Cisco UCS E-Series Integrated Management Controller GUI Configuration Guide, Release 3.2.x

First Published: 2020-05-20

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

This preface includes the following sections:

Audience

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

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

Conventions

Text Type	Indication
GUI elements	GUI elements such as tab titles, area names, and field labels appear in **this font**. Main titles such as window, dialog box, and wizard titles appear in **this font**.
Document titles	Document titles appear in *this font*.
TUI elements	In a Text-based User Interface, text the system displays appears in `this font`.
System output	Terminal sessions and information that the system displays appear in `this font`.
CLI commands	CLI command keywords appear in **this font**. Variables in a CLI command appear in *this font*.

Text Type	Indication
[ ]	Elements in square brackets are optional.
{x | y | z}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the document.

Tip Means *the following information will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

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

Warning IMPORTANT SAFETY INSTRUCTIONS

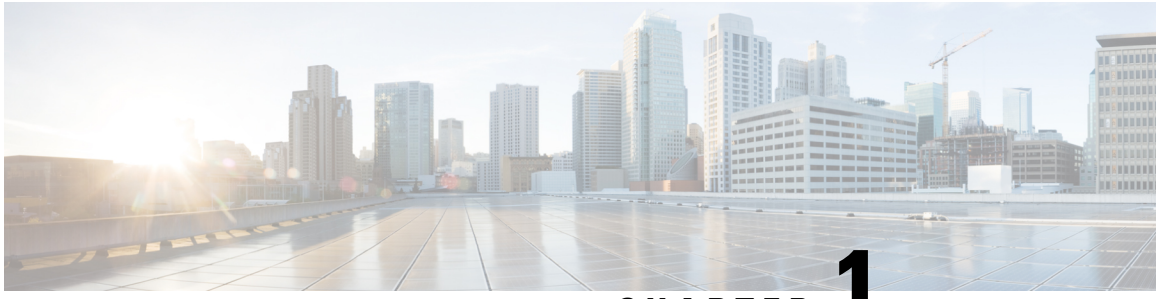
This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

Related Cisco UCS Documentation

Documentation Roadmaps

For a complete list of all E-Series documentation, see the Cisco UCS E-Series Servers Documentation Roadmap available at the following URL:
http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/e/1-0/roadmap/e_series_road_map.html



CHAPTER 1

Overview

This chapter includes the following sections:

Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine Overview

The Cisco UCS E-Series Servers (E-Series Servers) and Cisco UCS E-Series Network Compute Engine (NCE) are a family of size-, weight-, and power-efficient blade servers that are housed within the Generation 2 Cisco Integrated Services Routers (Cisco ISR G2) and the Cisco ISR 4000 series. These servers provide a general purpose compute platform for branch-office applications deployed either as bare-metal on operating systems, such as Microsoft Windows or Linux, or as virtual machines on hypervisors, such as VMware vSphere Hypervisor, Microsoft Hyper-V, or Citrix XenServer.

The E-Series Servers are purpose-built with powerful Intel Xeon processors for general purpose compute. They come in two form factors: single-wide and double-wide. The single-wide E-Series Server fits into one service module (SM) slot, and the double-wide E-Series Server fits into two SM slots.

The NCEs are price-to-power optimized modules that are built to host Cisco network applications and other lightweight general-purpose applications. They come in three form factors: SM, NIM, and EHWIC. The SM E-Series NCE fits into one SM slot, the NIM E-Series NCE fits into one NIM slot, and the EHWIC E-Series NCE fits into two EHWIC slots.

Note

- The EHWIC E-Series NCE can be installed in the the Cisco ISR G2 only.
- The NIM E-Series NCE can be installed in the Cisco ISR 4000 series only.
- The Cisco ISR 4331 has one SM slot. The Cisco ISR 4321 and the Cisco ISR 4431 have no SM slots.
- Citrix XenServer is supported on the E-Series Servers only.
- CIMC 3.2.x is not supported on EHWIC NCEs.

Note For information about the supported E-Series Servers and NCE, 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 Servers and the Cisco UCS E-Series Network Compute Engine*.

Server Software

E-Series Servers and NCE require three major software systems:

- CIMC firmware
- BIOS firmware
- Operating system or hypervisor

CIMC Firmware

Cisco Integrated Management Controller (CIMC) is a separate management module built into the motherboard of the E-Series Server or NCE. A dedicated ARM-based processor, separate from the main server CPU, runs the CIMC firmware. The system ships with a running version of the CIMC firmware. You can update the CIMC firmware, but no initial installation is needed.

CIMC is the management service for the E-Series Servers and NCE. You can use a web-based GUI or SSH-based CLI to access, configure, administer, and monitor the server.

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 manageability features 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 needed.

Operating System or Hypervisor

The main server CPU runs on an operating system, such as Microsoft Windows or Linux; or on a hypervisor. You can purchase an E-Series Server or NCE with a preinstalled Microsoft Windows Server or VMware vSphere Hypervisor, or you can install your own platform.

Note For information about the platforms that have been tested on the E-Series Servers or NCE, see the "Software Requirements" section in the *Release Notes for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine*.

Cisco Integrated Management Controller

The Cisco IMC is the management service for the E-Series servers. Cisco IMC runs within the server.

Note The management service is used only when the server is operating in Standalone Mode. If your E-Series server is integrated into a UCS system, you must manage it using UCS Manager. For information about using UCS Manager, see the configuration guides listed in the *Cisco UCS E-Series Servers Documentation Roadmap* at http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/e/1-0/roadmap/e_series_road_map.html.

Management Interfaces

You can use a web-based GUI or SSH-based CLI or an XML-based API to access, configure, administer, and monitor the server. Almost all tasks can be performed in either interface, and the results of tasks performed in one interface are displayed in another. However, you cannot do the following:

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

Tasks You Can Perform in

You can use to perform the following chassis management tasks:

- Power on, power off, power cycle, reset and shut down the server
- Toggle the locator LED
- Configure the server boot order
- View server properties and sensors
- Manage remote presence
- Create and manage local user accounts, and enable remote user authentication through Active Directory
- Configure network-related settings, including NIC properties, IPv4, VLANs, and network security
- Configure communication services, including HTTP, SSH, IPMI Over LAN, and SNMP.
- Manage certificates
- Configure platform event filters
- Update firmware
- Monitor faults, alarms, and server status
- Set time zone and view local time
- Install and activate firmware
- Install and activate BIOS firmware

- Install and activate CMC firmware

You can use to perform the following server management tasks:

- Manage remote presence
- Create and manage local user accounts, and enable remote user authentication through Active Directory
- Configure network-related settings, including NIC properties, IPv4, VLANs, and network security
- Configure communication services, including HTTP, SSH, IPMI Over LAN, and SNMP.
- Manage certificates
- Configure platform event filters
- Update firmware
- Monitor faults, alarms, and server status
- Set time zone and view local time

No Operating System or Application Provisioning or Management

provisions servers, and as a result, exists below the operating system on a server. Therefore, you cannot use it to provision or manage operating systems or applications on servers. For example, you cannot do the following:

- Deploy an OS, such as Windows or Linux
- Deploy patches for software, such as an OS or an application
- Install base software components, such as anti-virus software, monitoring agents, or backup clients
- Install software applications, such as databases, application server software, or web servers
- Perform operator actions, including restarting an Oracle database, restarting printer queues, or handling non- user accounts
- Configure or manage external storage on the SAN or NAS storage

Overview of the Cisco IMC User Interface

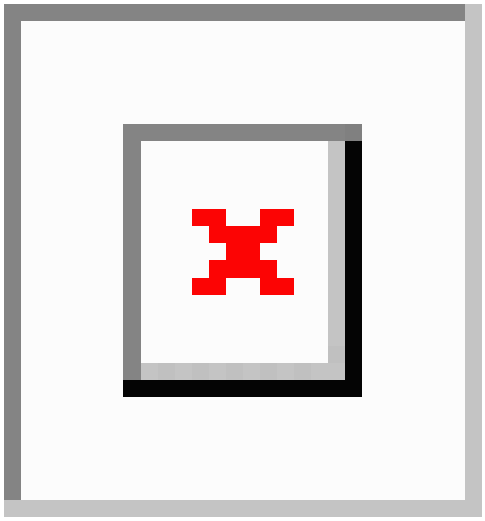
The Cisco IMC user interface is a web-based management interface for Cisco E-Series servers. The web user interface is developed using HTML5 with the eXtensible Widget Framework (XWT) framework. You can launch the user interface and manage the server from any remote host that meets the following minimum requirements:

- Microsoft Internet Explorer 6.0 or higher, Mozilla Firefox 3.0 or higher
- Microsoft Windows 7, Microsoft Windows XP, Microsoft Windows Vista, Apple Mac OS X v10.6, Red Hat Enterprise Linux 5.0 or higher operating systems
- Transport Layer Security (TLS) version 1.2

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 and the Cisco UCS E-Series Network Compute Engine. This guide is available at http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/e/1-0/roadmap/e_series_road_map.html.

Cisco IMC Home Page

When you first log into , the user interface looks similar to the following illustration:



Navigation and Work Panes

The Cisco Integrated Management Controller 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 **Server**, **Chassis**, **Compute**, **Storage** 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 select 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.

Note User interface options may vary depending on the server.

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

- **Chassis** Menu
- **Compute** Menu
- **Storage** 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...
Inventory	Servers, power supplies, Cisco VIC adapters, and Dynamic Storage management information.
Sensors	Power supply, fan, temperature, voltage, current, and LED readings.
Faults and Logs	Fault summary, fault history, system event log, Cisco IMC logs, and logging controls.

Compute Menu

The **Compute** menu contains information about the server, and the following information is displayed in the **Work** pane.

Compute Menu Node Name	Work Pane Tabs Provide Information About...
Inventory	Installed CPUs, memory cards, PCI adapters, Cisco VIC adapters, vNICs, storage information and trusted platform module (TPM).
BIOS	The installed BIOS firmware version and the server boot order.
Remote Management	KVM, virtual media, and Serial over LAN settings.
Troubleshooting	Bootstrap processing, Crash recording, and a player to view the last saved bootstrap process.
Power Policies	Power restore policy settings.
Host Image Mapping	Host image mapping information.

Storage Menu

Each node in the **Storage** menu corresponds to the LSI MegaRAID controllers that are installed in the Cisco UCS E-Series Rack-Mount Servers. Each node leads to one or more tabs that display in the **Work** pane and provide information about the installed controllers.

Storage Menu Node Name	Work Pane Tabs Provide Information About...
Controller Info	General information about the selected LSI MegaRAID controller.
Physical Drive Info	General drive information, identification information, and drive statusl
Virtual Drive Info	General drive information, RAID information, and physical drive information.
Battery Backup Unit	Backup battery information for the selected MegaRAID controller.
Storage Log	Storage messages.

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	Locally-defined user accounts, Active Directory settings, and current user session information.
Networking	NIC, IPv4, IPv6, VLAN, and LOM properties, along with network security and NTP settings.
Communication Services	HTTP, XML API, SSH, Redfish, IPMI over LAN, and SNMP settings.
Certificate Management	Security certificate information and management.
Event Management	Platform event management.
Firmware Management	Cisco IMC and BIOS firmware information and management.
Utilities	Technical support data collection, system configuration import and export options, and restore factory defaults settings.

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.

Button Name	Description
Launch KVM	Displays the drop-down menu to launch the Java based or HTML based KVM console.
Ping	Launches the **Ping Details** pop-up window.
Reboot	Enables you to reboot Cisco IMC.

Cisco Integrated Management Controller Online Help Overview

The GUI for the Cisco Integrated Management Controller (Cisco IMC) software is divided into two main sections, a Navigation pane on the left and a Work pane on the right.

This help system describes the fields on each Cisco IMC GUI page and in each dialog box.

To access the page help, do one of the following:

- In a particular tab in the Cisco IMC GUI, click the **Help** icon in the toolbar above the Work pane.
- In a dialog box, click the **Help** button in that dialog box.

Logging into Cisco IMC

Before you begin

If not installed, install Adobe Flash Player 10 or later on your local machine.

Procedure

Step 1 In your web browser, type or select the web link for .

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 refreshing the 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**.

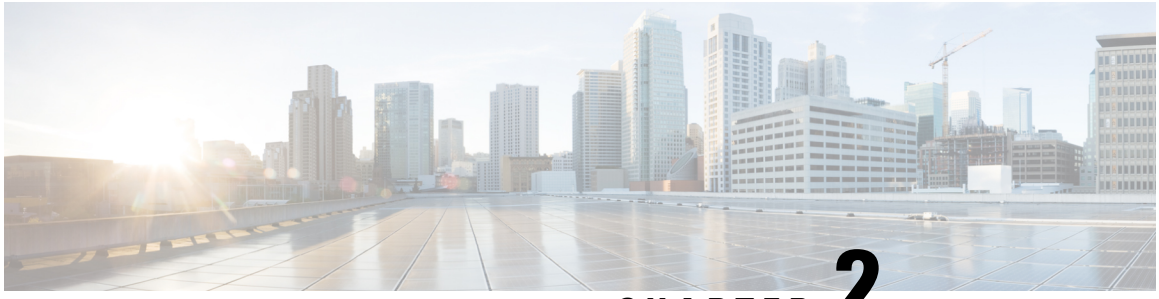
Logging out of Cisco IMC

Procedure

Step 1 In the upper right of , click **Log Out**.

Logging out returns you to the log in page.

Step 2 (Optional) Log back in or close your web browser.



CHAPTER 2

Installing the Server Operating System or Hypervisor

This chapter includes the following sections:

Operating System or Hypervisor Installation Methods

E-Series Servers and NCE 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. For example, you must use either the KVM console or the Host Image Mapping method. Using a combination of methods will cause the server to be in an undefined state.

KVM Console

The KVM console is an interface accessible from the CIMC that emulates a direct keyboard, video, and mouse connection to the server. The KVM console allows you to connect to the server from a remote location. Instead of using CD/DVD or floppy drives physically connected to the server, the KVM console uses virtual media, which are actual disk drives or disk image files that are mapped to virtual CD/DVD or floppy drives. You can map any of the following to a virtual drive:

- CD/DVD or floppy drive on your computer

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

You can use the KVM console to install an operating system or hypervisor 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.

  Note The CIMC Configuration Utility is not applicable to the EHWIC E-Series NCE and the NIM E-Series NCE.

- On Cisco UCS M1 and M2 servers, access the WebBIOS to configure RAID, by pressing **Ctrl-H** during bootup.

  On Cisco UCS M3 servers, access the MegaRAID controller to configure RAID, by pressing **Ctrl-R** during bootup.

  Note RAID is not supported on EHWIC E-Series NCE and NIM E-Series NCE. The **Ctrl-H** and **Ctrl-R** will not work on these SKUs.

Java Requirements to Launch the KVM Console

To launch the KVM console, you must have Java release 1.6 or later installed in your system.

If the KVM console fails to launch because the certificate is revoked by Java, you must change your Java settings. Do the following:

1. Access the Java control panel.
2. Click the **Advanced** tab
3. Under **Perform certificate revocation on**, choose the **Do not check (not recommended)** radio button. For more information, see http://www.java.com/en/download/help/revocation_options.xml.

