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

First Published: 01/07/2010

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-21562-01
The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

Notwithstanding any other warranty herein, all document files and software of these suppliers are provided "as is" with all faults. Cisco and the above-named suppliers disclaim all warranties, expressed or implied, including, without limitation, those of merchantability, fitness for a particular purpose and noninfringement or arising from a course of dealing, usage, or trade practice.

In no event shall Cisco or its suppliers be liable for any indirect, special, consequential, or incidental damages, including, without limitation, lost profits or loss or damage to data arising out of the use or inability to use this manual, even if Cisco or its suppliers have been advised of the possibility of such damages.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0910R)

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

© 2010 Cisco Systems, Inc. All rights reserved.
CONTENTS

Preface vii
  Audience vii
  Organization vii
  Conventions viii
  Related Documentation ix
  Documentation Feedback x
  Obtaining Documentation and Submitting a Service Request x

Overview 1
  Overview of the Cisco UCS C-Series Rack-Mount Servers 1
  Cisco Integrated Management Controller 2
  Server Software 3
  Server Ports 3
  CIMC GUI 4
    CIMC Elements 4
      Navigation Pane 4
      Work Pane 5
      Toolbar 7
    Cisco Integrated Management Controller GUI Online Help Overview 8
      Logging In to CIMC 8
      Logging Out of CIMC 8

Installing the Server OS 9
  OS Installation Methods 9
    KVM Console 9
    Installing an OS Using the KVM Console 10
    PXE Installation Servers 10
    Installing an OS Using a PXE Installation Server 11

Managing the Server 13
  Viewing Overall Server Status 13
Contents

Toggling the Locator LED 15
Resetting the Server Boot Order 15
Powering On the Server 16
Powering Off the Server 16
Power Cycling the Server 17
Resetting the Server 17
Shutting Down the Server 18

Viewing Server Properties 19
Viewing CPU Properties 19
Viewing Memory Properties 20
Viewing Power Supply Properties 20
Viewing Storage Properties 21

Viewing Server Sensors 23
Viewing Power Supply Sensors 23
Viewing Fan Sensors 25
Viewing Temperature Sensors 26
Viewing Voltage Sensors 27

Managing Remote Presence 29
Managing the Virtual KVM 29
   Enabling the Virtual KVM 29
   Disabling the Virtual KVM 30
   Configuring the Virtual KVM 30
Launching the KVM Console 31
Configuring Virtual Media 31
Configuring Serial Over LAN 32

Managing User Accounts 33
Configuring Local Users 33
Configuring Active Directory 34
   Configuring the Active Directory Server 34
   Configuring Active Directory in CIMC 35
Viewing User Sessions 36

Configuring Network-Related Settings 39
Server NIC Configuration 39
   Server NICs 39
   Configuring Server NICs 40
Configuring Common Properties 41
Configuring IPv4 41
Connecting to a VLAN 42
Network Security Configuration 43
  Network Security 43
  Configuring Network Security 43
Configuring Communication Services 45
  Configuring HTTP 45
  Configuring SSH 46
  IPMI Over LAN Configuration 47
    IPMI Over LAN 47
    Configuring IMPI over LAN 47
Managing Certificates 49
  Managing the Server Certificate 49
  Generating a Certificate Signing Request 49
  Creating a Self-Signed Certificate 49
  Uploading a Server Certificate 49
Configuring Platform Event Filters 51
  Platform Event Filters 51
  Enabling Platform Event Alerts 51
  Disabling Platform Event Alerts 52
  Configuring Platform Event Filters 52
  Configuring SNMP Trap Settings 53
CIMC Firmware Management 55
  Overview of Firmware 55
  Obtaining CIMC Firmware from Cisco 56
  Installing CIMC Firmware 56
    Installing CIMC Firmware Through the Browser 56
    Installing CIMC Firmware from the TFTP Server 57
  Activating Installed Firmware 57
Viewing Logs 59
  CIMC Log 59
    Viewing the CIMC Log 59
    Clearing the CIMC Log 60
  System Event Log 60
Contents

Viewing the System Event Log 60
Clearing the System Event Log 61

Server Utilities 63
Exporting Technical Support Data 63
Resetting the CIMC to Factory Defaults 64
Rebooting the CIMC 64
Recovering from a Corrupted BIOS 65
Preface

This preface includes the following sections:

• Audience, page vii
• Organization, page vii
• Conventions, page viii
• Related Documentation, page ix
• Documentation Feedback, page x
• Obtaining Documentation and Submitting a Service Request, page x

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:

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>Describes the Cisco UCS C-Series Rack-Mount Servers and the CIMC.</td>
</tr>
<tr>
<td>Installing the Server OS</td>
<td>Describes how to install supported operating systems on the server.</td>
</tr>
</tbody>
</table>
### Conventions

This document uses the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Indication</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>bold</strong> font</td>
<td>Commands, keywords, GUI elements, and user-entered text appear in <strong>bold</strong> font.</td>
</tr>
<tr>
<td><strong>italic</strong> font</td>
<td>Document titles, new or emphasized terms, and arguments for which you supply values are in <strong>italic</strong> font.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Elements in square brackets are optional.</td>
</tr>
<tr>
<td>Convention</td>
<td>Indication</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>{x</td>
<td>y</td>
</tr>
<tr>
<td>[x</td>
<td>y</td>
</tr>
<tr>
<td>string</td>
<td>A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.</td>
</tr>
<tr>
<td>courier font</td>
<td>Terminal sessions and information the system displays appear in <strong>courier</strong> font.</td>
</tr>
<tr>
<td>&lt;&gt;</td>
<td>Nonprinting characters such as passwords are in angle brackets.</td>
</tr>
<tr>
<td>[]</td>
<td>Default responses to system prompts are in square brackets.</td>
</tr>
<tr>
<td>!, #</td>
<td>An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.</td>
</tr>
</tbody>
</table>

**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

The following documents pertain to the C-Series Rack-Mount Servers:

• UCS Rack Servers Documentation Roadmap
Document 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:


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.
Overview

This chapter includes the following sections:

- Overview of the Cisco UCS C-Series Rack-Mount Servers, page 1
- Cisco Integrated Management Controller, page 2
- Server Software, page 3
- Server Ports, page 3
- CIMC GUI, page 4

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
- Cisco UCS C250 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.
UCS C250 M1 Rack-Mount Server

The Cisco UCS C250 M1 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 M1 server also can reduce the cost of smaller memory footprints.

