CLI Configuration Guide for Cisco UCS E-Series M6 Servers, Release 4.11.x

First Published: 2023-08-07

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

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

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

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

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

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

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

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

CONTENTS

PREFACE

New and Changed Information ix

Audience ix

Organization ix

Conventions xi

Related Documentation xii

Obtaining Documentation and Submitting a Service Request xii

CHAPTER 1

Overview 1

Cisco UCS E-Series M6 Servers Overview 1

Server Software 1

CIMC Overview 2

CIMC CLI 3

Command Modes 3

Command Mode Table 4

Completing or Exiting a Command 5

Command History 5

Committing, Discarding, and Viewing Pending Commands 5

Command Output Formats 6

Online Help for the CLI 7

CHAPTER 2

Installing the Server Operating System or Hypervisor 9

Operating System or Hypervisor Installation Methods 9

KVM Console 9

Installing an Operating System or Hypervisor Using the KVM Console 10

PXE Installation Servers 10

Installing an Operating System or Hypervisor Using a PXE Installation Server 10

Host Image Mapping 11
Mapping the Host Image 11
Unmapping the Host Image 13
Deleting the Host Image 13
Configuring ESX Network Connectivity through MGF (TE1) Interface 14

CHAPTER 3 **Managing the Server** 19
Configuring the Server Boot Order 19
Resetting the Server 20
Shutting Down the Server 21
Locking Cisco IOS CLI Configuration Changes 21
Unlocking Cisco IOS CLI Configuration Changes 23
Managing Server Power 24
Powering On the Server 24
Powering Off the Server 25
Power Cycling the Server 25
Configuring the Power Restore Policy 26
Locking the Server's Front Panel Power Button 27
Unlocking the Server's Front Panel Power Button 28
Configure the Boot Order 29
Configure the Server Boot Order Using UEFI Map and UEFIOS 29
Configuring BIOS Settings 31
Viewing BIOS Status 31
Configuring Server Management BIOS Settings 32
Clearing the BIOS CMOS 32
Setting the BIOS Password 33
Clearing the BIOS Password 33
Restoring BIOS Defaults 34
Server BIOS Settings 34

CHAPTER 4 **Viewing Server Properties** 39
Viewing Server Properties 39
Viewing the Actual Boot Order 40
Viewing CIMC Information 40

Viewing CPU Properties 41
Viewing Memory Properties 42
Viewing Hard Drive Presence 43
Viewing the MAC Address of an Interface 44
Viewing the Status of CIMC Network Connections 44

CHAPTER 5 **Viewing Server Sensors** 47
Viewing Temperature Sensors 47
Viewing Voltage Sensors 48
Viewing LED Sensors 49

CHAPTER 6 **Managing Remote Presence** 51
Managing the Virtual KVM 51
KVM Console 51
Configuring the Virtual KVM 51
Enabling the Virtual KVM 52
Disabling the Virtual KVM 53
Managing Serial over LAN 54
Serial over LAN 54
Guidelines and Restrictions for Serial over LAN 54
Configuring Serial Over LAN 54
Launching Serial over LAN 55

CHAPTER 7 **Managing User Accounts** 57
Configuring Local Users 57
LDAP Servers (Active Directory) 58
Configuring the LDAP Server 58
Configuring LDAP in CIMC 60
Configuring LDAP Groups in CIMC 61
TACACS+ Server 63
TACACS+ Operation 63
Configure TACACS+ Server 64
Viewing User Sessions 65
Terminating a User Session 66

CHAPTER 8

Configuring Network-Related Settings 67

CIMC NIC Configuration 67

CIMC NICs 67

Configuring CIMC NICs 68

Configuring Common Properties 69

Configuring IPv4 70

Configuring IPv6 72

Configuring the Server VLAN 74

Network Security Configuration 75

Network Security 75

Configuring Network Security 75

Configuring IP Filtering 76

NTP Settings Configuration 78

NTP Settings 78

Configuring NTP Settings 78

CHAPTER 9

Configuring Communication Services 81

Configuring HTTP 81

Configuring SSH 82

Enabling Redfish 83

Configuring the XML API 84

XML API for the CIMC 84

Enabling the XML API 84

Configuring IPMI 84

IPMI over LAN 84

Configuring IPMI over LAN 85

Configuring SNMP 86

SNMP 86

Configuring SNMP Properties 86

Configuring SNMP Trap Settings 88

Sending a Test SNMP Trap Message 89

Configuring SNMPv3 Users 89

CHAPTER 10 Managing Certificates 93

Managing the Server Certificate 93

Generating a Certificate Signing Request 93

Creating a Self-Signed Certificate 95

Uploading a Server Certificate 97

CHAPTER 11 Configuring Platform Event Filters 99

Platform Event Filters 99

Enabling Platform Event Alerts 99

Disabling Platform Event Alerts 100

Configuring Platform Event Filters 100

Interpreting Platform Event Traps 102

CHAPTER 12 Firmware Management 105

Overview of CIMC Firmware 105

Options for Upgrading Firmware 106

Obtaining Software from Cisco Systems 106

Installing CIMC Firmware from a Remote Server 107

Activating Installed CIMC Firmware 108

Changing Password Storage Format 109

Installing BIOS Firmware from the TFTP Server 110

Troubleshooting the UCS E-Series M6 Server Access Issues 111

Recovering from a Corrupted CIMC Firmware Image 111

Recovering from a Corrupted File System 113

Recovery Shell Commands 114

Recovering Password 115

CHAPTER 13 Viewing Faults and Logs 119

Faults 119

Viewing the Fault Summary 119

System Event Log 120

Viewing the System Event Log 120

Clearing the System Event Log 121

Cisco IMC Log 121

Viewing the CIMC Log 121

CHAPTER 14 Server Utilities 123

Exporting Technical Support Data to a Remote Server 123

Rebooting the CIMC 125

Resetting the CIMC to Factory Defaults 125

Exporting and Importing the CIMC Configuration 126

Exporting and Importing the CIMC Configuration 126

Exporting the CIMC Configuration 127

Importing a CIMC Configuration 128

New and Changed Information

The following table provides an overview of the significant changes to this guide for the current release:

Table 1: New Features in Cisco Integrated Management Controller Software, Release 4.11.1

Feature	Description	Where Documented
Support for UCS E-Series M6 servers (UCS-E1100D-M6).	Support added to install the UCS-E1100D-M6 servers into Cisco Catalyst 8300 Edge platforms.	Release Notes for Cisco UCS E-Series M6 Servers, Release 4.11.1

- Audience, on page ix
- Organization, on page ix
- Conventions, on page xi
- Related Documentation, on page xii
- Obtaining Documentation and Submitting a Service Request, on page xii

Audience

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

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

Organization

This document includes the following chapters:

Chapter	Title	Description
Chapter 1	Overview	Provides an overview of the Cisco UCS E-Series M6 Servers, and the CIMC.
Chapter 2	Installing the Server Operating System	Describes how to configure an operating system (OS) on the server.
Chapter 3	Managing the Server	Describes how to configure the server boot device order, how to manage the server power, how to configure power policies, and how to configure BIOS settings.
Chapter 4	Viewing Server Properties	Describes how to view the CPU, memory, power supply, storage, PCI adapter, and LOM properties of the server.
Chapter 5	Viewing Server Sensors	Describes how to view the temperature, voltage, and storage sensors.
Chapter 6	Managing Remote Presence	Describes how to configure and manage the virtual KVM, virtual media, and the serial over LAN connection.
Chapter 7	Managing User Accounts	Describes how to add or modify user accounts, how to configure Active Directory to authenticate users, and how to manage user sessions.
Chapter 8	Configuring Network-Related Settings	Describes how to configure network interfaces, network settings, network security, NAM, and NTP settings.
Chapter 9	Configuring Communication Services	Describes how to configure server management communication by HTTP, SSH, Redfish, IPMI, and SNMP.
Chapter 10	Managing Certificates	Describes how to generate, upload, and manage server certificates.
Chapter 11	Configuring Platform Event Filters	Describes how to configure and manage platform event filters.
Chapter 12	Firmware Management	Describes how to obtain, install, and activate firmware images.
Chapter 13	Viewing Faults and Logs	Describes how to view fault information and how to view, export, and clear the CIMC log and system event log messages.
Chapter 14	Server Utilities	Describes how to export support data, how to export and import the server configuration, how to reset the server configuration to factory defaults, and how to reboot the management interface.

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**.
User input	Text the user should enter exactly as shown or keys that a user should press appear in **`this font`**.
Document titles	Document titles appear 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**. Arguments in a CLI command appear in *this font*.
[ ]	Elements in square brackets are optional.
{x | y | z}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
< >	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.

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

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

Warning 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 Documentation

The Documentation Guide for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine provides links to all product documentation.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation.

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

CHAPTER 1

Overview

-
- Cisco UCS E-Series M6 Servers Overview, on page 1
- Server Software, on page 1
- CIMC Overview, on page 2
- CIMC CLI, on page 3

Cisco UCS E-Series M6 Servers Overview

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

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

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

Server Software

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

- CIMC firmware
- BIOS firmware
- Operating system or hypervisor

CIMC Firmware

Cisco Integrated Management Controller (CIMC) is a separate management module built into the motherboard ofthe E-Series M6 Servers. A dedicated 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 M6 Servers. 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 manageabilityfeatures allow you to interact with the hardware and use it. In addition, BIOS provides options to configure the system, and manage firmware.

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

Operating System or Hypervisor

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

Note For information about the platforms that are available on the E-Series M6 Servers, see section Software Requirements in the *Release Notes for Cisco UCS E-Series M6 Servers*.

CIMC Overview

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

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

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

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

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

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

CIMC CLI

The CIMC CLI is a command-line management interface for E-Series M6 Servers. You can launch the CIMC CLI in the following ways:

- By the serial port.
- Over the network by SSH.
- From the router. Use the following command:
    - **hw-module subslot** *slot/subslot* **session imc**—Use for E-Series M6 Servers installed in a Cisco Catalyst 8300 Edge Series platform.

A CLI user can have one of the three roles: admin, user (can control but cannot configure), and read-only.

Command Modes

The CLI is organized into a hierarchy of command modes, with the EXEC mode being the highest-level mode of the hierarchy. Higher-level modes branch into lower-level modes. You use the **scope** command to move from higher-level modes to modes in the next lower level , and the **exit** command to move up one level in the mode hierarchy. The **top** command returns to the EXEC mode.

Note Most command modes are associated with managed objects. The **scope** command does not create managed objects and can only access modes for which managed objects already exist.

Each mode contains a set of commands that can be entered in that mode. Most of the commands available in each mode pertain to the associated managed object. Depending on your assigned role, you may have access to only a subset of the commands available in a mode; commands to which you do not have access are hidden.

The CLI prompt for each mode shows the full path down the mode hierarchy to the current mode. This helps you to determine where you are in the command mode hierarchy and can be an invaluable tool when you need to navigate through the hierarchy.

Command Mode Table

The following table lists the first four levels of command modes, the commands used to access each mode, and the CLI prompt associated with each mode.