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 installation server 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**.

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 during PXE 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 Do one of the following as appropriate:

- To download the VMware vSphere Hypervisor 5.1 image, enter **ESXi-5.1.0-799733-custom-Cisco-2.1.0.3.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 5.1.0 GA Install CD**, and then click **Download**.
- To download the VMware vSphere Hypervisor 5.5 image, enter **ESXi-5.5.0-1331820-custom-Cisco-5.5.0.1.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 5.5.0 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 Microsoft Windows, 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 Server or NCE. 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 or .img as the file extension.

The Host Image Mapping feature also allows you to download and mount a diagnostics image. The diagnostics image must have .diag 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 The VMware vSphere Hypervisor requires a customized image. To download the customized image, see Downloading the Customized VMware vSphere Hypervisor Image, on page 13.

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-down list	The type of remote server on which the image is located. This can be one of the following: • **FTP** • **FTPS** • **HTTP** • **HTTPS** **Note** Depending on the remote server that you select, the fields that display change.
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. The path and filename can contain up to 80 characters. • If you are installing a host image, that image must have .iso or .img as the file extension. • If you are installing a diagnostics image, that image must have .diag as the file extension.
Username field	The username of the remote server. The username can contain 1 to 20 characters. **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. The password can contain 1 to 20 characters. **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 displays in the **Image Information** area.

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

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

- HDD—Hard disk drive
- FDD—Floppy disk drive
- CD/DVD—Bootable CD-ROM or DVD 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 work pane, click the **Host Image Mapping** tab.

Step 4 Click **Unmap Image**.

The mapped image is unmounted from the virtual drive of the USB controller.

Deleting the Host Image

Before you begin

Log in to CIMC as a user with admin privileges.

Procedure

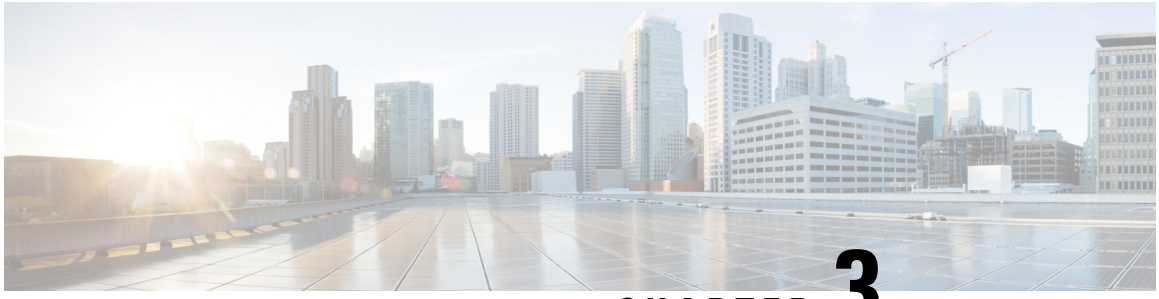
Step 1 In the **Navigation** pane, click the **Compute** menu.

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

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

Step 4 Click **Delete Selected Image**.

The image is removed from the SD card.



CHAPTER 3

Managing Chassis

This chapter includes the following sections:

Chassis Summary

Viewing Chassis Summary

By default when you log on to the Cisco UCS E-Series rack-mount server, the **Summary** pane of the Chassis is displayed in the Web 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.

Name	Description
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 IMC Information** area of the **Chassis Summary** pane, review the following information:

Name	Description
Hostname field	A user-defined hostname for the . 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 .
MAC Address field	The MAC address assigned to the active network interface to the .
Firmware Version field	The current firmware version.
Current Time field	The current date and time according to the clock. **Note** gets the current date and time from the server BIOS when the NTP is disabled. When NTP is enabled, 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. Then change the date or time using the options on the main BIOS configuration tab.

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

Name	Description
Router Model field	The router model name.
Serial Number field	The serial number for the router.

Step 6 In the **Chassis Status** area of the **Chassis Summary** pane, review the following information:

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

Name	Description
Overall DIMM Status field	The overall status of the memory modules. This can be one of the following: • **Good** • **Fault** • **Severe Fault** You can click the link in this field to view detailed status information.
Overall Storage Status field	The overall status of all controllers. This can be one of the following: • **Good** • **Moderate Fault** • **Severe Fault**

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 Click **Save Changes**.

Chassis Inventory

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
Device ID column	The identifier for the power supply unit.
Status column	The status of the power supply unit.
Input column	The input into the power supply, in watts.
Max Output column	The maximum output from the power supply, in watts.
FW Version column	The firmware version for the power supply.
Product ID column	The product identifier for the power supply assigned by the vendor.

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 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 ID 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.
External Ethernet Interfaces	**ID**—The ID for the external ethernet interface. **MAC Address**—The MAC address for the external ethernet interface.

Viewing 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** working area, click the **Power Supply** tab.

Step 4 Review the following sensor properties for power supply:

Properties Area

Name	Description
Redundancy Status field	The power supply redundancy status.

Threshold 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: • **Unknown** • **Informational** • **Normal** • **Warning** • **Critical** • **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.

Discrete 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: • **Unknown** • **Informational** • **Normal** • **Warning** • **Critical** • **Non-Recoverable**
Reading column	The basic state of the sensor.

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** working 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: • **Unknown** • **Informational** • **Normal** • **Warning** • **Critical** • **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.

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** working area, click the **Voltage** tab.

Step 4 Review the following voltage 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: • **Unknown** • **Informational** • **Normal** • **Warning** • **Critical** • **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** working area, click the **Current** tab.

Step 4 Review the following current sensor properties:

Viewing Storage Sensors

Procedure

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

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

Step 3 In the **Storage** tab's **Storage Sensors** area, view the following storage-related statistics for the server:

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

Faults Summary

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:

Table 1: Actions Area

Name	Description
Total	Displays the total number of rows in the Fault Entries table.
Column drop-down list	Allows you to choose the columns you wish to be displayed.

Name	Description
Show drop-down list	Customize the way you want to view fault entries using filters. These can be: • **Quick Filter** - Default view. • **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. Click **Go** to view the entries matching the filter criteria that you set. Click the **Save** icon to save the filter criteria that you set. This becomes a user-defined filter which you can use later. **Note** The user-defined filter appears in the **Manage Preset Filters** dialog box. • **All** - Displays all entries • **Manage Preset Filters** - Displays user-defined filters. You can edit or remove the user-defined filter from this dialog box. • **List of pre-defined filters** - Displays the system-defined filters. **Note** You can use the **Filter** icon to hide or unhide the filter fields.

Table 2: Fault Entries Area

Name	Description
Time	The time when the fault occurred.
Severity	This can be one of the following: • **Cleared** - A fault or condition was cleared. • **Critical** • **Info** • **Major** • **Minor** • **Warning**
Code	The unique identifier assigned to the fault.

Name	Description
DN	The distinguished name (DN) is a hierarchical representation of the device endpoint and its instance on the server.
Probable Cause	The unique identifier associated with the event that caused the fault.
Description	More information about the fault. It also includes a proposed solution.

Fault History

Viewing Faults 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

Table 3: Actions Area

Name	Description
Total	Displays the total number of rows in the Fault History table.
Column drop-down list	Allows you to choose the columns you wish to be displayed.

Name	Description
Show drop-down list	Customize the way you want to view fault history entries using filters. These can be: • **Quick Filter** - Default view. • **Advanced Filter** - Filter options to display the 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. Click **Go** to view the entries matching the filter criteria that you set. Click the **Save** icon to save the filter criteria that you set. This becomes a user-defined filter which you can use later. **Note** The user-defined filter appears in the **Manage Preset Filters** dialog box. • **All** - Displays all entries • **Manage Preset Filters** - Displays user-defined filters. You can edit or remove the user-defined filter from this dialog box. • **List of pre-defined filters** - Displays the system-defined filters. **Note** You can use the **Filter** icon to hide or unhide the filter fields.

Table 4: Faults History Area

Name	Description
Time	The time when the fault occurred.

Name	Description
Severity	This can be one of the following: • **Emergency** • **Alert** • **Critical** • **Error** • **Warning** • **Notice** • **Informational** • **Debug**
Source	The software module that logged the event.
Probable Cause	The unique identifier associated with the event that caused the fault.
Description	More information about the fault. It also includes a proposed solution.

What to do next

System Event Log

Viewing System Event Logs

Procedure

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

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

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

Table 5: Actions Area

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

Name	Description
Total	Displays the total number of rows in the System Event Log table.
Column drop-down list	Allows you to choose the columns you wish to be displayed.
Show drop-down list	Customize the way you want to view events using filters. These can be: • **Quick Filter** - Default view. • **Advanced Filter** - Filter options to display the events 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. Click **Go** to view the entries matching the filter criteria that you set. Click the **Save** icon to save the filter criteria that you set. This becomes a user-defined filter which you can use later. **Note** The user-defined filter appears in the **Manage Preset Filters** dialog box. • **All** - Displays all entries • **Manage Preset Filters** - Displays user-defined filters. You can edit or remove the user-defined filter from this dialog box. • **List of pre-defined filters** - Displays the system-defined filters. **Note** You can use the **Filter** icon to hide or unhide the filter fields.

Table 6: System Event Log Table

Name	Description
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.

Logging Controls

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:

Remote Logging

Name	Description
Enabled check box	If checked, the Cisco IMC sends log messages to the Syslog server named in the **IP Address** field.
Host Name/IP Address field	The address of the Syslog server on which the Cisco IMC log should be stored. 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.
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: • **Emergency** • **Alert** • **Critical** • **Error** • **Warning** • **Notice** • **Informational** • **Debug**

Note The Cisco IMC does not remotely log any messages with a severity below the selected severity. For example, if you select **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.

Local Logging

This area displays only the **Minimum Severity to Report** drop-down list as shown in the table above. You can specify the lowest level of messages to be included in the local log

What to do next

Sending the Cisco IMC Log to a Remote Server

You can configure profiles for one or two remote syslog servers to receive log entries.

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.

Procedure

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

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

Step 3 In either of the **Remote Syslog Server** areas, complete the following fields:

Name	Description
Enabled check box	If checked, the Cisco IMC sends log messages to the Syslog server named in the **IP Address** field.
Host Name/IP Address field	The address of the Syslog server on which the Cisco IMC log should be stored. 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.

Step 4 (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 select one of the following, in decreasing order of severity:

- **Emergency**
- **Alert**
- **Critical**
- **Error**

- **Warning**
- **Notice**
- **Informational**
- **Debug**

Note does not remotely log any messages with a severity below the selected severity. For example, if you select **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 5 Click **Save Changes**.

Configuring the Cisco IMC Log Threshold

Before you begin

Procedure

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

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

Step 3 Required: In the **Local Logging** area, use the **Minimum Severity to Report** drop-down list to specify the lowest level of messages that will be included in the log.

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

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

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

Sending a Test Cisco IMC 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.

Procedure

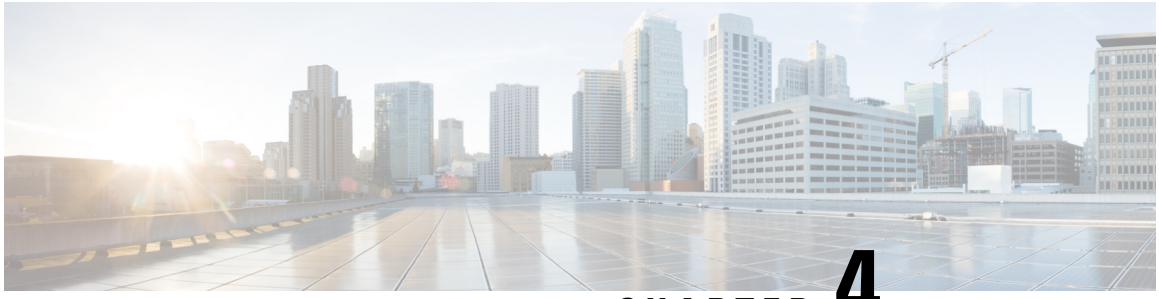
Step 1 In the **Navigation** pane, click the **Chassis** menu.

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

Step 3 In the **Faults and Logs** pane, click the **Logging Controls** tab.

Step 4 In the **Action** area, click **Send Test Syslog**.

A test log is sent to the configured remote servers.



CHAPTER 4

Managing the Server

This chapter includes the following sections:

Configuring BIOS Settings

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 first time. 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.

Configuring Main 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 In the **Configure BIOS** tab, click the **Main** tab.

Step 4 Specify whether the server should be rebooted after you save your changes.

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

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

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

Step 5 In the **Main** tab, update the BIOS settings fields.

Step 6 You can reset the parameters or restore the default values using the buttons at the bottom of the Main tab. The available options are:

Name	Description
Save button	Saves the settings for the BIOS parameters and closes the dialog box. If the **Reboot Host Immediately** check box is checked, the server is rebooted immediately and the new BIOS settings go into effect. Otherwise the changes are saved until the server is manually rebooted.
Reset button	Resets the values for the BIOS parameters on all three tabs to the settings that were in effect when this dialog box was first opened.
Restore Defaults button	Sets the BIOS parameters on all three tabs to their default settings.

Configuring Advanced BIOS Settings

Note Depending on your installed hardware, some configuration options described in this topic may not appear.

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 In the **Configure BIOS** tab, click the **Advanced** tab.

Step 4 Specify whether the server should be rebooted after you save your changes.

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

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

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

Step 5 In the **Advanced** tab, update the relevant fields:

Step 6 After you updated the fields, perform the following actions:

Name	Description
Save button	Saves the settings for the BIOS parameters on all three tabs and closes the dialog box.
Reset button	Restores the values for the BIOS parameters on all three tabs to the settings that were in effect when this dialog box was first opened.
Restore Defaults button	Sets the BIOS parameters on all three tabs to their default settings.

Configuring Server Management BIOS Settings

Procedure

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

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

Step 3 In the **Configure BIOS** tab, click **Server Management**.

Step 4 Specify whether the server should be rebooted after you save your changes.

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

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

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

Step 5 In the **Server Management** tab, update the relevant fields:

Step 6 Complete your action with the following options:

Name	Description
Save button	Saves the settings for the BIOS parameters on all three tabs and closes the dialog box.
Reset button	Restores the values for the BIOS parameters on all three tabs to the settings that were in effect when this dialog box was first opened.
Restore Defaults button	Sets the BIOS parameters on all three tabs to their default settings.

Entering BIOS Setup

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 **Navigation** pane, click the **Compute** menu.

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

Step 3 In the **Actions** area, click **Enter BIOS Setup**.

Step 4 Click **OK** at the prompt.
Enables enter BIOS setup. On restart, the server enters the BIOS setup.

Clearing the BIOS CMOS

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 **Navigation** pane, click the **Compute** menu.

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

Step 3 In the **Actions** area, click **Clear BIOS CMOS**.

Step 4 Click **OK** to confirm.
Clears the BIOS CMOS.

Restoring BIOS Manufacturing Custom Settings

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 **Navigation** pane, click the **Compute** menu.

Step 2 In the **Compute** menu, select a server.

Step 3 In the work pane, click the **BIOS** tab.

Step 4 In the **Actions** area, click **Restore Manufacturing Custom Settings**.

