# Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide, Release 1.1(2)

**First Published:** May 28, 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-22894-01

# 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 chapters:

| Title | Description |
|---|---|
| Overview | Describes the Cisco UCS C-Series Rack-Mount Servers and the CIMC . |
| 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. |
| 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. |
| [ ] | Elements in square brackets are optional. |

| Convention | Indication |
|---|---|
| {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 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

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 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.

### UCS C250 Rack-Mount Server

The Cisco UCS C250 server is a high-performance, memory-intensive, two-socket, 2 RU rack-mount server. It is designed to increase 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

Cisco Integrated Management Controller (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** Use product-specific installation documentation when installing an OS.

# 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

# 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:

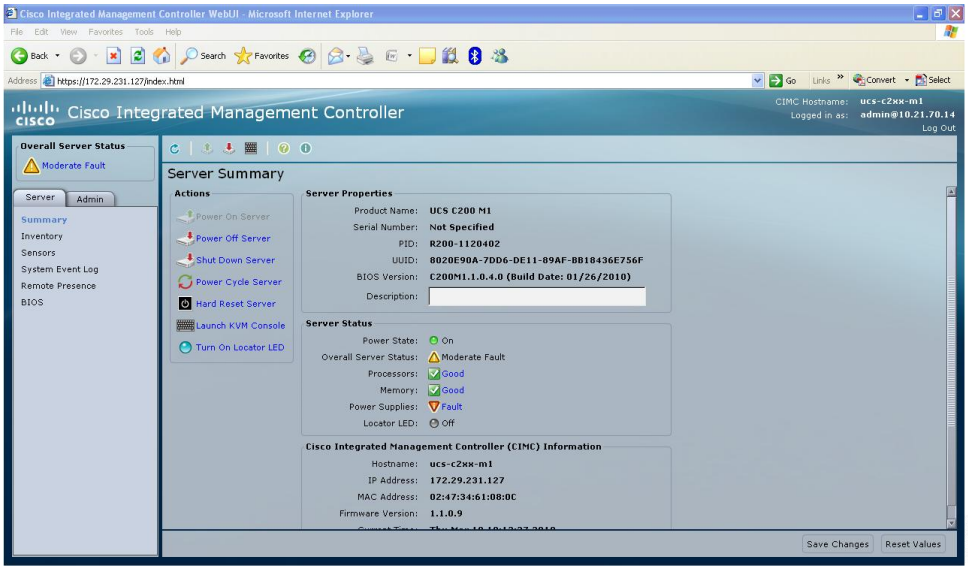
- Java 1.6 or higher
- HTTP and HTTPS enabled
- Adobe Flash Player 10 or higher

**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 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:<br>• **Summary**<br>• **Inventory** |

| | |
|---|---|
| | • **Sensors**<br>• **System Event Log**<br>• **Remote Presence**<br>• BIOS |
| **Admin** tab | The **Admin** tab is found in the **Navigation** pane. It contains links to the following pages:<br>• **Users Management**<br>• **Network**<br>• **Communication Services**<br>• **Certificate Management**<br>• **CIMC Log**<br>• **Event Management**<br>• **Firmware Management**<br>• **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:<br>• **CPUs**—Use this tab to view information about the CPU.<br>• **Memory**—Use this tab to view information about memory.<br>• **Power Supplies**—Use this tab to view information about power supplies.<br>• **Storage**—Use this tab to view information about storage. |
| **Sensors** | There are six tabs on the page:<br>• **Power Supply**—Use this tab to view the power supply sensor.<br>• **Fan**—Use this tab to view the fan sensor. |

| | |
|---|---|
| | • **Temperature**—Use this tab to view the temperature sensor.<br>• **Voltage**—Use this tab to view the voltage sensor.<br>• **Current**—Use this tab to view the current sensor.<br>• **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:<br>• **Virtual KVM**—Use this tab to set vKVM properties.<br>• **Virtual Media**—Use this tab to set virtual media properties.<br>• **Serial over LAN**—Use this tab to set serial over LAN properties. |
| **BIOS** | There are three areas on this page:<br>• **Actions**—Use this area to configure the server boot order, recover corrupted BIOS, and clear the BIOS CMOS.<br>• **BIOS Properties**—Use this area to view the running version of the BIOS.<br>• **Boot Order**—Use this area to view the configured and actual boot order. |
| **User Management** | There are three tabs on the page:<br>• **Local Users**—Use this tab to create users.<br>• **Active Directory**—Use this tab to set active directory properties.<br>• **Sessions**—Use this tab to view current user sessions. |
| **Network** | There are two tabs on the page:<br>• **Network Settings**—Use this tab to set network properties.<br>• **Network Security**—Use this tab to set up network security. |
| **Communications Services** | There are three areas on this page:<br>• **HTTP Properties**—Use this area to set HTTP properties.<br>• **SSH Properties**—Use this area to set SSH properties.<br>• **IPMI over LAN Properties**—Use this area to set IPMI over LAN properties. |
| **Certificate Management** | There are two areas on this page:<br>• **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:<br>• **Platform Event Filters**—Use this tab to set up platform event filters.<br>• **Trap Settings**—Use this tab to set up SNMP traps. |
| **Firmware Management** | There are four areas on this page:<br>• **Actions**—Use this area to install CIMC firmware from a client browser or TFTP server, or to activate installed CIMC firmware.<br>• **CIMC Firmware**—Use this area to view the status of the running, backup, and boot-loader versions of the firmware.<br>• **Last Firmware Install**—Use this area to view information about the last firmware update. |
| **Utilities** | There are three areas on this page:<br>• **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.<br>• **Last Technical Support Data Export**—Use this area to view information about the last technical support data export.<br>• **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 Into 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:

- 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 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 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:<br>• **Memory Test In Progress**—The server is performing a self-test of the installed memory. This condition normally occurs during the boot process.<br>• **Good** |

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

| Name | Description |
|---|---|
| | You can click the link in this field to view detailed status information.<br>**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:<br>• **HDD**—Hard disk drive<br>• **FDD**—Floppy disk drive<br>• **CDROM**—Bootable CD-ROM<br>• **PXE**—PXE boot<br>• **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.<br>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.<br>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

### 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 supported by the socket. |

| 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:<br>• **absent**<br>• **present** |

CHAPTER 5

# Viewing Server Sensors

This chapter includes the following sections:



## 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:<br>• **Unknown**<br>• **Informational**<br>• **Normal**<br>• **Warning** |

| Name | Description |
|---|---|
| | • **Critical**<br>• **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:<br>• **Unknown**<br>• **Informational**<br>• **Normal**<br>• **Warning**<br>• **Critical**<br>• **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:<br>• **Unknown**<br>• **Informational**<br>• **Normal**<br>• **Warning**<br>• **Critical**<br>• **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:<br>• **Unknown**<br>• **Informational**<br>• **Normal**<br>• **Warning**<br>• **Critical** |

| Name | Description |
|---|---|
| | • **Non-Recoverable** |
| **Reading** column | This can be:<br>• **absent**<br>• **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:<br>• **Unknown**<br>• **Informational**<br>• **Normal**<br>• **Warning**<br>• **Critical**<br>• **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:<br>• **Unknown**<br>• **Informational**<br>• **Normal**<br>• **Warning**<br>• **Critical**<br>• **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

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** field | The baud rate the system uses for Serial over LAN communication. |

**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.<br>**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.<br>**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.<br>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. |
| **Enable Local Server Video** check box | If checked, the KVM session is also displayed on any monitor attached to the server. |

**Step 5** Click **Save Changes**.

# Disabling the Virtual KVM

### Before You Begin

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

### Procedure

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

# Enabling the Virtual KVM

### Before You Begin

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

### Procedure

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

CHAPTER 7

# Managing User Accounts

This chapter includes the following sections:



## Active Directory

Active Directory is a technology that provides a variety of network services including LDAP-like directory services, Kerberos-based authentication, and DNS-based naming. The CIMC utilizes the Kerberos-based authentication service of Active Directory.

When Active Directory is enabled in the CIMC, 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.

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.<br>The LDAP attribute must have the following attribute ID:<br>1.3.6.1.4.1.9.287247.1<br>**Note** If you do not specify this property, user access is 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 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:<br>• **read-only**—This user can view information but cannot make any changes.<br>• **user**—This user can:<br>◦ View all information<br>◦ Manage the power control options such as power on, power cycle, and power off<br>◦ Launch the KVM console and virtual media<br>◦ Clear all logs<br>◦ Toggle the locator LED<br>• **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 user name 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**.<br>**Note** You cannot terminate your current session from this tab. |

CHAPTER 8

# Configuring Network-Related Settings

This chapter includes the following sections:



# Server NIC Configuration

## Server NICs

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

### NIC Mode

- 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.

**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

- 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 Installation and Service Guide for your platform.

