# GUI Configuration Guide for Cisco UCS E-Series M6 Servers, Release 4.11.1

**First Published:** 2023-08-07

**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

# CONTENTS

PREFACE

CHAPTER 1

CHAPTER 2

CHAPTER 3

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

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

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

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

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

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

# Preface

This preface describes the audience, organization, and conventions of this document. It also provides information on how to obtain other documentation.

This preface includes the following sections:

- Audience and Scope, on page ix
- Feature Compatibility, on page ix
- Document Conventions, on page x
- Communications, Services, and Additional Information, on page xi
- Documentation Feedback, on page xii
- Troubleshooting, on page xii

## Audience and Scope

This document is designed for the person who is responsible for configuring your Cisco Enterprise router. This document is intended primarily for the following audiences:

- Customers with technical networking background and experience.
- System administrators familiar with the fundamentals of router-based internetworking but who might not be familiar with Cisco IOS software.
- System administrators who are responsible for installing and configuring internetworking equipment, and who are familiar with Cisco IOS software.

## Feature Compatibility

For more information about the Cisco IOS XE software, including features available on your device as described in the configuration guides, see the respective router documentation set.

To verify support for specific features, use the Cisco Feature Navigator tool. This tool enables you to determine the Cisco IOS XE software images that support a specific software release, feature set, or a platform.

# Document Conventions

This documentation uses the following conventions:

| Convention | Description |
|---|---|
| ^ or **Ctrl** | The ^ and **Ctrl** symbols represent the Control key. For example, the key combination ^**D** or **Ctrl-D** means hold down the **Control** key while you press the **D** key. Keys are indicated in capital letters but are not case sensitive. |
| *string* | A string is a nonquoted set of characters shown in italics. For example, when setting an SNMP community string to public, do not use quotation marks around the string or the string will include the quotation marks. |

The command syntax descriptions use the following conventions:

| Convention | Description |
|---|---|
| **bold** | Bold text indicates commands and keywords that you enter exactly as shown. |
| *italics* | Italic text indicates arguments for which you supply values. |
| [x] | Square brackets enclose an optional element (keyword or argument). |
| \| | A vertical line indicates a choice within an optional or required set of keywords or arguments. |
| [x \| y] | Square brackets enclosing keywords or arguments separated by a vertical line indicate an optional choice. |
| {x \| y} | Braces enclosing keywords or arguments separated by a vertical line indicate a required choice. |

Nested sets of square brackets or braces indicate optional or required choices within optional or required elements. For example, see the following table.

| Convention | Description |
|---|---|
| [x {y \| z}] | Braces and a vertical line within square brackets indicate a required choice within an optional element. |

Examples use the following conventions:

| Convention | Description |
|---|---|
| `screen` | Examples of information displayed on the screen are set in Courier font. |
| **`bold screen`** | Examples of text that you must enter are set in Courier bold font. |
| < > | Angle brackets enclose text that is not printed to the screen, such as passwords. |
| ! | An exclamation point at the beginning of a line indicates a comment line. Exclamation points are also displayed by the Cisco IOS XE software for certain processes. |
| [ ] | Square brackets enclose default responses to system prompts. |

**Caution** Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

**Note** Means *reader take note*. Notes contain helpful suggestions or references to materials that may not be contained in this manual.

# Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you’re looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

### Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

# Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

# Troubleshooting

For the most up-to-date, detailed troubleshooting information, see the Cisco TAC website at https://www.cisco.com/en/US/support/index.html.

Go to **Products by Category** and choose your product from the list, or enter the name of your product. Look under **Troubleshoot and Alerts** to find information for the issue that you are experiencing.

CHAPTER 1

# Overview

This chapter includes the following sections:

## Cisco UCS E-Series M6 Servers Overview

The Cisco UCS E-Series M6 Servers are size-,weight-, and power-efficient blade servers that are housed within the Cisco Catalyst 8300 Series Edge platforms. These servers provide a general-purpose compute platform for branch-office applications deployed either as bare-metal on operating systems, such as Linux, or as virtual machines on hypervisors, such as VMware vSphere Hypervisor.

The UCS E-Series M6 Server is purpose-built with powerful Intel IceLake-D processors for general purpose compute. It comes in the double-wide form factor, that fits into two SM slots.

**Note** For information about the E-Series M6 Servers, and the maximum number of servers that can be installed per router, see the "Hardware Requirements" section in the Hardware Installation Guide for Cisco UCS E-Series M6 Servers.

## Server Software

The UCS E-Series M6 Servers require three major software systems:

- CIMC firmware
- BIOS firmware
- Operating system or hypervisor

### CIMC Firmware

Cisco Integrated Management Controller (CIMC) is a management module built into the motherboard of the UCS E-Series M6 Servers. A dedicated processor, separate from the main server CPU, runs the CIMC firmware. CIMC is the management service for the E-Series M6 Servers. You can use a web-based GUI or SSH-based CLI to access, configure, administer, and monitor the server.

The system ships with a running version of the CIMC firmware. You can update the CIMC firmware, but no initial installation is required.

### BIOS Firmware

BIOS initializes the hardware in the system, discovers bootable devices, and boots them in the provided sequence. It boots the operating system and configures the hardware for the operating system to use. BIOS manageabilityfeatures allow you to interact with the hardware and use it. In addition, BIOS provides options to configure the system, manage firmware, and create BIOS error reports.

The system ships with a running version of the BIOS firmware. You can update the BIOS firmware, but no initial installation is required.

### Operating System or Hypervisor

The main server CPU runs on an operating system, such as Linux; or on a hypervisor. You can purchase the E-Series M6 Servers with a preinstalled operating system or hypervisor.

**Note** For information about the operating systems and hypervisors that are available for the E-Series M6 Servers, see the "Software Requirements" section in the *Release Notes for Cisco UCS E-Series M6 Servers*.

# CIMC Overview

The Cisco Integrated Management Controller (CIMC) is the management service for the E-Series M6 Servers. CIMC runs within the server. You can use a web-based GUI or the SSH-based CLI to access, configure, administer, and monitor the server.

You can use CIMC to perform the following server management tasks:

- Power on, power off, power cycle, reset, and shut down the server.
- Configure the server boot order.
- View serverproperties, router information, and chassis status.
- Manage remote presence.
- Create and manage local user accounts, and enable remote user authentication through the Active Directory.
- Configure network-related settings, including NIC properties, IPv4, VLANs, and network security.
- Configure communication services, including HTTP, SSH, IPMI over LAN, SNMP, and Redfish.
- Manage certificates.
- Configure platform event filters.

- Monitor power supply, fan, temperature, voltage, current, LED and storage sensors.
- Update CIMC firmware.
- Update BIOS firmware.
- Install the host image from an internal repository.
- Monitor faults, alarms, and server status.
- Set the time zone and view local time.
- Collect technical support data in the event of server failure.

Most tasks can be performed in either the GUI interface or CLI interface, and the results of tasks performed in one interface are displayed in another. However, you *cannot*:

- Use the CIMC GUI to invoke the CIMC CLI.
- View a command that has been invoked through the CIMC CLI in the CIMC GUI.
- Generate CIMC CLI output from the CIMC GUI.

The CIMC 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 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- 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 the Cisco UCS E-Series M6 servers. You can launch the user interface and manage the server from a remote host. Supported browsers are:

- Chrome
- Microsoft Edge
- Mozilla Firefox

**Note** In case you lose or forget the password that you use to log in to Cisco IMC, see the password recovery instructions in the *Hardware Installation Guide for Cisco UCS E-Series Servers.*

# Logging Into CIMC

### Procedure

**Step 1** In your web browser, type or choose the web link for the CIMC.

**Step 2** If a security dialog box displays, do the following:

a) (Optional) Check the check box to accept all content from Cisco.

b) Click **Yes** to accept the certificate and continue.

**Step 3** In the log in window, enter your username and password.

**Tip** When logging in for the first time to an unconfigured system, use **admin** as the username and **password** as the password.

The following situations occur when you login to the Web UI for the first time:

- You cannot perform any operation until you change default admin credentials on the Web UI.
- You cannot close or cancel the password change pop-up window and opening it in a tab or refreshingthe browser page will continue to display the pop-up window. This pop-up window appears when you login after a factory reset.
- You cannot choose the word 'password' as your new password. If this creates problems for any scripts you may be running, you could change it to password by logging back into the user management options, but this is ENTIRELY at your own risk. It is not recommended by Cisco.

**Step 4** Click **Log In**.

The **Change Password** dialog box appears.

**Note** The **Change Password** dialog box only appears the first time you log into CIMC. It does not appear for subsequent reboots.

**Step 5** In the **New Password** field, enter your new password.

**Step 6** In the **Confirm Password** field, enter the password again to confirm it.

**Step 7** Click **Save Changes**.

The **Chassis Summary** page appears, which is the CIMC home page.

# CIMC Homepage

## CIMC Toolbar

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

| Button Name | Description |
|---|---|
| **Refresh** | Refreshes the current page. |

| | |
|---|---|
| **Host Power** | Displays the drop-down menu for you to choose power options. |
| **Launch vKVM** | Displays the drop-down menu to launch the virtual KVM console. |
| **Ping** | Launches the Ping Details pop-up window. |
| **CIMC Reboot** | Enables you to reboot Cisco IMC. |

## Navigation and Work Panes

The CIMC GUI comprises the **Navigation** pane on the left-hand side of the screen and the **Work** pane on the right hand side of the screen. Clicking links on the **Chassis**, **Compute**, or **Admin** menu in the **Navigation** pane displays the associated tabs in the **Work** pane on the right.

The **Navigation** pane header displays action buttons that allow you to view the navigation map of the entire GUI, view the index, or choose a favorite work pane to go to, directly. The **Pin** icon prevents the **Navigation** pane from sliding in once the **Work** pane displays.

The **Favorite** icon is a star shaped button which allows you to make any specific work pane in the application as your favorite. To do this, navigate to the work pane of your choice and click the **Favorite** icon. To access this work pane directly from anywhere else in the application, click the **Favorite** icon again.

The GUI header displays information about the overall status of the chassis and user login information.

The GUI header also displays the total number of faults (indicated in green or red), with a **Bell** icon next to it. However, clicking this icon displays the summary of only the critical and major faults of various components. To view all the faults, click the **View All** button to display the **Fault Summary** pane.

The **Navigation** pane has the following menus:

- **Chassis** Menu
- **Compute** Menu
- **Admin** Menu

### Chassis Menu

Each node in the **Chassis** menu leads to one or more tabs that display in the **Work** pane. These tabs provides access to the following information:

| Chassis Menu Node Name | Work Pane Tabs Provide Information About... |
|---|---|
| **Summary** | Server Properties, Cisco Integrated Management Controller (Cisco IMC) Information, Router Information, Chassis Status. |
| **Inventory** | CPUs, Memory, Power Supplies, Network Adapters, Storage Management, and Trusted Platform Module (TPM) information. |
| **Sensors** | Power Supply, Fan, Temperature, Voltage, Current, LEDs, and Storage sensor readings. |
| **Faults and Logs** | Fault Summary, Fault History, System Event Log, Cisco IMC Logs, and Logging Controls. |

### Compute Menu

Each node in the **Compute** menu leads to one or more tabs that display in the **Work** pane. These tabs provides access to the following information:

| Compute Menu Node Name | Work Pane Tabs Provide Information About... |
|---|---|
| **BIOS** | Configure BIOS, Configure Boot Order. |
| **Remote Management** | Virtual KVM, Virtual Media, And Serial Over LAN settings. |
| **Troubleshooting** | Bootstrap Process Recording, and Crash Recording information. |
| **Power Policies** | Power Restore Policy settings. |
| **Host Image Mapping** | Host Image Mapping information. |

### Admin Menu

Each node in the **Admin** menu leads to one or more tabs that display in the **Work** pane. These tabs provides access to the following information:

| Admin Menu Node Name | Work Pane Tabs Provide Information About... |
|---|---|
| **User Management** | Local User Management, Lightweight Active Directory Protocol (LDAP), TACACS, and Session Management information. |
| **Networking** | NIC, IPv4, IPv6, VLAN, and Port properties, along with Network Security and NTP settings. |
| **Communication Services** | HTTP, XML API, SSH, Redfish, TLS, IPMI over LAN, and SNMP settings. |
| **Security Management** | Certificate Management, Secure Key Management, and Security Configuration. |
| **Event Management** | Platform Event management. |
| **Firmware Management** | CIMC and BIOS firmware information and management. |
| **Utilities** | Technical support data collection and export, system configuration import and export options, hardware inventory data collection and export, and smart access USB settings. |

## CIMC Online Help

The GUI for the CIMC software is divided into two main sections, a **Navigation** pane on the left and a **Work** pane on the right.

The CIMC online help describes the fields on each CIMC GUI page and in each dialog box. To access the CIMC online help, do one of the following:

- In a particular tab in the CIMC GUI, click the **?** icon in the toolbar above the **Work** pane.
- In a dialog box, click the **?** icon in that dialog box.

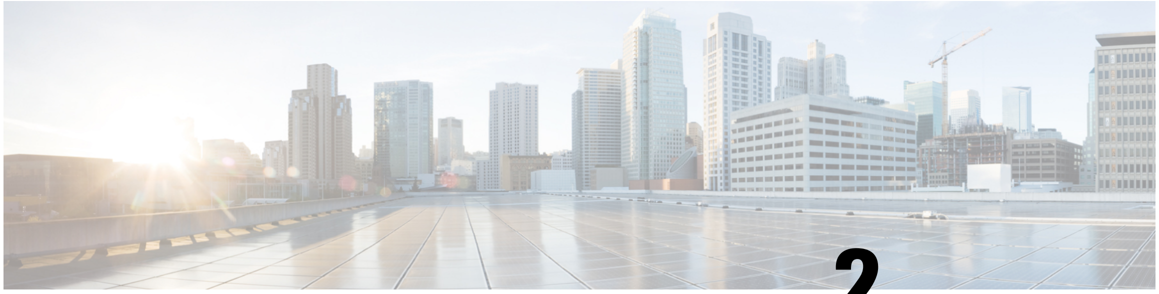
# Logging Out of CIMC

### Procedure

**Step 1** In the upper right pane of CIMC, click **Gear** icon, and choose **Log Out** from the drop-down menu.

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 Operating System or Hypervisor

## Operating System or Hypervisor Installation Methods

The UCS E-Series M6 Servers support several operating systems and hypervisors. Regardless of the platform being installed, you can install it on your server using one of the following methods:

- KVM Console
- PXE installation server
- Host image mapping

**Caution** You must use only one method to map virtual drives. Using a combination of methods will cause the server to be in an undefined state.

## vKVM Console

The vKVM console is an interface accessible from that emulates a direct keyboard, video, and mouse (KVM) connection to the server. The vKVM console allows you to connect to the server from a remote location and to map physical locations to virtual drives that can be accessed by the server during a vKVM session.

Instead of using CDs/DVDs physically connected to the server, the vKVM console uses virtual media, which are actual disk drives or disk image files that are mapped to virtual drives. You can map any of the following to a virtual drive:

- Disk image files (ISO files) on your computer
- USB flash drive on your computer

- Disk image files (ISO files) on the network
- USB flash drive on the network

You can use the KVM console to install an operating system on the server and to do the following:

- Access the BIOS setup menu by pressing **F2** during bootup.
- Access the CIMC Configuration Utility by pressing **F8** during bootup.

## Installing an Operating System or Hypervisor Using the KVM Console

### Before you begin

Locate the operating system or hypervisor installation disk or disk image file.

**Note** The VMware vSphere Hypervisor requires a customized image. To download the customized image, see Downloading the Customized VMware vSphere Hypervisor Image.

### Procedure

**Step 1** Load the operating system or hypervisor installation disk into vKVM-mapped vDVD, or copy the disk image files to your computer.

**Step 2** Log into the CIMC GUI.

**Step 3** To launch the console from the CIMC Home page, click **Launch vKVM** from the **Toolbar**.

**Step 4** Alternatively, in the **Navigation** pane, click the **Compute** menu, and then click the **Remote Management** tab.

**Step 5** In the **Remote Management** pane, click the **Virtual KVM** tab.

**Step 6** In the **Virtual KVM** tab, click the **Launch vKVM** link.

**Step 7** From the **vKVM** console, click the **Virtual Media** tab.

**Step 8** In the **Virtual Media** tab, map the virtual media using either of the following methods:

- Check the **Mapped** check box for the vKVM-mapped vDVD, containing the operating system or hypervisor installation disk.
- Click **Add Image**, navigate to and select the operating system or hypervisor 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 tab open during the installation process. Closing the tab unmaps all virtual media.

**Step 9** Set the boot order to make the vKVM-mapped vDVD as the boot device.

**Step 10** Reboot the server. When the server reboots, it begins the installation process from the vKVM-mapped vDVD. Refer to the installation guide for the platform being installed to guide you through the rest of the installation process.

**Step 11** If disk drives are not displayed after you install the operating system or hypervisor, you must install drivers. See the appropriate operating system or hypervisor documentation for instructions on how to install drivers.

# PXE Installation Servers

A Preboot Execution Environment (PXE) installation server allows a client to boot and install an operating system or hypervisor from a remote location. To use this method, a PXE environment must be configured and available on your VLAN, typically a dedicated provisioning VLAN. In addition, the server must be set to boot from the network. When the server boots, it sends a PXE request across the network. The PXE installationserver acknowledges the request, and starts a sequence of events that installs the operating system or hypervisor on the server.

PXE servers can use installation disks, disk images, or scripts to install the operating system or hypervisor. Proprietary disk images can also be used to install the platform, additional components, or applications.

**Note** PXE installation is an efficient method for installing a platform on a large number of servers. However, considering that this method requires setting up a PXE environment, it might be easier to use another installation method.

## Installing an Operating System or Hypervisor Using a PXE Installation Server

### Before you begin

Verify that the server can be reached over a VLAN.

### Procedure

**Step 1** Set the boot order to **PXE**.

See section Configuring the Boot Order for details.