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:

• 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.

Server Ports

Following is a list of server ports and their default port numbers:

• HTTP—By default, TCP port 80
• HTTPS—By default, TCP port 443
• TFTP—By default, UDP port 69
• SSH—By default, TCP port 22
• IPMI—By default, UDP port 623
• SoL—By default, TCP port 22
• KVM—By default, TCP port 2068

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:

<table>
<thead>
<tr>
<th>Element Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall Server Status area</td>
<td>The Overall Server Status area is found above the Server and Admin tabs. Click this area to refresh the Server Summary page.</td>
</tr>
<tr>
<td>Server tab</td>
<td>The Server tab is found in the Navigation pane. It contains links to the following pages:</td>
</tr>
<tr>
<td></td>
<td>• Summary</td>
</tr>
<tr>
<td></td>
<td>• Inventory</td>
</tr>
<tr>
<td></td>
<td>• Sensors</td>
</tr>
<tr>
<td></td>
<td>• System Event Log</td>
</tr>
<tr>
<td></td>
<td>• Remote Presence</td>
</tr>
<tr>
<td>Admin tab</td>
<td>The Admin tab is found in the Navigation pane. It contains links to the following pages:</td>
</tr>
<tr>
<td></td>
<td>• Users Management</td>
</tr>
<tr>
<td></td>
<td>• Network</td>
</tr>
<tr>
<td></td>
<td>• Communication Services</td>
</tr>
<tr>
<td></td>
<td>• Certificate Management</td>
</tr>
<tr>
<td></td>
<td>• CIMC Log</td>
</tr>
<tr>
<td></td>
<td>• Event Management</td>
</tr>
<tr>
<td></td>
<td>• Firmware Management</td>
</tr>
<tr>
<td></td>
<td>• Utilities</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Page or Element Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>On the page, you view server properties, server status, and CIMC information. You also perform actions like powering the server on and off.</td>
</tr>
<tr>
<td>Inventory</td>
<td>There are four tabs on the page:</td>
</tr>
<tr>
<td></td>
<td>• CPUs—Use this tab to view information about the CPU.</td>
</tr>
<tr>
<td>Sensors</td>
<td>There are four tabs on the page:</td>
</tr>
<tr>
<td>---------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>Power Supply Sensors</td>
<td>Use this tab to view the power supply sensor.</td>
</tr>
<tr>
<td>Fan Sensors</td>
<td>Use this tab to view the fan sensor.</td>
</tr>
<tr>
<td>Temperature Sensors</td>
<td>Use this tab to view the temperature sensor.</td>
</tr>
<tr>
<td>Voltage Sensors</td>
<td>Use this tab to view the voltage sensor.</td>
</tr>
</tbody>
</table>

| System Event Log | On the page, you can view the system event log. |

<table>
<thead>
<tr>
<th>Remote Presence</th>
<th>There are three tabs on the page:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual KVM</td>
<td>Use this tab to set vKVM properties.</td>
</tr>
<tr>
<td>Virtual Media</td>
<td>Use this tab to set virtual media properties.</td>
</tr>
<tr>
<td>Serial over LAN</td>
<td>Use this tab to set serial over LAN properties.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>User Management</th>
<th>There are three tabs on the page:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Users</td>
<td>Use this tab to create users.</td>
</tr>
<tr>
<td>Active Directory</td>
<td>Use this tab to set active directory properties.</td>
</tr>
<tr>
<td>Sessions</td>
<td>Use this tab to view current user sessions.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network</th>
<th>There are two tabs on the page:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Settings</td>
<td>Use this tab to set network properties.</td>
</tr>
<tr>
<td>Network Security</td>
<td>Use this tab to set up network security.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Communications Services</th>
<th>There are three areas on this page:</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Properties</td>
<td>Use this area to set HTTP properties.</td>
</tr>
<tr>
<td>SSH Properties</td>
<td>Use this area to set SSH properties.</td>
</tr>
<tr>
<td>IPMI over LAN Properties</td>
<td>Use this area to set IPMI over LAN properties.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Certificate Management</th>
<th>There are two areas on this page:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actions</td>
<td>Use this area to generate and upload a certificate.</td>
</tr>
<tr>
<td>Element Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>Current Certificate</td>
<td>Use this area to view the current certificate for the server.</td>
</tr>
<tr>
<td>CIMC Log</td>
<td>On this page, you view the CIMC Log.</td>
</tr>
<tr>
<td>Event Management</td>
<td>There are two tabs on the page:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Platform Event Filters</strong>—Use this tab to set up platform event filters.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Trap Settings</strong>—Use this tab to set up SNMP traps.</td>
</tr>
<tr>
<td>Firmware Management</td>
<td>There are four areas on this page:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Actions</strong>—Use this area to install CIMC firmware from a client browser or TFTP server, or to activate installed CIMC firmware.</td>
</tr>
<tr>
<td></td>
<td>• <strong>CIMC Firmware Image 1</strong>—Use this area to view version and status information for firmware image 1.</td>
</tr>
<tr>
<td></td>
<td>• <strong>CIMC Firmware Image 2</strong>—Use this area to view version and status information for firmware image 2.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Last Firmware Update</strong>—Use this area to view information about the last firmware update.</td>
</tr>
<tr>
<td>Utilities</td>
<td>There are two areas on this page:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Actions</strong>—Use this area to export technical support data, reset the CIMC to factory default, and reboot the CIMC.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Last Technical Support Data Export</strong>—Use this area to view information about the last technical support data export.</td>
</tr>
</tbody>
</table>

### Toolbar

The toolbar displays above the Work pane.