Step 5 Click **OK** to confirm.

Managing the Server Boot Order

Server Boot Order

When you change the boot order configuration, 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.

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

- BIOS encounters issues while trying to boot using the configured boot order.
- A user changes the boot order directly through BIOS.

Managing a Boot Device

Before you begin

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

Procedure

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

Step 2 In the **BIOS** tab, click the **Configure Boot Order** tab.

Step 3 In the **BIOS Properties** area, click **Configure Boot Order**.

A dialog box with boot order instructions appears.

Step 4 In the **Configure Boot Order** dialog box, clcik **Basic** tab and from the **Device Types** table, choose the device that you want add to the boot order.

To add the local HDD device, click **Advanced** tab, click **Add Local HDD**, and update the following parameters:

Name	Description
Name field	The name of the device. **Note** Once created, you cannot rename the device.
State drop-down list	The visibility of the device by BIOS. This can be one of the following: • **Enabled**—The device is visible to BIOS in a boot order configuration. • **Disabled**—The device is not visible to BIOS in a boot configuration.
Order field	The order of the device in the available list of devices. Enter between 1 and n, where n is the number of devices.
Slot field	The slot in which the device is installed. Enter the slot number from the available range.
Save Changes button	Adds the device to the **Boot Order** table.
Cancel button	Closes the dialog box without saving any changes made while the dialog box was open.

To add the PXE device, click **Add PXE**, and update the following parameters:

Name	Description
Name field	The name of the device. This name cannot be changed after the device has been created.
State drop-down list	The visibility of the device by BIOS. The state can be one of the following: • **Enabled**—The device is visible to BIOS in a boot order configuration. • **Disabled**—The device is not visible to BIOS in a boot order configuration.
Order field	The order of the device in the available list of devices. Enter between 1 and n, where n is the number of devices.
Slot field	
Port field	The port of the slot in which the device is present. Enter a number between 0 and 255.
Save Changes button	Adds the device to the **Boot Order** table.
Cancel button	Closes the dialog box without saving any changes made while the dialog box was open.

To add the SAN boot device, click **Add SAN**, and update the following parameters:

Name	Description
Name field	The name of the device. This name cannot be changed after the device has been created.
State drop-down list	The visibility of the device by BIOS. The state can be one of the following: • **Enabled**—The device is visible to BIOS in a boot order configuration. • **Disabled**—The device is not visible to BIOS in a boot order configuration.
Order field	The order of the device in the available list of devices. Enter between 1 and n, where n is the number of devices.
Slot field	The slot in which the device is installed. Enter the slot number from the available range.
LUN field	Logical unit in a slot where the device is present. Enter a number between 0 and 255.
Save Changes button	Adds the device to the **Boot Order** table.
Cancel button	Closes the dialog box without saving any changes made while the dialog box was open.

To add the iSCSI boot device, click **Add iSCSI**, and update the following parameters:

Name	Description
Name field	The name of the device. This name cannot be changed after the device has been created.
State drop-down list	The visibility of the device by BIOS. The state can be one of the following: • **Enabled**—The device is visible to BIOS in a boot order configuration. • **Disabled**—The device is not visible to BIOS in a boot order configuration.
Order field	The order of the device in the available list of devices. Enter between 1 and n, where n is the number of devices.
Slot field	The slot in which the device is installed. Enter the slot number from the available range.

Name	Description
Port field	The port of the slot in which the device is present. Enter a number between 0 and 255. **Note** In case of a VIC card, use a vNIC instance instead of the port number.
Save Changes button	Adds the device to the **Boot Order** table.
Cancel button	Closes the dialog box without saving any changes made while the dialog box was open.

To add the SD card, click **Add SD Card**, and update the following parameters:

Name	Description
Name field	The name of the device. This name cannot be changed after the device has been created.
State drop-down list	The visibility of the device by BIOS. This can be one of the following: • **Enabled**—The device is visible to BIOS in a boot order configuration. • **Disabled**—The device is not visible to BIOS in a boot configuration.
Order field	The order of the device in the available list of devices. Enter between 1 and n, where n is the number of devices.
Lun field	Logical unit in a slot where the device is present. Enter a number between 0 and 255.
Save Changes button	Adds the device to the **Boot Order** table.
Cancel button	Closes the dialog box without saving any changes made while the dialog box was open.

To add the USB device, click **Add USB**, and update the following parameters:

Name	Description
Name field	The name of the device. This name cannot be changed after the device has been created.
Sub Type drop-down list	The subdevice type under a certain device type. This can be one of the following: • **CD** • **FDD** • **HDD**

Name	Description
State drop-down list	The visibility of the device by BIOS. This can be one of the following: • **Enabled**—The device is visible to BIOS in a boot order configuration. • **Disabled**—The device is not visible to BIOS in a boot order configuration.
Order field	The order of the device in the available list of devices. Enter between 1 and n, where n is the number of devices.
Save Changes button	Adds the device to the **Boot Order** table.
Cancel button	Closes the dialog box without saving any changes made while the dialog box was open.

To add the virtual media, click **Virtual Media**, and update the following parameters:

Name	Description
Name field	The name of the device. This name cannot be changed after the device has been created.
Sub Type drop-down list	The subdevice type under a certain device type. This could be any one of the following: • **KVM Mapped DVD** • • **KVM Mapped HDD** • • **KVM Mapped FDD**
State drop-down list	The visibility of the device by BIOS. The state can be one of the following: • **Enabled**—The device is visible to BIOS in a boot order configuration. • **Disabled**—The device is not visible to BIOS in a boot order configuration.
Order field	The order of the device in the available list of devices. Enter between 1 and n, where n is the number of devices.
Save Changes button	Adds the device to the **Boot Order** table.
Cancel button	Closes the dialog box without saving any changes made while the dialog box was open.

To add the PCH storage device, click **PCH Storage**, and update the following parameters:

Name	Description
Name field	The name of the device. This name cannot be changed after the device has been created.
State drop-down list	The visibility of the device by BIOS. This can be one of the following: • **Enabled**—The device is visible to BIOS in a boot order configuration. • **Disabled**—The device is not visible to BIOS in a boot order configuration.
Order field	The order of the device in the available list of devices. Enter between 1 and n, where n is the number of devices.
LUN field	Logical unit in a slot where the device is present. • Enter a number between 0 and 255 • SATA in AHCI mode—Enter a value between 1 and 10 • SATA in SWRAID mode—Enter 0 for SATA , and enter 1 for SATA **Note** SATA mode is available only on some UCS E-Series servers.
Save Changes button	Adds the device to the **Boot Order** table.
Cancel button	Closes the dialog box without saving any changes made while the dialog box was open.

To add the UEFI shell device, click **Add UEFI Shell**, and update the following parameters:

Name	Description
Name field	The name of the device. This name cannot be changed after the device has been created.
State drop-down list	The visibility of the device by BIOS. The state can be one of the following: • **Enabled**—The device is visible to BIOS in a boot order configuration. • **Disabled**—The device is not visible to BIOS in a boot order configuration.
Order field	The order of the device in the available list of devices. Enter between 1 and n, where n is the number of devices.
Save Changes button	Adds the device to the **Boot Order** table.

Name	Description
Cancel button	Closes the dialog box without saving any changes made while the dialog box was open.

Enabling UEFI Secure Boot

Procedure

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

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

Step 3 In the **BIOS Properties** area of the **Configure Boot Order** tab, check **UEFI Secure Boot** checkbox.

Note If checked, the boot mode is set to UEFI secure boot. You cannot modify the **Configure Boot Mode** until UEFI secure boot option is disabled.

If you enable UEFI secure boot on a nonsupported OS, on the next reboot, you cannot boot from that particular OS. If you try to boot from the previous OS, an error is reported and recorded under the system software event in the web UI. You must disable the UEFI secure boot option by using Cisco IMC to boot from your previous OS.

Step 4 Click **Save Changes**.

What to do next

Reboot the server to have your configuration boot mode settings take place.

Disabling UEFI Secure Boot

Procedure

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

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

Step 3 In the **BIOS Properties** area, uncheck the **UEFI Secure Boot** check box.

Step 4 Click **Save Changes**.

What to do next

Reboot the server to have your configuration boot mode settings take place.

Configure Boot Order

Before you begin

You must log in as a user with admin privileges:

Procedure

Step 1 Log in to **CIMC**.

Step 2 From the **CIMC Compute**, select the **BIOS** tab.

Step 3 From the **CIMC Compute**, select the **BIOS** tab.

Step 4 From the **CIMC Compute**, select the **BIOS** tab.

Step 5 From the **CIMC Compute**, select the **BIOS** tab.

Step 6 From the **CIMC Compute**, select the **BIOS** tab.

Step 7 From the **CIMC Compute**, select the **BIOS** tab.

Step 8 From the **CIMC Compute**, select the **BIOS** tab.

Step 9 Select **Configure Boot Order** and the **Configure Boot Order**, the dialog box appears.

Step 10 From the **CD/DVD** page, select **Cisco vKVM-Mapped vDVD**, and select **Add**.

Step 11 From **HDD**, select **RAID Adapter**, and then select **Add**.

Step 12 Set the boot order sequence using the **Up** and **Down** options. The **Cisco vKVM-Mapped vDVD** boot order must be the first choice. **Save Changes** to complete the boot order setup.

Note To configure Boot Order for UEFI through CIMC, the supported BIOS version is 3.2.10 or later. If any other BIOS version is used, you must configure UEFI Boot Order through the BIOS setup menu and set **BootOrderRules** to **Loose**.

Enable UEFI Boot Order

Procedure

Select **Configure Boot Order**, the **dialog box** appears.

What to do next

Reboot the server to have your configuration boot order settings take place.

Viewing the Actual Server Boot Order

The actual 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 .

Procedure

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

Step 2 In the **BIOS** tab, click the **Configure Boot Order** tab.

Step 3 In the **BIOS Properties** area, click **Configure Boot Order**.

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

The **Configured Boot Devices** section displays the boot order (**Basic** or **Advanced**) configured through Cisco IMC. If this configuration changes, Cisco IMC sends this boot order to BIOS the next time that server boots. The Basic configuration allows you to specify only the device type. The Advanced configuration allows you to configure the device with specific parameters such as slot, port and LUN.

To change the configured boot order, or to restore the previously configured boot order, administrators can click the **Configure Boot Order** button. To have these changes take effect immediately, reboot the server. You can verify the new boot order by refreshing the **BIOS** tab.

Note This information is only sent to BIOS the next time the server boots. Cisco IMC does not send the boot order information to BIOS again until the configuration changes.

The **Actual Boot Devices** section displays the boot order actually used by BIOS when the server last booted. The actual boot order will differ from the configured boot order if either of the following conditions occur:

- The BIOS encounters issues while trying to boot using the configured boot order.
- A user changes the boot order directly through the BIOS. To override any manual changes, you can change the configured boot order through Cisco IMC and reboot the server.

Note When you create a new policy using the configured boot order, BIOS tries to map this new policy to the device or devices present in the system. It displays the actual device name and the policy name to which it is mapped under the **Actual Boot Order** area. If BIOS cannot map any device found to a particular policy in Cisco IMC, then the actual device name is stated as **NonPolicyTarget** under the **Actual Boot Order** area.

Configuring the Power Restore Policy for Modules on ISRG2

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

Note Even though you can see the changed settings in the GUI, you have to reboot the server for the settings to take effect.

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** and then the **Server Management** tab.

Step 3 In the **Server Management** area, update the following field:

Name	Description
Power Restore Policy	The action to be taken when chassis power is restored after an unexpected power loss. This can be one of the following: **Power On** – The server is powered on post the power outage. **Power Off** – The server remains in the power off state. **Restore Last State** – The server is set to the state it was in prior to the power outage.

Step 4 Click **Save**.

Configuring the Power Restore Policy for Modules on ISR4K

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 work pane, click the **Power Policies** tab.

Step 3 In the **Power Restore Policy** area, update the following field:

Name	Description
Power Restore Policy	The action to be taken when chassis power is restored after an unexpected power loss. This can be one of the following: **Power On** – The server is powered on post the power outage. **Power Off** – The server remains in the power off state. **Restore Last State** – The server is set to the state it was in prior to the power outage.

Step 4 Click **Save**.

Configure Boot Order

Configure Boot Order for UEFI Installation

Before you begin

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

Procedure

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

Step 2 In the **BIOS** tab, click the **Configure Boot Order** tab. Under **BIOS Properties**, you can see the Device Types table with **Configured Boot Devices** and **Actual Boot Devices**.

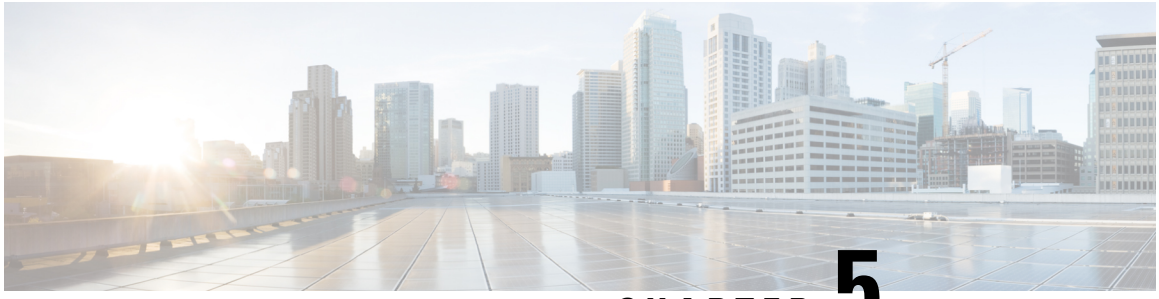
Step 3 In the **BIOS Properties** area, under the **Actual Boot Devices**, select **UEFI Image Map**, use the >> button to add the image map under the **Configured Boot Devices** table. Similarly, add **UEFI OS** to the device, click **Configure Boot Order**.

Note Using the << button removes the options from the configuration list.

Step 4 Click **Save Changes** to reflect the configured boot devices.

Name	Description
Configure Boot Order button	This opens a pop-up window with the **Basic** tab. Select the devices you wish to add under the **Configured Boot Devices** table.
Save Changes button	Adds the device to the **Configured Boot Devices** table.

Name	Description
Cancel button	Closes the dialog box without saving any changes made while the dialog box was open.



CHAPTER 5

Viewing Sensors

This chapter includes the following sections:

Viewing 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** working area, click the **Power Supply** tab.

Step 4 Review the following sensor properties for power supply:

Properties Area

Name	Description
Redundancy Status field	The power supply redundancy status.

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: • **Unknown** • **Informational** • **Normal** • **Warning** • **Critical** • **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.

Discrete 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: • **Unknown** • **Informational** • **Normal** • **Warning** • **Critical** • **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** working 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: • **Unknown** • **Informational** • **Normal** • **Warning** • **Critical** • **Non-Recoverable**
Speed (RPMS) column	The fan speed in RPM.
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** working 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: • **Unknown** • **Informational** • **Normal** • **Warning** • **Critical** • **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.

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** working 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: • **Unknown** • **Informational** • **Normal** • **Warning** • **Critical** • **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** working area, click the **Current** tab.