**Step 2** Reboot the server.

**Caution** If you are using the shared LOM interfaces to access CIMC, make sure that you do not use the CIMC GUI during the server reboot process. If you use the CIMC GUI, the GUI will disconnect duringPXE installation as the boot agent overrides the IP address that was previously configured on the Ethernet ports.

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 operating system or hypervisor being installed to guide you through the rest of the installation process.

### What to do next

After the installation is complete, reset the LAN boot order to its original setting.

## Downloading the Customized VMware vSphere Hypervisor Image

### Procedure

**Step 1** Navigate to https://my.vmware.com/web/vmware/login.

The VMware login page appears.

**Step 2** Enter your VMware credentials, and then click **Log In**.

If you do not have an account with VMware, click **Register** to create a free account.

**Step 3** Click **Downloads**, and then select **All Products** from the drop-down list.

**Step 4** To download the VMware vSphere Hypervisor 7.0U3G image, enter **VMware-ESXi-7.0.3-Custom-Cisco-20328353-4.11.1-a.iso** in the **Search** field, and then click the **Search** icon. From the **Search Results**, click **VMware vSphere** > **Drivers & Tools** > **Cisco Custom Image for ESXi 7.0U3G GA Install CD**, and then click **Download**.

### What to do next

Install the VMware vSpere Hypervisor image.

# Host Image Mapping

The Host Image Mapping feature allows you to download, map, unmap, or delete a host image. Download a host image, such as Linux or VMware, from a remote FTP or HTTP server onto the CIMC internal repository, and then map the image onto the virtual drive of a USB controller in the E-Series M6 Servers. After you map the image, set the boot order to make the virtual drive, in which the image is mounted, as the first boot device, and then reboot the server. The host image must have .iso as the file extension.

## Mapping the Host Image

### Before you begin

- Log in to CIMC as a user with admin privileges.
- Obtain the host image file from the appropriate third party.

**Note** If you start an image update while an update is already in process, both updates will fail.

### Procedure

**Step 1** In the **Navigation** pane, click the **Compute** menu.

**Step 2** In the **Work** pane, click the **Host Image Mapping** tab.

**Step 3** From the **Host Image Mapping** page, click **Add Image**.

The **Add New Mapping** dialog box opens. Complete the following fields:

| Name | Description |
|---|---|
| **Server Type** drop-downlist | The type of remote server on which the image is located. This can be one of the following:<br>• **FTP**<br>• **FTPS**<br>• **HTTP**<br>• **HTTPS**<br>• **SCP**<br>**Note** The displayed fields change depending on the remote server that you choose. |
| **Server IP Address** field | The IP address of the remote FTP or HTTP server. |
| **File Path** field | The path and filename of the remote FTP or HTTP server.<br>The path and filename can contain up to 235 characters.<br>**Note** If you are installing a host image, that image must have .iso as the file extension. |
| **Username** field | The username of the remote server.<br>**Note** If the username is not configured, enter **anonymous** for the username and any character(s) for the password. |
| **Password** field | The password for the username.<br>**Note** If the username is not configured, enter **anonymous** for the username and any character(s) for the password. |

**Step 4** Click **Download**.

The **Host Image Mapping** page opens. You can view the status of the image download in the **Host Image Mapping Status** area. After the image is downloaded and processed successfully, refresh the page. After the page refreshes, the new image status is reflected in the **Host Image Mapping Information** area.

**Step 5** From the **Current Mappings** area, select the image to map, and then click **Map Selected Image**.

The image is mapped and mounted on the virtual drive. The virtual drive can be one of the following:

- HDD—Hard disk drive

**Step 6** Set the boot order to make the virtual drive in which the image is mounted as the first boot device.

**Tip** To determine in which virtual drive the image is mounted, see the **Host Image Update Status** area in the **Host Image Mapping** page.

**Step 7** Reboot the server.

**Step 8** If the image contains an answer file, the operating system or hypervisor installation is automated and the image is installed. Otherwise, the installation wizard is displayed. Follow the wizard steps to install the image.

**Step 9** If disk drives are not displayed after you install the operating system or hypervisor, you must install drivers. See the appropriate operating system or hypervisor documentation for instructions on how to install drivers.

### What to do next

- After the installation is complete, reset the virtual media boot order to its original setting.

## Unmapping the Host Image

### Before you begin

Log in to CIMC as a user with admin privileges.

### Procedure

**Step 1** In the **Navigation** pane, click the **Compute** menu.

**Step 2** In the **Work** pane, click the **Host Image Mapping** tab.

**Step 3** In the **Current Mappings** area, choose the image to unmap.

**Step 4** Click **Unmap Image**.

The mapped image is unmounted.

## Deleting the Host Image

### Before you begin

Log in to CIMC as a user with admin privileges.

### Procedure

**Step 1** In the**Navigation** pane, click the **Compute** menu.

**Step 2** In the work pane, click the **Host Image Mapping** tab.

**Step 3** From the **Current Mappings** area, choose the image to delete.

**Step 4** **(Optional)** If the image that you want to delete is mapped, click **Unmap Image**.

**Step 5** Click **Delete Selected Image**.

The image is removed.

CHAPTER 3

# Managing the Toolbar

## Managing Server Power

### Before you begin

You must log in with user or admin privileges to perform this task.

### Procedure

**Step 1** In the **Toolbar** menu, click the **Host Power** link.

**Step 2** Select from the following drop-down options:

| Name | Description |
|---|---|
| **Power On** | Powers on the server. |
| **Power Off** | Powers off the server, even if tasks are running on that server.<br>**Note** If any firmware or BIOS updates are in progress, do not power off or reset the server until those tasks are complete. |
| **Power Cycle** | Powers off and powers on the server. |
| **Hard Reset** | Reboots the server. |
| **Shut Down** | Shuts down the server if the operating system supports that feature. |

# Pinging a Hostname or IP Address from the Web UI

### Before you begin

You must log in as a user with admin privileges to perform this task.

### Procedure

**Step 1** In the **Toolbar** menu, click the **Ping** icon.

**Step 2** In the **Ping Details** dialog box, update the following fields:

| Name | Description |
|---|---|
| ***Hostname/IPAddress** field | Hostname or IP address you want to reach out to. |
| ***Number of Retries** field | The maximum number of retries allowed to ping the IP address. The default value is 3. The valid range is from 1 to 10. |
| ***Timeout** field | The maximum response time for a pinging activity. The default value is 10 seconds. The valid range is from 1 to 20 seconds. |
| **Ping Status** field | Displays results of the pinging activity. |
| **Details** button | Displays details of the pinging activity. |
| **Ping** button | Pings the IP address. |
| **Cancel** button | Closes the dialog box without pinging. |

# Launching vKVM

### Before you begin

You must log in as a user with admin privileges to perform this task.

### Procedure

**Step 1** To launch the console from **CIMC Home** page, click the **Launch vKVM** link in the toolbar.

**Step 2** Alternatively, in the **Navigation** pane, click the **Compute** menu.

**Step 3** In the **Compute** menu work pane, click the **RemoteManagement** tab.

**Step 4** In the **Remote Management** pane, click the **Virtual KVM** tab.

**Step 5** In the **Virtual KVM** tab, click the **Launchv KVM** link.

**Step 6** Click the URL link displayed in the pop-up window (HTML based KVM console only) to load the client application.

**Note** You must click the link every time you launch the KVM console.

**Step 7**

# Rebooting CIMC

### Before you begin

You must log in as a user with admin privileges to perform this task.

### Procedure

**Step 1** In the **Toolbar** menu, click the **CIMC Reboot** link.

**Step 2** In the dialog box, click **OK** to proceed with the reboot, or click **Cancel** to cancel.

If you reboot, CIMC will be unavailable for the duration of the reboot. You must login again after the reboot is complete.

CHAPTER 4

# Managing the Chassis

# Chassis Summary

## Viewing Chassis Summary

By default, when you log on to CIMC, the **Summary** pane of the **Chassis** menu is displayed in the UI. You can also view the **Chassis Summary** when in another tab or working area, by completing the following steps:

### Procedure

**Step 1** In the **Navigation pane**, click the **Chassis** menu.

**Step 2** In the **Chassis** menu, click **Summary**.

**Step 3** In the **Server Properties** area of the **Chassis Summary** pane, review the following information:

| Name | Description |
|---|---|
| **Product Name** field | The model name of the chassis. |
| **Serial Number** field | The serial number for the chassis. |
| **PID** field | The product ID. |
| **UUID** | The UUID assigned to the server. |
| **BIOS Version** | The BIOS version name. |
| **FPGA Version** | The FPGA version number. |
| **SBFPGA Version** | The SBFPGA version number. |
| **MCU Version** | The MCU version number. |

| Name | Description |
|---|---|
| **AIKIDO Version** | The AIKIDO version number. |
| **Last Reboot Reason** field | Reason for the last reboot. |
| **Uptime** | The uptime for the server. |
| **Description** field | A user-defined description for the server. |
| **Asset Tag** field | A user-defined tag for the server. By default, the asset tag for a new server displays **Unknown**. |

**Step 4** In the **Cisco Integrated Management Controller (Cisco IMC) Information** area of the **Chassis Summary** pane, review the following information:

| Name | Description |
|---|---|
| **Hostname** field | A user-defined hostname for the CIMC. By default, the hostname appears in EXXXX-YYYYYYYYYYY format, where XXXX is the model number and YYYYYYYYYYY is the serial number of the server. |
| **IP Address** field | The IP address for the CIMC. |
| **MAC Address** field | The MAC address for the CIMC. |
| **Firmware Version** field | The current firmware version. |
| **Current Time** field | The current date and time according to the clock.<br>**Note** CIMC gets the current date and time from the server BIOS when NTP is disabled. When NTP is enabled, CIMC gets the current time and date from the NTP server. To change this information, reboot the server and press **F2** when prompted, to access the BIOS configuration menu. Update the date or time using the options on the main BIOS configuration tab. |
| **Local Time** field | The local date and time for the CIMC. |
| **Timezone** field | The time zone for the CIMC. |
| **Select Timezone** dialog box | Dialog box to select the time zone for the CIMC. |

**Step 5** In the **Router Information** area of the **Chassis Summary** pane, review the following information:

| Name | Description |
|---|---|
| **Power State** field | The current power state. |

| Name | Description |
|---|---|
| **Post Completion Status** field | The post completion status. |
| **Overall Server Status** field | The overall status of the server. This can be one of the following:<br>• **Memory Test In Progress**—Theserver is performing a self-test of the installed memory. This condition normally occurs during the boot process.<br>• **Good**<br>• **Moderate Fault**<br>• **Severe Fault**<br>You can click the link in this field to view detailed status information. |
| **Overall DIMM Status** field | The overall status of the memory modules. This can be one of the following:<br>• **Good**<br>• **Fault**<br>• **Severe Fault**<br>You can click the link in this field to view detailed status information. |

# Creating a Server Asset Tag

### 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 **Chassis** menu.

**Step 2** In the **Chassis** menu, click **Summary**.

**Step 3** Enter the **Asset Tag Details** in the text box.

**Step 4** Click **Save Changes**.

## Selecting a Time Zone

### 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 **Chassis** menu.

**Step 2** In the **Chassis** menu, click **Summary**.

**Step 3** In the **Cisco Integrated Management Controller (Cisco IMC) Information** area, click the **Select Timezone** link.

**Step 4** In the **Select Timezone** dialog box, click your location on the map to select your time zone, or select your time zone from the **Timezone** drop-down menu.

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

# Chassis Inventory

## Viewing CPU Properties

### Procedure

**Step 1** In the **Navigation** pane, click the **Chassis** menu.

**Step 2** In the **Chassis** menu, click **Inventory**.

**Step 3** In the **Inventory** work pane, click the **CPU** tab and review the following information for each CPU:

| Name | Description |
|---|---|
| **Socket Name** column | The CPU socket name. |
| **Vendor** column | The CPU vendor. |
| **Family** column | The CPU product family. |
| **Number of Threads** column | The number of threads. |
| **Version** column | The CPU version. |
| **Speed** column | The CPU speed (Mhz). |
| **Number of Cores** column | The number of cores in the CPU. |
| **Status** column | The CPU status. |

| Name | Description |
|---|---|
| **Signature** column | The CPU signature. |

# Viewing Memory Properties

### Procedure

**Step 1** In the **Navigation** pane, click the **Chassis** menu.

**Step 2** In the **Chassis** menu, click **Inventory**.

**Step 3** In the **Inventory** work pane, click the **Memory** tab and review the following information:

| Name | Description |
|---|---|
| **Name** column | The DIMM name. |
| **Capacity** column | The DIMM capacity. |
| **Channel Speed** column | The DIMM channel speed (Mhz). |
| **Channel Type** column | The DIMM channel type. |
| **Memory Type Detail** column | The DIMM memory type. |
| **Bank Locator** column | The DIMM bank locator. |
| **Manufacturer** column | The DIMM manufacturer name. |
| **Serial Number** column | The DIMM serial number. |
| **Asset Tag** column | The DIMM asset tag. |
| **Part Number** column | The DIMM part number. |
| **Visibility** column | The DIMM visibility status. |
| **Operability** column | The DIMM operability status. |
| **Data Width** column | The DIMM data width. |

# Viewing Power Supply Properties

### Procedure

**Step 1** In the **Navigation** pane, click the **Chassis** menu.

**Step 2** In the **Chassis** menu, click **Inventory**.

**Step 3** In the **Inventory** work pane, click the **Power Supplies** tab and review the following information for each power supply:

| Name | Description |
|---|---|
| **Name** column | The name for the power supply unit. |
| **Status** column | The status of the power supply unit. |
| **Product ID** column | The product identifier for the power supply assigned by the vendor. |
| **Serial** column | The serial number of the power supply unit. |
| **Power** column | The power supply, in watts. |

# Viewing Network Adapter Properties

### Before you begin

The server must be powered on, or the properties will not display.

### Procedure

**Step 1** In the **Navigation** pane, click the **Chassis** menu.

**Step 2** In the **Chassis** menu, click **Inventory**.

**Step 3** In the **Inventory** work pane, click the **Network Adapters** tab and review the following information:

| Name | Description |
|---|---|
| **Slot** column | The slot in which the adapter is installed. |
| **Product Name** column | The product name for the adapter. |
| **Number of Interfaces** column | The number of interfaces for the adapter. |

| Name | Description |
|---|---|
| **External Ethernet Interfaces** | **ID**—The ID for the external ethernet interface.<br>**MAC Address**—The MAC address for the external ethernet interface. |

# Viewing Storage Properties

### Before you begin

The server must be powered on, or the properties will not display.

### Procedure

**Step 1** In the **Navigation** pane, click the **Chassis** menu.

**Step 2** In the **Chassis** menu, click **Inventory**.

**Step 3** In the **Inventory** work pane, click the **Storage** tab and review the following information:

| Name | Description |
|---|---|
| **Controller** field | PCIe slot in which the controller drive is located. |
| **PCI Slot** field | The name of the PCIe slot in which the controller drive is located. |
| **Product Name** field | Name of the controller. |
| **Serial Number** field | The serial number of the storage controller. |
| **Firmware Package Build** field | The active firmware package version number. |
| **Product ID** field | Product ID of the controller. |
| **Battery Status** field | Status of the battery. |
| **Cache Memory Size** field | The size of the cache memory, in megabytes. |
| **Health** field | The health of the controller. |

# Viewing TPM Properties

### Before you begin

The server must be powered on, or the properties will not display.