<table>
<thead>
<tr>
<th>Element Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refresh</td>
<td>Refreshes the current page.</td>
</tr>
<tr>
<td>Power On Server</td>
<td>Powers on the server.</td>
</tr>
<tr>
<td>Power Off Server</td>
<td>Powers off the server.</td>
</tr>
<tr>
<td>Launch KVM Console</td>
<td>Launches the KVM console.</td>
</tr>
<tr>
<td>Help</td>
<td>Launches help.</td>
</tr>
<tr>
<td>Info</td>
<td>Launches server information.</td>
</tr>
</tbody>
</table>
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.
Installing the Server OS

This chapter includes the following sections:

- OS Installation Methods, page 9
- KVM Console, page 9
- Installing an OS Using the KVM Console, page 10
- PXE Installation Servers, page 10
- Installing an OS Using a PXE Installation Server, page 11

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.
Managing the Server

This chapter includes the following sections:

• Viewing Overall Server Status, page 13
• Toggling the Locator LED, page 15
• Resetting the Server Boot Order, page 15
• Powering On the Server, page 16
• Powering Off the Server, page 16
• Power Cycling the Server, page 17
• Resetting the Server, page 17
• Shutting Down the Server, page 18

Viewing Overall Server Status

Procedure

Step 1
In the Overall Server Status 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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power State field</td>
<td>The current power state.</td>
</tr>
<tr>
<td>Overall Server Status field</td>
<td>The overall status of the server. This can be:</td>
</tr>
<tr>
<td></td>
<td>• Memory Test In Progress — The server is performing a self-test of the installed memory. This condition normally occurs during the boot process.</td>
</tr>
<tr>
<td></td>
<td>• Good</td>
</tr>
<tr>
<td></td>
<td>• Moderate Fault</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>• Severe Fault</td>
</tr>
<tr>
<td></td>
<td>• Powered Off</td>
</tr>
<tr>
<td><strong>Processors field</strong></td>
<td>The overall status of the processors. This can be:</td>
</tr>
<tr>
<td></td>
<td>• Good</td>
</tr>
<tr>
<td></td>
<td>• Fault</td>
</tr>
<tr>
<td></td>
<td>You can click the link in this field to view more information about the processors.</td>
</tr>
<tr>
<td><strong>Memory field</strong></td>
<td>The overall status of the memory modules. This can be:</td>
</tr>
<tr>
<td></td>
<td>• Good</td>
</tr>
<tr>
<td></td>
<td>• Fault</td>
</tr>
<tr>
<td></td>
<td>You can click the link in this field to view detailed status information.</td>
</tr>
<tr>
<td><strong>Power Supplies field</strong></td>
<td>The overall status of the power supplies. This can be:</td>
</tr>
<tr>
<td></td>
<td>• Good</td>
</tr>
<tr>
<td></td>
<td>• Fault</td>
</tr>
<tr>
<td></td>
<td>You can click the link in this field to view detailed status information.</td>
</tr>
<tr>
<td><strong>Fans field</strong></td>
<td>The overall status of the power supplies. This can be:</td>
</tr>
<tr>
<td></td>
<td>• Good</td>
</tr>
<tr>
<td></td>
<td>• Fault</td>
</tr>
<tr>
<td></td>
<td>• Powered Off</td>
</tr>
<tr>
<td></td>
<td>You can click the link in this field to view detailed status information. <strong>Note</strong> This field is only displayed for some C Series servers.</td>
</tr>
<tr>
<td><strong>HDD field</strong></td>
<td>The overall status of the hard drives. This can be:</td>
</tr>
<tr>
<td></td>
<td>• Good</td>
</tr>
<tr>
<td></td>
<td>• Fault</td>
</tr>
<tr>
<td></td>
<td>• Powered Off</td>
</tr>
<tr>
<td></td>
<td>You can click the link in this field to view detailed status information. <strong>Note</strong> This field is only displayed for some C Series servers.</td>
</tr>
<tr>
<td><strong>Locator LED field</strong></td>
<td>Whether the locator LEDs are on or off.</td>
</tr>
</tbody>
</table>
Toggling the Locator LED

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

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Navigation pane, click the Server tab.</td>
</tr>
<tr>
<td>Step 2</td>
<td>On the Server tab, click Summary.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the Actions area, click Turn On Locator LED. The locator LED turns on and is blinking.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the Actions area, click Turn Off Locator LED. The locator LED turns off.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Navigation pane, click the Server tab.</td>
</tr>
<tr>
<td>Step 2</td>
<td>On the Server tab, click Summary.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the Boot Order area, update the following properties:</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>Device Types table</td>
<td>The server boot options. You can select one or more of the following:</td>
</tr>
<tr>
<td></td>
<td>• HDD—Hard disk drive</td>
</tr>
<tr>
<td></td>
<td>• FDD—Floppy disk drive</td>
</tr>
<tr>
<td></td>
<td>• CDROM—Bootable CD-ROM</td>
</tr>
<tr>
<td></td>
<td>• PXE—PXE boot</td>
</tr>
<tr>
<td></td>
<td>• EFI—Extensible Firmware Interface</td>
</tr>
<tr>
<td>Add &gt;</td>
<td>Moves the selected device type to the Boot Order table.</td>
</tr>
</tbody>
</table>
Managing the Server