Mode Name	Command to Access	Mode Prompt
`EXEC`	**top** command from any mode	#
`bios`	**scope bios** command from EXEC mode	/bios #
`certificate`	**scope certificate** command from EXEC mode	/certificate #
`chassis`	**scope chassis** command from EXEC mode	/chassis #
`cimc`	**scope cimc** command from EXEC mode	/cimc #
`fault`	**scope fault** command from EXEC mode	/fault #
`host-image-mapping`	**scope host-image-mapping** command from EXEC mode	/host-image-mapping#
`http`	**scope http** command from EXEC mode	/http #
`ipmi`	**scope ipmi** command from EXEC mode	/ipmi #
`kvm`	**scope kvm** command from EXEC mode	/kvm #
`ldap`	**scope ldap** command from EXEC mode	/ldap #
`sel`	**scope sel** command from EXEC mode	/sel #
`sensor`	**scope sensor** command from EXEC mode	/sensor #
`snmp`	**scope snmp** command from EXEC mode	/snmp #
`sol`	**scope sol** command from EXEC mode	/sol #

Mode Name	Command to Access	Mode Prompt
ssh	**scope ssh** command from EXEC mode	/ssh #
tacacs+	**scope tacacs+** command from EXEC mode	/tacacs+
user	**scope user** *user-number* command from EXEC mode	/user #
user-policy	**scope user-policy** *policy-number* command from EXEC mode	/user-policy #
user-session	**scope user-session** *session-number* command from EXEC mode	/user-session #
vmedia	**scope vmedia** command from EXEC mode	/vmedia #

Completing or Exiting a Command

You can use the Tab key in any mode to complete a command. Partially typing a command name and pressing Tab causes the command to be displayed in full or to the point where another keyword must be chosen or an argument value must be entered.

When you are inside a scope, the **exit** command allows you to move one level up. For example, if the scope is **/chassis/dimm-summary**, and you enter **exit**, the scope will move one level up to **/chassis**.

Command History

The CLI stores all commands used in the current session. You can step through the previously used commands by using the Up Arrow or Down Arrow keys. The Up Arrow key steps to the previous command in the history, and the Down Arrow key steps to the next command in the history. If you get to the end of the history, pressing the Down Arrow key does nothing.

All commands in the history can be entered again by simply stepping through the history to recall the desired command and pressing Enter. The command is entered as if you had manually typed it. You can also recall a command and change it before you enter it.

Committing, Discarding, and Viewing Pending Commands

When you enter a configuration command in the CLI, the command is not applied until you enter the **commit** command. Until committed, a configuration command is pending and can be discarded by entering a **discard** command. When any command is pending, an asterisk (*) appears before the command prompt. The asterisk disappears when you enter the **commit** command, as shown in this example:

```
Server# scope kvm
Server /kvm # set enabled yes
Server /kvm *# commit
Server /kvm #
```

You can accumulate pending changes in multiple command modes and apply them together with a single **commit** command. You can view the pending commands by entering the **show configuration pending** command in any command mode.

Note Committing multiple commands together is not an atomic operation. If any command fails, the successful commands are applied despite the failure. Failed commands are reported in an error message.

Caution The **commit** command must be used to commit changes that are made within the same scope. If you try to use the **commit** command to submit changes made in a different scope, you will get an error, and you will have to redo and recommit those changes.

Command Output Formats

Most CLI **show** commands accept an optional **detail** keyword that causes the output information to be displayed as a list rather than as a table.

Depending on how you want the output information of the **detail** command to be displayed, use one of the following commands:

- **set cli output default**—Default format for easy viewing. The command output is presented in a compact list.

  This example shows the command output in the default format:

  ```
  Server /chassis # set cli output default
  Server /chassis # show hdd detail
  Name HDD_01_STATUS:
      Status : present
  Name HDD_02_STATUS:
      Status : present
  Name HDD_03_STATUS:
      Status : present

  Server /chassis #
  ```

- **set cli output yaml**—YAML format for easy parsing by scripts. The command output is presented in the YAML Ain't Markup Language (YAML) data serialization language, delimited by defined character strings.

  This example shows the command output in the YAML format:

  ```
  Server /chassis # set cli output yaml
  Server /chassis # show hdd detail
  ---
      name: HDD_01_STATUS
      hdd-status: present

  ---
      name: HDD_02_STATUS
      hdd-status: present
  ```

```
---
    name: HDD_03_STATUS
    hdd-status: present

...

Server /chassis #
```

For detailed information about YAML, see http://www.yaml.org/about.html.

Online Help for the CLI

At any time, you can type the **?** character to display the options available at the current state of the command syntax. If you have not typed anything at the prompt, typing ? lists all available commands for the mode you are in. If you have partially typed a command, typing ? lists all available keywords and arguments available at your current position in the command syntax.

CHAPTER 2

Installing the Server Operating System or Hypervisor

-
- Operating System or Hypervisor Installation Methods, on page 9
- KVM Console, on page 9
- PXE Installation Servers, on page 10
- Host Image Mapping, on page 11
- Configuring ESX Network Connectivity through MGF (TE1) Interface, on page 14

Operating System or Hypervisor Installation Methods

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

- KVM console
- PXE installation server
- Host image mapping

Caution You must use only one method to map virtual drives. 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. You can map any of the following to a virtual drive:

- CD/DVD 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.

Installing an Operating System or Hypervisor Using the KVM Console

Because the KVM console is operated only through the GUI, you cannot install an operating system or hypervisor using the CLI. To install a platform using the KVM console, follow the instructions in section Installing an Operating System or Hypervisor Using the KVM Console of the *GUI Configuration Guide for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine.*.

PXE Installation Servers

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

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

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

Installing an Operating System or Hypervisor Using a PXE Installation Server

Before you begin

Verify that the server can be reached over a VLAN.

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

For more information about setting the boot order, see section Configure the Server Boot Order Using UEFI Map and UEFIOS.

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.

Host Image Mapping

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

Mapping the Host Image

Before you begin

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

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

Procedure

	Command or Action	Purpose
Step 1	Server# **scope host-image-mapping**	Enters the remote install command mode.
Step 2	Server /host-image-mapping # **download-image** {**ftp** | **ftps** | **http** | **https** | **scp**} *server-ip-address path / filename* [**username** *username* **password** *password*]	Downloads the image from the specified remote server onto the CIMC internal repository. The host image must have .iso as the file extension. The remote server can be an FTP, FTPS, SCP, HTTP, or HTTPS server. If the remote server requires user authentication, you must add the username and password of the remote server. **Note** If the image file exceeds the size limit, an error message is displayed.