**Procedure**

**Step 1** In the **Navigation** pane, click the **Chassis** menu.

**Step 2** In the **Chassis** menu, click **Inventory**.

**Step 3** In the **Inventory** work pane, click the **TPM** tab and review the following information:

| Name | Description |
|---|---|
| **Version** field | The TPM version. |
| **Model** field | The TPM model. |
| **Vendor** field | The TPM vendor. |
| **Revision** field | The TPM revision. |
| **Firmware Version** field | The TPM firmware version. |
| **Presence** field | The TPM presence. |
| **Enabled Status** field | The TPM enabled status. |
| **Active Status** field | The TPM active status. |
| **Ownership** field | The TPM ownership. |

# Chassis Sensors

## Viewing Power Supply Sensors

**Procedure**

**Step 1** In the **Navigation** pane, click the **Chassis** menu.

**Step 2** In the **Chassis** menu, click **Sensors**.

**Step 3** In the **Sensors** area, click the **Power Supply** tab.

**Step 4** Review the following sensor properties for power supply:

*Table 1: Threshold Sensors Area*

| Name | Description |
|---|---|
| **Sensor Name** column | The name of the sensor. |

| Name | Description |
|---|---|
| **Sensor Status** column | The status of the sensor. This can be one of the following:<br>• **Unknown**<br>• **Informational**<br>• **Normal**<br>• **Warning**<br>• **Critical**<br>• **Non-Recoverable** |
| **Reading** column | The current power usage, in watts. |
| **Critical Threshold Min** column | The minimum critical threshold. |
| **Critical Threshold Max** column | The maximum critical threshold. |
| **Non-Recoverable Threshold Min** column | The minimum non-recoverable threshold. |
| **Non-Recoverable Threshold Max** column | The maximum non-recoverable threshold. |

*Table 2: Discreet Sensors Area*

| Name | Description |
|---|---|
| **Sensor Name** column | The name of the sensor. |
| **Sensor Status** column | The status of the sensor. This can be one of the following:<br>• **Unknown**<br>• **Informational**<br>• **Normal**<br>• **Warning**<br>• **Critical**<br>• **Non-Recoverable** |
| **Reading** column | The basic state of the sensor. |

# Viewing Fan Sensors

### Procedure

**Step 1** In the **Navigation** pane, click the **Chassis** menu.

**Step 2** In the **Chassis** menu, click **Sensors**.

**Step 3** In the **Sensors** area, click the **Fan** tab.

**Step 4** Review the following fan sensor properties:

| Name | Description |
|---|---|
| **Sensor Name** column | The name of the sensor. |
| **Sensor Status** column | The status of the sensor. This can be one of the following:<br>• **Unknown**<br>• **Informational**<br>• **Normal**<br>• **Warning**<br>• **Critical**<br>• **Non-Recoverable** |
| **Speed** column | The current fan speed, in RPMS. |
| **Critical Threshold Min** column | The minimum critical threshold. |
| **Critical Threshold Max** column | The maximum critical threshold. |
| **Non-Recoverable Threshold Min** column | The minimum non-recoverable threshold. |
| **Non-Recoverable Threshold Max** column | The maximum non-recoverable threshold. |

# Viewing Temperature Sensors

### Procedure

**Step 1** In the **Navigation** pane, click the **Chassis** menu.

**Step 2** In the **Chassis** menu, click **Sensors**.

**Step 3** In the **Sensors** area, click the **Temperature** tab.

**Step 4** Review the following temperature sensor properties:

| Name | Description |
|---|---|
| **Sensor Name** column | The name of the sensor. |
| **Sensor Status** column | The status of the sensor. This can be one of the following:<br>• **Unknown**<br>• **Informational**<br>• **Normal**<br>• **Warning**<br>• **Critical**<br>• **Non-Recoverable** |
| **Temperature** column | The current temperature, in Celsius. |
| **Critical Threshold Min** column | The minimum critical threshold. |
| **Critical Threshold Max** column | The maximum critical threshold. |
| **Non-Recoverable Threshold Min** column | The minimum non-recoverable threshold. |
| **Non-Recoverable Threshold Max** column | The maximum non-recoverable threshold. |

# Viewing Voltage Sensors

### Procedure

**Step 1** In the **Navigation** pane, click the **Chassis** menu.

**Step 2** In the **Chassis** menu, click **Sensors**.

**Step 3** In the **Sensors** area, click the **Voltage** tab.

**Step 4** Review the following voltage sensor properties:

| Name | Description |
|---|---|
| **Sensor Name** column | The name of the sensor. |

| Name | Description |
|---|---|
| **Sensor Status** column | The status of the sensor. This can be one of the following:<br>• **Unknown**<br>• **Informational**<br>• **Normal**<br>• **Warning**<br>• **Critical**<br>• **Non-Recoverable** |
| **Voltage (V)** column | The current voltage, in Volts. |
| **Critical Threshold Min** column | The minimum critical threshold. |
| **Critical Threshold Max** column | The maximum critical threshold. |
| **Non-Recoverable Threshold Min** column | The minimum non-recoverable threshold. |
| **Non-Recoverable Threshold Max** column | The maximum non-recoverable threshold. |

# Viewing Current Sensors

### Procedure

**Step 1** In the **Navigation** pane, click the **Chassis** menu.

**Step 2** In the **Chassis** menu, click **Sensors**.

**Step 3** In the **Sensors** area, click the **Current** tab.

**Step 4** Review the following current sensor properties:

| Name | Description |
|---|---|
| **Sensor Name** column | The name of the sensor. |

| Name | Description |
|---|---|
| **Sensor Status** column | The status of the sensor. This can be one of the following:<br>• **Unknown**<br>• **Informational**<br>• **Normal**<br>• **Warning**<br>• **Critical**<br>• **Non-Recoverable** |
| **Current** column | The current, in Ampere. |
| **Critical Threshold Min** column | The minimum critical threshold. |
| **Critical Threshold Max** column | The maximum critical threshold. |
| **Non-Recoverable Threshold Min** column | The minimum non-recoverable threshold. |
| **Non-Recoverable Threshold Max** column | The maximum non-recoverable threshold. |

# Viewing LED Sensors

### Procedure

**Step 1** In the **Navigation** pane, click the **Chassis** menu.

**Step 2** In the **Chassis** menu, click **Sensors**.

**Step 3** In the **Sensors** area, click the **LEDs** tab.

**Step 4** Review the following LED properties:

| Name | Description |
|---|---|
| **LED Status** column | The status of the LED. This can be one of the following:<br>• **ON**<br>• **OFF**<br>• **BLINKING** |

| Name | Description |
|---|---|
| **LED Color** column | The current color of the LED.<br>For details about what the colors mean, see the hardware installation guide for the type of server you are using. |

## Viewing Storage Sensors

### Procedure

**Step 1** In the **Navigation** pane, click the **Chassis** menu.

**Step 2** In the **Chassis** menu, click **Sensors**.

**Step 3** In the **Sensors** area, click the **Storage** tab.

**Step 4** Review the following storage properties:

| Name | Description |
|---|---|
| **Name** column | The name of the storage device. |
| **Status** column | A brief description of the storage device status. |

# Faults and Logs

## Viewing the Fault Summary

### Procedure

**Step 1** In the **Navigation** pane, click the **Chassis** menu.

**Step 2** In the **Chassis** menu, click **Faults and Logs**.

**Step 3** In the **Faults Summary** tab, review the following information:

| Name | Description |
|---|---|
| **Show** drop-downlist | Customizethe way you want to view fault entries using filters. These can be:<br>• **QuickFilter** - Default view.<br>• **Advanced Filter** - Filter options to display the fault entries based on one or more criteria. Using the matching rule, you can view entries matching all the rules or any one combination of rules you specified in the **Filter** fields.<br>Click **Go** to view the entries matching the filter criteria that you set.<br>Click the **Save** icon to save the filter criteria that you set. This becomes a user-defined filter which you can use later.<br>**Note** The user-defined filter appears in the **Manage Preset Filters** dialog box.<br>• **All**- Displays all entries<br>• **Manage Preset Filters** -Displays user-defined filters. You can edit or remove the user-defined filter from this dialog box.<br>• **List of pre-defined filters** -Displays the system-defined filters.<br>**Note** You can use the **Filter** icon to hide or unhide the filter fields. |
| **Time** column | The time when the fault occurred. |
| **Severity** column | This can be one of the following:<br>• **Cleared**-A fault or condition was cleared.<br>• **Critical**<br>• **Info**<br>• **Major**<br>• **Minor**<br>• **Warning** |
| **Code** column | The unique identifier assigned to the fault. |
| **Domain Name** column | The distinguished name (DN) is a hierarchical representation of the device endpoint and its instance on the server. |

| Name | Description |
|---|---|
| **Probable Cause** column | The unique identifier associated with the event that caused the fault. |
| **Description** column | More information about the fault.<br>It also includes a proposed solution. |

# Viewing the Fault History

### Procedure

**Step 1** In the **Navigation** pane, click the **Chassis** menu.

**Step 2** In the **Chassis** menu, click **Faults and Logs**.

**Step 3** In the **Faults History** tab, review the following information:

| Name | Description |
|---|---|
| **Show** drop-downlist | Customizethe way you want to view fault entries using filters. These can be:<br>• **QuickFilter** - Default view.<br>• **Advanced Filter** - Filter options to display the fault entries based on one or more criteria. Using the matching rule, you can view entries matching all the rules or any one combination of rules you specified in the **Filter** fields.<br>Click **Go** to view the entries matching the filter criteria that you set.<br>Click the **Save** icon to save the filter criteria that you set. This becomes a user-defined filter which you can use later.<br>**Note** The user-defined filter appears in the **Manage Preset Filters** dialog box.<br>• **All**- Displays all entries<br>• **Manage Preset Filters** -Displays user-defined filters. You can edit or remove the user-defined filter from this dialog box.<br>• **List of pre-defined filters** -Displays the system-defined filters.<br>**Note** You can use the **Filter** icon to hide or unhide the filter fields. |
| **Time** column | The time when the fault occurred. |
| **Severity** column | This can be one of the following:<br>• **Emergency**<br>• **Alert**<br>• **Critical**<br>• **Error**<br>• **Warning**<br>• **Notice**<br>• **Informational**<br>• **Debug** |

| Name | Description |
|---|---|
| **Probable Cause** column | The unique identifier associated with the event that caused the fault. |
| **Description** column | More information about the fault.<br>It also includes a proposed solution. |

# Viewing the System Event Log

### Procedure

**Step 1** In the **Navigation** pane, click the **Chassis** menu.

**Step 2** In the **Chassis** menu, click **Faults and Logs**.

**Step 3** In the **System Event Log** tab, review the following information:

| Name | Description |
|---|---|
| **Clear Log** button | Clears all events from the log file.<br>**Note** This option is only available if your user ID is assigned the admin or user role. |

| Name | Description |
|---|---|
| **Show** drop-downlist | Customizethe way you want to view fault entries using filters. These can be:<br>• **QuickFilter** - Default view.<br>• **Advanced Filter** - Filter options to display the fault entries based on one or more criteria. Using the matching rule, you can view entries matching all the rules or any one combination of rules you specified in the **Filter** fields.<br>Click **Go** to view the entries matching the filter criteria that you set.<br>Click the **Save** icon to save the filter criteria that you set. This becomes a user-defined filter which you can use later.<br>**Note** The user-defined filter appears in the **Manage Preset Filters** dialog box.<br>• **All**- Displays all entries<br>• **Manage Preset Filters** -Displays user-defined filters. You can edit or remove the user-defined filter from this dialog box.<br>• **List of pre-defined filters** -Displays the system-defined filters.<br>**Note** You can use the **Filter** icon to hide or unhide the filter fields. |
| **Time** column | The date and time the event occurred. |
| **Severity** column | The severity field includes both text and a color-coded icon. For the icon, green indicates normal operation, yellow is informational, and warning, critical, and non-recoverable errors are shown in shades of red. |
| **Description** column | A description of the event. |

# Viewing the CIMC Log

### Procedure

**Step 1** In the **Navigation** pane, click the **Chassis** menu.

**Step 2** In the **Chassis** menu, click **Faults and Logs**.

**Step 3** In the **Cisco IMC Log** tab, review the following information:

| Name | Description |
|---|---|
| **Clear Log** button | Clears all events from the log file.<br>**Note** This option is only available if your user ID is assigned the admin or user role. |
| **Show** drop-downlist | Customizethe way you want to view fault entries using filters. These can be:<br>• **QuickFilter** - Default view.<br>• **Advanced Filter** - Filter options to display the fault entries based on one or more criteria. Using the matching rule, you can view entries matching all the rules or any one combination of rules you specified in the **Filter** fields.<br>Click **Go** to view the entries matching the filter criteria that you set.<br>Click the **Save** icon to save the filter criteria that you set. This becomes a user-defined filter which you can use later.<br>**Note** The user-defined filter appears in the **Manage Preset Filters** dialog box.<br>• **All**- Displays all entries<br>• **Manage Preset Filters** -Displays user-defined filters. You can edit or remove the user-defined filter from this dialog box.<br>• **List of pre-defined filters** -Displays the system-defined filters.<br>**Note** You can use the **Filter** icon to hide or unhide the filter fields. |
| **Time** column | The date and time the event occurred. |
| **Severity** column | The severity field includes both text and a color-coded icon. For the icon, green indicates normal operation, yellow is informational, and warning, critical, and non-recoverable errors are shown in shades of red. |
| **Source** column | The source of the event. |

| Name | Description |
|---|---|
| **Description** column | A description of the event. |

# Viewing Logging Controls

### Procedure

**Step 1** In the **Navigation** pane, click the **Chassis** menu.

**Step 2** In the **Chassis** menu, click **Faults and Logs**.

**Step 3** In the **Logging Controls** tab, review the following information:

*Table 3: Remote Logging Area*

| Name | Description |
|---|---|
| **Enabled** checkbox | If checked, the CIMC sends log messages to the syslog server named in the **IP Address** field. |
| **Enable Secure Remote Syslog** check box | If checked, the CIMC enables secure remote syslog. |
| **HostName/IP Address** field | The address of the Syslog server on which the Cisco IMC log should bestored. You can set an IPv4 or IPv6 address or a domain name as the remote system address. |
| **Port** field | Enter a destination port number of the Syslog server within the range 1 to 65535. The default port number is 514. |
| **Protocol** field | The transport layer protocol for transmission of syslog messages. You can select one of the following:<br>• TCP<br>• UDP |
| **Handshake** field | Displays the handshake status. |

| Name | Description |
|---|---|
| **Minimum Severity to Report** field | Specify the lowest level of messages that will be included in the remote logs. You can select one of the following:<br>• **Emergency**<br>• **Alert**<br>• **Critical**<br>• **Error**<br>• **Warning**<br>• **Notice**<br>• **Informational**<br>• **Debug** |

*Table 4: Local Logging Area*

| | |
|---|---|
| **Minimum Severity to Report** drop-down | Specify the lowest level of messages that will be included in the remote logs. You can select one of the following:<br>• **Emergency**<br>• **Alert**<br>• **Critical**<br>• **Error**<br>• **Warning**<br>• **Notice**<br>• **Informational**<br>• **Debug** |

**Note** The Cisco IMC does not remotely log any messages with a severity below the selected severity. For example, if you choose **Error**, then the Cisco IMC remote log contains all messages with the severity **Emergency**, **Alert**, **Critical**, or **Error**. It does not show **Warning**, **Notice**, **Informational**, or **Debug** messages.

*Table 5: Upload Status Area*

| | |
|---|---|
| **Certificate Upload Status** field | Displays the certificate upload status. |

| | |
|---|---|
| **Certificate Upload Progress** field | Displays the certificate upload progress. |

## Sending the CIMC Log to a Remote Server

### Before you begin

- The remote syslog server must be configured to receive logs from a remote host.
- The remote syslog server must be configured to receive all types of logs, including authentication-related logs.
- The remote syslog server's firewall must be configured to allow syslog messages to reach the syslog server.
- You can use the **Send Test Syslog** link to test the server.

### Procedure

**Step 1** In the **Navigation** pane, click the **Chassis** menu.

**Step 2** In the **Chassis** menu, click **Faults and Logs**.

**Step 3** Click the **Logging Controls** tab.

**Step 4** In either of the **Remote Syslog Server** areas, complete the following fields:

| Name | Description |
|---|---|
| **Enabled** check box | If checked, the CIMC sends log messages to the syslog server named in the **IP Address** field. |
| **Enable Secure Remote Syslog** check box | If checked, the CIMC enables secure remote syslog. |
| **Host Name/IP Address** field | The address of the Syslog server on which the Cisco IMC log should bestored. You can set an IPv4 or IPv6 address or a domain name as the remote system address. |
| **Port** field | Enter a destination port number of the Syslog server within the range 1 to 65535. The default port number is 514. |
| **Protocol** field | The transport layer protocol for transmission of syslog messages. You can select one of the following:<br>• TCP<br>• UDP |

**Step 5** (Optional) In the **Minimum Severity to Report** drop-down list, specify the lowest level of messages that will be included in the remote logs.

You can choose one of the following, in decreasing order of severity:

- **Emergency**
- **Alert**
- **Critical**
- **Error**
- **Warning**
- **Notice**
- **Informational**
- **Debug**

**Note** The system does not remotely log any messages with a severity below the chosen severity. For example, if you choose **Error**, then the remote log will contain all messages with the severity **Emergency**, **Alert**, **Critical**, or **Error.** It will not show **Warning**, **Notice**, **Informational**, or **Debug** messages.

**Step 6** Click **Save Changes**.

# Uploading a Remote Syslog Certificate

### Before you begin

At least one of the remote syslog servers must be enabled before uploading the remote syslog certificate.

### Procedure

**Step 1** In the **Chassis** menu, click **Faults and Logs**.

**Step 2** In the **Faults and Logs** work are, click the **Logging Controls** tab.

**Step 3** Click the **Upload Remote Syslog Certificate** link.

**Step 4** In the **Upload Remote Syslog Certificate** dialog box, enter the following information:

| Name | Description |
|---|---|
| **Select Server** drop-down | Selects the server to which the certificate is uploaded. |
| **Upload from remote location** radio button | If the certificate resides on a remote server, click this radio button, complete the required fields, and then click **Upload** to upload the certificate. |

| Name | Description |
|---|---|
| **Upload from remote location** drop-down | The remote server type. This can be one of the following:<br>• **TFTP**<br>• **FTP**<br>• **SFTP**<br>• **SCP**<br>• **HTTP** |
| **Server IP/Hostname** field | The IP address or hostname of the server on which the certificate file resides. Depending on the setting in the **Upload from remote location** drop-down list, the fields displayed may vary. |
| **Path and Filename** field | The path and filename of the certificate file on the remote server. |
| **Username** field | Username for the server. |
| **Password** field | Password for the server. |
| **Upload through Browser Client** button | Allows you to browse and upload the certificate. |
| **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. |
| **Paste Content** radio button | Opens a dialog box that allows you to copy the entire content of the certificate and paste it in the **Paste Remote Syslog Certificate** text field. |
| **Upload** button | Uploads the content. |
| **Close** button | Cancels the process and closes the dialog box. |

**Step 5** Click **Save Changes** to save your changes, or **Reset Values** to reset the parameters to previous values.

# Configuring the CIMC Log Threshold

### Procedure

**Step 1** In the **Navigation** pane, click the **Chassis** menu.

**Step 2** In the **Chassis** menu, click **Faults and Logs**.

**Step 3** Click the **Logging Controls** tab.

**Step 4** In the **Minimum Severity to Report** drop-down list, specify the lowest level of messages that will be included in the remote logs.

You can choose one of the following, in decreasing order of severity:

- **Emergency**
- **Alert**
- **Critical**
- **Error**
- **Warning**
- **Notice**
- **Informational**
- **Debug**

**Note** The system does not remotely log any messages with a severity below the chosen severity. For example, if youchoose **Error**, then the remote log will contain all messages with the severity **Emergency**, **Alert**, **Critical**, or **Error.** It will not show **Warning**, **Notice**, **Informational**, or **Debug** messages.

CHAPTER 5

# Managing the Server

# Configuring BIOS

## BIOS Settings

### Before you begin

- You must log in with admin privileges to perform this task.
- You must configure the BIOS password using the server CLI. See *Setting the BIOS Password* in the CLI Configuration Guide for Cisco UCS E-Series M6 Servers.

### Procedure

**Step 1** In the **Navigation** pane, click the **Compute** menu.

**Step 2** In the work pane, click the **BIOS** tab.

Under the BIOS tab, there are several options for further BIOS configuration.