### 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

1. **Step 1** In the Navigation pane, click the Server tab.
2. **Step 2** On the Server tab, click Summary.
3. **Step 3** In the Actions area, click Power On Server.
   A dialog box with the message Power on the server? appears.
4. **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.
Viewing Server Properties

This chapter includes the following sections:

- Viewing CPU Properties, page 19
- Viewing Memory Properties, page 20
- Viewing Power Supply Properties, page 20
- Viewing Storage Properties, page 21

Viewing CPU Properties

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the <strong>Navigation</strong> pane, click the <strong>Server</strong> tab.</td>
</tr>
<tr>
<td>Step 2</td>
<td>On the <strong>Server</strong> tab, click <strong>Inventory</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the <strong>Inventory</strong> pane, click the <strong>CPUs</strong> tab.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Review the following information for each CPU:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Socket Name</strong> field</td>
<td>The socket in which the CPU is installed.</td>
</tr>
<tr>
<td><strong>Serial Number</strong> field</td>
<td>The serial number for the CPU.</td>
</tr>
<tr>
<td><strong>Vendor</strong> field</td>
<td>The vendor for the CPU.</td>
</tr>
<tr>
<td><strong>Version</strong> field</td>
<td>The CPU version.</td>
</tr>
<tr>
<td><strong>Number of Cores</strong> field</td>
<td>The number of cores in the CPU.</td>
</tr>
<tr>
<td><strong>Signature</strong> field</td>
<td>The CPU signature.</td>
</tr>
<tr>
<td><strong>Max Speed</strong> field</td>
<td>The maximum CPU speed supported by the socket.</td>
</tr>
</tbody>
</table>
### Viewing Memory Properties

**Procedure**

1. **Step 1** In the Navigation pane, click the Server tab.
2. **Step 2** On the Server tab, click Inventory.
3. **Step 3** In the Inventory pane, click the Memory tab.
4. **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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name column</td>
<td>The name of the DIMM slot in which the memory module is installed.</td>
</tr>
<tr>
<td>Capacity column</td>
<td>The size of the DIMM, in megabytes.</td>
</tr>
<tr>
<td>Speed column</td>
<td>The clock speed of the memory module, in megahertz.</td>
</tr>
<tr>
<td>Type column</td>
<td>The memory type.</td>
</tr>
</tbody>
</table>

### Viewing Power Supply Properties

**Procedure**

1. **Step 1** In the Navigation pane, click the Server tab.
2. **Step 2** On the Server tab, click Inventory.
3. **Step 3** In the Inventory pane, click the Power Supplies tab.
4. **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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device ID column</td>
<td>The identifier for the power supply unit.</td>
</tr>
</tbody>
</table>
### Viewing Storage Properties

#### Procedure

1. **Step 1** In the Navigation pane, click the Server tab.
2. **Step 2** On the Server tab, click Inventory.
3. **Step 3** In the Inventory pane, click the Storage tab.
4. **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, page 23
- Viewing Fan Sensors, page 25
- Viewing Temperature Sensors, page 26
- Viewing Voltage Sensors, page 27

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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensor Name</td>
<td>The name of the sensor.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the sensor. This can be:</td>
</tr>
<tr>
<td></td>
<td>• Unknown</td>
</tr>
<tr>
<td></td>
<td>• Informational</td>
</tr>
<tr>
<td></td>
<td>• Normal</td>
</tr>
</tbody>
</table>
# Viewing Power Supply Sensors

## Description

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Warning</td>
</tr>
<tr>
<td></td>
<td>• Critical</td>
</tr>
<tr>
<td></td>
<td>• Non-Recoverable</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Reading column</th>
<th>The current power supply usage, in watts.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Warning Threshold Min</strong> column</td>
<td>The minimum warning threshold.</td>
</tr>
<tr>
<td><strong>Warning Threshold Max</strong> column</td>
<td>The maximum warning threshold.</td>
</tr>
<tr>
<td><strong>Critical Threshold Min</strong> column</td>
<td>The minimum critical threshold.</td>
</tr>
<tr>
<td><strong>Critical Threshold Max</strong> column</td>
<td>The maximum critical threshold.</td>
</tr>
</tbody>
</table>

## Step 6

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sensor Name</strong> column</td>
<td>The name of the sensor.</td>
</tr>
<tr>
<td><strong>Status</strong> column</td>
<td>The status of the sensor. This can be:</td>
</tr>
<tr>
<td></td>
<td>• Unknown</td>
</tr>
<tr>
<td></td>
<td>• Informational</td>
</tr>
<tr>
<td></td>
<td>• Normal</td>
</tr>
<tr>
<td></td>
<td>• Warning</td>
</tr>
<tr>
<td></td>
<td>• Critical</td>
</tr>
<tr>
<td></td>
<td>• Non-Recoverable</td>
</tr>
<tr>
<td><strong>Reading</strong> column</td>
<td>This can be:</td>
</tr>
<tr>
<td></td>
<td>• absent</td>
</tr>
<tr>
<td></td>
<td>• present</td>
</tr>
</tbody>
</table>
# Viewing Fan Sensors

## Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Navigation pane, click the Server tab.</td>
</tr>
<tr>
<td>Step 2</td>
<td>On the Server tab, click Sensors.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the Sensors pane, click the Fan Sensors tab.</td>
</tr>
<tr>
<td>Step 4</td>
<td>View the following fan-related statistics for the server:</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensor Name column</td>
<td>The name of the sensor.</td>
</tr>
<tr>
<td>Status column</td>
<td>The status of the sensor. This can be:</td>
</tr>
<tr>
<td></td>
<td>• Unknown</td>
</tr>
<tr>
<td></td>
<td>• Informational</td>
</tr>
<tr>
<td></td>
<td>• Normal</td>
</tr>
<tr>
<td></td>
<td>• Warning</td>
</tr>
<tr>
<td></td>
<td>• Critical</td>
</tr>
<tr>
<td></td>
<td>• Non-Recoverable</td>
</tr>
<tr>
<td>Speed column</td>
<td>The fan speed in RPM.</td>
</tr>
<tr>
<td>Warning Threshold Min column</td>
<td>The minimum warning threshold.</td>
</tr>
<tr>
<td>Warning Threshold Max column</td>
<td>The maximum warning threshold.</td>
</tr>
<tr>
<td>Critical Threshold Min column</td>
<td>The minimum critical threshold.</td>
</tr>
<tr>
<td>Critical Threshold Max column</td>
<td>The maximum critical threshold.</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensor Name column</td>
<td>The name of the sensor.</td>
</tr>
<tr>
<td>Status column</td>
<td>The status of the sensor. This can be:</td>
</tr>
<tr>
<td></td>
<td>• Unknown</td>
</tr>
<tr>
<td></td>
<td>• Informational</td>
</tr>
<tr>
<td></td>
<td>• Normal</td>
</tr>
<tr>
<td></td>
<td>• Warning</td>
</tr>
<tr>
<td></td>
<td>• Critical</td>
</tr>
<tr>
<td></td>
<td>• Non-Recoverable</td>
</tr>
<tr>
<td>Temperature column</td>
<td>The current temperature, in Celsius.</td>
</tr>
<tr>
<td>Warning Threshold Min column</td>
<td>The minimum warning threshold.</td>
</tr>
<tr>
<td>Warning Threshold Max column</td>
<td>The maximum warning threshold.</td>
</tr>
<tr>
<td>Critical Threshold Min column</td>
<td>The minimum critical threshold.</td>
</tr>
<tr>
<td>Critical Threshold Max column</td>
<td>The maximum critical threshold.</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensor Name column</td>
<td>The name of the sensor.</td>
</tr>
<tr>
<td>Status column</td>
<td>The status of the sensor. This can be:</td>
</tr>
<tr>
<td></td>
<td>• Unknown</td>
</tr>
<tr>
<td></td>
<td>• Informational</td>
</tr>
<tr>
<td></td>
<td>• Normal</td>
</tr>
<tr>
<td></td>
<td>• Warning</td>
</tr>
<tr>
<td></td>
<td>• Critical</td>
</tr>
<tr>
<td></td>
<td>• Non-Recoverable</td>
</tr>
<tr>
<td>Voltage column</td>
<td>The current voltage, in volts.</td>
</tr>
<tr>
<td>Warning Threshold Min column</td>
<td>The minimum warning threshold.</td>
</tr>
<tr>
<td>Warning Threshold Max column</td>
<td>The maximum warning threshold.</td>
</tr>
<tr>
<td>Critical Threshold Min column</td>
<td>The minimum critical threshold.</td>
</tr>
<tr>
<td>Critical Threshold Max column</td>
<td>The maximum critical threshold.</td>
</tr>
</tbody>
</table>
Viewing Voltage Sensors
Managing Remote Presence

This chapter includes the following sections:

- Managing the Virtual KVM, page 29
- Launching the KVM Console, page 31
- Configuring Virtual Media, page 31
- Configuring Serial Over LAN, page 32

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**

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

1. In the Navigation pane, click the **Server** tab.
2. On the **Server** tab, click **Remote Presence**.
3. In the **Remote Presence** pane, click the **Virtual KVM** tab.
4. On the **Virtual KVM** tab, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enabled</strong> check box</td>
<td>If checked, the virtual KVM is enabled.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> 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.</td>
</tr>
<tr>
<td><strong>Max Sessions</strong> field</td>
<td>The maximum number of concurrent KVM sessions allowed. Enter an integer between 1 and 4.</td>
</tr>
<tr>
<td><strong>Active Sessions</strong> field</td>
<td>The number of KVM sessions running on the server.</td>
</tr>
<tr>
<td><strong>Remote Port</strong> field</td>
<td>The port used for KVM communication.</td>
</tr>
<tr>
<td><strong>Enable Video Encryption</strong></td>
<td>If checked, the server encrypts all video information sent through the KVM.</td>
</tr>
</tbody>
</table>
### Managing Remote Presence

**Launching the KVM Console**

**Before You Begin**

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

**Procedure**

1. **Step 1** In the Navigation pane, click the Server tab.
2. **Step 2** On the Server tab, click Remote Presence.
3. **Step 3** In the Remote Presence pane, click the Virtual KVM tab.
4. **Step 4** In the Actions area, click Launch KVM Console. The KVM console opens in a separate window.

   **Note**  
   When launching the KVM console with Microsoft Internet Explorer, the browser fails with the message "Internet Explorer was not able to open this Internet site. The requested site is either unavailable or cannot be found." This error occurs with Microsoft Internet Explorer browsers with a specific setting.

   From the Internet Explorer toolbar, select Tools -> Internet Options. The Internet Options dialog box appears. Select the Advanced tab and uncheck the Do not save encrypted pages to disk option.

**Configuring Virtual Media**

**Before You Begin**

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

**Procedure**

1. **Step 1** In the Navigation pane, click the Server tab.
2. **Step 2** On the Server tab, click Remote Presence.
3. **Step 3** In the Remote Presence pane, click the Virtual Media tab.
4. **Step 4** In the Virtual Media Properties area, update the following properties:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Local Server Video check box</td>
<td>If checked, the KVM session is also displayed on any monitor attached to the server.</td>
</tr>
</tbody>
</table>
Configuring Serial Over LAN

Configure serial over LAN 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**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In the Navigation pane, click the Server tab.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>On the Server tab, click Remote Presence.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the Remote Presence pane, click the Serial over LAN tab.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the Serial over LAN Properties area, update the following properties:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enabled</strong> check box</td>
<td>If checked, Serial over LAN is enabled on this server.</td>
</tr>
<tr>
<td><strong>Baud Rate</strong> field</td>
<td>The baud rate the system uses for Serial over LAN communication.</td>
</tr>
</tbody>
</table>