Step 4 Review the following current sensor properties:

Viewing Storage Sensors

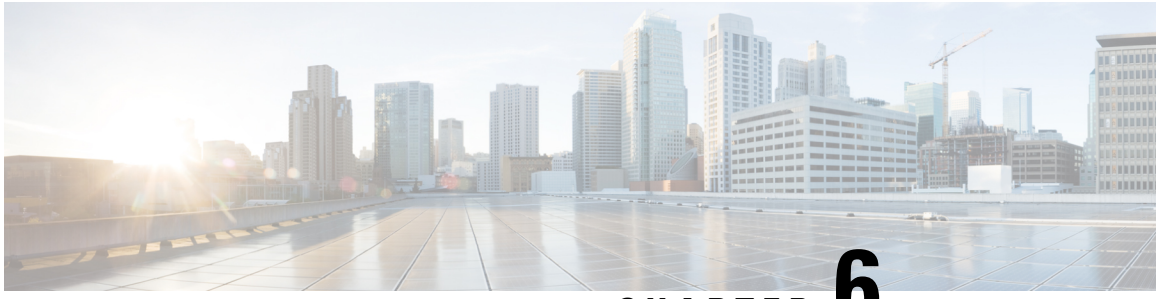
Procedure

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

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

Step 3 In the **Storage** tab's **Storage Sensors** area, view the following storage-related statistics for the server:

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



CHAPTER 6

Managing Remote Presence

This chapter includes the following sections:

Configuring Serial Over LAN

Serial over LAN enables the input and output of the serial port of a managed system to be redirected over IP. Configure and use serial over LAN on your server when you want to reach the host console with .

Before you begin

You must log in as a user with admin privileges to configure serial over LAN.

Procedure

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

Name	Description
Baud Rate drop-down list	The baud rate the system uses for SoL communication. This can be one of the following: • **9600 bps** • **19.2 kbps** • **38.4 kbps** • **57.6 kbps** • **115.2 kbps**
Com Port drop-down list	The serial port through which the system routes SoL communication. **Note** This field is available only on some E-Series servers. If it is not available, the server always uses COM port 0 for SoL communication. You can select one of the following: • **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. If you select this option, the system enables SoL and disables the RJ45 connection, which means that the server can no longer support an external serial device. • **com1**—SoL communication is routed through COM port 1, an internal port accessible only through SoL. If you select this option, you can use SoL on COM port 1 and the physical RJ45 connection on COM port 0. **Note** Changing the Com Port setting disconnects any existing SoL sessions.
SSH Port filed	The port through which you can access Serial over LAN directly. The port enables you to by-pass the Cisco IMC shell to provide direct access to SoL. The valid range is 1024 to 65535. The default value is 2400. **Note** Changing the SSH Port setting disconnects any existing SSH sessions.

Step 5 Click **Save Changes**.

Configuring Virtual Media

Before you begin

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

Procedure

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

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

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

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

Name	Description
Enabled check box	If checked, virtual media is enabled. **Note** If you clear this check box, all virtual media devices are automatically detached from the host.
Active Sessions field	The number of virtual media sessions that are currently running.
Enable Virtual Media Encryption check box	If checked, all virtual media communications are encrypted.

Step 5 Click **Save Changes**.

Creating a Cisco IMC Mapped vMedia Volume

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 **Remote Management** tab.

Step 3 In the **Remote Management** tab, 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.

Name	Description
Mount Type drop-down list	The type of mapping. This can be one of the following: **Note** Ensure that the communication port of the mount type that you choose 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. • **NFS**—Network File System. • **CIFS**—Common Internet File System. • **WWW(HTTP/HTTPS)**—HTTP-based or HTTPS-based system. **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 selected **Mount Type**: • **NFS**—Use **`serverip:/share`**. • **CIFS**—Use **`//serverip/share`**. • **WWW(HTTP/HTTPS)**—Use **`http[s]://serverip/share`**.
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 selected **Mount Type**. If you are using **NFS**, leave the field blank or enter one or more of the following: • **`ro`** • **`rw`** • **`nolock`** • **`noexec`** • **`soft`** • **`port=VALUE`** • **`timeo=VALUE`** • **`retry=VALUE`** If you are using **CIFS**, leave the field blank or enter one or more of the following: • **`soft`** • **`nounix`** • **`noserverino`** • **`guest`** • **`username=VALUE`**—ignored if **`guest`** is entered. • **`password=VALUE`**—ignored if **`guest`** is entered. • **`sec=VALUE`** 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: • **None**—No authentication is used • **Ntlm**—NT LAN Manager (NTLM) security protocol. Use this option only with Windows 2008 R2 and Windows 2012 R2. • **Ntlmi**—NTLMi security protocol. Use this option only when you enable Digital Signing on the CIFS Windows server. • **Ntlmssp**—NT LAN Manager Security Support Provider (NTLMSSP) protocol. Use this option only with Windows 2008 R2 and Windows 2012 R2. • **Ntlmsspi**—NTLMSSPi protocol. Use this option only when you enable Digital Signing on the CIFS Windows server.

Name	Description
	• **Ntlmv2**—NTLMv2 security protocol. Use this option only with Samba Linux. • **Ntlmv2i**—NTLMv2i security protocol. Use this option only with Samba Linux. If you are using **WWW(HTTP/HTTPS)**, leave the field blank or enter the following: • `noauto` **Note** Before mounting the virtual media, tries to verify reachability to the end server by pinging the server. • `username=VALUE` • `password=VALUE`
User Name field	The username for the specified **Mount Type**, if required.
Password field	The password for the selected username, if required.

Step 6 Click **Save**.

Viewing Cisco IMC-Mapped vMedia Volume Properties

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, select a server.

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

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

Step 5 Select 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 selected image.
Unmap button	Unmaps the mounted vMedia.

Name	Description
Last Mapping Status	The status of the last mapping attempted.
Volume column	The identity of the image.
Mount Type drop-down list	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: • **OK**—The mapping is successful. • **In Progress**—The mapping is in progress. • **Stale**— displays a text string with the reason why the mapping is stale. • **Error**— displays a text string with the reason for the error.

Removing a Cisco IMC-Mapped vMedia Volume

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, select a server.

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

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

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

Step 6 Click **Unmap**.

KVM Console

The KVM console is an interface accessible from that emulates a direct keyboard, video, and mouse (KVM) connection to the server. The KVM console allows you to connect to the server from a remote location.

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

- CD/DVD or floppy drive on your computer
- Disk image files (ISO or IMG files) on your computer
- USB flash drive on your computer
- CD/DVD or floppy drive on the network
- Disk image files (ISO or IMG files) on the network
- USB flash drive on the network

You can use the KVM console to install an OS on the server.

Launching KVM Console

You can launch the KVM console from either the Home page or from the Remote Management area.

Procedure

Step 1 To launch the console from Home page, in the **Navigation** pane, click the **Chassis** menu.

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

Step 3 From the tool bar, click **Launch KVM** and select **Java based KVM** or **HTML based KVM**.

Step 4 Alternatively, in the **Navigation** pane, click the **Compute** menu.

Step 5 In the **Compute** menu, select a server.

Step 6 In the work pane, click the **Remote Management** tab.

Step 7 In the **Remote Management** pane, click the **Virtual KVM** tab.

Step 8 In the **Virtual KVM** tab, click **Launch Java based KVM console** or **Launch HTML based KVM console**.

Step 9 Required: Click the URL link displayed in the pop-up window (HTML based KVM console only) to load the client application. You need to click the link every time you launch the KVM console.

Virtual KVM Console (HTML Based)

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

File Menu

Menu Item	Description
Capture to File button	Opens the **Save** dialog box that allows you to save the current screen as a JPG image.
Exit button	Closes the KVM console.

View Menu

Menu Item	Description
Keyboard	Displays the virtual keyboard for the KVM console, which you can use to input data.
Refresh	Updates the console display with the server's current video output.
Full Screen	Expands the KVM console so that it fills the entire screen.

Macros Menu

Choose the keyboard shortcut you want to execute on the remote system.

Menu Item	Description
Server Macros menu	Displays the server side macros downloaded from the Cisco IMC, if any. If no server side macros have been downloaded, then the menu item is disabled.
Static Macros menu	Displays a predefined set of macros.
User Defined Macros menu	Displays the user-defined macros that have been created.
Manage button	Opens the **Configure User Defined Macros** dialog box, which allows you to create and manage macros. System-defined macros cannot be deleted.

Tools Menu

Menu Item	Description

Session Options	Opens the **Session Options** dialog box that lets you specify:
	• **Scaling**—Specify whether or not you want to maintain the aspect ratio of the screen. Check or uncheck the **Maintain Aspect Ratio** checkbox (checked by default).
	• The mouse acceleration to use on the target system. The default is **Absolute positioning (Windows, Newer Linux & MAC OS X)**. Other options are:
	  • **Relative Positioning, no acceleration**
	  • **Relative Positioning (RHEL, Older Linux)**

Menu Item	Description
Session User List	Opens the **Session User List** dialog box that shows all the user IDs that have an active KVM session.
Chat	Opens the **Chat** box to communicate with other users.

Power Menu

Menu Item	Description
Power On System button	Powers on the system. This option is disabled when the system is powered on and it is enabled when the system is not powered.
Power Off System button	Powers off the system from the virtual console session. This option is enabled when the system is powered on and disabled when the system is not powered on.
Reset System (warm boot)button	Reboots the system without powering it off. This option is enabled when the system is powered on and disabled when the system is not powered on.
Power Cycle System (cold boot) button	Turns off system and then back on. This option is enabled when the system is powered on and disabled when the system is not powered on.

Virtual Media Menu

Name	Description
Activate Virtual Devices	Activates a vMedia session that allows you to attach a drive or image file from your local computer or network.
Map CD/DVD	You can map a CD or a DVD image from your local machine and map the drive to the image. **Note** This option is available when you click **Activate Virtual Devices**.
Map Removable Disk	You can map a removable disk image from your local machine and map the drive to the image. **Note** This option is available when you click **Activate Virtual Devices**.

Name	Description
Map Floppy Disk	You can map a floppy disk image from your local machine and map the drive to the image. **Note** This option is available when you click **Activate Virtual Devices**.

Help Menu

Name	Description
Help Topics	Clicking this option brings you back to this window.
About KVM Viewer	Displays the version number of the KVM viewer.

Settings

The **Settings** icon is located on the top right hand corner of the HTML KVM viewer window.

Name	Description
Logged in as:	Displays your user role ID.
Host Name	Displays the host name.
Log Out	Allows you to log out of the KVM viewer.

Comparison Between Java Based KVM and HTML5 Based KVM

The following table lists the differences between Java based KVM and HTML5 based KVM.

Menu Option	Action	Available in Java Based KVM	Available in HTML5 Based KVM
File	Open	Yes	NA
	Capture to file	Yes	Yes
	Paste Text from Clipboard	Yes	No
	Paste Text from File	Yes	No
	Exit	Yes	Yes
View	Refresh	Yes	Yes
	Fit	Yes	No
	Video-Scaling	Yes	No
	Full-Screen	Yes	Yes

Menu Option	Action	Available in Java Based KVM	Available in HTML5 Based KVM
	Mini-Mod	Yes	No
	Keyboard	NA	Yes
Macros	Server Macros	Yes	Yes
	Static Macros	Yes	Yes
	User Defined Macros	Yes	Yes
	Manage	Yes	Yes
Tool	Session Option	Yes	Yes
	Single Cursor	Yes	No
	Stats	Yes	No
	Session User List	Yes	Yes
	Chat	Yes	Yes
	Recorder/Playback Controls	Yes	No
	Export Video	Yes	No
Power	Power On	Yes	Yes
	Power OFF	Yes	Yes
	Reset System	Yes	Yes
	Power Cycle system	Yes	Yes
Virtual Media	Create Image	Yes	No
	Activate Virtual Devices	Yes	Yes
	Physical Device Mapping	Yes	No

Configuring the Virtual KVM

Before you begin

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

Procedure

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

Step 2 In the **Compute** menu, select a server.

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

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

Step 5 On the **Virtual KVM** tab, complete the following fields:

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

Step 6 Click **Save Changes**.

Enabling the Virtual KVM

Before you begin

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

Procedure

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

Step 2 In the **Compute** menu, select a server.

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

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

Step 5 On the **Virtual KVM** tab, check the **Enabled** check box.

Step 6 Click **Save Changes**.

Disabling the Virtual KVM

Before you begin

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

Procedure

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

Step 2 In the **Compute** menu, select a server.

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

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

Step 5 On the **Virtual KVM** tab, uncheck the **Enabled** check box.

Step 6 Click **Save Changes**.

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 Microsoft Windows, 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 Server or NCE. 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 or .img as the file extension.

The Host Image Mapping feature also allows you to download and mount a diagnostics image. The diagnostics image must have .diag 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 The VMware vSphere Hypervisor requires a customized image. To download the customized image, see Downloading the Customized VMware vSphere Hypervisor Image, on page 13.

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-down list	The type of remote server on which the image is located. This can be one of the following: • **FTP** • **FTPS** • **HTTP** • **HTTPS** **Note** Depending on the remote server that you select, the fields that display change.
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. The path and filename can contain up to 80 characters. • If you are installing a host image, that image must have .iso or .img as the file extension. • If you are installing a diagnostics image, that image must have .diag as the file extension.
Username field	The username of the remote server. The username can contain 1 to 20 characters. **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. The password can contain 1 to 20 characters. **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 displays in the **Image Information** area.

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

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

- HDD—Hard disk drive
- FDD—Floppy disk drive
- CD/DVD—Bootable CD-ROM or DVD 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 work pane, click the **Host Image Mapping** tab.

Step 4 Click **Unmap Image**.

The mapped image is unmounted from the virtual drive of the USB controller.

Deleting the Host Image

Before you begin

Log in to CIMC as a user with admin privileges.

Procedure

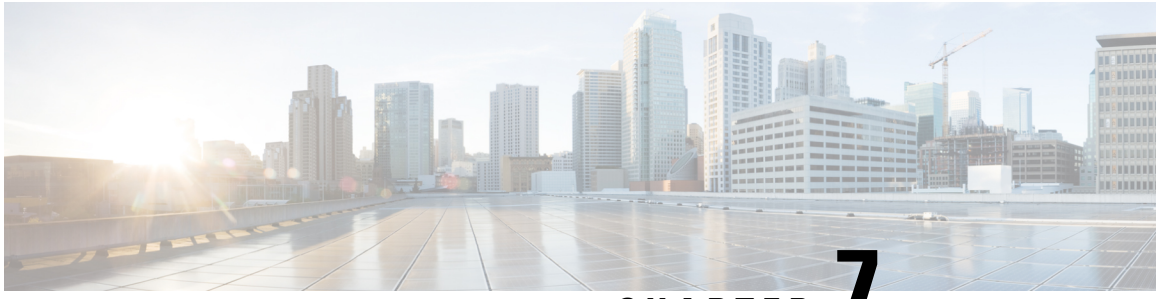
Step 1 In the **Navigation** pane, click the **Compute** menu.

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

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

Step 4 Click **Delete Selected Image**.

The image is removed from the SD card.



CHAPTER 7

Managing User Accounts

This chapter includes the following sections:

Configuring Local Users

The Cisco IMC now implements a strong password policy wherein you are required to follow guidelines and set a strong password when you first 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 configure or modify local user accounts.