## Entering BIOS Setup

When you enter the BIOS setup for the first time, ensure that you secure the BIOS by setting up an admin-level and a user-level password. You have to set up the admin password when you access the BIOS menu for the firsttime. The user password (which only gives access to a small subset of BIOS options) must be set inside the BIOS setup menu.

To set up the admin password, press **F2** when the system boots up. You will be prompted to set the password.

To set up the user password, after you log in, go to the **Security** tab and set the password.

### Before you begin

- The server must be powered on.
- You must log in with admin privileges to perform this task.

### Procedure

**Step 1** In the **BIOS** tab, click the **Enter BIOS Setup** link.

**Step 2** In the dialog box, click **OK** to proceed to BIOS setup, or **Cancel** to return to the BIOS UI.

**Step 3** Clicking **OK** reboots the host. On restart, the server enters the BIOS setup.

## Clearing the BIOS CMOS

**Note** On rare occasions, troubleshooting a server may require you to clear the server's BIOS CMOS memory. This procedure is not part of the normal maintenance of a server.

### Before you begin

- The server must be powered off.
- You must log in with admin privileges to perform this task.

### Procedure

**Step 1** In the **BIOS** tab, click the **Clear BIOS CMOS** link.

**Step 2** In the dialog box, click **OK** to clear the BIOS CMOS, or **Cancel** to return to the BIOS UI.

## Restore Manufacturing Custom Settings

### Before you begin

You must log in with admin privileges to perform this task.

### Procedure

**Step 1** In the **BIOS** tab, click the **Restore Manufacturing Custom Settings** link.

Step 2 In the dialog box, click **OK** to proceed, or **Cancel** to return to the BIOS UI.

## Restore Defaults

### Procedure

Step 1 In the **BIOS** tab, click the **Restore Defaults** link.

Step 2 In the dialog box, click **OK** to proceed and reboot the host, or **Cancel** to return to the BIOS UI.

# Configuring Advanced BIOS Settings

### Before you begin

You must log in with admin privileges to perform this task.

### Procedure

Step 1 In the **Navigation** pane, click the **Compute** menu.

Step 2 In the work pane, click the **BIOS** tab.

Step 3 Click the **Configure BIOS** tab.

## Configuring Server Management BIOS Settings

### Procedure

Step 1 In the **Configure BIOS** tab, click **Server Management**.

Step 2 Specify whether the server should be rebooted after you save your changes.

If you want your changes applied automatically after you click **Save**, check the **Reboot Host Immediately** check box. The server reboots immediately and the changes are applied.

If you want to apply your changes at a later time, unchceck the **Reboot Host Immediately** check box. CIMC stores the changes and applies them the next time the server reboots.

**Note** If there are existing BIOS parameter changes pending, CIMC automatically overwrites the stored values with the current settings when you click **Save**.

Step 3 In the **Server Management** tab, update the relevant fields. The following fields are available:

| Name | Description |
|---|---|
| **Baud rate** drop-down | What BAUD rate is used for the serial port transmission speed. If you disable Console Redirection, this option is not available. This can be one of the following:<br>• **9.6k**—A 9600 BAUD rate is used.<br>• **19.2k**—A 19200 BAUD rate is used.<br>• **38.4k**—A 38400 BAUD rate is used.<br>• **57.6k**—A 57600 BAUD rate is used.<br>• **115.2k**—A 115200 BAUD rate is used. |
| **Console redirection** drop-down | This can be one of the following:<br>• COM 0<br>• COM 1<br>• Disabled |
| **Flow Control** drop-down | Whether a handshake protocol is used for flow control. Request to Send / Clear to Send (RTS/CTS) helps to reduce frame collisions that can be introduced by a hidden terminal problem. This can be one of the following:<br>• **None**—No flow control is used.<br>• **RTS-CTS**—RTS-CTS is used for flow control. |
| **Terminal type** drop-down | This can be one of the following:<br>• **PC-ANSI**—The PC-ANSI terminal font is used.<br>• **VT100**—A supported VT100 video terminal and its character set are used.<br>• **VT100-PLUS**—A supported vt100-plus video terminal and its character set are used.<br>• **VT-UTF8**—A video terminal with the UTF-8 character set is used. |
| **Boot Order Rules** drop-down | This can be one of the following:<br>• CIMC-config<br>• BIOS-menu |

| Name | Description |
|---|---|
| **OS Watchdog Timer** drop-down | This can be one of the following:<br>• Enabled<br>• Disabled |
| **OS Watchdog Timer Policy** drop-down | This can be one of the following:<br>• Power Off<br>• Reset |
| **OS Watchdog Timer Timeout** drop-down | This can be one of the following:<br>• 5 minutes<br>• 10 minutes<br>• 15 minutes<br>• 20 minutes |
| **FRB 2 Timer** drop-down | This can be one of the following:<br>• Enabled<br>• Disabled |

**Step 4** Click **Save** to save your changes, or **Reset** to restore the previous values for all parameters.

# Configuring BIOS Security

### Procedure

**Step 1** In the **Configure BIOS** tab, click **Security**.

**Step 2** Specify whether the server should be rebooted after you save your changes.

If you want your changes applied automatically after you click **Save**, check the **Reboot Host Immediately** check box. The server reboots immediately and the changes are applied.

If you want to apply your changes at a later time, unchceck the **Reboot Host Immediately** check box. CIMC stores the changes and applies them the next time the server reboots.

**Note** If there are existing BIOS parameter changes pending, CIMC automatically overwrites the stored values with the current settings when you click **Save**.

**Step 3** In the **Security** tab, update the relevant fields. The following fields are available:

| Name | Description |
|---|---|
| **Trusted Platform Module State** drop-down | Trusted Platform Module (TPM ) is a microchip designed to provide basic security-related functions primarily involving encryption keys. This option allows you to control the TPM Security Device support for the system. It can be one of the following:<br>• **Disabled**<br>• **Enabled**<br>**Note** Contact your operating system vendor to make sure the operating system supports this feature. |
| **TPM Pending Operation** drop-down | Displays TPM pending operations. It can be one of the following:<br>• **None**—No pending operation.<br>• **TPM Clear**—Clears the TPM. |

**Step 4** Click **Save** to save your changes, or **Reset** to restore the previous values for all parameters.

# Configuring BIOS I/O

### Procedure

**Step 1** In the **Configure BIOS** tab, click **I/O**.

**Step 2** Specify whether the server should be rebooted after you save your changes.

If you want your changes applied automatically after you click **Save**, check the **Reboot Host Immediately** check box. The server reboots immediately and the changes are applied.

If you want to apply your changes at a later time, unchceck the **Reboot Host Immediately** check box. CIMC stores the changes and applies them the next time the server reboots.

**Note** If there are existing BIOS parameter changes pending, CIMC automatically overwrites the stored values with the current settings when you click **Save**.

**Step 3** In the **I/O** tab, update the relevant fields. The following fields are available:

| Name | Description |
|---|---|
| **USB Port 0 Support** drop-down | This can be one of the following:<br>• Enabled<br>• Disabled |

| Name | Description |
|---|---|
| **USB Port 1 Support** drop-down | This can be one of the following:<br>• Enabled<br>• Disabled |
| **IPv6 PXE Support** drop-down | This can be one of the following:<br>• Enabled<br>• Disabled |
| **Network Stack** drop-down | This can be one of the following:<br>• Enabled<br>• Disabled<br>**Note** Network Stack must be enabled to configure IPv4/IPv6 PXE support. If Network Stack is disabled, PXE is also disabled. |
| **IPv4 PXE Support** drop-down | This can be one of the following:<br>• Enabled<br>• Disabled |

**Step 4** Click **Save** to save your changes, or **Reset** to restore the previous values for all parameters.

# Configuring the Processor

### Procedure

**Step 1** In the **Configure BIOS** tab, click **Processor**.

**Step 2** Specify whether the server should be rebooted after you save your changes.

If you want your changes applied automatically after you click **Save**, check the **Reboot Host Immediately** check box. The server reboots immediately and the changes are applied.

If you want to apply your changes at a later time, unchceck the **Reboot Host Immediately** check box. CIMC stores the changes and applies them the next time the server reboots.

**Note** If there are existing BIOS parameter changes pending, CIMC automatically overwrites the stored values with the current settings when you click **Save**.

**Step 3** In the **Processor** tab, update the relevant fields. The following fields are available:

| Name | Description |
|---|---|
| **Package C State** drop-down | This can be one of the following:<br>• Auto<br>• C0 C1 State<br>• C2<br>• C6 Non Retention |
| **Cores Enabled** drop-down | This can be one of the following:<br>• Values 1 through 10<br>• All |

**Step 4** Click **Save** to save your changes, or **Reset** to restore the previous values for all parameters.

# Managing the Server Boot Order

When you change the boot order configuration, CIMC sends the configured boot order to BIOS the next time that server is rebooted. To implement the new boot order, reboot the server after you make the configuration change. The new boot order takes effect on any subsequent reboot. The configured boot order remains until the configuration is changed again in or in the BIOS setup.

The server boot order is the boot order actually used by BIOS when the server last booted. The actual boot order can differ from the boot order configured in CIMC.

**Note** The actual boot order differs from the configured boot order if either of the following conditions occur:

- BIOS does not detect a boot option in the configured boot order.
- A user changes the boot order directly through BIOS, by configuring Boot Order Rules for the BIOS menu.

### Procedure

**Step 1** In the **BIOS** tab, click the **Configure Boot Order** tab.

This area displays the boot order devices configured through Cisco IMC, as well as the actual boot order used by the server BIOS.

**Step 2** The **Configured Boot Devices** section displays the boot order configured through Cisco IMC. If this configuration changes, Cisco IMC sends this boot order to BIOS the next time that server boots.

# Configuring the Boot Order

### Before you begin

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

### Procedure

**Step 1** In the **BIOS** tab, click the **Configure Boot Order** tab.

**Step 2** Click the **Configure Boot Order** button.

**Step 3** In the **Configure Boot Order** dialog box, update the relevant fields. The following fields are available:

| Name | Description |
|---|---|
| **Device Types** column | Displays the device types from which this server can boot. |
| **Boot Order** column | Displays the order in which the boot is attempted. |
| **Left** and **Right** arrow buttons | Move the selected devices to and from the Boot Order column. |
| **Up** and **Down** buttons | Move the selected devices up or down in the Boot Order column. |

**Step 4** Click **Save Changes** to save your changes, or **Close** to close the dialog box without saving the changes.

Cisco IMC sends these changes to BIOS the next time that server boots. To have these changes take effect immediately, reboot the server. You can verify the new boot order by refreshing the **BIOS** tab.

# Configuring Power Policies

The power restore policy determines how power is restored to the server after a chassis power loss.

### Before you begin

You must log in with admin privileges to perform this task.

### Procedure

**Step 1** In the **Navigation** pane, click the **Compute** menu.

**Step 2** In the **Compute** menu work pane, click the **Remote Management** tab.

**Step 3** Enter the required information:

| Name | Description |
|---|---|
| **Power Restore Policy** drop down | Provides options for the power restore policy.<br>• **Power Off**<br>• **Restore Last State** |

**Step 4** Click **Save Changes** to save your changes, or **Reset Values** to reset the parameters to previous values.

CHAPTER 6

# Managing Remote Presence

# Managing the Virtual KVM

## vKVM Console

The vKVM console is an interface accessible from that emulates a direct keyboard, video, and mouse (KVM) connection to the server. The vKVM console allows you to connect to the server from a remote location and to map physical locations to virtual drives that can be accessed by the server during a vKVM session.

Instead of using CDs/DVDs physically connected to the server, the vKVM console uses virtual media, which are actual disk drives or disk image files that are mapped to virtual drives. You can map any of the following to a virtual drive:

- Disk image files (ISO files) on your computer
- USB flash drive on your computer
- Disk image files (ISO files) on the network
- USB flash drive on the network

You can use the KVM console to install an operating system on the server and to do the following:

- Access the BIOS setup menu by pressing **F2** during bootup.
- Access the CIMC Configuration Utility by pressing **F8** during bootup.

## Launching vKVM

### Before you begin

You must log in as a user with admin privileges to perform this task.

### Procedure

**Step 1** To launch the console from **CIMC Home** page, click the **Launch vKVM** link in the toolbar.

**Step 2** Alternatively, in the **Navigation** pane, click the **Compute** menu.

**Step 3** In the **Compute** menu work pane, click the **RemoteManagement** tab.

**Step 4** In the **Remote Management** pane, click the **Virtual KVM** tab.

**Step 5** In the **Virtual KVM** tab, click the **Launchv KVM** link.

**Step 6** Click the URL link displayed in the pop-up window (HTML based KVM console only) to load the client application.

**Note** You must click the link every time you launch the KVM console.

**Step 7**

## vKVM Navigation

### Before you begin

You must log in as a user with admin privileges to perform this task.

### Procedure

In the vKVM UI, view the available navigation menus. The following menus are available:

*Table 6: Toolbar Menu*

| Name | Description |
|---|---|
| **Session User List** | Displays the list of users in the current session. |
| **Help** | Launches the help pop-up. |
| **Language** drop-down | Provides a list of available languages for the user to choose from. |

| Name | Description |
|---|---|
| **Profile** menu | Provides the user's profile settings, including:<br>• **Role**<br>• **Server**<br>• **Settings**<br>  • Maintain Aspect Ration<br>  • Mouse Mode<br>  • Video Inactivity Timeout<br>  • Number of Terminal Scrollback Lines<br>  • Theme<br>• **Sign Out** |

*Table 7: Console Menu*

| Name | Description |
|---|---|
| **KVM** | The SOL (Serial Over Lan) console provides console access to the host. |
| **Activate SOL** | Use the following configuration to activate the SOL:<br>`device#`<br>`device # scope sol`<br>`device /sol # set enabled yes`<br>`device /sol *# commit`<br>`show detail`<br>`device /sol # show detail`<br>`Serial Over LAN:`<br>`    Enabled: yes`<br>`Baud Rate(bps): 115200`<br>`    Com Port: com0`<br>`    SOL SSH Port: 2400`<br>`device /sol #` |

*Table 8: File Menu*

| Name | Description |
|---|---|
| **Paste Clipboard Text** | Opens the Paste Clipboard text dialog box with the following fields:<br>• When an unsupported character is found in pasted text dropdown<br>• Enter **Text to Paste** field |

| Name | Description |
|---|---|
| **Capture to File** | Saves the current screen as a JPG image in the local Downloads folder. |

Table 9: View Menu

| Name | Description |
|---|---|
| **Refresh** | Updatesthe console display with the server's current video output. |
| **Video Quality** | Provides the dropdown list for video quality options:<br>• High<br>• Medium<br>• Low<br>• Ultra Low |
| **Clear SOL Console** | Clears the SOL console. |
| **Full Screen** | Expands the KVM console so that it fills the entire screen. |

Table 10: Macros Menu

| Name | Description |
|---|---|
| **Static Macros** | Displays a predefined set of macros. |
| **Manage Macros** | Opens the **Manage Macros** dialog box, which allows you to create and manage macros.<br>System-defined macros cannot be deleted. |

Table 11: Tools Menu

| Name | Description |
|---|---|
| **Stats** | Opens the **KVM Stats**dialog box. |
| **Session User List** | Opens the **Session User List** dialog box that shows all the user IDs that have an active KVM session. |
| **Keyboard** | Opens the virtual keyboard pop-up. |
| **USB Reset** | Provides a dropdown list to reset:<br>• Keyboard and mouse<br>• Virtual media |

*Table 12: Power Menu*

| Name | Description |
|---|---|
| **Power On System** | Powers on the system.<br>This option is disabled when the system is powered onand it is enabled when the system is not powered. |
| **Power Off System** | Powers off the system from the virtual console session.<br>This option is enabled when the system is powered on anddisabled when the system is not powered on. |
| **Reset System** | Reboots the system without powering it off.<br>This option is enabled when the system is powered on anddisabled when the system is not powered on. |
| **Power Cycle System** | Turns off system and then back on.<br>This option is enabled when the system is powered on anddisabled when the system is not powered on. |

*Table 13: Boot Device Menu*

| Name | Description |
|---|---|
| **Boot Device** | Choose a one-time boot device. The boot device selected will be used once, on the next boot. The configured boot device will be used for subsequent boots. |

*Table 14: Virtual Media Menu*

| Name | Description |
|---|---|
| **Create Image** | Create a .iso image, and manage virtual media devices. |
| **vKVM-Mapped vDVD** | Maps the selected image file as vKVM mapped vDVD |
| **vKVM-Mapped vHDD** | Maps the selected image file as vKVM mapped vHDD |
| **vKVM-Mapped vFDD** | Maps the selected image file as vKVM mapped vFDD |
| **CIMC-Mapped vDVD** | Maps the selected image file as CIMC mapped vDVD |
| **CIMC-Mapped vHDD** | Maps the selected image file as CIMC mapped vHDD |
| **Host-Mapped vDVD** | Maps the selected image file as Host-Image mapped vDVD |
| **Host-Mapped vHDD** | Maps the selected image file as Host-Image mapped vHDD |

*Table 15: Chat Menu*

| Name | Description |
|---|---|
| **Chat** | Opens the **Chat**box to communicate with other users. |

# Configuring the Virtual KVM

### Before you begin

You must log in as a user with admin privileges to eprform this task.

### Procedure

**Step 1** In the **Navigation** pane, click the **Compute** menu.

**Step 2** In the **Compute** menu work pane, click the **RemoteManagement** tab.

**Step 3** In the **RemoteManagement** 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** drop-down | The maximum number of concurrent KVM sessions allowed. You can choose any number between 1 and 4. |
| **Active Sessions** field | The number of KVM sessions running on the server. |
| **Remote Port** field | The port used for KVM communication. |
| **Enable 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** to save your changes, or **Reset Values** to reset the parameters to previous values.

## Enabling or Disabling the Virtual KVM

### Before you begin

You must log in as a user with admin privileges to perform this task.