	Command or Action	Purpose
		Note The HTTP server does not support user authentication; only FTP supports user authentication.
Step 3	(Optional) Server /host-image-mapping # **show detail**	Displays the status of the image download.
Step 4	Server /host-image-mapping # **map-image** *image_name.iso*	Mounts the image on a virtual drive of the USB controller. The virtual drive can be one of the following: • HDD—Hard disk drive • CDROM—Bootable CD-ROM
Step 5	(Optional) Server /host-image-mapping # **show detail**	Displays the status of the host image mapping.

Example

This example shows how to maps the host image:

```
Server /host-image-mapping # download-image http 10.126.254.155 /download/image_name.iso
Username:
Password:
Image download has started.
Please check the status using "show detail".
Current Mapped Image: None
Host Image Status: "Downloading ..Please wait: 8.1%"

Server /host-image-mapping # show detail
Current Mapped Image: None
Host Image Status: Image Downloaded and Processed Successfully
Server /host-image-mapping # map-image
Please check the status using "show detail".

Server /host-image-mapping # show detail
Current Mapped Image: image_name.iso
Host Image Status: Image mapped successfully, set HDD as the Boot device.
Server /host-image-mapping #
```

What to do next

1. Set the boot order to make the virtual drive in which the image is installed as the first boot device. See section Configure the Server Boot Order Using UEFI Map and UEFIOS.
2. Reboot the server. If the image contains an answer file, the operating system installation is automated and the image is installed. Otherwise, the installation wizard displays. Follow the wizard steps to install the image.
3. If disk drives are not displayed after you install the operating system or hypervisor, you must install drivers. See section Overview of CIMC Firmware for details.
4. 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 the CIMC as a user with admin privileges.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope host-image-mapping**	Enters the remote install command mode.
Step 2	Server /host-image-mapping # **unmap-image**	Unmounts the image from the virtual drive of the USB controller.
Step 3	Server /host-image-mapping # **show detail**	(Optional) Displays the status of the host image unmapping.

Example

This example shows how to unmap the host image:

```
Server /host-image-mapping # unmap-image
Please check the status using "show detail".
Server /host-image-mapping # show detail
Current Mapped Image: None
Host Image Status: Unmap Successful!!
Server /host-image-mapping #
```

Deleting the Host Image

Before you begin

Log in to the CIMC as a user with admin privileges.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope host-image-mapping**	Enters remote install mode.
Step 2	Server /host-image-mapping # **delete-image**	Removes the image from the CIMC internal repository.

Example

This example deletes the host image:

```
Server# scope host-image-mapping
Server /host-image-mapping # delete-image
```

Configuring ESX Network Connectivity through MGF (TE1) Interface

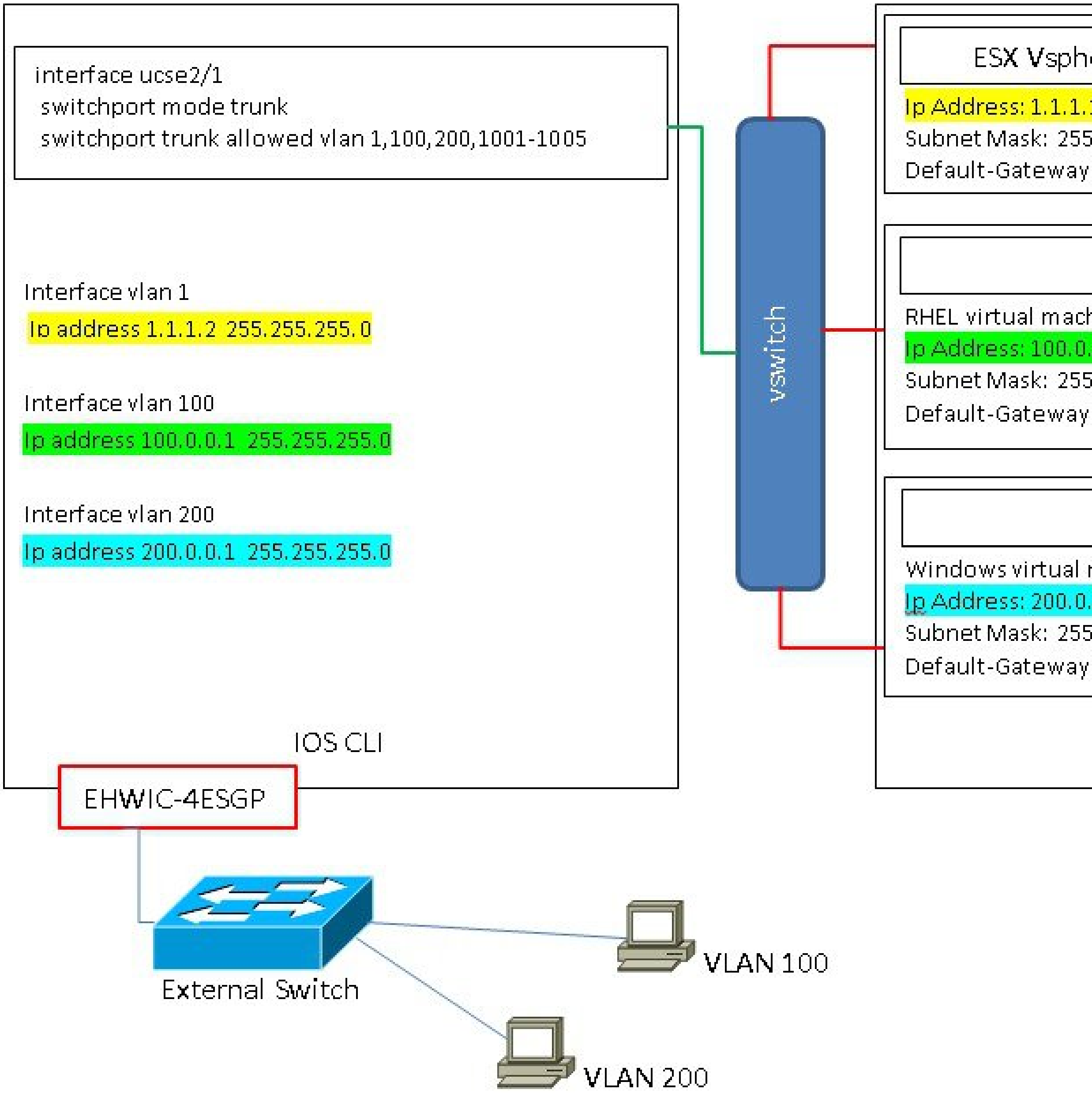
On the E-Series M6 Servers, the MGF (TE1) interface connects internally to the Ethernet Switch Module through the backplane. This section explains how to set up a communication link between the UCS E-Series hosts with the external network.