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 configure or modify a local user account, click a row in the **Local User Management** pane 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.

Name	Description
Username field	The username for the user. Enter between 1 and 16 characters.

Role Played field	The role assigned to the user. This can be one of the following:
	• **read-only**—A user with this role can view information but cannot make any changes.
	• **user**—A user with this role can perform the following tasks:
	  • View all information
	  • Manage the power control options such as power on, power cycle, and power off
	  • Launch the KVM console and virtual media
	  • Clear all logs
	  • Toggle the locator LED
	  • Set time zone
	  • Ping
	• **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 .
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 user name.

Name	Description

New Password field	The password for this user name. When you move the mouse over the help icon beside the field, the following guidelines to set the password are displayed:
	• The password must have a minimum of 8 and a maximum of 20 characters.
	• The password must not contain the User's Name.
	• The password must contain characters from three of the following four categories:
	  • English uppercase characters (A through Z).
	  • English lowercase characters (a through z).
	  • Base 10 digits (0 through 9).
	  • Non-alphabetic characters (!, @, #, $, %, ^, &, *, -, _, , =, ").
	
	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 Enter password information.

Step 7 Click **Save Changes**.

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 would be common to all users. Upon password expiry, the user is notified on login and would not be allowed to login unless the password is reset.

Note When you downgrade to an older database, existing users are deleted. The database returns to default settings. Previously configured users are cleared and the database is empty, that is, the database has the default username - 'admin' and password - 'password'. Since the server is left with the default user database, the change default credential feature is enabled. This means that when the 'admin' user logs on to the database for the first time after a downgrade, the user must mandatorily change the default credential.

Password Set Time

A 'Password set time' is configured for every existing user, to the time when the migration or upgrade occurred. For new users (users created after an upgrade), the Password Set time is configured to the time when the user

was created, and the password is set. For users in general (new and existing), the Password Set Time is updated whenever the password is changed.

LDAP Servers

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 , 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 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 . 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.

The following steps must be performed on the LDAP server.

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`

Properties	Value
Syntax	`Case Sensitive String`

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

a) Expand the **Classes** node in the left pane and type `U` to select the user class.
b) Click the **Attributes** tab and click **Add**.
c) Type `C` to select the CiscoAVPair attribute.
d) Click **OK**.

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

Role	CiscoAVPair Attribute Value
admin	`shell:roles="admin"`
user	`shell:roles="user"`
read-only	`shell:roles="read-only"`

Note For more information about adding values to attributes, see the article at http://technet.microsoft.com/en-us/library/bb727064.aspx.

What to do next

Use the to configure the LDAP server.

Configuring LDAP Settings and Group Authorization in Cisco IMC

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 check box	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.

Name	Description
Base DN field	Base Distinguished Name. This field describes where to load users and groups from. 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. This field is required unless you specify at least one Global Catalog server address.
Enable Encryption check box	If checked, the server encrypts all information it sends to the LDAP server.
Enable Binding CA Certificate check box	If checked, allows you to bind the LDAP CA certificate.
Timeout (0 - 180) seconds	The number of seconds the waits until the LDAP search operation times out. If the search operation times out, tries to connect to the next server listed on this tab, if one is available. **Note** The value you specify for this field could impact the overall time.
User Search Precedence	Allows you to specify the order of search between the local user database and LDAP user database. This can be one of the following: • **Local User Database** (Default setting) • **LDAP User Database**

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.

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 fields	

Name	Description
Server	The IP address of the 6 LDAP servers. If you are using Active Directory for LDAP, then servers 1, 2 and 3 are domain controllers, while servers 4, 5 and 6 are Global Catalogs. If you are not Active Directory for LDAP, then you can configure a maximum of 6 LDAP servers. **Note** You can provide the IP address of the host name as well.
Port	The port numbers for the servers. 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. 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 fields	
Source	Specifies how to obtain the domain name used for the DNS SRV request. It can be one of the following: • **Extracted**—specifies using domain name extracted-domain from the login ID • **Configured**—specifies using the configured-search domain. • **Configured-Extracted**—specifies using the domain name extracted from the login ID than the configured-search domain.
Domain to Search	A configured domain name that acts as a source for a DNS query. This field is disabled if the source is specified as **Extracted**.
Forest to Search	A configured forest name that acts as a source for a DNS query. 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	It can be one of the following: • **Anonymous**—requires NULL username and password. If this option is selected and the LDAP server is configured for Anonymous logins, then the user can gain access. • **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. • **Login Credentials**—requires the user credentials. If the bind process fails, the user is denied access. By default, the **Login Credentials** option is selected.
Binding DN	The distinguished name (DN) of the user. This field is editable only if you have selected **Configured Credentials** option as the binding method.
Password	The password of the user. This field is editable only if you have selected **Configured Credentials** option as the binding method.

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

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

Name	Description
Attribute	An LDAP attribute that contains the role and locale information for the user. This property is always a name-value pair. The system queries the user record for the value that matches this attribute name. The LDAP attribute 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**. **Note** If you do not specify this property, the user cannot login. Although the object is located on the LDAP server, it should be an exact match of the attribute that is specified in this field.
Nested Group Search Depth (1-128)	Parameter to search for an LDAP group nested within another defined group in an LDAP group map. The parameter defines the depth of a nested group search.

Step 8 (Optional) 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. If you check this box, 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:
	• **read-only**—A user with this role can view information but cannot make any changes.
	• **user**—A user with this role can perform the following tasks:
	  • View all information
	  • Manage the power control options such as power on, power cycle, and power off
	  • Launch the KVM console and virtual media
	  • Clear all logs
	  • Toggle the locator LED
	  • Set time zone
	  • Ping
	• **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 Overview

Cisco E-series 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** tab.

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	This field displays the status of the LDAP CA certificate download.
Export Status	This field displays the status of the LDAP CA certificate export.

Exporting an LDAP CA Certificate

Before you begin

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

You should have downloaded a signed LDAP CA Certificate before you can export it.

Procedure

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

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.

The **Export LDAP CA Certificate** dialog box appears.

Name	Description
Export to Remote Location	Selecting this option allows you to choose the certificate from a remote location and export it. Enter the following details: • • **TFTP Server** • **FTP Server** • **SFTP Server** • **SCP Server** • **HTTP Server** **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. 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 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. • **Path and Filename** field — The path and filename Cisco IMC should use when downloading the certificate from 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.
Export to Local Desktop	Selecting this option allows you to choose the certificate stored on a drive that is local to the computer and export it.

Step 5 Click **Export Certificate**.

Downloading an LDAP CA Certificate

Before you begin

- You must log in as a user with admin privileges to perform this action.
- You must enable Binding CA Certificate to perform this action.

Note Only CA certificates or chained CA certificates must be used in Cisco IMC. By default, CA certificate is in .cer format. If it is a chained CA certificate, then it needs to be converted to .cer format before downloading it to Cisco IMC.

Procedure

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

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

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

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

The **Download LDAP CA Certificate** dialog box appears.

Name	Description
Download from remote location radio button	Selecting this option allows you to choose the certificate from a remote location and download it. Enter the following details: • • **TFTP Server** • **FTP Server** • **SFTP Server** • **SCP Server** • **HTTP Server** **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. 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 LDAP CA certificate file should be stored. Depending on the setting in the **Download Certificate from** drop-down list, the name of the field may vary. • **Path and Filename** field — The path and filename should use when downloading 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.
Download through browser client radio button	Selecting this option allows you to navigate to the certificate stored on a drive that is local to the computer running the Cisco IMC GUI. When you select this option, Cisco IMC GUI displays a **Browse** button that lets you navigate to the file you want to import.
Paste Certificate content radio button	Selecting this option allows you to copy the entire content of the signed certificate and paste it in the **Paste certificate content** text field. **Note** Ensure the certificate is signed before uploading.
Download Certificate button	Allows you to download the certificate to the server.

Testing LDAP Binding

Before you begin

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

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.

Procedure

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

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.

The **Test LDAP CA Certificate Binding** dialog box appears.

Name	Description
Username field	Enter the user name.
Password field	Enter the corresponding password.

Step 5 Click **Test**.

Deleting an LDAP CA Certificate

Before you begin

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

Procedure

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

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

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

Step 4 Click the **Delete LDAP CA Certificate** link and click **OK** to confirm.

TACACS+ Server

TACACS+ is a security application that provides centralized validation of users attempting to gain access to a router or network access server. TACACS+ services are maintained in a database on a TACACS+ server running, typically, on a UNIX or Windows NT workstation. You must configure a TACACS+ server before you configure the TACACS+ features on your network access server and make them available.

On the TACACS+ server, ensure you configure Cisco attribute-value (AV) pair privilege level (priv-lvl) for Cisco Integrated Management Controller (CIMC) service for the minimum privilege level of administrators and operators.

Note In CIMC 3.2.10 release or earlier, users with no privilege level or users with a privilege level less than the operator's privilege level were considered as auditors with read-only permissions.

From CIMC 3.2.10 release, users with privilege level zero do not have permissions to login to CIMC.

After the software is downgraded to a version that supports 15 characters, ensure to change the shared key to 15 characters.

Restrictions for TACACS+ Server

The following restrictions are applicable for CIMC 3.2.10 release:

- CIMC 3.2.10 release supports connection to a single TACACS+ server. From CIMC 3.2.12 release onwards, 3 TACACS+ server configuration is supported.
- Users must first successfully complete TACACS+ authentication before proceeding to TACACS+ authorization.
- Accounting is not supported in CIMC 3.2.10 release. From CIMC 3.2.13 release onwards, TACACS accounting is supported. TACACS accounting will send all the configuration commands executed in CIMC GUI/CLI to TACACS server. Show commands executed in CIMC CLI/GUI will not be sent to TACACS server.
- TACACS+ and LDAP configurations are exclusive, only one configuration is enabled at a time
- Default time out is five seconds
- Default TCP port connection is 49
- Default login is PAP login where the username and password arrive at the network access server in a PAP protocol packet instead of details entered by the user.
- Supports only for IPv4
- Pre-shared key size is 15 characters. From CIMC 3.2.12 release onwards, shared key size is increased from 15 to 32.

  Supported special characters in shared secret key are: **! @ % ^ * - _ & + =**

Configure TACACS Server

Before you begin

Log in to CIMC as a user with admin privileges.

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** menu, click **TACACS** tab.

Step 4 In the TACACS Settings area, update the following properties:

Table 7:

Enable TACACS check box	If checked, user authentication and role authorization is performed first by the TACACS server, followed by user accounts that are not found in the local user database.
Admin priv	Sets the privilege level to the administrator. The privilege level 14 is assigned to the administrator role, and privilege level 9 is assigned to the operator role - a user with privilge level 14 or higher has admin privileges when the user logs into the system. By default, admin privilege is 15.
Oper priv	A user with privilege level 9 or higher has all privileges of an operator at the time of login. By default, operator privilege is 11.
TACACS Server	Enter the TACACS server IP address. This option provides three slots for storing IP addresses (TACACS Server IP 1, 2, and 3). After you set the TACACS Server IP, set the corresponding Pre-Shared key.
Pre-Shared Key	Sets the pre-shared key to initiate authentication with the server. This option provides three slots for Pre-Shared key (Shared Key 1,2, and 3). From CIMC 3.2.12 release onwards, the maximum length of the key is 32 characters.

TACACS Accounting check box	If enabled, TACACS Accounting functionality will be enabled and all the configuration commands executed in CIMC GUI/CLI will be sent to TACACS server. Show commands executed in CIMC CLI/GUI will not be sent to TACACS server.

Verify the TACACS+ Server Configuration for CIMC version 3.2.10 and 3.2.11

```
ENCS5406-FGL224331J8/tacacs#show detail
tacacs Settings:
Server domain name or IP address: 10.197.82.23
Enable tacacs: yes
shared-secret key: ******
admin-priv: 14
oper-priv: 10
```

Verify the TACACS+ Server Configuration for CIMC with Accounting

This example shows TACACS+ configuration with Accounting.

```
ENCS5406 # scope tacacs
ENCS5406 /tacacs # show detail
TACACS Settings:
Enable tacacs: yes
Enable tacacs cmd accounting: yes
Server1 domain name or IP addr: 192.168.1.1
Server2 domain name or IP addr: 192.168.1.2
Server3 domain name or IP addr: 192.168.1.3
Server1 Shared-secret key: ******
Server2 Shared-secret key: ******
Server3 Shared-secret key: ******
Admin-priv: 15
Oper-priv: 11
```

Viewing User Sessions

Procedure

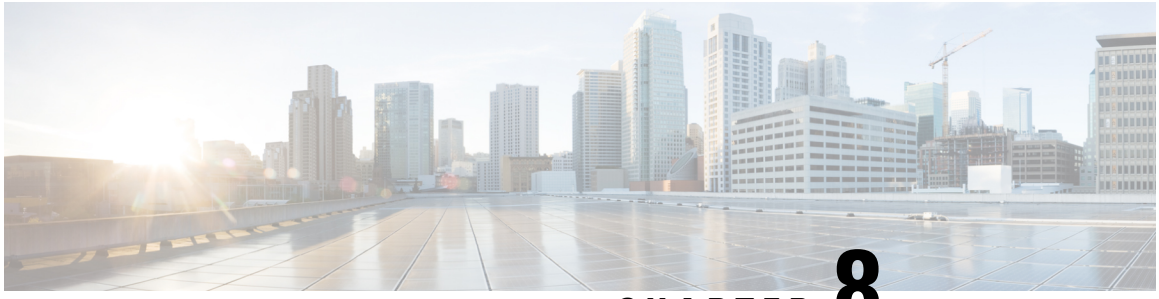
Step 1 In the **Navigation** pane, click the **Admin** menu.

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 information about current user sessions:

Name	Description
Session ID column	The unique identifier for the session.
User name 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: • **webgui**— indicates the user is connected to the server using the web UI. • **CLI**— indicates the user is connected to the server using CLI. • **serial**— indicates the user is connected to the server using the serial port.



CHAPTER 8

Configuring Chassis Related Settings

This chapter includes the following sections:

Managing Server Power

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 toolbar above the work pane, click the **Host Power** link.

Pinging a Hostname/IP Address from the Web UI

Before you begin

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

Procedure

Step 1 In the toolbar above the work pane, click the **Ping** icon.

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

Actions	Description
***Hostname/IP Address** 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.

Step 3 Click **Ping**.

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.

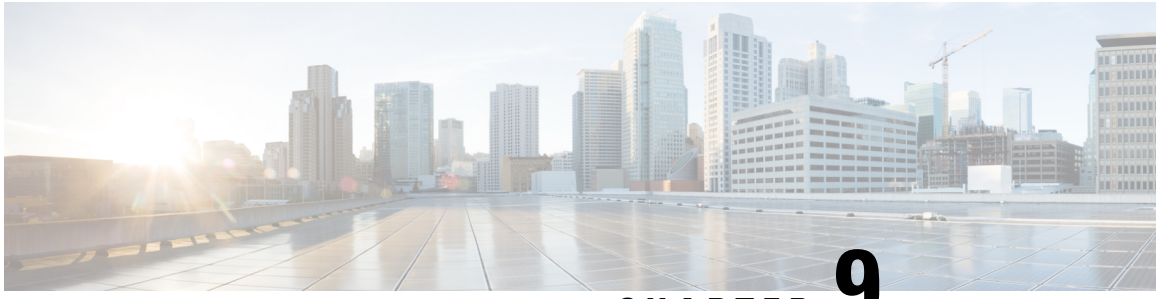
Step 2 In the **Chassis** menu, click **Summary**.