### Procedure

**Step 1** In the **Remote Management** pane, click the **Virtual KVM** tab.

**Step 2** In the **Virtual KVM** tab, check or uncheck the **Enabled** check box.

**Step 3** Click **Save Changes** to save your changes, or **Reset Values** to reset the parameters to previous values.

# Configuring Virtual Media

### Before you begin

You must log in as a user with admin privileges to perform this task.

### Procedure

**Step 1** In the **Navigation** pane, click the **Compute** menu.

**Step 2** In the **Compute** menu work pane, click the **RemoteManagement** tab.

**Step 3** In the **Remote Management** pane, click the **Virtual Media** tab.

**Step 4** In the **vKM Console Based vMedia 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 that are currently running. |

**Step 5** Click **Save Changes** to save your changes, or **Reset Values** to reset the parameters to previous values.

# Viewing CIMC-Mapped vMedia Properties

### Procedure

**Step 1** In the **Navigation** pane, click the **Compute** menu.

**Step 2** In the **Compute** menu work pane, click the **Remote Management** tab.

**Step 3** In the **Remote Management** pane, click the **Virtual Media** tab.

**Step 4** In the **Cisco IMC-Mapped vMedia** area, review the **Last Mapping Status**.

**Step 5** Choose a row from the **Current Mappings** table.

**Step 6** Click **Properties** and review the following information:

| Name | Description |
|---|---|
| **Add New Mapping** button | Opens a dialog box that allows you to add a new image. |
| **Properties** button | Opens a dialog box that allows you to view or change the properties for the chosen image. |
| **Unmap** button | Unmaps the mounted vMedia. |
| **Last Mapping Status** field | The status of the last mapping attempted. |
| **Volume** column | The identity of the image. |
| **Mount Type** drop down | The type of mapping. |
| **Remote Share** field | The URL of the image. |
| **Remote File** field | The exact file location of the image. |
| **Status** field | The current status of the map. This can be one of the following:<br>• **OK**—The mapping is successful.<br>• **InProgress**—The mapping is in progress.<br>• **Stale**—displays a text string with the reason why the mapping is stale.<br>• **Error**—displays a text string with the reason for the error. |

# Creating a CIMC-Mapped vMedia

### Before you begin

You must log in with admin privileges to perform this task.

### Procedure

**Step 1** In the **Navigation** pane, click the **Compute** menu.

**Step 2** In the **Compute** menu work pane, click the **Remote Management** tab.

**Step 3** In the **Remote Management** pane, click the **Virtual Media** tab.

**Step 4** In the **Current Mappings** area, click **Add New Mapping**.

**Step 5** In the **Add New Mapping** dialog box, update the following fields:

| Name | Description |
|---|---|
| **Volume** field | The identity of the image mounted for mapping. |
| **Mount Type** drop-down | The type of mapping. This can be one of the following:<br>**Note** Ensure that the communication port of the mount type that youchoose is enabled on the switch. For example, when you are using CIFS as your mount type, ensure port 445 (which is its communication port) is enabled on the switch. Similarly, enable ports 80 for HTTP, 443 for HTTPS and 2049 for NFS when you use them.<br>• **NFS**—Network File System.<br>• **CIFS**—Common Internet File System.<br>• **WWW(HTTP/HTTPS)**—HTTP-based or HTTPS-based system.<br>**Note** Before mounting the virtual media,tries to verify reachability to the end server by pinging the server. |
| **Remote Share** field | The URL of the image to be mapped. The format depends on the chosen **Mount Type**:<br>• **NFS**—Use `serverip:/share`<br>• **CIFS**—Use `//serverip/share`<br>• **WWW(HTTP/HTTPS)**—Use `http[s]://serverip/share` |

| Name | Description |
|---|---|
| **Remote File** field | The name and location of the .iso or .img file in the remote share. |

| Name | Description |
|---|---|
| **Mount Options** field | |

| Name | Description |
|---|---|
| | Industry-standard mount options entered in a comma separated list. The options vary depending on the chosen Mounty Type.<br>If you are using **NFS**, leave the field blank or enter one or more of the following:<br>• `ro`<br>• `rw`<br>• `nolock`<br>• `noexec`<br>• `soft`<br>• `port=VALUE`<br>• `timeo=VALUE`<br>• `retry=VALUE`<br>If you are using **CIFS**, leave the field blank or enter one or more of the following:<br>• `soft`<br>• `nounix`<br>• `noserverino`<br>• `guest`<br>• `username=VALUE`—ignored if `guest` is entered.<br>• `password=VALUE`—ignored if `guest` is entered.<br>• `sec=VALUE`<br>The protocol to use for authentication when communicating with the remote server. Based on the configuration of CIFS share, the **VALUES** can be one of the following:<br>• **None**—No authentication is used<br>• **Ntlm**—NT LAN Manager (NTLM) security protocol.<br>• **Ntlmi**—NTLMi security protocol.<br>• **Ntlmssp**—NT LAN Manager Security Support Provider (NTLMSSP) protocol.<br>• **Ntlmsspi**—NTLMSSPi protocol.<br>• **Ntlmv2**—NTLMv2security protocol. Use this |

| Name | Description |
|---|---|
| | option only with Samba Linux.<br>If you are using **WWW(HTTP/HTTPS)**, leave the field blank or enter the following:<br>• `noauto`<br>**Note** Before mounting the virtual media,tries to verify reachability to the end server by pinging the server.<br>• `username=VALUE`<br>• `password=VALUE` |
| **Username** field | The username for the specified **Mount Type**, if required. |
| **Password** field | The password for the chosen username, if required. |

**Step 6** Click **Save**.

# Unmapping a CIMC-Mapped vMedia

### Before you begin

You must log in with admin privileges to perform this task.

### Procedure

**Step 1** In the **Navigation** pane, click the **Compute** menu.

**Step 2** In the **Compute** menu work pane, choose a server.

**Step 3** In the **Compute** menu work pane, click the **Remote Management** tab.

**Step 4** In the **Remote Management** pane, click the **Virtual Media** tab.

**Step 5** Choose a row from the **Current Mappings** table, and click **Unmap**.
The selected media is unmapped.

# Remapping a CIMC-Mapped vMedia

### Before you begin

You must log in with admin privileges to perform this task.

### Procedure

**Step 1** In the **Navigation** pane, click the **Compute** menu.

**Step 2** In the **Compute** menu work pane, choose a server.

**Step 3** In the **Compute** menu work pane, click the **Remote Management** tab.

**Step 4** In the **Remote Management** pane, click the **Virtual Media** tab.

**Step 5** Choose a row from the **Current Mappings** table, and click **Remap**.
The selected media is remapped.

## Deleting a CIMC-Mapped vMedia

### Before you begin

You must log in with admin privileges to perform this task.

### Procedure

**Step 1** In the **Navigation** pane, click the **Compute** menu.

**Step 2** In the **Compute** menu work pane, choose a server.

**Step 3** In the **Compute** menu work pane, click the **Remote Management** tab.

**Step 4** In the **Remote Management** pane, click the **Virtual Media** tab.

**Step 5** Choose a row from the **Current Mappings** table, and click **Delete**.
The selected media is deleted.

# 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 perform this task.

### Procedure

**Step 1** In the **Navigation** pane, click the **Compute** menu.

**Step 2** In the work pane, click the **Remote Management** tab.

**Step 3** In the **Remote Management** 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 (SoL) is enabled on the server. |
| **Baud Rate** drop down | The baud rate the system uses for SoL communication. This can be one of the following:<br>• **9600 bps**<br>• **19.2 kbps**<br>• **38.4 kbps**<br>• **57.6 kbps**<br>• **115.2kbps** |
| **Com Port** drop down | The serial port through which the system routes SoL communication.<br>You can choose one of the following:<br>• **com0**—SoL communication is routed through COM port 0, an externally accessible serial port that supports either a physical RJ45 connection to an external device or a virtual SoL connection to a network device.<br>If you choose this option, the system enables SoL and disables the RJ45 connection, which means that the server can no longer support an external serial device.<br>• **com1**—SoLcommunication is routed through COM port 1, an internal port accessible only through SoL.<br>If you choose this option, you can use SoL on COM port 1 and the physical RJ45 connection on COM port 0.<br>**Note** Changing the Com Port setting disconnects any existing SoL sessions. |
| **SSH Port** field | The port through which you can access Serial over LAN directly. The portenables you to by-pass the Cisco IMC shell to provide direct access to SoL.<br>The valid range is 1024 to 65535. The default value is 2400.<br>**Note** Changing the SSH Port setting disconnects any existing SSH sessions. |

**Step 5** Click **Save Change**s to save your changes, or **Reset Values** to reset the parameters to previous values.

CHAPTER 7

# Managing User Accounts

## Local User Management

The Local User Management tab allows you to configure users, modify password and lockout details, and upload SSH keys.

### Before you begin

You must log in with admin privileges to perform this task.

### Procedure

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

**Step 2** In the **Admin** menu, click **User Management**.

**Step 3** In the **User Management** pane, click the **Local User Management** tab.

Under the **Local User Management** tab, there are several options for further configuration.

# Disabling Strong Password

The Cisco IMC implements a strong password policy wherein you are required to follow guidelines and set a strong password when you log on to the server for the first time. The **Local User** tab displays a **Disable Strong Password** button which allows you to disable the strong password policy and set a password of your choice by ignoring the guidelines. Once you disable the strong password, an **Enable Strong Password** button is displayed. By default, the strong password policy is enabled.

### Before you begin

You must log in as a user with admin privileges to perform this task.

### Procedure

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

**Step 2** In the **Admin** menu, click **User Management**.

**Step 3** In the **User Management** pane, click the **Local User Management** tab.

**Step 4** Click **Disable Strong Password**.

**Step 5** In the dialog box, click **OK** to proceed, or **Cancel** to return to the previous page.

# Password Expiry

You can set a shelf life for a password, after which it expires. As an administrator, you can set this time in days. This configuration is common to all users. When the password expires, the user is notified on login and is not allowed to login unless the password is reset.

### Before you begin

You must log in as a user with admin privileges to perform this task.

### Procedure

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

**Step 2** In the **Admin** menu, click **User Management**.

**Step 3** In the **User Management** pane, click the **Local User Management** tab.

**Step 4** Click **Password Expiration Details**.

**Step 5** In the **Password Expiration Details** dialog box, update the relevant fields. The following fields are available:

| Name | Description |
|---|---|
| **Enable Password Expiry** check box | If checked, allows you to configure the Password Expiry Duration. Uncheck the check box to disable password expiry. |

| Name | Description |
|---|---|
| **Password Expiry Duration** field | The time period that you can set for the existing password to expire (from the time you set a new password or modify an existing one). The range is between 1 to 3650 days. |
| **Password History** field | The number of occurrences when a password was entered. When this is enabled, you cannot repeat a password. Enter a value between 0 to 5. Entering 0 disables this field. |
| **Notification Period** field | Notifies the time by when the password expires. Enter a value between 0 to 15 days. Entering 0 disables this field. |
| **Grace Period** field | Time period till when the existing password can still be used, after it expires. Enter a value between 0 to 5 days. Entering 0 disables this field. |

**Step 6** Complete your action with one of the following:

| Name | Description |
|---|---|
| **Save Changes** button | Saves the updated settings and closes the dialog box. |
| **Reset Values** button | Resets the dialog box fields to previous values. |
| **Restore Default** button | Restores the default values for the dialog box. |
| **Cancel** button | Cancels the process and closes the dialog box. |

# Account Lockout Details

You can set a lockout period for accounts, after which the account is locked out. As an administrator, you can set this time in minutes. You can also set the number of attempts allowed before the account is locked. This configuration is common to all users.

### Before you begin

You must log in as a user with admin privileges to perform this task.

### Procedure

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

**Step 2** In the **Admin** menu, click **User Management**.

**Step 3** In the **User Management** pane, click the **Local User Management** tab.

**Step 4** Click **Account Lockout Details**.

**Step 5** In the **Account Lockout Details** dialog box,update the relevant fields. The following fields are available:

| Name | Description |
|---|---|
| **Allowed Attempts** field | The number of attempts allowed.<br>Enter a value between 0 and 20. |
| **Lockout Period** field | The lockout duration in minutes.<br>Enter a value between 0 and 60. |
| **Disable User on Lockout** check box | If checked, the user is disabled on the Cisco IMC after lockout. |

# Disabling IPMI User Mode

### Before you begin

You must log in as a user with admin privileges to perform this task.

### Procedure

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

**Step 2** In the **Admin** menu, click **User Management**.

**Step 3** In the **User Management** pane, click the **Local User Management** tab.

**Step 4** Click **Disable IPMI User Mode**.

**Step 5** In the dialog box, click **OK**.

# Configuring User Authentication Precedence

### Before you begin

You must log in as a user with admin privileges to perform this task.

### Procedure

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

**Step 2** In the **Admin** menu, click **User Management**.

**Step 3** In the **User Management** pane, click the **Local User Management** tab.

**Step 4** Click **Configure User Authentication Precedence**.

**Step 5** In the **Configure User Authentication Precedence** dialog box, choose the database to be updated.

**Step 6** Use the **Up** and **Down** arrows to move this database priority higher or lower.

**Step 7** Click **Save Changes**.

# Configuring Local Users

## Adding a New User

### Before you begin

You must log in as a user with admin privileges to perform this task.

### Procedure

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

**Step 2** In the **Admin** menu, click **User Management**.

**Step 3** In the **User Management** pane, click the **Local User Management** tab.

**Step 4** Choose an ID to add the new user to, click the ID rowin the **Local User Management** pane, and click **Add User**.

**Step 5** In the **Local User Details** dialog box, update the following properties:

| Name | Description |
|---|---|
| **ID** field | The unique identifier for the user. |
| **Username** field | The username for the user.<br>Enter between 1 and 16 characters. |

| Name | Description |
|---|---|
| **Role Played** field | The role assigned to the user. This can be one of the following:<br>• **read-only**—A user with this role can view information but cannot make any changes.<br>• **user**—A user with this role can perform the following tasks:<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>  • Set time zone<br>  • Ping<br>• **admin**—A user with this role can perform all actions available through the GUI, CLI, and IPMI. |
| **Enabled** check box | If checked, the user is enabled on the CIMC. |

| Name | Description |
|---|---|
| **Password** field | The password for this username. When you move the mouse over the help icon beside the field, the following guidelines to set the password are displayed:<br>• The password must have a minimum of 8 and a maximum of 20 characters.<br>• The password must not contain the user's name.<br>• The password must contain characters from three of the following four categories:<br>  • English uppercase characters (A through Z).<br>  • English lowercase characters (a through z).<br>  • Base10 digits (0 through 9).<br>  • Non-alphabetic characters (!, @, #, $, %, ^, &, *, -, _, , =, ").<br>These rules are meant to define a strong password for the user, for security reasons. However, if you want to set a password of your choice ignoring these guidelines, click the **Disable Strong Password** button on the **Local Users** tab. While setting a password when the strong password option is disabled, you can use between 1- 20 characters. |
| **Suggest** button | Generates a strong random password. |
| **Confirm New Password** field | The password repeated for confirmation purposes. |

**Step 6** Click **Save**.

# Modifying an Existing User

### Before you begin

You must log in as a user with admin privileges to perform this task.

### Procedure

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

**Step 2** In the **Admin** menu, click **User Management**.

**Step 3** In the **User Management** pane, click the **Local User Management** tab.

**Step 4** Choose the ID row of the user to be modified,and click **Modify User**.

**Step 5** In the **Modify User Details** dialog box, update the following properties:

| Name | Description |
|---|---|
| **ID** field | The unique identifier for the user. |
| **Username** field | The username for the user.<br>Enter between 1 and 16 characters. |
| **Role Played** field | The role assigned to the user. This can be one of the following:<br>• **read-only**—A user with this role can view information but cannot make any changes.<br>• **user**—A user with this role can perform the following tasks:<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>• Set time zone<br>• Ping<br>• **admin**—A user with this role can perform all actions available through the GUI, CLI, and IPMI. |
| **Enabled** check box | If checked, the user is enabled on the CIMC. |
| **Change Password** check box | If checked, when you save the changes, the password for this user will be changed. You must check this box if this is a new username. |

| Name | Description |
|---|---|
| **New Password** field | The password for this username. When you move the mouse over the help icon beside the field, the following guidelines to set the password are displayed:<br>• The password must have a minimum of 8 and a maximum of 20 characters.<br>• The password must not contain the user's name.<br>• The password must contain characters from three of the following four categories:<br>  • English uppercase characters (A through Z).<br>  • English lowercase characters (a through z).<br>  • Base10 digits (0 through 9).<br>  • Non-alphabetic characters (!, @, #, $, %, ^, &, *, -, _, , =, ").<br>These rules are meant to define a strong password for the user, for security reasons. However, if you want to set a password of your choice ignoring these guidelines, click the **Disable Strong Password** button on the **Local Users** tab. While setting a password when the strong password option is disabled, you can use between 1- 20 characters. |
| **Confirm New Password** field | The password repeated for confirmation purposes. |

**Step 6** Click **Save**.

# Deleting an Existing User

### Before you begin

You must log in as a user with admin privileges to perform this task.

### Procedure

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

**Step 2** In the **Admin** menu, click **User Management**.

**Step 3** In the **User Management** pane, click the **Local User Management** tab.

**Step 4** To delete a local user account, click a row in the **Local User Management** pane and click **Delete User**.

**Step 5** In the dialog box, click **OK** to delete the user.

**Step 6** Click **Save Changes**.

# Configuring SSH Keys

### Before you begin

You must log in as a user with admin privileges to perform this task.