**Step 5** Click Save Changes.
Managing User Accounts

This chapter includes the following sections:

• Configuring Local Users, page 33
• Configuring Active Directory, page 34
• Viewing User Sessions, page 36

Configuring Local Users

Before You Begin
You must log in as a user with admin privileges to configure local users.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Navigation pane, click the Admin tab.</td>
</tr>
<tr>
<td>Step 2</td>
<td>On the Admin tab, click User Management.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the User Management pane, click the Local User tab.</td>
</tr>
<tr>
<td>Step 4</td>
<td>To configure a local user, click in a row.</td>
</tr>
<tr>
<td>Step 5</td>
<td>In the User Details dialog box, update the following properties:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID column</td>
<td>The unique identifier for the user.</td>
</tr>
<tr>
<td>Enabled check box</td>
<td>If checked, the user is enabled on the CIMC.</td>
</tr>
<tr>
<td>User Name column</td>
<td>The user name for the user.</td>
</tr>
<tr>
<td>Role column</td>
<td>The role assigned to the user. This can be:</td>
</tr>
<tr>
<td></td>
<td>• read-only—This user can view information but cannot make any changes.</td>
</tr>
</tbody>
</table>

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

1. **Step 1** Ensure that the Active Directory schema snap-in is installed.
2. **Step 2** Using the Active Directory schema snap-in, add a new attribute with the following properties:

<table>
<thead>
<tr>
<th>Properties</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Name</td>
<td>CiscoAVPair</td>
</tr>
</tbody>
</table>

---

#### Description

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <strong>user</strong>—This user can:</td>
<td></td>
</tr>
<tr>
<td>◦ View all information</td>
<td></td>
</tr>
<tr>
<td>◦ Manage the power control options such as power on, power cycle, and power off</td>
<td></td>
</tr>
<tr>
<td>◦ Launch the KVM console and virtual media</td>
<td></td>
</tr>
<tr>
<td>◦ Clear all logs</td>
<td></td>
</tr>
<tr>
<td>◦ Toggle the locator LED</td>
<td></td>
</tr>
<tr>
<td>• <strong>admin</strong>—This user can perform all actions available through the GUI, CLI, and IPMI.</td>
<td></td>
</tr>
</tbody>
</table>
### 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:

<table>
<thead>
<tr>
<th>Role</th>
<th>CiscoAVPair Attribute Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>shell:roles=&quot;admin&quot;</td>
</tr>
<tr>
<td>user</td>
<td>shell:roles=&quot;user&quot;</td>
</tr>
<tr>
<td>read-only</td>
<td>shell:roles=&quot;read-only&quot;</td>
</tr>
</tbody>
</table>

**Note**

### 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:
**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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session ID column</td>
<td>The unique identifier for the session.</td>
</tr>
<tr>
<td>Username column</td>
<td>The user name for the user.</td>
</tr>
<tr>
<td>IP Address column</td>
<td>The IP address from which the user accessed the server.</td>
</tr>
</tbody>
</table>
### Viewing User Sessions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type column</strong></td>
<td>The method by which the user accessed the server.</td>
</tr>
<tr>
<td><strong>Action column</strong></td>
<td>If your user account has admin privileges, this column displays <strong>Terminate</strong> if you can force the associated user session to end. Otherwise it displays <strong>N/A</strong>.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>You cannot terminate your current session from this tab.</td>
</tr>
</tbody>
</table>
Chapter 8

Configuring Network-Related Settings

This chapter includes the following sections:

- Server NIC Configuration, page 39
- Configuring Common Properties, page 41
- Configuring IPv4, page 41
- Connecting to a VLAN, page 42
- Network Security Configuration, page 43

Server NIC Configuration

Server NICs

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

NIC Mode

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

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

**NIC Redundancy**

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

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

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Navigation pane, click the Admin tab.</td>
</tr>
<tr>
<td>Step 2</td>
<td>On the Admin tab, click Network.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the Network pane, click the Network Settings tab.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the NIC Properties area, update the following properties:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIC Mode drop-down list</td>
<td>The NIC mode. This can be:</td>
</tr>
<tr>
<td></td>
<td>- Dedicated — The management port is used to access the CIMC.</td>
</tr>
<tr>
<td></td>
<td>- Shared LOM — The LOM (LAN On Motherboard) ports are used to access the CIMC.</td>
</tr>
<tr>
<td></td>
<td>- Shipping — The out-of-the-box defaults will be used for all options.</td>
</tr>
<tr>
<td>NIC Redundancy drop-down list</td>
<td>This can be:</td>
</tr>
<tr>
<td></td>
<td>- None — Each port associated with the configured NIC mode operates independently. The ports do not failover if there is a problem. This is option is only available if the NIC mode is set to Shipping.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>• active-active</td>
<td>If supported, all ports associated with the configured NIC mode operate simultaneously. This increases throughput and provides multiple paths to the CIMC.</td>
</tr>
<tr>
<td>• active-standby</td>
<td>If a port associated with the configured NIC mode fails, traffic will failover to one of the other ports associated with the NIC mode.</td>
</tr>
<tr>
<td>Note</td>
<td>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.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable IPv4 check box</td>
<td>If checked, IPv4 is enabled.</td>
</tr>
<tr>
<td>Use DHCP check box</td>
<td>If checked, the CIMC uses DHCP.</td>
</tr>
<tr>
<td>IP Address field</td>
<td>The IP address for the CIMC.</td>
</tr>
<tr>
<td>Subnet Mask field</td>
<td>The subnet mask for the IP address.</td>
</tr>
<tr>
<td>Gateway field</td>
<td>The gateway for the IP address.</td>
</tr>
<tr>
<td>Obtain DNS Server Addresses from DHCP check box</td>
<td>If checked, the CIMC retrieves the DNS server addresses from DHCP.</td>
</tr>
<tr>
<td>Preferred DNS Server field</td>
<td>The IP address of the primary DNS server.</td>
</tr>
<tr>
<td>Alternate DNS Server field</td>
<td>The IP address of the secondary DNS server.</td>
</tr>
</tbody>
</table>