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

Select Timezone screen appears.

Step 4 In the **Select Timezone** pop-up screen, mouse over the map and click on the location to select your time zone or choose your time zone from the **Timezone** drop-down menu.

Step 5 Click **Save**.



CHAPTER 9

Configuring Network-Related Settings

This chapter includes the following sections:

Server NIC Configuration

Server NICs

NIC Mode

The NIC mode setting determines which ports can reach the Cisco IMC. The following network mode options are available, depending on your platform:

- **Dedicated**—The management port that is used to access the Cisco IMC.

Configuring Server NICs

Configure a server NIC when you want to set the NIC mode and NIC redundancy.

Before you begin

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

Procedure

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

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

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

Name	Description
NIC Mode drop-down list	The ports that can be used to access . This can be one of the following: • **Dedicated**—The management port that is used to access the . • **Shared LOM**—The LOM (LAN On Motherboard) ports are used to access the CIMC.
NIC Interface field	The network interface that is selected in the **NIC Mode** field.

Step 4 Click **Save Changes**.

Common Properties Configuration

Overview to Common Properties Configuration

Hostname

The Dynamic Host Configuration Protocol (DHCP) enhancement is available with the addition of the hostname to the DHCP packet, which can either be interpreted or displayed at the DHCP server side. The hostname, which is now added to the options field of the DHCP packet, sent in the DHCP DISCOVER packet that was initially sent to the DHCP server.

The default hostname of the server is EXXXX-YYYYYYYYYYY, where XXXX is the model number and YYYYYYYYYYY is the serial number of the server. This unique string acts as a client identifier, allows you to track and map the IP addresses that are leased out to from the DHCP server. The default serial number is provided by the manufacturer as a sticker or label on the server to help you identify the server.

Configuring Common Properties

Use common properties to describe your server.

Before you begin

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

Procedure

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

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

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

a) In the **Management Hostname** field, enter the name of the host.

By default, the hostname appears in EXXXX-YYYYYYYYYYY format, where XXXX is the model number and YYYYYYYYYYY is the serial number of the server.

Note If DHCP is enabled, the DHCP DISCOVER packet sent out will also carry the hostname in it.

Step 4 Click **Save Changes**.

Network Security Configuration

Network Security

The uses IP blocking as network security. IP blocking prevents the connection between a server or website and certain IP addresses or ranges of addresses. IP blocking effectively bans undesired connections from those computers to a website, mail server, or other Internet servers.

IP banning is commonly used to protect against denial of service (DoS) attacks. bans IP addresses by setting up an IP blocking fail count.

Configuring Network Security

Configure network security if you want to set up an IP blocking fail count.

Before you begin

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

Procedure

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

Step 2 In the **Networking** pane, click **Network Security**.

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

Name	Description
Enable IP Blocking check box	Check this box to enable IP blocking.
IP Blocking Fail Count field	The number of times a user can attempt to log in unsuccessfully before the system locks that user out for a specified length of time. The number of unsuccessful login attempts must occur within the time frame specified in the **IP Blocking Fail Window** field. Enter an integer between 3 and 10.
IP Blocking Fail Window field	The length of time, in seconds, in which the unsuccessful login attempts must occur in order for the user to be locked out. Enter an integer between 60 and 120.

Name	Description
IP Blocking Penalty Time field	The number of seconds the user remains locked out if they exceed the maximum number of login attempts within the specified time window. Enter an integer between 300 and 900.

Step 4 In the **IP Filtering** area, update the following properties:

Name	Description
Enable IP Filtering check box	Check this box to enable IP filtering.
IP Filter fields	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)	Click the [+] ("Plus" button) to add a new filter. You can configure upto 20 filters.

Note If the filters are removed from the middle, filters will be re-arranged automatically.

Step 5 Click **Save Changes**.

Network Time Protocol Settings

Network Time Protocol Service Setting

By default, when 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, synchronizes the time with the configured NTP server. The NTP service can be modified only through .

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

Configuring Network Time Protocol Settings

Configuring NTP disables the IPMI **Set SEL time** command.

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 **Networking**.

Step 3 In the **Networking** pane, click **NTP Setting**.

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

Name	Description
Enable NTP	Check this box to enable the NTP service.
Server 1	The IP/DNS address of one of the four servers that act as an NTP server or the time source server.
Server 2	The IP/DNS address of one of the four servers that act as an NTP server or the time source server.
Server 3	The IP/DNS address of one of the four servers that act as an NTP server or the time source server.
Server 4	The IP/DNS address of one of the four servers that act as an NTP server or the time source server.
Status message	Indicates whether or not the server is able to synchronize its time with the remote NTP server. This can be one of the following: • **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. • **unsynchronized** — When the NTP service is enabled and an unknown or unreachable server is added. • **NTP service disabled** — When the NTP service is disabled.

Step 5 Click **Save Changes**.

CHAPTER 10

Managing Storage Adapters

This chapter includes the following sections:

Managing Storage Adapters

Self Encrypting Drives (Full Disk Encryption)

Cisco IMC supports self encrypting drives (SED). A special hardware in the drives encrypts incoming data and decrypts outgoing data in real-time. This feature is also called Full Disk Encryption (FDE).

The data on the drive is encrypted on its way into the drive and decrypted on its way out. However, if you lock the drive, no security key is required to retrieve the data.

When a drive is locked, an encryption key is created and stored internally. All data stored on this drive is encrypted using that key, and stored in encrypted form. Once you store the data in this manner, a security key is required in order to un-encrypt and fetch the data from the drive. Unlocking a drive deletes that encryption key and renders the stored data unusable. This is called a Secure Erase. The FDE comprises a key ID and a security key.

The FDE feature supports the following operations:

- Enable and disable security on a controller
- Create a secure virtual drive
- Secure a non-secure drive group
- Unlock foreign configuration drives
- Enable security on a physical drive (JBOD)
- Clear secure SED drives
- Clear secure foreign configuration

Scenarios to consider While Configuring Controller Security in a Dual SIOC Environment

Note Dual SIOC connectivity is available only on some servers.

Controller security can be enabled, disabled, or modified independently. However, local and remote key management applies to all the controllers on the server. Therefore security action involving switching the key management modes must be performed with caution. In a scenario where both controllers are secure, and you decide to move one of the controllers to a different mode, you need to perform the same operation on the other controller as well.

Consider the following two scenarios:

- Scenario 1—Key management is set to remote; both controllers are secure and use remote key management. If you now wish to switch to local key management, switch the key management for each controller and disable remote key management.
- Scenario 2—Key management is set to local; both controllers are secure and use local key management. If you now wish to switch to remote key management, enable remote key management and switch the key management for each controller.

If you do not modify the controller security method on any one of the controllers, it renders the secure key management in an unsupported configuration state.

Creating Virtual Drive from Unused Physical Drives

Before you begin

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

Procedure

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

Step 2 In the **Storage** menu, click the appropriate LSI MegaRAID controller.

Step 3 In the **Actions** area, click **Create Virtual Drive from Unused Physical Drives**.

The **Create Virtual Drive from Unused Physical Drives** dialog box displays.

Step 4 In the **Create Virtual Drive from Unused Physical Drives** dialog box, select the RAID level for the new virtual drives:

This can be one of the following:

- **Raid 0**—Simple striping.
- **Raid 1**—Simple mirroring.
- **Raid 5**—Striping with parity.
- **Raid 6**—Striping with two parity drives.
- **Raid 10**—Spanned mirroring.
- **Raid 50**—Spanned striping with parity.

- **Raid 60**—Spanned striping with two parity drives.

Step 5 In the **Create Drive Groups** area, choose one or more physical drives to include in the group.

Use the >> button to add the drives to the **Drive Groups** table. Use the << button to remove physical drives from the drive group.

Note The size of the smallest physical drive in the drive group defines the maximum size used for all the physical drives. To ensure maximum use of space for all physical drives, it is recommended that the size of all the drives in the drive group are similar.

Note Cisco IMC manages only RAID controllers and not HBAs attached to the server.

Step 6 In the **Virtual Drive Properties** area, update the following properties:

Name	Description
Virtual Drive Name field	The name of the new virtual drive you want to create.
Read Policy drop-down list	The read-ahead cache mode.
Cache Policy drop-down list	The cache policy used for buffering reads.
Strip Size drop-down list	The size of each strip, in KB.
Write Policy drop-down list	This can be one of the following • **Write Through**— Data is written through the cache and to the physical drives. Performance is improved, because subsequent reads of that data can be satisfied from the cache. • **Write Back**— Data is stored in the cache, and is only written to the physical drives when space in the cache is needed. Virtual drives requesting this policy fall back to **Write Through** caching when the BBU cannot guarantee the safety of the cache in the event of a power failure. • **Write Back Bad BBU**—With this policy, write caching remains **Write Back** even if the battery backup unit is defective or discharged.
Disk Cache Policy drop-down list	This can be one of the following • **Unchanged**— The disk cache policy is unchanged. • **Enabled**— Allows IO caching on the disk. • **Disabled**— Disallows disk caching.
Access Policy drop-down list	This can be one of the following • **Read Write**— Enables host to perform read-write on the VD. • **Read Only**— Host can only read from the VD. • **Blocked**— Host can neither read nor write to the VD.

Name	Description
Size field	The size of the virtual drive you want to create. Enter a value and select one of the following units: • MB • GB • TB

Step 7 Click the **Generate XML API Request** button to generate an API request.

Step 8 Click **Close**.

Step 9 Click **Create Virtual Drive**.

Creating Virtual Drive from an Existing Drive Group

Before you begin

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

Procedure

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

Step 2 In the **Storage** menu, click the appropriate LSI MegaRAID controller.

Step 3 In the **Actions** area, click **Create Virtual Drive from an Existing Virtual Drive Group**.

The **Create Virtual Drive from an Existing Virtual Drive Group** dialog box displays.

Step 4 In the **Create Virtual Drive from an Existing Virtual Drive Group** dialog box, select the virtual drive whose drive group you want to use to create a new virtual drive.

Step 5 In the **Virtual Drive Properties** area, update the following properties:

Name	Description
Virtual Drive Name field	The name of the new virtual drive you want to create.
Read Policy drop-down list	The read-ahead cache mode.
Cache Policy drop-down list	The cache policy used for buffering reads.
Strip Size drop-down list	The size of each strip, in KB.

Name	Description
Write Policy drop-down list	This can be one of the following • **Write Through**— Data is written through the cache and to the physical drives. Performance is improved, because subsequent reads of that data can be satisfied from the cache. • **Write Back**— Data is stored in the cache, and is only written to the physical drives when space in the cache is needed. Virtual drives requesting this policy fall back to **Write Through** caching when the BBU cannot guarantee the safety of the cache in the event of a power failure. • **Write Back Bad BBU**—With this policy, write caching remains **Write Back** even if the battery backup unit is defective or discharged.
Disk Cache Policy drop-down list	This can be one of the following • **Unchanged**— The disk cache policy is unchanged. • **Enabled**— Allows IO caching on the disk. • **Disabled**— Disallows disk caching.
Access Policy drop-down list	This can be one of the following • **Read Write**— Enables host to perform read-write on the VD. • **Read Only**— Host can only read from the VD. • **Blocked**— Host can neither read nor write to the VD.
Size field	The size of the virtual drive you want to create. Enter a value and select one of the following units: • MB • GB • TB

Step 6 Click the **Generate XML API Request** button to generate an API request.

Step 7 Click **Close**.

Step 8 Click **Create Virtual Drive**.

Setting a Virtual Drive to Transport Ready State

You can move a virtual drive from one MegaRAID controller to another using the **Set Transport Ready** feature. This allows all the pending IOs of the virtual drive to complete their activities, hide the virtual drive from the operating system, flush cache, pause all the background operations, and save the current progress in

disk data format, allowing you to move the drive. When you move a virtual drive, all other drives belonging to the same drive group inherit the same change as the moved drive.

When the last configured physical drive on the group is removed from the current controller, the drive group becomes foreign and all foreign configuration rules apply to the group. However, the Transport Ready feature does not change any foreign configuration behavior.

You can also clear a virtual drive from the Transport Ready state. This makes the virtual drive available to the operating systems.

Following restrictions apply to a transport ready virtual drive:

- Only a maximum of 16 transport ready drive groups are currently supported.
- This feature is not supported on high availability.
- A virtual drive cannot be set as transport ready under these conditions:
  - When a virtual drive of a drive group is being reconstructed
  - When a virtual drive of a drive group contains a pinned cache
  - When a virtual drive of a drive group is marked as cacheable or associated with a cachecade virtual drive
  - If a virtual drive is a cachecade virtual drive
  - If a virtual drive is offline
  - If a virtual drive is a bootable virtual drive

Setting a Virtual Drive as Transport Ready

Before you begin

- You must log in with admin privileges to perform this task.
- The virtual drive must be in optimal state to enable transport ready.

Procedure

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

Step 2 On the **Storage** menu, click the appropriate LSI MegaRAID Controller.

Step 3 On the **Work** pane, click the **Virtual Drive Info** tab.

Step 4 In the **Virtual Drives** area, choose the drive that you want set as transport ready.

Step 5 In the **Actions** area, click **Set Transport Ready**.

The **Set Transport Ready** dialog box displays.

Step 6 Update the following properties in the dialog box:

Name	Description
Initialize Type drop-down list	Allows you to select the initialization type using which you can set the selected virtual drive as transport ready. This can be one of the following: • **Exlude All**— Excludes all the dedicated hot spare drives. • **Include All**— Includes any exclusively available or shared dedicated hot spare drives. • **Include Dedicated Hot Spare Drive**— Includes exclusive dedicated hot spare drives.
Set Transport Ready button	Sets the selected virtual drive as transport ready.
Cancel button	Cancels the action.

Note When you set a virtual drive to transport ready all the physical drives associated with it are displayed as **Ready to Remove**.

Clearing a Virtual Drive from Transport Ready State

Before you begin

- You must log in with admin privileges to perform this task.
- The virtual drive must be transport ready.

Procedure

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

Step 2 On the **Storage** menu, click the appropriate LSI MegaRAID controller.

Step 3 On the **Work** pane, click the **Virtual Drive Info** tab.

Step 4 In the **Virtual Drives** area, choose the drive to set as transport ready.

Step 5 In the **Actions** area, click **Clear Transport Ready**.

This reverts the selected transport ready virtual drive to its original optimal state.

Clearing Foreign Configuration

Important This task clears all foreign configuration on the controller. Also, all configuration information from all physical drives hosting foreign configuration is deleted. This action cannot be reverted.

Before you begin

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

Procedure

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

Step 2 On the **Storage** menu, click the appropriate LSI MegaRAID controller.
In the **RAID Controller** area, the **Controller Info** tab displays by default.