### Procedure

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

**Step 2** In the **Admin** menu, click **User Management**.

**Step 3** In the **User Management** pane, click the **Local User Management** tab.

**Step 4** Choose a row in the **Local User Management** pane and click **SSH Keys**.

**Step 5** In the **SSH Keys** dialog box, update the following properties:

| Name | Description |
|---|---|
| **+ Add Key** button | Button to add SSH key(s) to a user. Opens the **Add Key** area. |
| **Modify Key** button | Button to modify SSH keys for a user. |
| **X Delete Key** button | Button to delete SSH keys for a user. |
| **ID** | User ID |
| **Comment** | Comments for SSH keys. |
| **Key** | Key details. |
| **Add Key** area | Methods to add SSH keys for a user. |
| **Paste SSH Key** radio button | Provides space to paste the SSH key. |
| **Upload from Local** radio button | Provides a **Browse** button to browse to the file location, select and upload the SHH key. |

| Name | Description |
|---|---|
| **Upload from Remote Location** radio button | Provides options to upload the SHH key from remote locations.<br>• **Upload SSH Key from** drop-down<br>  • TFTP<br>  • FTP<br>  • SFTP<br>  • SCP<br>  • HTTP<br>• **Server IP/Hostname** field<br>• **Path and Filename** field<br>• **Username** field<br>• **Password** field |

**Step 6** Click **Upload SSH Key**.

# LDAP Servers - Overview

Cisco IMC supports directory services that organize information in a directory, and manage access to this information. supports Lightweight Directory Access Protocol (LDAP), which stores and maintains directory information in a network. In addition, supports Microsoft Active Directory (AD). 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 utilizes the Kerberos-based authentication service of LDAP.

When LDAP is enabled in the Cisco IMC, user authentication and role authorization is performed by the LDAP server for user accounts not found in the local user database. The LDAP user authentication format is username@domain.com.

You can require the server to encrypt data sent to the LDAP server.

## Configuring the LDAP Server

The CIMC can be configured to use LDAP for user authentication and authorization. To use LDAP, 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 user roles and locales or you can modify the LDAP 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.

**Important** For more information about altering the schema, see the article at http://technet.microsoft.com/en-us/library/bb727064.aspx.

**Note** This example creates a custom attribute named CiscoAVPair, but you can also use an existing LDAP attribute that is mapped to the user roles and locales.

### Before you begin

You must log in as a user with admin privileges to perform this task.

### Procedure

**Step 1** Ensure that the LDAP schema snap-in is installed.

**Step 2** Using the 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 | `CaseSensitive String` |

**Step 3** Add the CiscoAVPair attribute to the user class using the snap-in:

- Expand the **Classes** node in the left pane and type `U` to choose the user class.
- Click the **Attributes** tab and click **Add**.
- Type `C` to choose the Cisco AVPair attribute.
- Click **OK**.

**Step 4** Add the following user role values to the CiscoAVPair attribute, for the users that you want to have access to:

| 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.

# Configuring LDAP Settings and Group Authorization

### Before you begin

You must log in as a user with admin privileges to perform this task.

### Procedure

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

**Step 2** In the **Admin** menu, click **User Management**.

**Step 3** In the **User Management** pane, click **LDAP**.

**Step 4** In the **LDAP Settings** area, update the following properties:

| Name | Description |
|---|---|
| **Enable LDAP** checkbox | If checked, user authentication and role authorization is performed first by the LDAP server, followed by user accounts that are not found in the local user database. |
| **Base DN** field | Base Distinguished Name. This field describes where to load users and groups from.<br>It must be in the `dc=domain,dc=com`format for Active Directory servers. |
| **Domain** field | The IPv4 domain that all users must be in.<br>This field is required unless you specify at least one Global Catalog server address. |
| **Timeout (0 - 180) seconds** field | The number of seconds the CIMC waits until the LDAP search operation times out.<br>If the search operation times out, CIMC tries to connect to the next server listed on this tab, if one is available.<br>**Note** The value you specify for this field could impact the overall time. |

**Step 5** In the **Configure LDAP Servers** area, update the following properties:

| Name | Description |
|---|---|
| **Pre-Configure LDAP Servers** radio button | If checked, the Active Directory uses the pre-configured LDAP servers. |
| **LDAP Servers** | |

| Name | Description |
|---|---|
| **Server** field | The IP address of the 6 LDAP servers.<br>If you are using Active Directory for LDAP, then servers 1, 2 and 3 are domain controllers, while servers4, 5 and 6 are Global Catalogs. If you are not Active Directory for LDAP, then you can configure a maximum of 6 LDAP servers.<br>**Note** You can provide the IP address of the host name as well. |
| **Port** field | The port numbers for the servers.<br>If you are using Active Directory for LDAP, then for servers 1, 2 and 3, which are domain controllers, the default port number is 389. For servers 4, 5 and 6, which are Global Catalogs, the default port number is 3268.<br>LDAPS communication occurs over the TCP 636 port. LDAPS communication to a global catalog server occurs over TCP 3269 port. |
| **Use DNS to Configure LDAP Servers** radio button | If checked, you can use DNS to configure access to the LDAP servers. |
| **DNS Parameters** | |
| **Source** field | Specifies how to obtain the domain name used for the DNS SRV request. It can be one of the following:<br>• **Extracted**—specifies using domain name extracted-domain from the login ID<br>• **Configured**—specifies using the configured-search domain.<br>• **Configured-Extracted**—specifies using the domain name extracted from the login ID than the configured-search domain. |
| **Domain to Search** field | A configured domain name that acts as a source for a DNS query.<br>This field is disabled if the source is specified as **Extracted**. |
| **Forest to Search** field | A configured forest name that acts as a source for a DNS query.<br>This field is disabled if the source is specified as **Extracted**. |

**Step 6** In the **Binding Parameters** area, update the following properties:

| Name | Description |
|---|---|
| **Method** field | It can be one of the following:<br>• **Anonymous**—requires NULL username and password. If this option is chosen and the LDAP server is configured for Anonymous logins, then the user can gain access.<br>• **Configured Credentials**—requires a known set of credentials to be specified for the initial bind process. If the initial bind process succeeds, then the distinguished name (DN) of the user name is queried and re-used for the re-binding process. If the re-binding process fails, then the user is denied access.<br>• **Login Credentials**—requires the user credentials. If the bind process fails, the user is denied access.<br>By default, the **Login Credentials** option is chosen. |
| **Binding DN** field | The distinguished name (DN) of the user. This field is editable only if you have chosen **Configured Credentials** option as the binding method. |
| **Password** field | The password of the user. This field is editable only if you have chosen **Configured Credentials** option as the binding method. |

**Step 7** In the **Search Parameters** area, update the following properties:

| Name | Description |
|---|---|
| **Filter Attribute** field | This field must match the configured attribute in the schema on the LDAP server.<br>By default, this field displays **sAMAccountName**. |
| **Group Attribute** field | This field must match the configured attribute in the schema on the LDAP server.<br>By default, this field displays **memberOf**. |

| Name | Description |
|---|---|
| **Attribute** 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 can use an existing LDAP attribute that is mapped to the user roles and locales, or can modify the schema such that a new LDAP attribute can be created. For example, **CiscoAvPair**.<br>**Note** If you do not specify this property, the user cannot login. Although the object is located onthe LDAP server, it should be an exact match of the attribute that is specified in this field. |
| **Nested Group Search Depth (1-128)** field | Parameter to search for an LDAP group nested within another defined group in an LDAP group map. The parameterdefines the depth of a nested group search. |

**Step 8** In the **Group Authorization** area, update the following properties:

| Name | Description |
|---|---|
| **LDAP Group Authorization** check box | If checked, user authentication is also done on the group level for LDAP users that are not found in the local user database.<br>If you check this box, CIMC enables the **Configure Group** button. |
| **Group Name** column | The name of the group in the LDAP server database that is authorized to access the server. |
| **Group Domain** column | The LDAP server domain the group must reside in. |

| Name | Description |
|---|---|
| **Role** column | The role assigned to all users in this LDAP server group. This can be one of the following:<br>• **read-only**—A user with this role can view information but cannot make any changes.<br>• **user**—A user with this role can perform the following tasks:<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>  • Set time zone<br>  • Ping<br>• **admin**—A user with this role can perform all actions available through the GUI, CLI, and IPMI. |
| **Configure** button | Configures an active directory group. |
| **Delete** button | Deletes an existing LDAP group. |

**Step 9** Click **Save Changes.**

# LDAP Certificates

UCS E-series M6 servers allow an LDAP client to validate a directory server certificate against an installed CA certificate or chained CA certificate during an LDAP binding step. This feature is introduced in the event where anyone can duplicate a directory server for user authentication and cause a security breach due to the inability to enter a trusted point or chained certificate into the Cisco IMC for remote user authentication.

An LDAP client needs a new configuration option to validate the directory server certificate during the encrypted TLS/SSL communication.

## Viewing LDAP CA Certificate Status

### Procedure

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

**Step 2** In the **Admin** menu, click **User Management**.

**Step 3** In the **User Management** pane, click the **LDAP** tab.

**Step 4** In the **Certificate Status** area, view the following fields:

| Name | Description |
|---|---|
| **Download Status** field | This field displays the status of the LDAP CA certificate download. |
| **Export Status** field | This field displays the status of the LDAP CA certificate export. |

## Exporting an LDAP CA Certificate

### Procedure

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

**Step 2** In the **Admin** menu, click **User Management**.

**Step 3** In the **User Management** pane, click the **LDAP** tab.

**Step 4** Click the **Export LDAP CA Certificate** link.

**Step 5** In the **Export LDAP CA Certificate** dialog box, update the following fields:

| Name | Description |
|---|---|
| **Export to Remote Location** drop down | Choosing this option allows you to choose the certificate from a remote location and export it. Enter the following details:<br>• TFTP Server<br>• FTP Server<br>• SFTP Server<br>• SCP Server<br>• HTTP Server<br>**Note** If you chose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message *Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*. Click **Yes** or **No** depending on the authenticity of the server fingerprint.<br>The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.<br>• **Server IP/Hostname** field— The IP address or hostname of the server on which the LDAP CA certificate file should be exported. Depending on the setting in the **Download Certificate from** drop-down list, the name of the field may vary.<br>• **Path and Filename** field — The path and filename Cisco IMC should use when downloadingthe certificate from the remote server.<br>• **Username** field — The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP.<br>• **Password**field— The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP. |
| **Export to Local Desktop** field | Choosing this option allows you to choose the certificate stored on a drive that is local to the computer and export it. |

**Step 6** Click **Export Certificate**.

## Testing LDAP Binding

**Note** If you checked the **Enable Encryption** and the **Enable Binding CA Certificate** check boxes, enter the fully qualified domain name (FQDN) of the LDAP server in the LDAP Server field. To resolve the FQDN of the LDAP server, configure the preferred DNS of Cisco IMC network with the appropriate DNS IP address.

### Before you begin

You must log in as a user with admin privileges to perform this task.

### Procedure

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

**Step 2** In the **Admin** menu, click **User Management**.

**Step 3** In the **User Management** pane, click the **LDAP** tab.

**Step 4** Click the **Test LDAP Binding** link.

**Step 5** In the **Test LDAP CA Certificate Binding** dialog box, view the following fields:

| Name | Description |
|---|---|
| **Username** field | Enter the username. |
| **Password** field | Enter the corresponding password. |

**Step 6** Click **Test**.

## Viewing User Sessions

### Procedure

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

**Step 2** In the **Admin** menu, click **User Management**.

**Step 3** In the **User Management** pane, click **Session Management**.

**Step 4** In the **Sessions** pane, view the following fields:

| Name | Description |
|---|---|
| Session ID column | The unique identifier for the session. |
| Username column | The username for the user. |
| IP Address column | The IP address from which the user accessed the server. If this is a serial connection, it displays **N/A**. |
| Type column | The type of session the user chose to access the server. This can be one of the following:<br>• **webgui**—indicates the user is connected to the server using the web UI.<br>• **CLI**—indicates the user is connected to the server using CLI.<br>• **serial**— indicates the user is connected to the server using the serial port. |

CHAPTER 8

# Managing Network-Related Settings

## Configuring Network Settings

CIMC provides options to configure network parameters, including NIC properties, Port properties, VLAN properties, and IPv4 and IPv6 properties. You can configure a server NIC when you want to set the NIC mode and NIC redundancy.

### Before you begin

You must log in with admin privileges to perform this task.

### Procedure

**Step 1** In the **Navigation** pane, click the **Admin** menu, and click **Networking**.

**Step 2** In the work pane, click the **Network** tab.

**Step 3** Review and update the following information:

*Table 16: NIC Properties Menu*

| Name | Description |
|---|---|
| **NIC Mode** drop-down | The NIC mode setting determines which ports can reach the Cisco IMC. The following network mode options are available, depending on your platform:<br>• **Dedicated**—The management port that is used to access the CIMC.<br>• **Shared LOM**—The LOM (LAN On Motherboard) ports are used to access the CIMC. |

| Name | Description |
|---|---|
| **NIC Redundancy** drop-down | The available NIC redundancy options depend on the selected NIC mode and the model of the server that you are using. If you do not see a particular option, it is not available for the selected mode or server model.<br>This value is set to **None**. |
| **NIC Interface** field | The network interface that is selected in the **NIC Mode** field. |
| **MAC Address** field | The MAC address of the Cisco IMC network interface that is selected in the **NIC Mode** field. |

*Table 17: Common Properties Menu*

| Name | Description |
|---|---|
| **Management Hostname** field | The user-defined management hostname of the system that manages the various components of Cisco IMC. |
| **Dynamic DNS** check box | If checked, updates the resource records to the DNS from the Cisco IMC. |
| **Dynamic DNS Update Domain** field | The domain name that is appended to a hostname for a Dynamic DNS (DDNS) update. If left blank, only a hostname is sent to the DDNS update request. |
| **Dynamic DNS Refresh Interval** field | The refresh interval for the dynamic DNS, in hours.<br>Value can be set between 0 and 8736 hours. |

*Table 18: IPv4 Properties Menu*

| Name | Description |
|---|---|
| **Enable IPv4** check box | If checked, IPv4 is enabled. |
| **Use DHCP** check box | If checked, the Cisco IMC uses DHCP. |
| **Management IP Address** field | The management IP address. An external virtual IP address that helps manage 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 Cisco IMC retrieves the DNS server addresses from DHCP.<br>**Note** You can use this option only when the **Use DHCP** option is enabled. |

| Name | Description |
|---|---|
| **Preferred DNS Server** field | The IP address of the primary DNS server. |
| **Alternate DNS Server** field | The IP address of the secondary DNS server. |

*Table 19: Port Properties Menu*

| Name | Description |
|---|---|
| **Port Profile** field | The port profile that the Cisco IMC uses to configure the management interface, the virtual Ethernet, and the VIF on supported adapter cards.<br>You can enter up to 80 alphanumeric characters. You cannot use spaces or other special characters except for - (hyphen) and _ (underscore). In addition, the port profile name cannot begin with a hyphen.<br>**Note** The port profile must be defined on the switch to which this server is connected. |
| **Auto Negotiation** check box | Using this option, you can either set the network port speed and duplex values for the switch, or allow the system to automatically derive the values from the switch. This option is available for dedicated mode only.<br>• If checked, the network port speed and duplex settings are ignored by the system and the Cisco IMC retains the speed at which the switch is configured.<br>• If unchecked, you can configure the network port speed and duplex values. |

| Name | Description |
|---|---|
| **Admin Mode** Area | **Network Port Speed** field<br>The network speed of the port. This can be one of the following:<br>• 10 Mbps<br>• 100 Mbps<br>• 1 Gbps<br>The default value is 100 Mbps. In the **Dedicated** mode, if you disable **Auto Negotiation**, you can configure the network speed and duplex values.<br>**Note** Before changing the port speed, ensure that the device you connected to has the same port speed.<br>**Duplex** drop-down list<br>The duplex mode for the Cisco IMC management port.<br>This can be one of the following:<br>• **Half**<br>• **Full**<br>By default, the duplex mode is set to **Full**. |
| **Operation Mode** Area | Displays the operation network port speed and duplex values.<br>If you checked the **Auto Negotiation** check box, the network port speed and duplex details of the switch are displayed. If unchecked, the network port speed and duplex values that you set at the **Admin Mode** are displayed. |

**Note** You can configure a VLAN or a port profile, but you cannot use both. If you want to use a port profile, make sure that the **Enable VLAN** check box in the **VLAN Properties** area is not checked.

*Table 20: VLAN Properties Menu*

| Name | Description |
|---|---|
| **Enable VLAN** check box | If checked, the Cisco IMC is connected to a virtual LAN.<br>**Note** You can configure a VLAN or a port profile, but you cannot use both. If you want to use a port profile, make sure that this check box is not checked. |

| Name | Description |
|---|---|
| **VLAN ID** field | The VLAN ID. |
| **Priority** field | The priority of this system on the VLAN. |

*Table 21: IPv6 Properties Menu*

| Name | Description |
|---|---|
| **Enable IPv6** check box | If checked, IPv6 is enabled. |
| **Use DHCP** check box | If checked, the Cisco IMC uses DHCP. |
| **Management IP Address** field | The management IPv6 address.<br>**Note** Only global unicast addresses are supported. |
| **Prefix Length** field | The prefix length for the IPv6 address. Enter a value within the range 1 to 127. The default value is 64. |
| **Gateway** field | The gateway for the IPv6 address.<br>**Note** Only global unicast addresses are supported. |
| **Obtain DNS Server Addresses from DHCP** check box | If checked, the Cisco IMC retrieves the DNS server addresses from DHCP.<br>**Note** You can use this option only when the **Use DHCP** option is enabled. |
| **Preferred DNS Server** field | The IPv6 address of the primary DNS server. |
| **Alternate DNS Server** field | The IPv6 address of the secondary DNS server. |
| **Link Local Address** field | The link local address for the IPv6 address. |
| **SLAAC Address** field | The Stateless Address Auto Configuration (SLAAC) depends on the Router Advertisement (RA) of the network. |

**Step 4** Click **Save Changes** to save your changes, or **Reset Values** to reset the parameters to previous values.

# Configuring 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 filtering is commonly used to protect against denial of service (DoS) attacks. You can filter IP addresses by enabling the configuration, and setting up the filters.

### Before you begin

You must log in as a user with admin privileges to perform this task.