There are two scenarios where you can configure ESX Network Connectivity through the MGF (TE1) interface:

- L2NETWORKING: Hosts and VMs in the Same Subnet.
- L3 NETWORKING: Hosts and VMs in Different Networks
- L3 NETWORKING: Hosts and VMs in the Same Network

L2 NETWORKING: Hosts and VMs in the Same Subnet

In this scenario, the UCS E-Series M6 Server is hosting the VMS in VLAN 100 and 200.The traffic enters the routerand passes through UCSE2/1/ GE1 interface and switches to the physical hosts by the EHWIC module.



```
interface ucse2/1
 switchport mode trunk
 switchport trunk allowed vlan 1,100,200,1001-1005
```

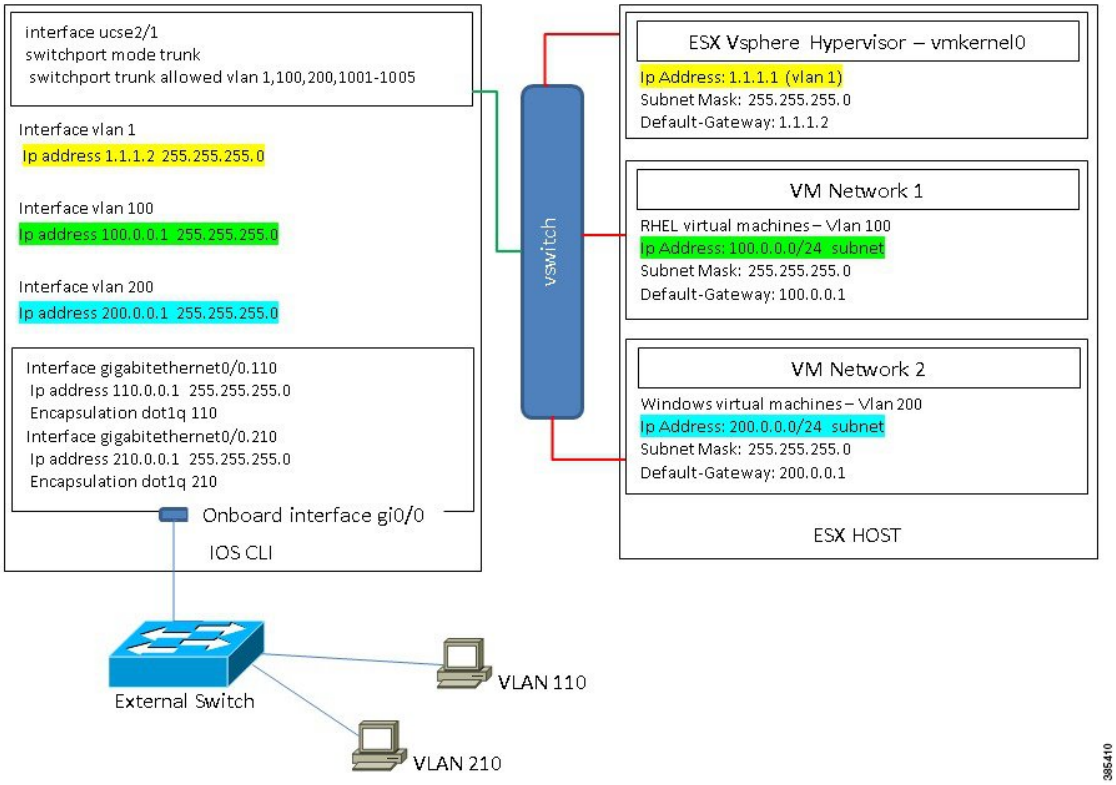
```
Interface vlan 1
 Ip address 1.1.1.2  255.255.255.0

Interface vlan 100
Ip address 100.0.0.1  255.255.255.0

Interface vlan 200
Ip address 200.0.0.1  255.255.255.0
```

L3 NETWORKING: Hosts and VMs in Different Network

In this scenario, the VMs communicate with hosts in different subnet by sending the traffic to the router throughthe UCSE1/0/1. On the router, the traffic hits the VLAN interface and gets L3 routed by the Catalyst 8300 Series Edge platform.



```
interface ucse2/1
switchport mode trunk
 switchport trunk allowed vlan 1,100,200,1001-1005

Interface vlan 1
 Ip address 1.1.1.2 255.255.255.0

Interface vlan 100
Ip address 100.0.0.1  255.255.255.0

Interface vlan 200
Ip address 200.0.0.1  255.255.255.0

Interface gigabitethernet0/0.110
 Ip address 110.0.0.1  255.255.255.0
 Encapsulation dot1q 110
Interface gigabitethernet0/0.210
 Ip address 210.0.0.1  255.255.255.0
 Encapsulation dot1q 210
```