**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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable VLAN check box</td>
<td>If checked, the CIMC is connected to a virtual LAN.</td>
</tr>
</tbody>
</table>
### 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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable IP Blocking</strong></td>
<td>Check this box to enable IP blocking.</td>
</tr>
<tr>
<td><strong>IP Blocking Fail Count</strong></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>The number of unsuccessful login attempts must occur within the time frame specified in the <strong>IP Blocking Fail Window</strong> field.</td>
</tr>
<tr>
<td></td>
<td>Enter an integer between 3 and 10.</td>
</tr>
</tbody>
</table>
### Network Security Configuration

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP Blocking Fail Window</strong> field</td>
<td>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.</td>
</tr>
<tr>
<td><strong>IP Blocking Penalty Time</strong> field</td>
<td>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.</td>
</tr>
</tbody>
</table>
Configuring Communication Services

This chapter includes the following sections:

- Configuring HTTP, page 45
- Configuring SSH, page 46
- IPMI Over LAN Configuration, page 47

Configuring HTTP

**Before You Begin**

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

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In the Navigation pane, click the Admin tab.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>On the Admin tab, click Communication Services.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the HTTP Properties area, update the following properties:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP/S Enabled</td>
<td>Whether HTTP and HTTPS are enabled on the CIMC.</td>
</tr>
<tr>
<td>HTTP Port field</td>
<td>The port to use for HTTP communication. The default is 80.</td>
</tr>
<tr>
<td>HTTPS Port field</td>
<td>The port to use for HTTPS communication. The default is 443.</td>
</tr>
<tr>
<td>Session Timeout field</td>
<td>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.</td>
</tr>
<tr>
<td>Max Sessions field</td>
<td>The maximum number of concurrent HTTP and HTTPS sessions allowed on the CIMC.</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH Enabled check box</td>
<td>Whether SSH is enabled on the CIMC.</td>
</tr>
<tr>
<td>SSH Port field</td>
<td>The port to use for secure shell access. The default is 22.</td>
</tr>
<tr>
<td>SSH Timeout field</td>
<td>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.</td>
</tr>
<tr>
<td>Max Sessions field</td>
<td>The maximum number of concurrent SSH sessions allowed on the CIMC. This value may not be changed.</td>
</tr>
<tr>
<td>Active Sessions field</td>
<td>The number of SSH sessions currently running on the CIMC.</td>
</tr>
</tbody>
</table>

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 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Navigation pane, click the Admin tab.</td>
</tr>
<tr>
<td>Step 2</td>
<td>On the Admin tab, click Communication Services.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the IPMI over LAN Properties area, update the following properties:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled check box</td>
<td>Whether IPMI access is allowed on this server.</td>
</tr>
<tr>
<td>Privilege Level Limit drop-down list</td>
<td>The user role that must be assigned to users accessing the system though IPMI. This can be:</td>
</tr>
</tbody>
</table>

- **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 |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>This user can perform all actions available through the GUI, CLI, and IPMI.</td>
</tr>
</tbody>
</table>

**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, page 49
- Generating a Certificate Signing Request, page 49
- Creating a Self-Signed Certificate, page 49
- Uploading a Server Certificate, page 49

Managing the Server Certificate

Generating a Certificate Signing Request

Creating a Self-Signed Certificate

Uploading a Server Certificate
Managing Certificates

Uploading a Server Certificate
Configuring Platform Event Filters

This chapter includes the following sections:

- Platform Event Filters, page 51
- Enabling Platform Event Alerts, page 51
- Disabling Platform Event Alerts, page 52
- Configuring Platform Event Filters, page 52
- Configuring SNMP Trap Settings, page 53

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.
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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>The unique filter ID.</td>
</tr>
<tr>
<td>Event</td>
<td>The name of the event filter.</td>
</tr>
</tbody>
</table>
Foreach 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

For each filter that you want to send an alert, check the associated check box in this column.

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.

### Configuring SNMP Trap Settings

**Before You Begin**

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

**Procedure**

1. In the **Navigation** pane, click the **Admin** tab.
2. On the **Admin** tab, click **Event Management**.
3. In the **Event Management** pane, click the **Trap Settings** tab.
4. In the **SNMP Community** area, enter the name of the SNMP community to which trap information should be sent.
5. In the **Trap Destinations** area, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID column</td>
<td>The trap destination ID. This value cannot be modified.</td>
</tr>
</tbody>
</table>
### Configuring SNMP Trap Settings

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enabled column</strong></td>
<td>For each SNMP trap destination that you want to use, check the associated check box in this column.</td>
</tr>
<tr>
<td><strong>Trap Destination IP Address column</strong></td>
<td>The IP address to which SNMP trap information is sent.</td>
</tr>
</tbody>
</table>

**Step 6** Click **Save Changes**.
CIMC Firmware Management

This chapter includes the following sections:

- Overview of Firmware, page 55
- Obtaining CIMC Firmware from Cisco, page 56
- Installing CIMC Firmware, page 56
- Activating Installed Firmware, page 57

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.
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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Navigation pane, click the Admin tab.</td>
</tr>
<tr>
<td>Step 2</td>
<td>On the Admin tab, click Firmware Management.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the Actions area, click Install CIMC Firmware from TFTP Server.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the Install Firmware dialog box, complete the following fields:</td>
</tr>
<tr>
<td></td>
<td><strong>Name</strong></td>
</tr>
<tr>
<td>TFTP Server IP Address field</td>
<td>The IP address of the TFTP server on which the firmware image resides.</td>
</tr>
<tr>
<td>Image Path and Filename field</td>
<td>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.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Install Firmware.</td>
</tr>
</tbody>
</table>

What to Do Next

Activate the CIMC firmware.