### Procedure

**Step 1** In the **Navigation** pane, click the **Admin** menu, and click **Networking**.

**Step 2** In the work pane, click the **Network Security** tab.

**Step 3** Review and update the following properties:

*Table 22: IP Blocking Properties Area*

| 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. |
| **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. |

*Table 23: IP Filtering Area*

| Name | Description |
|---|---|
| **Enable IP Filtering** check box | Check this box to enable IP filtering. |

| Name | Description |
|---|---|
| **IP Filter** field | To provide secure access to the server, you can now set a filter to allow only a selected set of IPs to access it. This option provides four slots for storing IP addresses (IP Filter 1, 2, 3, and 4). You can either assign a single IP address or a range of IP addresses while setting the IP filters. Once you set the IP filter, you would be unable to access the server using any other IP address. |
| + button | + button to add multiple IP Filter fields. Up to 20 fields can be added. |

**Step 4** Click **Save Changes** to save your changes, or **Reset Values** to reset the parameters to previous values.

# Configuring Network Time Protocol (NTP) Settings

By default, when CIMC is reset, it synchronizes the time with the host. With the introduction of the NTP service, you can configure to synchronize the time with an NTP server. The NTP server does not run in by default.

You must enable and configure the NTP service by specifying the IP/DNS address of at least one server or a maximum of four servers that function as NTP servers or time source servers. When you enable the NTP service, CIMC synchronizes the time with the configured NTP server. The NTP service can be modified only through CIMC.

**Note** To enable the NTP service, it is preferable to specify the IP address of a server rather than the DNS address.

### Before you begin

You must log in with admin privileges to perform this task.

### Procedure

**Step 1** In the **Navigation** pane, click the **Admin** menu, and click **Networking**.

**Step 2** In the work pane, click the **NTP Settings** tab.

**Step 3** Review and update the following information:

*Table 24: Common Properties Menu*

| Name | Description |
|---|---|
| **NTP Enabled** check box | Check this box to enable the NTP service. |

| Name | Description |
|---|---|
| **Server 1** field | The IP/DNS address of one of the four servers that act as an NTP server or the time source server. |
| **Server 2** field | The IP/DNS address of one of the four servers that act as an NTP server or the time source server. |
| **Server 3** field | The IP/DNS address of one of the four servers that act as an NTP server or the time source server. |
| **Server 4** field | The IP/DNS address of one of the four servers that act as an NTP server or the time source server. |
| **Status** field | Indicates whether or not the server is able to synchronize its time with the remote NTP server. This can be one of the following:<br>• **synchronized to NTP server (RefID) at stratum 7**— When the NTP service is enabled and multiple or individual IPv4 or IPv6 based NTP servers are added.<br>• **unsynchronized** — When the NTP service is enabled and an unknown or unreachable server is added.<br>• **NTP service disabled** — When the NTP service is disabled.<br>**Note** If you move the mouse over the help icon, a pop-up is displayed that explains what Stratum stands for. |

**Step 4** Click **Save Changes** to save your changes, or **Reset Values** to reset the parameters to previous values.

CHAPTER 9

# Managing Communication Services

## Configuring HTTP

### Before you begin

You must log in as a user with admin privileges to perform this task.

### Procedure

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

**Step 2** In the **Admin** menu, click **Communication Services**.

**Step 3** In the **HTTP Properties** area, update the following properties:

| Name | Description |
|---|---|
| **HTTPS Enabled** check box | Check box to indicate whether HTTPS is enabled on the CIMC. |
| **HTTP Enabled** check box | Check box to indicate whether HTTP is enabled on the CIMC. |
| **Redirect HTTP to HTTPS Enabled** check box | If enabled, all attempts to communicate via HTTP are redirected to the equivalent HTTPS address.<br>It is recommended that you enable this option if you enable HTTP. |
| **HTTP Port** field | The port to use for HTTP communication. The default is 80. |

| Name | Description |
|---|---|
| **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 times out and terminates the session.<br>Enter an integer between 60 and 10,800. The default is 1800 seconds. |
| **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 perform this task.

### Procedure

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

**Step 2** In the **Admin** menu, click **Communication Services**.

**Step 3** In the **SSH Properties** area, update the following properties:

| Name | Description |
|---|---|
| **SSH Enabled** check box | Check box to enable or disable SSH. |
| **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 1800 seconds. |

| Name | Description |
|---|---|
| **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**.

# Configuring IPMI over LAN

Intelligent Platform Management Interface (IPMI) defines the protocols for interfacing with a service processor embedded in a server platform. This service processor is called the Cisco Integrated Management Controller (CIMC), and resides on the server motherboard. The CIMC links to the main processor and other on-board elements using a simple serial bus.

During normal operations, IPMI lets a server operating systemobtain 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 CIMC to increase fan speed or reduce processor speed to address the problem.

### Before you begin

You must log in as a user with admin privileges to perform this task.

### Procedure

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

**Step 2** In the **Admin** menu, click **Communication Services**.

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

| Name | Description |
|---|---|
| **Enabled** check box | Check box to enable or disable IPMI access. |

| Name | Description |
|---|---|
| **Privilege Level Limit** drop down | The highest privilege level that can be assigned to an IPMI session on this server. This can be one of the following:<br>• **read-only**—IPMI users can view information but cannot make any changes. If you choose this option, IPMI users with the "Administrator", "Operator", or "User" user roles can only create read-only IPMI sessions, regardless of their other IPMI privileges.<br>• **user**—IPMI users can perform some functions but cannot perform administrative tasks. If you choose this option, IPMI users with the "Administrator" or "Operator" user role can create user and read-only sessions on this server.<br>• **admin**—IPMI users can perform all available actions. If you choose this option, IPMI users with the "Administrator" user role can create admin, user, and read-only sessions on this server. |
| **Encryption Key** field | The IPMI encryption key to use for IPMI communications. |

**Step 4** Click **Save Changes**.

# Configuring XML API

The Cisco XML application programming interface (API) is a programmatic interface for the UCS E-Series M6 Server. The API accepts XML documents through HTTP or HTTPS.

### Before you begin

You must log in as a user with admin privileges to perform this task.

### Procedure

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

**Step 2** In the **Admin** menu, click **Communication Services**.

**Step 3** In the **XML API Properties** area, update the following properties:

| Name | Description |
|---|---|
| **XML API Enabled** check box | Check box to enable or disable API access. |

| Name | Description |
|---|---|
| **Max Sessions** field | The maximum number of concurrent API sessions allowed on the CIMC.<br>This value may not be changed. |
| **Active Sessions** field | The number of API sessions currently running on the CIMC. |

**Step 4** Click **Save Changes**.

# Configuring Redfish

### Before you begin

You must log in as a user with admin privileges to perform this task.

### Procedure

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

**Step 2** In the **Admin** menu, click **Communication Services**.

**Step 3** In the **Redfish Properties** area, update the following properties:

| Name | Description |
|---|---|
| **Redfish Enabled** check box | Check box enable or disable Redfish. |
| **Max Sessions** field | The maximum number of concurrent redfish sessions allowed on CIMC. |
| **Active Sessions** field | The number of Redfish sessions currently running on CIMC. |

**Step 4** Click **Save Changes**.

# SNMP - Overview

The Cisco UCS E-Series M6 Servers support the Simple Network Management Protocol (SNMP) for viewing the server configuration and status, and for sending fault and alert information by SNMP traps.

# Configuring SNMP Properties

### Before you begin

You must log in as a user with admin privileges to perform this task.

### Procedure

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

**Step 2** In the **Admin** menu, click **Communication Services**.

**Step 3** In the **Communication Services** pane, click the **SNMP** tab.

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

| Name | Description |
|---|---|
| **SNMP Enabled** check box | Check box to enable or disable sending SNMP traps to the designated host.<br>**Note** After you check this check box, you need to click **Save Changes** before you can configure SNMP users or traps. |
| **SNMP Port** field | The port on which SNMP agent runs. |
| **Access Community String** field | The default SNMP v1 or v2c community name includes on any SNMP get operations.<br>Enter a string up to 18 characters. |
| **SNMP Community Access** drop down | This can be one of the following:<br>• **Disabled**—This option blocks access to the information in the inventory tables.<br>• **Limited**—This option provides partial access to read the information in the inventory tables.<br>• **Full**—This option provides full access to read the information in the inventory tables.<br>**Note** SNMP Community Access is applicable only for SNMP v1 and v2c users. |
| **Trap Community String** field | The name of the SNMP community group used for sending SNMP trap to other devices.<br>Enter a string up to 18 characters.<br>**Note** This field is visible only for SNMP v1 and v2c users. SNMP v3 users need to use SNMP v3 credentials. |

| Name | Description |
|---|---|
| **System Contact** field | The system contact person responsible for the SNMP implementation.<br>Enter a string up to 64 characters, such as an email address or a name and telephone number. |
| **System Location** field | The location of the host on which the SNMP agent (server) runs.<br>Enter a string up to 64 characters. |
| **SNMP Input Engine ID** field | User-defined unique identification of the static engine. |
| **SNMP Engine ID** field | Unique string to identify the device for administration purpose. This is generated from the SNMP Input Engine ID if it is already defined, else it is derived from the CIMC serial number. |

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

# Managing SNMP Users

### Before you begin

- You must log in as a user with admin privileges to perform this task.
- SNMP must be enabled.

### Procedure

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

**Step 2** In the **Admin** menu, click **Communication Services**.

**Step 3** In the **Communication Services** area, click the **SNMP** tab.

**Step 4** In the **v3 User Settings** area, update the following properties:

| Name | Description |
|---|---|
| **Add  User** button | Click an available row in the table then click this button to add a new SNMP user. |
| **Modify User** button | Select the user you want to change in the table then click this button to modify the selected SNMP user. |
| **Delete User** button | Select the user you want to delete in the table then click this button to delete the selected SNMP user. |
| **ID** column | The system-assigned identifier for the SNMP user. |

| Name | Description |
|---|---|
| **Name** column | The SNMP user name. |
| **Auth Type** column | The user authentication type. |
| **Privacy Type** column | The user privacy type. |

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

# Configuring SNMP Users

### Before you begin

- You must log in as a user with admin privileges to perform this task.
- SNMP must be enabled.

### Procedure

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

**Step 2** In the **Admin** menu, click **Communication Services**.

**Step 3** In the **Communication Services** pane, click the **SNMP** tab.

**Step 4** In the **v3 User Settings** area, perform one of the following actions:

- Choose an existing user from the table and click **Modify User**.
- Choose a row in the **Users** area and click **Add User** to create a new user.

**Step 5** In the **SNMP User Details** dialog box, update the following properties:

| Name | Description |
|---|---|
| **ID** field | The unique identifier for the user. This field cannot be changed. |
| **User Name** field | The SNMP username.<br>Enter between 1 and 31 characters or spaces.<br>**Note** Cisco IMC automatically trims leading or trailing spaces. |

| Name | Description |
|---|---|
| **Security Level** drop-down list | The security level for this user. This can be one of the following:<br>• **no auth, no priv**—The user does not require an authorization or privacy password.<br>• **auth, no priv**—The user requires an authorization password but not a privacy password. If you select this option, Cisco IMC enables the Auth fields described below.<br>• **auth, priv**—The user requires both an authorization password and a privacy password. If you select this option, Cisco IMC enables the Auth and Privacy fields. |
| **Auth Type** drop-down | The authorization type. This can be one of the following:<br>• **MD5**<br>• **SHA** |
| **Change Auth Password** field | The authorization password for this SNMP user.<br>Enter between 8 and 64 characters or spaces.<br>**Note** Cisco IMC automatically trims leading or trailing spaces. |
| **Confirm Auth Password** field | The authorization password again for confirmation purposes. |
| **Privacy Type** drop down | The privacy type. This can be one of the following:<br>• **DES**<br>• **AES** |
| **Privacy Password** field | The privacy password for this SNMP user.<br>Enter between 8 and 64 characters or spaces.<br>**Note** Cisco IMC automatically trims leading or trailing spaces. |
| **Confirm Privacy Password** field | The authorization password again for confirmation purposes. |

**Step 6** Click **Save Changes**.

**Step 7** If you want to delete a user, choose the user and click **Delete User**, and click **OK** in the delete confirmation prompt.

# Configuring v2c Properties

### Before you begin

You must log in as a user with admin privileges to perform this task.

### Procedure

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

**Step 2** In the **Admin** menu, click **Communication Services**.

**Step 3** In the **Communication Services** pane, click the **SNMP** tab.

**Step 4** In the **v2c Properties** area, update the following properties:

| Name | Description |
|---|---|
| **SNMP v2c Enabled** check box | Check box to enable or disable sending SNMP v2c traps to the designated host.<br>**Note** After you check this check box, you need to click **Save Changes** before you can configure SNMP users or traps. |
| **Access Community String** field | The default SNMP v1 or v2c community name Cisco IMC includes on any SNMP get operations.<br>Enter a string up to 18 characters. |
| **SNMP Community Access** drop down | This can be one of the following:<br>• **Disabled** — This option blocks access to the information in the inventory tables.<br>• **Limited** — This option provides partial access to read the information in the inventory tables.<br>• **Full** — This option provides full access to read the information in the inventory tables.<br>**Note** SNMP Community Access is applicable only for SNMP v1 and v2c users. |
| **Trap Community String** field | The name of the SNMP community group used for sending SNMP trap to other devices.<br>Enter a string up to 18 characters.<br>**Note** This field is visible only for SNMP v1 and v2c users. SNMP v3 users need to use SNMP v3 credentials. |

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

# Configuring v3c Properties

### Before you begin

You must log in as a user with admin privileges to perform this task.

### Procedure

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

**Step 2** In the **Admin** menu, click **Communication Services**.

**Step 3** In the **Communication Services** pane, click the **SNMP** tab.

**Step 4** In the **v3c Properties** area, update the following properties:

| Name | Description |
|---|---|
| **SNMP v3 Enabled** check box | Check box to enable or disable sending SNMP v3c traps to the designated host.<br>**Note** After you check this check box, you need to click **Save Changes** before you can configure SNMP users or traps. |
| **SNMP Engine ID** field | Unique string to identify the device for administration purpose. This is generated from the SNMP Input Engine ID if it is already defined, else it is derived from the BMC serial number. |
| **SNMP Input Engine ID** field | User-defined unique identification of the static engine. |

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

## Configuring SNMP Trap Settings

### Before you begin

You must log in as a user with admin privileges to perform this task.

### Procedure

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

**Step 2** In the **Admin** menu, click **Communication Services**.

**Step 3** In the **Communication Services** pane, click the **SNMP** tab.

**Step 4** In the **Trap Destinations** area, you can perform one of the following:

- Choose an existing user from the table and click **Modify Trap**.
- Click **Add Trap** to create a new trap.

**Step 5** In the **Trap Details** dialog box, 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. |
| **Version** column | The SNMP version and model used for the trap. This can be one of the following:<br>• **V2**<br>• **V3** |
| **Type** column | The type of trap to send. This can be one of the following:<br>• **Trap**: If this option is chosen, the trap will be sent to the destination but you do not receive any notifications.<br>• **Inform**: You can choose this option only for V2 users. If chosen, an acknowledgment is sent to the SNMP engine. |
| **User** column | Displays the user for each trap. |
| **Community String** column | Displays the community string for each trap. |
| **Destination Address** column | The IP address to which SNMP trap information is sent. |
| **Port** column | The port that the server uses to communicate with the trap destination.<br>The port number can be 1 to 65535. |

**Step 6** Click **Save Changes**.

**Step 7** If you want to delete a trap destination, choose the row and click **Delete Trap**, and then click **OK** in the delete confirmation prompt.

**Step 8** Click **Save Changes**.

# Sending an SNMP Test Trap Message

### Before you begin

You must log in as a user with admin privileges to perform this task.

### Procedure

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

**Step 2** In the **Admin** menu, click **Communication Services**.

**Step 3** In the **Communication Services** pane, click the **SNMP** tab.

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

**Step 5** Click **Send SNMP Test Trap**.

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

An SNMP test trap message is sent to the trap destination.

CHAPTER 10

# Event Management

## 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 and Disabling Platform Event Filters

### Before you begin

You must log in as a user with admin privileges to perform this task.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | In the **Navigation** pane, click the **Admin** menu. | |
| **Step 2** | In the **Admin** menu, click **Event Management**. | |
| **Step 3** | In the **Event Management** area, click **Disable Platform Event Filters**. | Platform event filters are disabled. The button changes to **Enable Platform Event Filters**. |
| **Step 4** | Click **Enable Platform Event Filters**. | Platform event filters are enabled. The button changes to **Disable Platform Event Filters**.<br>**Note** There are no prompts for this process. |

# Resetting Platform Event Filters

### Before you begin

You must log in as a user with admin privileges to perform this task.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | In the **Navigation** pane, click the **Admin** menu. | |
| **Step 2** | In the **Admin** menu, click **Event Management**. | |
| **Step 3** | In the **Event Management** area, click **Reset Event Filters**. | Platform event filters are reset.<br>**Note** There are no prompts for this process. |

# Setting the Platform Event Filter Actions

### Before you begin

You must log in as a user with admin privileges to perform this task.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | In the **Navigation** pane, click the **Admin** menu. | |
| **Step 2** | In the **Admin** menu, click **Event Management**. | |
| **Step 3** | In the **Platform Event Filters** area, choose an event. | The **Select Action** drop-down is enabled. |
| **Step 4** | From the **Select Action** drop-down list, select the action to be performed for the chosen event filter. | The action for the chosen event filter is updated.<br>**Note** There are no prompts for this process. |

CHAPTER 11

# Managing Firmware

## Firmware Overview

You can manage the following firmware components from the Cisco IMC:

- Adapter firmware —The main operating firmware, consisting of an active and a backup image, can be installed from different interfaces such as:
  - Host Upgrade Utility (HUU)
  - Web UI — Local and remote protocols
  - XML API — Remote protocols

  You can upload a firmware image from either a local file system or a TFTP, FTP, SCP, SFTP, or HTTP server.

- Bootloader firmware—The bootloader firmware cannot be installed from the Cisco IMC. You can install this firmware using the Host Upgrade Utility.

Firmware for the following individual components can be updated:

- CIMC
- BIOS
- Logic FPGA
- SB FPGA
- MCU
- AIKIDO

Note: It is recommended to enable **maintenance-mode** on the Catalyst 8300 Series Edge platform for the UCS E-Series M6 Server.