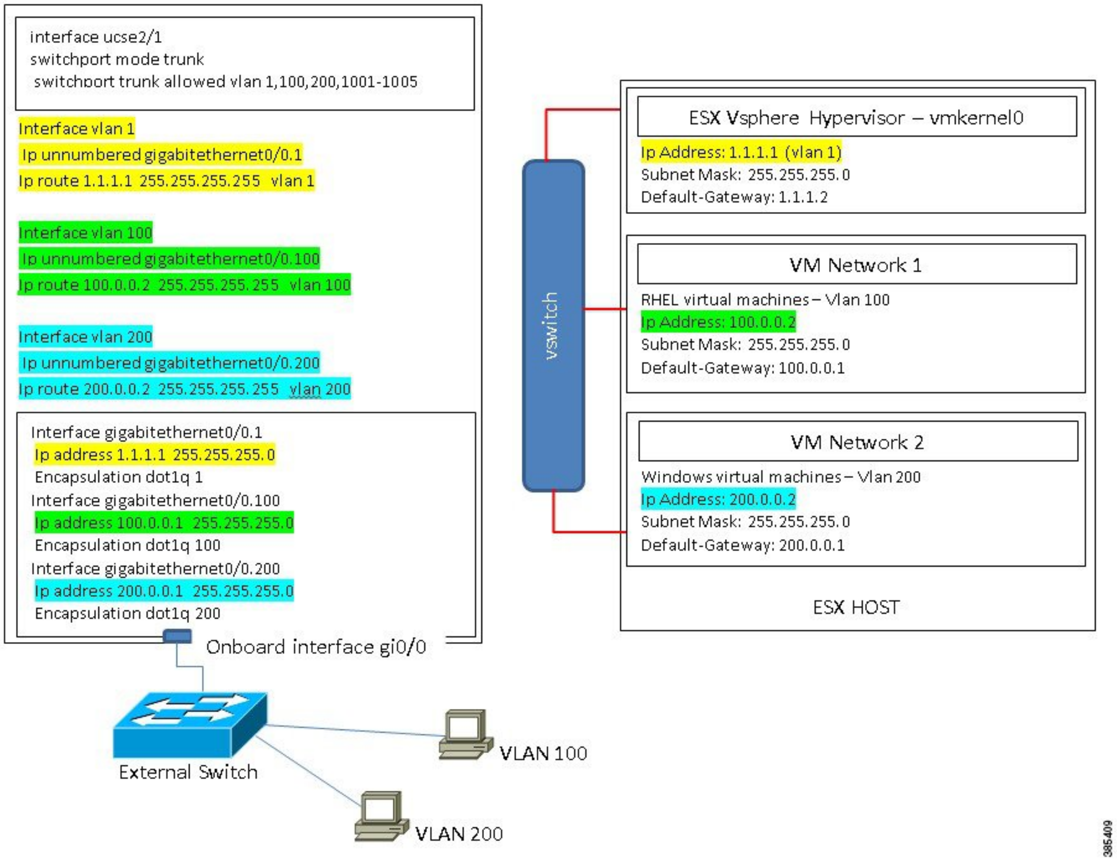
ESX Vsphere Hypervisor – vmkernel0
Ip Address: 1.1.1.1 (vlan 1)
Subnet Mask: 255.255.255.0
Default-Gateway: 1.1.1.2

VM Network 1
RHEL virtual machines – Vlan 100
Ip Address: 100.0.0.0/24 subnet
Subnet Mask: 255.255.255.0
Default-Gateway: 100.0.0.1

VM Network 2
Windows virtual machines – Vlan 200
Ip Address: 200.0.0.0/24 subnet
Subnet Mask: 255.255.255.0
Default-Gateway: 200.0.0.1

L3 NETWORKING: Hosts and VMs in the Same Network

In this scenario, the physical hosts are in the same subnet as the VMs. The physical hosts can be connected to the onboard L3 interface with the following configuration to enable the communication between the VMs and the physical hosts.



```
interface ucse2/1
switchport mode trunk
 switchport trunk allowed vlan 1,100,200,1001-1005

Interface vlan 1
 Ip unnumbered gigabitethernet0/0.1
Ip route 1.1.1.1  255.255.255.255  vlan 1

Interface vlan 100
 Ip unnumbered gigabitethernet0/0.100
Ip route 100.0.0.2  255.255.255.255  vlan 100

Interface vlan 200
 Ip unnumbered gigabitethernet0/0.200
Ip route 200.0.0.2  255.255.255.255  vlan 200

Interface gigabitethernet0/0.1
 Ip address 1.1.1.1  255.255.255.0
 Encapsulation dot1q 1
Interface gigabitethernet0/0.100
 Ip address 100.0.0.1  255.255.255.0
 Encapsulation dot1q 100
Interface gigabitethernet0/0.200
 Ip address 200.0.0.1  255.255.255.0
 Encapsulation dot1q 200
```

ESX Vsphere Hypervisor – vmkernel0

Ip Address: 1.1.1.1 (vlan 1)
Subnet Mask: 255.255.255.0
Default-Gateway: 1.1.1.2

VM Network 1

RHEL virtual machines – Vlan 100
Ip Address: 100.0.0.2
Subnet Mask: 255.255.255.0
Default-Gateway: 100.0.0.1

VM Network 2

Windows virtual machines – Vlan 200
Ip Address: 200.0.0.2
Subnet Mask: 255.255.255.0
Default-Gateway: 200.0.0.1

CHAPTER 3

Managing the Server

-
- Configuring the Server Boot Order, on page 19
- Resetting the Server, on page 20
- Shutting Down the Server, on page 21
- Locking Cisco IOS CLI Configuration Changes, on page 21
- Unlocking Cisco IOS CLI Configuration Changes, on page 23
- Managing Server Power, on page 24
- Configure the Boot Order, on page 29
- Configuring BIOS Settings, on page 31

Configuring the Server Boot Order

Note Do not change the boot order while the host is performing BIOS power-on self test (POST).