Activating Installed Firmware

Before You Begin

Install the CIMC firmware on the server.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Navigation pane, click the Admin tab.</td>
</tr>
<tr>
<td>Step 2</td>
<td>On the Admin tab, click Firmware Management.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the Actions area, click Activate CIMC Firmware.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the Activate Firmware dialog box, choose the firmware image to activate.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Activate Firmware.</td>
</tr>
</tbody>
</table>
CHAPTER 13

Viewing Logs

This chapter includes the following sections:

- CIMC Log, page 59
- System Event Log, page 60

CIMC Log

Viewing the CIMC Log

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Navigation pane, click the Admin tab.</td>
</tr>
<tr>
<td>Step 2</td>
<td>On the Admin tab, click CIMC Log.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Review the following information for each CIMC event in the log.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timestamp</td>
<td>The date and time the event occurred.</td>
</tr>
<tr>
<td>Source</td>
<td>The software module that logged the event.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the event.</td>
</tr>
</tbody>
</table>

| 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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timestamp column</td>
<td>The date and time the event occurred.</td>
</tr>
<tr>
<td>Severity column</td>
<td>The event severity. This can be:</td>
</tr>
<tr>
<td></td>
<td>• Unknown</td>
</tr>
<tr>
<td></td>
<td>• Informational</td>
</tr>
<tr>
<td></td>
<td>• Normal</td>
</tr>
<tr>
<td></td>
<td>• Warning</td>
</tr>
<tr>
<td></td>
<td>• Critical</td>
</tr>
<tr>
<td></td>
<td>• Non-Recoverable</td>
</tr>
<tr>
<td>Description column</td>
<td>A description of the event.</td>
</tr>
</tbody>
</table>
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.
Clearing the System Event Log
Server Utilities

This chapter includes the following sections:

- Exporting Technical Support Data, page 63
- Resetting the CIMC to Factory Defaults, page 64
- Rebooting the CIMC, page 64
- Recovering from a Corrupted BIOS, page 65

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: |

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TFTP Server IP Address field</td>
<td>The IP address of the TFTP server on which the support data file should be stored.</td>
</tr>
<tr>
<td>Path and Filename field</td>
<td>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.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Export.</td>
</tr>
</tbody>
</table>
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.

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.

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.

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.
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 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.

Step 1 In the Navigation pane, click the Admin tab.
Step 2 On the Admin tab, click Firmware Management.
Step 3 In the Firmware Management pane, click Recover Corrupt BIOS.
The Recover Corrupt BIOS wizard appears.
Use the Recover Corrupt BIOS wizard to recover your corrupt BIOS.
INDEX

A
active directory 35
Active Directory 34

C
CICM GUI 4
CIMC
  clearing log 60
  firmware
    about 55
    activating 57
    installing from TFTP server 57
    installing through browser 56
    obtaining from Cisco 56
  rebooting 64
  resetting to factory defaults 64
  viewing log 59
CIMC overview 2
  common properties 41
  communication services properties
    HTTP properties 45
    IMPI over LAN properties 47
    SSH properties 46
  CPU properties 19

D
disabling KVM 30

E
enabling KVM 29, 30
  encrypting virtual media 31
  event filters, platform
    about 51
    configuring 52
  event log, system
    clearing 61
    viewing 60
  events
    platform
      disabling alerts 52
      enabling alerts 51

F
  fan sensors 25
  firmware
    about 55
    activating 57
    installing from TFTP server 57
    installing through browser 56
    obtaining from Cisco 56
  floppy disk emulation 31

G
gui elements 4

H
HTTP properties 45

I
IMPI over LAN properties 47
IP blocking 43
IPMI over LAN 47
IPv4 properties 41
K

KVM
- configuring 30
- disabling 30
- enabling 29, 30
- launching console 31

KVM console 9

L

launching KVM Console 31
- local users 33
- locator LED 15
- logging in 8
- logging out 8

M

memory properties 20

N

navigation pane 4
- network properties
  - common properties 41
  - IPv4 properties 41
  - NIC properties 40
  - VLAN properties 42
- network security 43
- NIC properties 40

O

operating system installation 10
- OS installation 9, 10, 11
  - KVM console 10
  - PXE 11

P

platform event filters
- about 51
  - configuring 52
- platform events
  - disabling alerts 52
  - enabling alerts 51
- power supply properties 20

power supply sensors 23
- powering cycling the server 17
- powering off the server 16
- powering on the server 16
- PXE installation 10

R

recovering from a corrupted bios 65
- remote presence
  - KVM Console 31
  - serial over LAN 32
  - virtual KVM 29, 30
  - virtual media 31
  - resetting the boot order 15
  - resetting the server 17

S

sensors
- fan 25
- power supply 23
- temperature 26
- voltage 27
- serial over LAN 32
- server health 13
- server management
  - locator LED 15
  - power cycling the server 17
  - powering off the server 16
  - powering on the server 16
  - resetting the boot order 15
  - resetting the server 17
  - server health 13
  - shutting down the server 18
- server NIC 39
- server overview 1
- server software 3
- shutting down the server 18
- SNMP traps 53
- SSH properties 46
- starting KVM Console 31
- storage properties 21
- system event log
  - clearing 61
  - viewing 60

T

technical support data, exporting 63
temperaturesensors 26
toolbar 7

U
user management
  active directory 35
  local users 33
  user sessions 36
user sessions 36

V
virtual KVM 29, 30
virtual media 31
VLAN properties 42
voltage sensors 27

W
work pane 5