Step 3 In the **Actions** area, click **Clear Foreign Config**.

Step 4 Click **OK** to confirm.

Clearing Controller Configuration

Before you begin

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

Procedure

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

Step 2 In the **Storage** menu, click the appropriate LSI MegaRAID controller.

Step 3 In the **Controller Info** area, click **Clear All Configuration**.

Step 4 Click **OK** to confirm.

This clears the existing controller configuration.

Preparing a Drive for Removal

Note You can perform this task only on physical drives that display the **Unconfigured Good** status.

Before you begin

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

Procedure

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

Step 2 On the **Storage** menu, click the appropriate LSI MegaRAID controller.

Step 3 In the **RAID Controller** area, click the **Physical Drive Info** tab.

Step 4 In the **Physical Drives** area, select the drive you want to remove.

Step 5 In the **Actions** area, click **Prepare for Removal**.

Step 6 Click **OK** to confirm.

Undo Preparing a Drive for Removal

Before you begin

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

Procedure

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

Step 2 On the **Storage** menu, click the appropriate LSI MegaRAID controller.

Step 3 On the **RAID Controller** area, click the **Physical Drive Info** tab.

Step 4 In the **Physical Drives** area, select a drive with a status of **Ready to Remove**.

Step 5 In the **Actions** area, click **Undo Prepare for Removal**.

Step 6 Click **OK** to confirm.

Making a Dedicated Hot Spare

Before you begin

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

Procedure

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

Step 2 On the **Storage** menu, click the appropriate LSI MegaRAID controller.

Step 3 On the **RAID Controller** area, click the **Physical Drive Info** tab.

Step 4 In the **Physical Drives** area, select an unconfigured good drive you want to make a dedicated hot spare.

Step 5 In the **Actions** area, click **Make Dedicated Hot Spare**.

The **Make Dedicated Hot Spare** dialog box displays.

Step 6 In the **Virtual Drive Details** area, update the following properties:

Name	Description
Virtual Drive Number drop-down list	Select the virtual drive to which you want to dedicate the physical drive as hot spare.

Name	Description
Virtual Drive Name field	The name of the selected virtual drive.
Make Dedicated Hot Spare button	Creates the dedicated hot spare.
Cancel button	Closes the dialog box without saving any changes made while the dialog box was open.

Step 7 Click **Make Dedicated Hot Spare** to confirm.

Making a Global Hot Spare

Before you begin

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

Procedure

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

Step 2 On the **Storage** menu, click the appropriate LSI MegaRAID controller.

Step 3 In the **RAID Controller** area, click the **Physical Drive Info** tab.

Step 4 In the **Physical Drives** area, select an unconfigured good drive you want to make a global hot spare.

Step 5 In the **Actions** area, click **Make Global Hot Spare**.

Removing a Drive from Hot Spare Pools

Before you begin

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

Procedure

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

Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.

Step 3 On the **Work** pane, click the **Physical Drive Info** tab.

Step 4 In the **Physical Drives** area, select the global or dedicated hot spare you want to remove from the hot spare pools.

Step 5 In the **Actions** area, click **Remove From Hot Spare Pools**.

Initializing a Virtual Drive

All data on a virtual drive is lost when you initialize the drive. Before you run an initialization, back up any data on the virtual drive that you want to save.

Before you begin

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

Procedure

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

Step 2 On the **Storage** menu, click the appropriate LSI MegaRAID controller.

Step 3 In the **RAID Controller** area, click the **Virtual Drive Info** tab.

Step 4 In the **Virtual Drives** area, choose the drive that you want to initialize.

Step 5 In the **Actions** area, click **Initialize**.

The **Initialize Virtual Drive** dialog box displays.

Step 6 Choose the type of initialization you want to use for the virtual drive.

This can be one of the following:

- **Fast Initialize**—This option allows you to start writing data to the virtual drive immediately.
- **Full Initialize**—A complete initialization is done on the new configuration. You cannot write data to the new virtual drive until the initialization is complete.

Step 7 Click **Initialize VD** to initialize the drive, or **Cancel** to close the dialog box without making any changes.

Step 8 To view the status of the task running on the drive, in the **Operations** area, click **Refresh**.

The following details are displayed:

Name	Description
Operation	Name of the operation that is in progress on the drive.
Progress in %	Progress of the operation, in percentage complete.
Elapsed Time in secs	The number of seconds that have elapsed since the operation began.

Set as Boot Drive

Before you begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Storage** menu.
Step 2 On the **Storage** menu, click the appropriate LSI MegaRAID controller.
Step 3 In the **RAID Controller** area, click the **Virtual Drive Info** tab.
Step 4 In the **Virtual Drives** area, choose the drive from which the controller must boot.
Step 5 In the **Actions** area, click **Set as Boot Drive**.
Step 6 Click **OK** to confirm.

Deleting a Virtual Drive

Important This task deletes a virtual drive, including the drives that run the booted operating system. So back up any data that you want to retain before you delete a virtual drive.

Before you begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Storage** menu.
Step 2 On the **Storage** menu, click the appropriate LSI MegaRAID controller.
Step 3 In the **RAID Controller** area, click the **Virtual Drive Info** tab.
Step 4 In the **Virtual Drives** area, select the virtual drive you want to delete.
Step 5 In the **Actions** area, click **Delete Virtual Drive**.
Step 6 Click **OK** to confirm.

Hiding a Virtual Drive

Before you begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Storage** menu.
Step 2 On the **Storage** menu, click the appropriate LSI MegaRAID controller.
Step 3 On the **RAID Controller** area, click the **Virtual Drive Info** tab.

Step 4 In the **Virtual Drives** area, select the virtual drive you want to hide.

Step 5 In the **Actions** area, click **Hide Drive**.

Step 6 Click **OK** to confirm.

Starting Learn Cycles for a Battery Backup Unit

Before you begin

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

Procedure

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

Step 2 On the **Storage** menu, click the appropriate LSI MegaRAID controller.

Step 3 In the **RAID Controller** area, click the **Battery Backup Unit** tab.

Step 4 From the **Actions** pane, click **Start Learn Cycle**.

A dialog prompts you to confirm the task.

Step 5 Click **OK**.

Viewing Storage Controller Logs

Before you begin

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

Procedure

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

Step 2 On the **Storage** menu, click the appropriate LSI MegaRAID controller.

Step 3 In the **RAID Controller** area, click **Storage Log** tab and review the following information:

Name	Description
Time column	The date and time the event occurred.

Name	Description
Severity column	The event severity. This can be one of the following: • Emergency • Alert • Critical • Error • Warning • Notice • Informational • Debug
Description column	A description of the event.

Compatibility of UCS-E M3 Module with 4K Native Drives

Data on a disk has historically been relegated to a standard 512 bytes of data per sector. 4K Native (4Kn) Drives or Advanced Format (AF) refers to the next generation in default media allocation size.

4K-sized sectors provide quicker paths to higher areal densities and hard drive capacities as well as more robust error correction. With the ever-increasing demand for higher density storage and with file sizes ever increasing, 4Kn drives are the only option available because 4Kn drives are the most cost-efficient. For example, 512 bytes goes into 4K exactly 8 times. This means that as long as we are aligned in storage parlance, we minimize the amount of unnecessary disk activity.

The software emulation layer uses the 4Kn drives with legacy OS, applications, and existing VMs to run on newer 4Kn drives. Readiness of the support for 4 KB logical sectors within operating systems differs among their types, vendors and versions. For example, Microsoft Windows supports 4Kn drives since Windows 8 and Windows Server 2012.

Note Ensure your application is 4Kn ready to avoid mismatch of what is intended and what actually occurs. The most critical are applications like databases.

Some of the benefits of 4Kn drives over 512 sector size drives are:

- Higher capacity and improved performance from the more optimized placement of data on the drive.
- Efficient space utilization with optimized meta-data giving up to 10% more available data.
- Improved drive reliability and error correction with larger meta-data by increasing the ECC block from 50 to 100 bytes. This provides a much-needed improvement in error correction efficiency.

Limitations of 4Kn Drives

- Only local SAS, SATA HDDs are supported
- Ensure to use VMFS6
- The BIOS must be configured in full UEFI mode while booting from 4Kn drives
- 4Kn SSD, NVMe, and RDM to GOS are not supported
- Third party multi-pathing plugins are not supported

How to use 4Kn Drives as Boot Drives on UCS-E M3 Modules

- Set boot order rules in CIMC's BIOS configuration to 'loose'.
- Check the box for UEFI secure boot in CIMC's BIOS boot order configuration or scope BIOS in CLI. This sets the module in full UEFI mode on next reboot, so that no legacy boot options appears.
- Map the OS installation image in vKVM or the host image mapping in CIMC (or use physical DVD). If you are installing VMware ESXi, use the ESXi 6.7 version or later.
- Reboot the server and press F6 to enter boot override menu when the logo screen appears.
- Select the UEFI option corresponding to your installation media. For instance, "UEFI: CIMC-mapped vDVD".
- When you start the OS installation, check for the 4Kn HDD, and then start the installation on the 4Kn drive.

CHAPTER 11

Configuring Communication Services

This chapter includes the following sections:

Configuring HTTP

Before you begin

You must log in as a user with admin privileges to 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
HTTP/S Enabled check box	Whether HTTP and HTTPS are enabled on the .
Redirect HTTP to HTTPS Enabled check box	If enabled, all attempts to communicate via HTTP are redirected to the equivalent HTTPS address. We strongly recommend that you enable this option if you enable HTTP.
HTTP Port field	The port to use for HTTP communication. The default is 80.
HTTPS Port field	The port to use for HTTPS communication. The default is 443

Name	Description
Session Timeout field	The number of seconds to wait between HTTP requests before the times out and terminates the session. Enter an integer between 60 and 10,800. The default is 1,800 seconds.
Max Sessions field	The maximum number of concurrent HTTP and HTTPS sessions allowed on the . This value may not be changed.
Active Sessions field	The number of HTTP and HTTPS sessions currently running on the .

Step 4 Click **Save Changes**.

Configuring SSH

Before you begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Admin** 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	Whether SSH is enabled on the .
SSH Port field	The port to use for secure shell access. The default is 22.
SSH Timeout field	The number of seconds to wait before the system considers an SSH request to have timed out. Enter an integer between 60 and 10,800. The default is 1,800 seconds.
Max Sessions field	The maximum number of concurrent SSH sessions allowed on the . This value may not be changed.
Active Sessions field	The number of SSH sessions currently running on the .

Step 4 Click **Save Changes**.

Configuring Redfish

Before you begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Admin** 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	Whether Redfish is enabled on the .
Max Sessions field	The number of maximmum sessions.
Active Sessions field	The number of active sessions.

Step 4 Click **Save Changes**.

Configuring XML API

XML API for

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

Enabling the XML API

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	Whether API access is allowed on this server.
Max Sessions field	The maximum number of concurrent API sessions allowed on the . This value may not be changed.
Active Sessions field	The number of API sessions currently running on the .

Step 4 Click **Save Changes**.

Configuring IPMI

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 a Baseboard Management Controller (BMC) and resides on the server motherboard. The BMC links to a main processor and other on-board elements using a simple serial bus.

During normal operations, IPMI lets a server operating system obtain information about system health and control system hardware. For example, IPMI enables the monitoring of sensors, such as temperature, fan speeds and voltages, for proactive problem detection. If server temperature rises above specified levels, the server operating system can direct the BMC to increase fan speed or reduce processor speed to address the problem.

Configuring IPMI over LAN

Configure IPMI over LAN when you want to manage the with IPMI messages.

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 for BMC 1, BMC 2, CMC 1, or CMC 2:

Name	Description
Enabled check box	Whether IPMI access is allowed on this server.

Name	Description
Privilege Level Limit drop-down list	The highest privilege level that can be assigned to an IPMI session on this server. This can be one of the following: • **read-only**—IPMI users can view information but cannot make any changes. If you select 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. • **user**—IPMI users can perform some functions but cannot perform administrative tasks. If you select this option, IPMI users with the "Administrator" or "Operator" user role can create user and read-only sessions on this server. • **admin**—IPMI users can perform all available actions. If you select 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 SNMP

SNMP

The Cisco UCS E-Series Rack-Mount 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 **Communications Services** pane, click the **SNMP** tab.

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

Name	Description
SNMP Enabled check box	Whether this server sends SNMP traps to the designated host. **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. Enter a string up to 18 characters.
SNMP Community Access drop-down list	This can be one of the following: • **Disabled** — This option blocks access to the information in the inventory tables. • **Limited** — This option provides partial access to read the information in the inventory tables. • **Full** — This option provides full access to read the information in the inventory tables. **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. Enter a string up to 18 characters. **Note** This field is visible only for SNMP v1 and v2c users. SNMP v3 users need to use SNMP v3 credentials.
System Contact field	The system contact person responsible for the SNMP implementation. 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. 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 BMC serial number.

Step 5 Click **Save Changes**.

What to do next

Configure SNMP trap settings.

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 **Communications Services** pane, click the **SNMP** tab.

Step 4 Click on **Trap Destinations** tab.

Step 5 In the **Trap Destinations** area, you can perform one of the following:

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

Note If the fields are not highlighted, select **Enabled**.

Step 6 In the **Trap Details** dialog box, complete the following fields:

Name	Description
ID field	The trap destination ID. This value cannot be modified.
Enabled	If checked, then this trap is active on the server.
Version drop-down list	The SNMP version and model used for the trap. This can be one of the following: • **V2** • **V3**
Type	The type of trap to send. This can be one of the following: • **Trap**: If this option is chosen, the trap will be sent to the destination but you do not receive any notifications. • **Inform**: You can choose this option only for V2 users. If chosen, you will receive a notification when a trap is received at the destination.
User drop-down list	The drop-down list displays all available users, select a user from the list.

Step 7 Click **Save Changes**.

Step 8 If you want to delete a trap destination, select the row and click **Delete**.

Click **OK** in the delete confirmation prompt.

Note From CIMC 3.2.13 release, SNMP trap support for storage disk removal or insertion is supported in ENCS.

Sending a Test SNMP 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 **SNMP**.

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

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

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

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

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 **Communications Services** pane, click the **SNMP** tab.

Step 4 In the **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 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 **Communications Services** pane, click the **SNMP** tab.

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

- Select an existing user from the table and click **Modify User**.
- Select 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.
Name field	The SNMP username. Enter between 1 and 31 characters or spaces. **Note** 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: • **no auth, no priv**—The user does not require an authorization or privacy password. • **auth, no priv**—The user requires an authorization password but not a privacy password. If you select this option, enables the Auth fields described below. • **auth, priv**—The user requires both an authorization password and a privacy password. If you select this option, enables the Auth and Privacy fields.
Auth Type drop-down	The authorization type. This can be one of the following: • **MD5** • **SHA**
Auth Password field	The authorization password for this SNMP user. Enter between 8 and 64 characters or spaces. **Note** 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: • **DES** • **AES**
Privacy Password field	The privacy password for this SNMP user. Enter between 8 and 64 characters or spaces. **Note** 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, select the user and click **Delete User**.

Click **OK** in the delete confirmation prompt.

CHAPTER 12

Managing Firmware

This chapter includes the following sections:

Cisco IMC Firmware

Note If you are running CIMC version 2.2.x, first upgrade to version 2.3.2 and then upgrade to 3.2.x.