Before you begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# **scope bios**	Enters BIOS command mode.
Step 2	Server /bios # **set boot-order** *device1, device2, device3....*	Specifies the boot device options and order. **Note** The options are not case sensitive. You can select one or more of the following: • uefimap • uefios • uefipxeTE0/TE1/TE3/TE4

	Command or Action	Purpose
		• uefipxeGE2
Step 3	Server /bios # **commit**	Commits the transaction to the system configuration.
Step 4	(Optional) Server /bios # **show detail**	Displays the server boot order.

The next BIOS boot uses the new boot order.

Example

This example sets the boot order and commits the transaction:

```
server /bios # set boot-order uefimap,uefios
To manage boot-order:
- Reboot server to have your boot-order settings take place
- Do not disable boot options via BIOS screens
- If a specified device type is not seen by the BIOS, it will be removed
from the boot order configured on the BMC
- Your boot order sequence will be applied subject to the previous rule.
The configured list will be appended by the additional device types
seen by the BIOS
- Legacy Boot Order configuration will disable all the active Boot Devices which will
hide them from BIOS

server /bios *# commit
Changes to BIOS set-up parameters will require a reboot.
Do you want to reboot the system?[y|N]y
A system reboot has been initiated.

server /bios # show detail
BIOS:
BIOS Version: UCSEDM6_1.08
BIOS Flash: 1
Backup BIOS Version: UCSEDM6_1.08
Backup BIOS Flash: 0
BIOS Post Complete: 0
Boot Order: UEFIMAP,UEFIOS
FW Update Status: Done, OK
Password: ******
server /bios #
```

Resetting the Server

Before you begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters chassis command mode.

	Command or Action	Purpose
Step 2	Server /chassis # **power hard-reset**	After a prompt to confirm, resets the server. **Note** Power cycling the server is the same as powering off and then powering on the x86 server. **Note** Powerhard-reset is the same as pressing the physical reset button on the server.

Example

This example resets the server:

```
Server# scope chassis
Server /chassis # power hard-reset
This operation will change the server's power state.
Continue?[y|N]y
```

Shutting Down the Server

Before you begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **power shutdown**	After the prompt to confirm, shuts down the server.

Example

This example shuts down the server:

```
Server# scope chassis
Server /chassis # power shutdown

This operation will change the server's power state.
Do you want to continue?[y|N]y
```

Locking Cisco IOS CLI Configuration Changes

Use this procedure to prevent configuration changes from being made using the Cisco IOS CLI.

Before you begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **show detail**	(Optional) Displays server properties, which allows you to determine the current status of the IOS lockout (whether it is locked or unlocked).
Step 3	Server /chassis # **set ios-lockout locked**	Prevents configuration changes from being made using the Cisco IOS CLI.
Step 4	Server /chassis* # **commit**	Commits the changes.
Step 5	Server /chassis # **show detail**	(Optional) Displays server properties, which allows you to determine the current status of the IOS lockout (whether it is locked or unlocked).

Example

This example prevents configuration changes from being made using the Cisco IOS CLI:

```
Server /chassis # show detail
Chassis:
Power: off
    IOS Lockout: unlocked
    Power Button: unlocked
    Reset Button: unlocked
    Serial Number: FOC26285Q4B
    Product Name: UCS E1100D M6
    PID: UCS-E1100D-M6
    UUID: 1CD1E026-089C-0000-E822-D9826168E8F8
    Description:
    Asset Tag: Unknown
    FPGA Version: 3.4.2
    Uptime: 22 hours, 54 minutes
    SBFPGA Version: 1.0.2
    MCU Version: 240.10
    AIKIDO Version: 2711-270
    Last Reboot Reason: Flash Reset
Server /chassis # set ios-lockout locked
Server /chassis *# commit
Server /chassis # show detail
Chassis:
    Power: off
    IOS Lockout: locked
    Power Button: unlocked
    Reset Button: unlocked
    Serial Number: FOC26285Q4B
    Product Name: UCS E1100D M6
    PID : UCS-E1100D-M6
    UUID: 1CD1E026-089C-0000-E822-D9826168E8F8
    Description:
    Asset Tag: Unknown
    FPGA Version: 3.4.2
    Uptime: 22 hours, 54 minutes
    SBFPGA Version: 1.0.2
    MCU Version: 240.10
    AIKIDO Version: 2711-270
    Last Reboot Reason: Flash Reset
```

Unlocking Cisco IOS CLI Configuration Changes

Use this procedure to allow configuration changes to be made using the Cisco IOS CLI.

Before you begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **show detail**	(Optional) Displays server properties, which allows you to determine the current status of the IOS lockout (whether it is locked or unlocked).
Step 3	Server /chassis # **set ios-lockout unlocked**	Allows configuration changes to be made using the Cisco IOS CLI.
Step 4	Server /chassis* # **commit**	Commits the changes.
Step 5	Server /chassis # **show detail**	(Optional) Displays server properties, which allows you to determine the current status of the IOS lockout (whether it is locked or unlocked).

