 In the **Platform Event Alerts** area, uncheck the **Enable Platform Event Alerts** check box.
Step 5 Click **Save Changes**.

Configuring Platform Event Filters

Before You Begin

You must log in as a user with admin privileges to configure platform event filters.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.
Step 2 On the **Admin** tab, click **Event Management**.
Step 3 In the **Event Management** pane, click the **Platform Event Filters** tab.
Step 4 In the **Platform Event Filters** area, complete the following fields for each event:

Name	Description
ID column	The unique filter ID.
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: • **None**—An alert is sent but no other action is taken • **Reboot**—An alert is sent and the server is rebooted • **Power Cycle**—An alert is sent and the server is power cycled • **Power Off**—An alert is sent and 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 Alerts** 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 55
- Configuring SNMP Trap Settings, page 57

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 12

CIMC Firmware Management

This chapter includes the following sections:

Overview of Firmware

C-Series servers use firmware obtained from and certified by Cisco to upgrade firmware on the server. After you have obtained a firmware image 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.

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 In a web browser, navigate to the web link provided by Cisco to obtain firmware images for your server.
Step 2 Select one or more firmware images and copy them to a network server.
Step 3 Read the release notes provided with the image or images.

What to Do Next

Install the CIMC firmware on the server.

Installing CIMC Firmware

Installing CIMC Firmware Through the Browser

Before You Begin

- Obtain the CIMC firmware from Cisco.
- You must log in as a user with admin privileges to install CIMC firmware through the browser.

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, do one of the following:
- Click **Browse** and use the **Choose File** dialog box to select the firmware image that you want to install.
- Enter the full path and filename of the firmware image that you want to install.

Step 5 Click **Install Firmware**.

What to Do Next

Activate the CIMC firmware.

Installing CIMC Firmware from the TFTP Server

Before You Begin

- Obtain the CIMC firmware from Cisco.
- You must log in as a user with admin privileges to install CIMC firmware from an FTP 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 file name 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.

Activating Installed Firmware

Before You Begin

Install the 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**.

Step 4 In the **Activate Firmware** dialog box, choose the firmware image to activate.

Step 5 Click **Activate Firmware**.

CHAPTER 13

Viewing Logs

This chapter includes the following sections:

CIMC Log

Viewing the CIMC Log

Procedure

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

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

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

Name	Description
Timestamp column	The date and time the event occurred.
Source column	The software module that logged the event.
Description column	A description of the event.

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**.

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 (Optional) From the **Entries Per Page** drop-down list, select the number of system events to display on each page.

Step 5 (Optional) 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 14

Server Utilities

This chapter includes the following sections:

Exporting Technical Support Data

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

Procedure

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

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

Step 3 In the **Actions** area of the **Utilities** pane, click **Export Technical Support Data**.

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

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

Step 5 Click **Export**.

What to Do Next

Provide the generated report file to Cisco TAC.

Resetting the 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**.

Rebooting the 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.

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**.

INDEX

K

L

M

N

O

P

R

S

T

U

V

W