You can manage the following firmware components from a single page in the web UI:

- 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 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:

- BMC
- BIOS
- CMC

Firmware for the Hard Disk Drive (HDD) can also be installed from the same interfaces as the adapter firmware mentioned above.

Viewing Firmware Components

Procedure

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

Step 2 In the **General** tab's **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 select which available firmware version you would like to activate on the server. **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**. **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.
Bootloader Version column	The bootloader version associated with the boot-loader software of the component.
Status column	The status of the firmware activation on this server.
Progress in % 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, BMC 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, select a component from the **Component** column and click **Update**.

The **Update Firmware** dialog box appears.

Step 3 Review the following information in the dialog box:

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 select the file, click **Install Firmware**.

Step 6 To update the firmware using remote server, select 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.

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

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

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, select a component from the **Component** column and click **Activate**.

The **Activate Firmware** dialog box appears.

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

Step 4 Click **Activate Firmware**.

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

Important While the activation is in progress, do not:

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

CHAPTER 13

Viewing Faults and Logs

This chapter includes the following sections:

Faults Summary

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:

Table 8: Actions Area

Name	Description
Total	Displays the total number of rows in the Fault Entries table.
Column drop-down list	Allows you to choose the columns you wish to be displayed.

Name	Description
Show drop-down list	Customize the way you want to view fault entries using filters. These can be: • **Quick Filter** - Default view. • **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. Click **Go** to view the entries matching the filter criteria that you set. Click the **Save** icon to save the filter criteria that you set. This becomes a user-defined filter which you can use later. **Note** The user-defined filter appears in the **Manage Preset Filters** dialog box. • **All** - Displays all entries • **Manage Preset Filters** - Displays user-defined filters. You can edit or remove the user-defined filter from this dialog box. • **List of pre-defined filters** - Displays the system-defined filters. **Note** You can use the **Filter** icon to hide or unhide the filter fields.

Table 9: Fault Entries Area

Name	Description
Time	The time when the fault occurred.
Severity	This can be one of the following: • **Cleared** - A fault or condition was cleared. • **Critical** • **Info** • **Major** • **Minor** • **Warning**
Code	The unique identifier assigned to the fault.

Name	Description
DN	The distinguished name (DN) is a hierarchical representation of the device endpoint and its instance on the server.
Probable Cause	The unique identifier associated with the event that caused the fault.
Description	More information about the fault. It also includes a proposed solution.

Fault History

Viewing Faults 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

Table 10: Actions Area

Name	Description
Total	Displays the total number of rows in the Fault History table.
Column drop-down list	Allows you to choose the columns you wish to be displayed.

Name	Description
Show drop-down list	Customize the way you want to view fault history entries using filters. These can be: • **Quick Filter** - Default view. • **Advanced Filter** - Filter options to display the 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. Click **Go** to view the entries matching the filter criteria that you set. Click the **Save** icon to save the filter criteria that you set. This becomes a user-defined filter which you can use later. **Note** The user-defined filter appears in the **Manage Preset Filters** dialog box. • **All** - Displays all entries • **Manage Preset Filters** - Displays user-defined filters. You can edit or remove the user-defined filter from this dialog box. • **List of pre-defined filters** - Displays the system-defined filters. **Note** You can use the **Filter** icon to hide or unhide the filter fields.

Table 11: Faults History Area

Name	Description
Time	The time when the fault occurred.

Name	Description
Severity	This can be one of the following: • **Emergency** • **Alert** • **Critical** • **Error** • **Warning** • **Notice** • **Informational** • **Debug**
Source	The software module that logged the event.
Probable Cause	The unique identifier associated with the event that caused the fault.
Description	More information about the fault. It also includes a proposed solution.

What to do next

System Event Log

Viewing System Event Logs

Procedure

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

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

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

Table 12: Actions Area

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

Name	Description
Total	Displays the total number of rows in the System Event Log table.
Column drop-down list	Allows you to choose the columns you wish to be displayed.
Show drop-down list	Customize the way you want to view events using filters. These can be: • **Quick Filter** - Default view. • **Advanced Filter** - Filter options to display the events 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. Click **Go** to view the entries matching the filter criteria that you set. Click the **Save** icon to save the filter criteria that you set. This becomes a user-defined filter which you can use later. **Note** The user-defined filter appears in the **Manage Preset Filters** dialog box. • **All** - Displays all entries • **Manage Preset Filters** - Displays user-defined filters. You can edit or remove the user-defined filter from this dialog box. • **List of pre-defined filters** - Displays the system-defined filters. **Note** You can use the **Filter** icon to hide or unhide the filter fields.

Table 13: System Event Log Table

Name	Description
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.

Logging Controls

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:

Remote Logging

Name	Description
Enabled check box	If checked, the Cisco IMC sends log messages to the Syslog server named in the **IP Address** field.
Host Name/IP Address field	The address of the Syslog server on which the Cisco IMC log should be stored. 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.
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: • **Emergency** • **Alert** • **Critical** • **Error** • **Warning** • **Notice** • **Informational** • **Debug**

Note The Cisco IMC does not remotely log any messages with a severity below the selected severity. For example, if you select **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.

Local Logging

This area displays only the **Minimum Severity to Report** drop-down list as shown in the table above. You can specify the lowest level of messages to be included in the local log

What to do next

Sending the Cisco IMC Log to a Remote Server

You can configure profiles for one or two remote syslog servers to receive log entries.

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.

Procedure

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

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

Step 3 In either of the **Remote Syslog Server** areas, complete the following fields:

Name	Description
Enabled check box	If checked, the Cisco IMC sends log messages to the Syslog server named in the **IP Address** field.
Host Name/IP Address field	The address of the Syslog server on which the Cisco IMC log should be stored. 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.

Step 4 (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 select one of the following, in decreasing order of severity:

- **Emergency**
- **Alert**
- **Critical**
- **Error**

- **Warning**
- **Notice**
- **Informational**
- **Debug**

Note does not remotely log any messages with a severity below the selected severity. For example, if you select **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 5 Click **Save Changes**.

Configuring the Cisco IMC Log Threshold

Before you begin

Procedure

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

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

Step 3 Required: In the **Local Logging** area, use the **Minimum Severity to Report** drop-down list to specify the lowest level of messages that will be included in the log.

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

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

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

Sending a Test Cisco IMC 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.

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 and Logs** pane, click the **Logging Controls** tab.

Step 4 In the **Action** area, click **Send Test Syslog**.

A test log is sent to the configured remote servers.

CHAPTER 14

Server Utilities

This chapter includes the following sections:

Exporting Technical Support Data

Exporting Technical Support Data

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

Procedure

Step 1 In the **Navigation** pane, click the **Admin** 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 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 In the **Download Technical Support Data to Local File** dialog box, complete the following fields:

Name	Description
Generate Technical Support Data radio button	disables this radio button when there is no technical support data file to download. 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.
Download to local file radio button	enables this radio button when a technical support data file is available to download. To download the existing file, select this option and click **Download**. **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 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..

What to do next

Provide the generated report file to Cisco TAC.

Resetting to Factory Default

On rare occasions, such as an issue with the current running firmware or troubleshooting a server, you might require to reset 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 BMC 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 reset the server components to factory defaults.

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 In the **Reset to Factory Default** dialog box, review the following information:

Step 5 Click **Reset** to reset the selected components to the factory-default settings.

A reboot of Cisco IMC, while the host is performing BIOS POST (Power on Self Test) or is in EFI shell, powers down the host for a short amount of time. Cisco IMC powers on when it is ready. Upon restart, the network configuration mode is set to **Cisco Card** mode by default.

Exporting and Importing the Cisco IMC Configuration

Exporting and Importing the 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 - BIOS Parameters

  Note Precision boot is not supported.

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

Exporting the Cisco IMC 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 In the **Export Configuration** dialog box, complete the following fields:

Name	Description
Export To drop-down list	The location where you want to save the XML configuration file. This can be one of the following: • **Local**: Select this option and click **Export** to save the XML configuration file to a drive that is local to the computer running the .. When you select this option, displays a **File Download** dialog box that lets you navigate to the location to which the configuration file should be saved. • **Remote Server**: Select this option to import the XML configuration file from a remote server. When you select this option, displays the remote server fields.
Export To drop-down list	The remote server type. This can be one of the following: • **TFTP Server** • **FTP Server** • **SFTP Server** • **SCP Server** • **HTTP Server** **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. 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	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	The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP.
Passphrase	The passphrase that uses the AES256 algorithm to encrypt the LDAP and SNMP 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 Cisco IMC 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 In the **Import Configuration** dialog box, complete the following fields:

Name	Description
Import From drop-down list	The location of the XML configuration file. This can be one of the following: • **Local**: Select this option to import the XML configuration file to a drive that is local to the computer running . When you select this option, displays a **Browse** button that lets you navigate to the file you want to import. • **Remote Server**: Select this option to import the XML configuration file from a remote server. When you select this option, displays the remote server fields.

Name	Description
Import From drop-down list	**Note** These options are available only when you choose **Remote**. The remote server type. This can be one of the following: • **TFTP Server** • **FTP Server** • **SFTP Server** • **SCP Server** • **HTTP Server** **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. 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	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	The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP.
Passphrase	The passphrase that uses the AES256 algorithm to encrypt the LDAP and SNMP v3 user passwords in the imported configuration files. Enter a string of 6 to 127 characters. Do not enter the following characters: ! # $ & < > ? ; ' | ` ~ \ % ^ ( )" **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**.

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 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 **Generate NMI to Host** dialog box, review the following information:

Actions	Description
Generate NMI to drop-down list	Allows you to select the server for which you want to generate the non maskable interrupt (NMI). This can be one of the following: • **Server 1** • **Server 2**

Step 5 Click **Send**.

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. Complete the following steps:

Before you begin

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 In the **Add/Update Cisco IMC Banner** dialog box, complete the following fields:

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 checkbox	When checked, the active SSH sessions are terminated after you click the **Save Banner** button.

Step 5 Click **Save Banner**.

What to do next

Viewing Cisco IMC Last Reset Reason

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: • **watchdog-reset**—The watchdog-timer resets when the Cisco IMC memory reaches full capacity. • **ac-cycle**— PSU power cables are removed (no power input). • **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 **Generate Inventory Data**.

Step 4 In the **Generate Inventory Data** dialog box, complete the following fields:

Name	Description
Generate Inventory Data radio button	displays this radio button when there is no hardware inventory data file to download.
Download to local file radio button	enables this radio button when a inventory data file is available to download. To download the existing file, select this option and click **Download**.

Step 5 Click **Generate** to create the data file. When data collection is complete, select 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 In the **Export Hardware Inventory Data** dialog box, complete the following fields:

Name	Description
Export Hardware Inventory Data to drop-down list	The remote server type. This can be one of the following: • **TFTP Server** • **FTP Server** • **SFTP Server** • **SCP Server** • **HTTP Server** **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. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.

Name	Description
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 Hardware Inventory Data to** drop-down list, the name of the field may vary.
Path and Filename field	The path and filename should use when exporting the file to the remote server.
Username	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	The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP.

Step 5 Click **Export**.

CHAPTER 15

Troubleshooting

This chapter includes the following sections:

Recording the Last Boot Process

Procedure

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

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

Step 3 In the **Bootstrap Process Recording** area of the **Troubleshooting** tab, check **Enable Recording** check-box.

By default, this option is enabled.

Caution This task is for troubleshooting purpose, and might impact Cisco IMC performance if it is enabled all the time.

Step 4 (Optional) If you want to record the boot process until BIOS POST, then check **Stop On BIOS POST** check-box.

Step 5 Click **Save Changes**

Step 6 On the tool bar above the **Work** pane, click **Power On Server**.

Step 7 In the **Actions** area, of the **Bootstrap Process Recording** pane, click **Play Recording**.

A confirmation dialog box with instructions on supported Java version appears.

Step 8 Review the instructions and click **Ok**.

The **DVR Player Controls** dialog box opens. This dialog box plays the recording of the last boot process. If you have enabled **Stop On BIOS POST** option then the system plays the recording process only till BIOS POST.

This recording can be reviewed to analyze the factors that caused the system to reboot.

Step 9 In the **Actions** area of the **Bootstrap Process Recording** area, click **Download Recording**.

Follow the instructions to download.

Note The file is saved in a `.dvc` format to a local drive. You can view this recording using KVM player or an offline player. Every time you choose **Download Recording** option, the last boot process is recorded, it autogenerate the file name, and save it in the path specified earlier.

Step 10 Once the download is complete, you can select the file that you want play the video of the recording, and click **Open**.
A **DVR Player Controls** window opens and plays the video of the selected file.

Recording the Last Crash

Procedure

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

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

Step 3 In the **Crash Recording** area of the **Troubleshooting** tab, check the **Enable Recording** check-box.

Caution This task is for troubleshooting purpose, and might impact Cisco IMC performance if it is enabled all the time.

Step 4 Click **Save Changes**.
Capture Recording button in the **Actions** area is enabled.

Step 5 (Optional) In the **Actions** area, click **Capture Recording**, to capture the recording of the system that crashed automatically.

Note If you choose this option, it overwrites the existing crash records file. Click **OK** to continue.

Step 6 Click **Play Recording** in the **Actions** area to view the recording of the operations that ran on the server.

A confirmation dialog box with instructions on supported Java version appears.

Step 7 Review the instructions and click **Ok**.

The **DVR Player Controls** dialog box appears. This dialog box plays the recording of the operations that ran on the server in the last few minutes. This recording can be reviewed to analyze the factors that caused system to crash.

Step 8 In the **Actions** area of the **Crash Recording** area, click **Download Recording**.

Follow the instructions to download.

Note The file is saved in a `.dvc` format to a local drive. You can view this recording using KVM player or an offline player. Every time you choose **Download Recording** option, the last crash process is recorded, it autogenerate the file name, and save it in the path specified earlier.

Step 9 Once the download is complete, you can select the file that you want play the video of the recording, and click **Open**.

A **DVR Player Controls** window opens and plays the video of the selected file.

Downloading a DVR Player

Procedure

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

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

Step 3 In the **Player** area of the **Troubleshooting** tab, click **Download Player**.

Step 4 Follow the instructions to download. These files are saved to your local drive as a zipped file in a .tgz file format.

The offline player is stored for Windows, Linux, and MAC.

Step 5 Extract the zip file. The zip file generally gets saved below the bootstrap file, and its name follows the format `offline.tgz`

Step 6 Open the script file that you want to review the video recording.

Note If you want to play the recording for Windows, then ensure that the Java version running on your system and in the script file are the same. If the Windows script file fails to play the recording, then follow these steps:

a) Extract the Windows script file to your desktop.
b) Open the file using notepad.
c) Search for jre, and replace the Java version to match the version running on your system. By default, the Java version is set to jre7.
d) Save the file.

After you update the Java version, you can delete the extracted files from your desktop.

Note Verification of Java version is required only for Windows OS. For Linux and MAC, the Java version is picked automatically.

Step 7 Navigate to the folder in which these files are downloaded and open the script file that you want to play the video recording.
The DVR player is launched, playing the video of the operations that ran on the server.