# 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:<br>• **Dedicated**—The management port is used to access the CIMC.<br>• **Shared LOM**—The LOM (LAN On Motherboard) ports are used to access the CIMC.<br>• **Shipping**—The out-of-the-box defaults will be used for all options.<br>**Note** This option is only available for some C-Series servers. |
| **NIC Redundancy** drop-down list | The NIC redundancy options depend on the mode chosen in the **NIC Mode** drop-down list. If you do not see a particular option, then it is not available for the selected mode.<br>The available options are:<br>• **None**—Each port associated with the configured NIC mode operates independently. The ports do not failover if there is a problem.<br>• **active-active**—If supported, all ports associated with the configured NIC mode operate simultaneously. This increases throughput and provides multiple paths to the CIMC. |

| Name | Description |
|---|---|
| | • **active-standby**—If a port associated with the configured NIC mode fails, traffic will failover to one of the other ports associated with the NIC mode.<br>**Note** If you select this option, make sure all ports associated with the configured NIC mode are connected to the same subnet to ensure that traffic is secure regardless of which port is used. |
| **MAC Address** field | The MAC address of the CIMC network interface selected in the **NIC Mode** field. |

**Step 5** Click **Save Changes**.

# Configuring Common Properties

Use common properties to describe your server.

### Before You Begin

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

### Procedure

**Step 1** In the **Navigation** pane, click the **Admin** tab.
**Step 2** On the **Admin** tab, click **Network**.
**Step 3** In the **Network** pane, click the **Network Settings** tab.
**Step 4** In the **Hostname** field, enter the name of the host.
**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. |

| Name | Description |
|---|---|
| **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.<br>The number of unsuccessful login attempts must occur within the time frame specified in the **IP Blocking Fail Window** field.<br>Enter an integer between 3 and 10. |

| Name | Description |
|---|---|
| **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.<br>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.<br>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 |
| **Session Timeout** field | The number of seconds to wait between HTTP requests before the CIMC times out and terminates the session.<br>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.<br>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.<br>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.<br>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:<br>• **read-only**—This user can view information but cannot make any changes.<br>• **user**—This user can:<br>◦ View all information<br>◦ Manage the power control options such as power on, power cycle, and power off<br>◦ Launch the KVM console and virtual media<br>◦ Clear all logs<br>◦ Toggle the locator LED<br>• **admin**—This user can perform all actions available through the GUI, CLI, and IPMI. |

| Name | Description |
|---|---|
| | **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 IPMI encryption key to use for IPMI 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*<br><br>**Example:**<br>`# openssl genrsa -out ca.key 1024` | This command generates an RSA private key that will be used by the CA.<br>**Note** To allow the CA to access the key without user input, do not use the -des3 option for this command.<br>The specified file name contains an RSA key of the specified key size. |
| **Step 2** | **openssl req -new -x509 -days** *numdays* **-key** *CA_keyfilename* **-out** *CA_certfilename*<br><br>**Example:**<br>`# openssl req -new -x509 -days 365 -key ca.key -out ca.crt` | This command generates a new self-signed certificate for the CA using the specified key. The certificate is valid for the specified period. The command prompts the user for additional certificate information.<br>The certificate server is an active CA. |
| **Step 3** | **echo "nsCertType = server" > openssl.conf**<br><br>**Example:**<br>`# echo "nsCertType = server" > openssl.conf` | This command adds a line to the OpenSSL configuration file to designate the certificate as a server-only certificate. This designation is a defense against a man-in-the-middle attack, in which an authorized client attempts to impersonate the server.<br>The OpenSSL configuration file openssl.conf contains the statement "nsCertType = server". |
| **Step 4** | **openssl x509 -req -days** *numdays* **-in** *CSR_filename* **-CA** *CA_certfilename* **-set_serial 04 -CAkey** *CA_keyfilename* **-out** *server_certfilename* **-extfile openssl.conf**<br><br>**Example:**<br>`# 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.<br>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:<br>• **None**—An alert is sent but no other action is taken<br>• **Reboot**—An alert is sent and the server is rebooted<br>• **Power Cycle**—An alert is sent and the server is power cycled<br>• **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.<br>**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 57
- Configuring SNMP Trap Settings, page 59

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

The firmware you downloads 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.

**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.

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 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.

# 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 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**.

# 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:<br>• **Unknown**<br>• **Informational**<br>• **Normal**<br>• **Warning**<br>• **Critical**<br>• **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 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.

# 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** field | 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. |
| **Export to TFTP server** field | Select this option to save the XML configuration file to a TFTP server. |
| **TFTP Server IP Address** field | The IP address of the TFTP server to which the 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 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** field | 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. |
| **Import from TFTP server** field | Select this option to import the XML configuration file from a TFTP server. |
| **TFTP Server IP Address** field | The IP address of the TFTP server on which the configuration file resides. |
| **Path and Filename** field | The path and filename of the configuration file on the TFTP server. |

**Step 5** Click **Import**.

# INDEX

## I



## K



## L



## M



## N



## O



## P



## R



## S

## T



## U



## V



## W