1. First, update both CIMC and BIOS firmware.
2. Activate the updated CIMC and BIOS firmware.
3. The remaining components are updated sequentially.

# Viewing Firmware Components

### Procedure

**Step 1** In the Admin menu, click Firmware Management.

**Step 2** In the Firmware Management area, review the following information:

| Name | Description |
|---|---|
| **Update** button | Opens a dialog box that allows you to install a firmware image file that is available to your local machine or on a remote server. |
| **Activate** button | Opens a dialog box that allows you to choose which available firmware version you would like to activate on the server.<br>**Important** If any firmware or BIOS updates are in progress, do not activate new firmware until those tasks complete. |
| **Component** column | List of components available for which you can update the firmware. |
| **Running Version** column | The firmware version of the component that is currently active. |
| **Backup Version** column | The alternate firmware version installed on the server, if any. The backup version is not currently running. To activate it, click **Activate**.<br>**Note** When you install new firmware, any existing backup version is deleted and the new firmware becomes the backup version. You must manually activate the new firmware if you want the server to run the new version. |

| Name | Description |
|---|---|
| **Bootloader Version** column | The bootloader version associated with the bootloader software of the component. |
| **Status** column | The status of the firmware activation on this server. |
| **Progression %** column | The progress of the operation, in percentage. |

# Updating the Firmware

You can install the firmware package from a local disk or from a remote server, depending on the component you choose from the **Firmware Management** area. After you confirm the installation, CIMC replaces the firmware version in the component's backup memory slot with the selected version.

### Procedure

**Step 1** In the **Admin** menu, click **Firmware Management.**

**Step 2** In the **Firmware Management** area, choose a component from the **Component** column and click **Update**.

**Step 3** In the **Update Firmware** dialog box, review the following information:

| Name | Description |
|---|---|
| **Install Firmware through Browser Client** radio button | If the firmware package resides on a local machine, click this radio button. |
| **Install Firmware through Remote Server** radio button | If the firmware package resides on a remote server, click this radio button. |

**Step 4** To install the firmware through the browser client, click **Browse** and navigate to the firmware file that you want to install.

**Step 5** After you choose the file, click **Install Firmware**.

**Step 6** To update the firmware using remote server, choose the remote server type from the **Install Firmware from** drop-down list. This could be one of the following:

- **TFTP**
- **FTP**
- **SFTP**
- **SCP**
- **HTTP**

**Step 7** Depending on the remote server type you choose, enter details in the server's **IP/Hostname** and **Image Path and Filename** fields.

**Note** For FTP, SFTP, and SCP server types, you need to provide user credentials.

Once you install the firmware, the new image replaces the non-active image. You can activate the image after it is installed.

**Step 8** Click **Install Firmware** to begin download and installation.

# Activating the Firmware

### Procedure

**Step 1** In the **Admin** menu, click **Firmware Management.**

**Step 2** In the **Firmware Management** area, choose a component from the **Component** column and click **Activate**.

**Step 3** In the **Activate Firmware** dialog box, choose the desired firmware image (radio button) to activate. This image becomes the running version.

**Step 4** Click **Activate Firmware**.

**Step 5** Depending on the firmware image you chose, the activation process begins.

**Note** While the activation is in progress, do not:

- Reset, power off, or shut down the server.
- Reboot or reset CIMC.
- Activate any other firmware.
- Export technical support or configuration data.

CHAPTER 12

# Managing Server Utilities

## Exporting Technical Support Data to a Remote Server

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** menu.

**Step 2** In the **Admin** menu, click **Utilities**.

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

**Step 4** Review the following information in the dialog box:

| Name | Description |
|---|---|
| **Export Technical Support Data to** drop down | The remote server type. This can be one of the following:<br>• **TFTP Server**<br>• **FTP Server**<br>• **SFTP Server**<br>• **SCP Server**<br>• **HTTP Server**<br>**Note** If you choose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message *Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*. Click Yes or No depending on the authenticity of the server fingerprint. |
| **Server IP/Hostname** field | The IP address or hostname of the server on which the support data file should be stored. Depending on the setting in the **Export Technical Support Data to** drop-down list, the name of the field may vary. |
| **Path and Filename** field | The path and filename Cisco IMC should use when exporting the file to the remote server.<br>**Note** If the server includes any of the supported network adapter cards, the data file also includes technical support data from the adapter card. |
| **Username** field | The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP. |
| **Password** field | The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP. |

**Step 5** Click **Export**.

### What to do next

Provide the generated report file to Cisco TAC.

# Downloading Technical Support Data to a Local File

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** menu.

**Step 2** In the **Admin** menu, click **Utilities**.

**Step 3** In the **Actions** area of the **Utilities** pane, click **Generate Technical Support Data for Local Download**.

**Step 4** Review the following information in the dialog box:

| Name | Description |
|---|---|
| **Generate Technical Support Data** radio button | CIMC disables this radio button when there is no technical support data file to download.<br>Click **Generate** to create the data file. When data collection is complete, click **DownloadTechnical Support Data to Local File** in the **Actions** area to download the file. |
| **Download to local file** radio button | CIMC enablesthis radio button when a technical support data file is available to download.<br>To download the existing file, choose this option and click **Download**.<br>**Note** If the server includes any of the supported network adapter cards,the data file also includes technical support data from the adapter card. |
| **Generate and Download** button | Allows you to generate and download the technical support data file. |
| **Generate** button | Allows you to generate the technical support data file. |
| **Download** button | Allows you to download the technical support data file after it is generated. |

**Step 5** Click **Generate** to create the data file. When data collection is complete, click **Download Technical Support Data to Local File** in the **Actions** area to download the file.

**Note** Once the technical support file is locally downloaded, it will be deleted from the Cisco IMC.

### What to do next

Provide the generated report file to Cisco TAC.

# Exporting and Importing the CIMC Configuration

To perform a backup of the configuration, you take a snapshot of the system configuration and export the resulting configuration file to a location on your network. The export operation saves information from the management plane only; it does not back up data on the servers. Sensitive configuration information such as user accounts and the server certificate are not exported.

You can restore an exported configuration file to the same system or you can import it to another 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 configuration file is an XML text file whose structure and elements correspond to the command modes. When performing an export or import operation, consider these guidelines:

- You can perform an export or an import while the system is up and running. While an export operation has no impact on the server or network traffic, some modifications caused by an import operation, such as IP address changes, can disrupt traffic or cause a server reboot.
- You cannot execute an export and an import simultaneously.

You can perform an import or an export operation on the following features:

- Version

**Note** You can only export this information.

- Network settings
- Technical support
- Logging control for local and remote logs
- Power policies
- BIOS Parameters

**Note** Precision boot is not supported.

- Communication services
- Remote presence
- User management - LDAP
- SNMP

# Exporting the CIMC Configuration

**Note** For security reasons, this operation does not export user accounts or the server certificate.

### Before you begin

Obtain the backup remote server IP address.

### Procedure

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

**Step 2** In the **Admin** menu, click **Utilities**.

**Step 3** In the **Actions** area of the **Utilities** pane, click **Export Configuration**.

**Step 4** Review the following information in the dialog box:

| Name | Description |
|---|---|
| **Select Component for Export** drop down | Allows you to select the component for export. |
| **Export To** drop down | The location where you want to save the XML configuration file. This can be one of the following:<br>• **Local**: Choose this option and click **Export** to save the XML configuration file to a drive that is local to the computer running the Cisco IMC.<br>When you choose this option, CIMC displays a **File Download** dialog box that lets you navigate to the location to which the configuration file should be saved.<br>• **Remote Server**: Choose this option to import the XML configuration file from a remote server.<br>When you choose this option, CIMC displays the remote server fields. |

| Name | Description |
|---|---|
| **Export To** drop down | **Note** These options are available only when you choose **Remote Server**.<br>The remote server type. This can be one of the following:<br>• **TFTP Server**<br>• **FTP Server**<br>• **SFTP Server**<br>• **SCP Server**<br>• **HTTP Server**<br>**Note** If you chose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message *Server (RSA) key fingerprint is <server_finger_print_ID> Do you wish to continue?*. Click Yes or No depending on the authenticity of the server fingerprint.<br>The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to. |
| **Path and Filename** field | The path and filename should use when exporting the file to the remote server. |
| **Username** field | The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP. |
| **Password** field | The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP. |
| **Passphrase** field | The passphrase that uses the AES256 algorithm to encrypt the LDAP andSNMP v3 user passwords in the exported configuration files. Enter a string of 6 to 127 characters. Do not enter the following characters: ! # $ & < > ? ; ' \| ` ~ \ % ^ ( )" |

**Step 5** Click **Export**.

# Importing the CIMC Configuration

### Before you begin

If you want to restore the SNMP configuration information when you import the configuration file, make sure that SNMP is disabled on this server before you do the import. If SNMP is enabled when you perform the import, does not overwrite the current values with those saved in the configuration file.

### Procedure

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

**Step 2** In the **Admin** menu, click **Utilities**.

**Step 3** In the **Actions** area of the **Utilities** pane, click **import Configuration**.

**Step 4** Review the following information in the dialog box:

| Name | Description |
|---|---|
| **Import From** drop down | The location of the XML configuration file. This can be one of the following:<br>• **Local**: Choose this option to import the XML configuration file to a drive that is local to the computer running the Cisco IMC.<br>When you choose this option, CIMC displays a **Browse** button that lets you navigate to the file you want to import.<br>• **Remote Server**: Choose this option to import the XML configuration file from a remote server.<br>When you choose this option, CIMC displays the remote server fields. |

| Name | Description |
|---|---|
| **Import From** drop down | **Note** These options are available only when you choose **Remote Server**.<br>The remote server type. This can be one of the following:<br>• **TFTP Server**<br>• **FTP Server**<br>• **SFTP Server**<br>• **SCP Server**<br>• **HTTP Server**<br>**Note** If you chose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message *Server (RSA) key fingerprint is <server_finger_print_ID> Do you wish to continue?*. Click Yes or No depending on the authenticity of the server fingerprint.<br>The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to. |
| **Path and Filename** field | The path and filename of the configuration file on the remote server. |
| **Username** field | The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP. |
| **Password** field | The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP. |
| **Passphrase** field | The passphrase that uses the AES256 algorithm to encrypt the LDAP andSNMP v3 user passwords in the exported configuration files. Enter a string of 6 to 127 characters. Do not enter the following characters: ! # $ & < > ? ; ' \| ` ~ \ % ^ ( )"<br>**Note** If you edit the encrypted sections in the configuration file and try to import it, the edits will be ignored and the import operation displays a partially successful message. |

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

# Resetting to Factory Default

On rare occasions, such as an issue with the current running firmware or troubleshooting a server, you might require resetting the server components 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 server components, you are logged off and must log in again. You might also lose connectivity and might need to reconfigure the network settings. Some of the inventory information might not be available during this transition.

When you reset the CIMC to factory settings, the serial number is displayed in the Cisco IMCXXXXXX format, where XXXXXX is the serial number of the server.

### Before you begin

You must log in as a user with admin privileges to perform this task.

### Procedure

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

**Step 2** In the **Admin** menu, click **Utilities**.

**Step 3** In the **Actions** area of the **Utilities** pane, click **Reset to Factory Default**.

**Step 4** Review the following information in the dialog box:

| Name | Description |
|---|---|
| **All** check box | Selects all available components for reset. |
| **BMC** check box | Selects BMC (CIMC) for reset. |

**Step 5** Click **Reset** to reset the selected components to the factory-default settings.

# Generating Non Maskable Interrupts to the Host

In some situations, the server might hang and not respond to traditional debug mechanisms. By generating a non maskable interrupt (NMI) to the host, you can create and send a crash dump file of the server and use it to debug the server.

Depending on the type of operating system associated with the server, this task might restart the host OS.

### Before you begin

- You must log in as a user with admin privileges.

- The server must be powered on.

### Procedure

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

**Step 2** In the **Admin** menu, click **Utilities**.

**Step 3** In the **Actions** area of the **Utilities** pane, click **Generate NMI to Host**.

**Step 4** In the dialog box, click **OK** to proceed, or click **Cancel** to cancel.

This action sends an NMI signal to the host, which might restart the OS.

# Adding or Updating the Cisco IMC Banner

You can add or update the Cisco IMC banner by entering important information such as copyright or customized messages.

### Procedure

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

**Step 2** In the **Admin** menu, click **Utilities**.

**Step 3** In the **Actions** area of the **Utilities** pane, click **Add/Update Cisco IMC Banner**.

**Step 4** Review the following information in the dialog box:

| Name | Description |
|---|---|
| **Banner (80 Chars per line. Max 2K Chars.)** field | Enter copyright information or messages that you want to display on the login screen, before logging on to the Web UI or the command line interface. |
| **Restart SSH** check box | When checked, the active SSH sessions are terminated after you click the **Save Banner** button. |

**Step 5** Click **Save Banner** to save your updates, **Clear banner** to clear the text, or **Cancel** to close the dialog box and return to the previous page.

# Viewing Cisco IMC Last Reset Reason

You can set a lockout period for accounts, after which the account is locked out. As an administrator, you can set this time in minutes. You can also set the number of attempts allowed before the account is locked. This configuration is common to all users.

### Before you begin

You must log in as a user with admin privileges to perform this task.

### Procedure

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

**Step 2** In the **Admin** menu, click **Utilities**.

**Step 3** In the **Actions** area of the **Utilities** pane, view the following information under the **Last Reset Reason** area:

| Name | Description |
|---|---|
| **Component** field | The component that was last reset. |
| **Status** field | The reason why the component was last reset. This can be one of the following:<br>• **watchdog-reset**—The watchdog-timer resets when the Cisco IMC memory reaches full capacity.<br>• **ac-cycle**—PSU power cables are removed (no power input).<br>• **graceful-reboot**—Cisco IMC reboot occurs. |

# Downloading Hardware Inventory to a Local File

### Procedure

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

**Step 2** In the **Admin** menu, click **Utilities**.

**Step 3** In the **Actions** area of the **Utilities** pane, click **Download Hardware Inventory Data to Local Download**.

**Step 4** Review the following information in the dialog box:

| Name | Description |
|---|---|
| **Generate Inventory Data** radio button | Cisco IMC displaysthis radio button when there is no hardware inventory data file to download. Click this button to generate data. |
| **Download inventory data to local file** radio button | Cisco IMC enablesthis radio button when a inventory data file is available to download.<br>To download the existing file, choose this option and click **Download**. |

**Step 5** Click **Generate** to create the data file. When data collection is complete, choose the **Download inventory data to local file** radio button and click **Download** to download the file locally.

# Exporting Hardware Inventory Data to a Remote Server

### Procedure

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

**Step 2** In the **Admin** menu, click **Utilities**.

**Step 3** In the **Actions** area of the **Utilities** pane, click **Export Hardware Inventory Data to Remote**.

**Step 4** Review the following information in the dialog box:

| Name | Description |
|---|---|
| **Export Technical Support Data to** drop down | The remote server type. This can be one of the following:<br>• **TFTP Server**<br>• **FTP Server**<br>• **SFTP Server**<br>• **SCP Server**<br>• **HTTP Server**<br>**Note** If you choose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message *Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*. Click Yes or No depending on the authenticity of the server fingerprint.<br>The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to. |
| **Server IP/Hostname** field | The IP address or hostname of the server on which the data file should be stored. Depending on the setting in the **Export Technical Support Data to** drop-down list, the name of the field may vary. |
| **Path and Filename** field | The path and filename Cisco IMC should use when exporting the file to the remote server. |

| Name | Description |
|---|---|
| **Username** field | The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP. |
| **Password** field | The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP. |

**Step 5** Click **Export.**

# Enabling Smart Access USB

You can enable smart access USB from Cisco IMC.

### Procedure

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

**Step 2** In the **Admin** menu, click **Utilities**.

**Step 3** In the **Actions** area of the **Utilities** pane, click **Enable Smart Access USB**.

**Step 4** In the dialog box, click **OK**.

This process disables the front-panel USBs on the host operating system.

# Viewing Utilities Data

### Procedure

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

**Step 2** In the **Admin** menu, click **Utilities**.

**Step 3** Review the following fields:

*Table 25: Last Technical Support Data Export Area*

| Name | Description |
|---|---|
| **Status** field | The status of the last technical support data export or file generation operation, if any. |
| **Last Generated Time** field | The time of last generation of technical support data. |
| **Cancel** button | Cancels the process. |

*Table 26: Cisco IMC Last Reset Area*

| Name | Description |
|---|---|
| **Status** field | The reason why the component was last reset. This can be one of the following:<br>- **watchdog-reset**—The watchdog-timer resets when the Cisco IMC memory reaches full capacity.<br>- **ac-cycle**— PSU power cables are removed (no power input).<br>- **graceful-reboot**— Cisco IMC reboot occurs. |

*Table 27: Cisco IMC Configuration Import/Export Area*

| Name | Description |
|---|---|
| **Action** field | If the configuration for this server has been previously exported or imported, this field displays whether the most recent operation was an import or an export. |
| **Status** field | The status of the last import or export operation performed on this server, if any. |
| **Diagnostic Message** field | If the import or export operation fails, this field displays the reason for failure. |

*Table 28: Front Panel USB Area*

| Name | Description |
|---|---|
| **Smart Access USB** field | The status of the smart access USB, if any. |
| **Storage Device Attached** field | The status of storage device attached, if any. |

*Table 29: PID Catalog Area*

| Name | Description |
|---|---|
| **Upload Status** field | The status of the PID catalog upload. |
| **Activation Status** field | The activation status of the PID catalog. |
| **Current Activated Version** field | The current activated version of the PID catalog. |

*Table 30: Inventory Data Area*

| Name | Description |
|---|---|
| **Status** field | The status of the last hardware inventory data export or file generation operation, if any. |

*Table 31: Factory Default Status Area*

| Name | Description |
|---|---|
| **CIMC** field | CIMC factory default status. |
| **Storage** field | Storage factory default status. |
| **VIC** field | VIC factory default status. |