Example

This example allows configuration changes to be made using the Cisco IOS CLI:

```
Server /chassis # show detail
Chassis:
    Power: off
    IOS Lockout: locked
    Power Button: unlocked
    Reset Button: unlocked
    Serial Number: FOC26285Q4B
    Product Name: UCS E1100D M6
    PID : UCS-E1100D-M6
    UUID: 1CD1E026-089C-0000-E822-D9826168E8F8
    Description:
    Asset Tag: Unknown
    FPGA Version: 3.4.2
    Uptime: 22 hours, 54 minutes
    SBFPGA Version: 1.0.2
    MCU Version: 240.10
    AIKIDO Version: 2711-270
    Last Reboot Reason: Flash Reset
Server /chassis # set ios-lockout unlocked
Server /chassis *# commit
Server /chassis # show detail
Chassis:
    Power: off
    IOS Lockout: unlocked
    Power Button: unlocked
    Reset Button: unlocked
    Serial Number: FOC26285Q4B
    Product Name: UCS E1100D M6
    PID : UCS-E1100D-M6
    UUID: 1CD1E026-089C-0000-E822-D9826168E8F8
    Description:
    Asset Tag: Unknown
    FPGA Version: 3.4.2
    Uptime: 22 hours, 54 minutes
    SBFPGA Version: 1.0.2
    MCU Version: 240.10
    AIKIDO Version: 2711-270
    Last Reboot Reason: Flash Reset
Server /chassis #
```

Managing Server Power

Powering On the Server

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

Before you begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **power on**	After the prompt to confirm, turns on the server power.

Example

This example turns on the server:

```
Server /chassis # power on
This operation will change the server's power state.
Do you want to continue?[y|N]y
Server /chassis # show
Power   Serial Number    Product Name      PID    UUID
```

```
----- --------------- ----------------- -----------------   --------------------------
on      FOC26071VZY      UCS E1100D M6     UCS-E1100D-M6    1CD1E026-0311-0000-
0F12-FC9ABB95AA0A

Server /chassis #
```

Powering Off the Server

Before you begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **power off**	Turns off the server.

Example

This example turns off the server:

```
Server# scope chassis
Server /chassis # power off
This operation will change the server's power state.
Do you want to continue?[y|N]y
Server /chassis # show
Power  Serial Number  Product Name    PID   UUID
----- ------------- ---------------- ------------- --------------------------
off   FOC26071VZY     UCS E1100D M6   UCS-E1100D-M6  1CD1E026-0311-0000-0F12-FC9ABB95AA0A

Server /chassis #
```

Power Cycling the Server

Before you begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **power cycle**	After the prompt to confirm, power cycles the server.

	Command or Action	Purpose
		Note • Power cycling the server is the same as powering off and then powering on the x86 server. • Power hard-reset is the same as pressing the physical reset button on the server.

Example

This example power cycles the server:

```
Server# scope chassis
Server /chassis # power cycle

This operation will change the server's power state.
Continue?[y|N]y
```

Configuring the Power Restore Policy

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 user or admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters CIMC command mode.
Step 2	Server /cimc #**scope power-restore-policy**	Enters the power restore policy command mode.
Step 3	Server /cimc/power-restore-policy # **set policy** {**power-off** | **power-on** | **restore-last-state**}	Specifies the action to be taken when chassis power is restored. Select one of the following: • **power-off**—Server power will remain off until manually turned on. • **power-on**—Server power will be turned on when chassis power is restored. • **restore-last-state**—Restores the server to the same power state (off or on) that it was in when the power was lost. This is the default action.
Step 4	Server /cimc/power-restore-policy# **commit**	Commits the transaction to the system configuration.

Example

This example sets the power restore policy to power-on and commits the transaction:

```
Server# scope CIMC
Server /CIMC # scope power-restore-policy
Server /CIMC/power-restore-policy # set policy power-on
Server /CIMC/power-restore-policy *# commit
Server /CIMC/power-restore-policy #  show detail
Power Restore Policy:
    Power Restore Policy: power-on

Server /CIMC/power-restore-policy #
```

Locking the Server's Front Panel Power Button

Use this procedure to disable the physical power button, which is located on the front panel of the physical server. Once the power button is disabled, you cannot use the front panel power button to turn the server power on or off.

Before you begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **show detail**	(Optional) Displays server properties, which allows you to determine the current status of the power button (whether it is locked or unlocked).
Step 3	Server /chassis # **set power-button locked**	Disables the power button. You cannot use the front panel power button to turn the server power on or off.
Step 4	Server /chassis* # **commit**	Commits the changes.
Step 5	Server /chassis # **show detail**	(Optional) Displays server properties, which allows you to determine the current status of the power button (whether it is locked or unlocked).

Example

This example disables the server's physical power button, which is located on the front panel of the physical server:

```
Server# scope chassis
Server /chassis # show detail
Chassis:
    Power: off
    IOS Lockout: unlocked
    Power Button: unlocked
    Reset Button: unlocked
    Serial Number: FOC26285PBW
    Product Name: UCS E1100D M6
    PID : UCS-E1100D-M6
    UUID: 1CD1E026-05DC-0000-88E4-3E11AF0AA302
    Description:
    Asset Tag: Unknown
    FPGA Version: 3.4.2
    Uptime: 4 hours, 22 minutes
    SBFPGA Version: 1.0.2
    MCU Version: 240.9
    AIKIDO Version: 271e-270
    Last Reboot Reason: Flash Reset
Server /chassis # set power-button locked
Server /chassis *# commit
Server /chassis # show detail
Chassis:
    Power: off
    IOS Lockout: unlocked
    Power Button: locked
    Reset Button: unlocked
    Serial Number: FOC26285PBW
    Product Name: UCS E1100D M6
    PID : UCS-E1100D-M6
    UUID: 1CD1E026-05DC-0000-88E4-3E11AF0AA302
    Description:
    Asset Tag: Unknown
    FPGA Version: 3.4.2
    Uptime: 4 hours, 22 minutes
    SBFPGA Version: 1.0.2
    MCU Version: 240.9
    AIKIDO Version: 271e-270
    Last Reboot Reason: Flash Reset
Server /chassis #
```

Unlocking the Server's Front Panel Power Button

Use this procedure to enable the physical power button, which is located on the front panel of the physical server. Once the power button is enabled, you can use the front panel power button to turn the server power on or off.

Before you begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **show detail**	(Optional) Displays server properties, which allows you to determine the current status of the power button (whether it is locked or unlocked).
Step 3	Server /chassis # **set power-button unlocked**	Enables the power button. You can use the front panel power button to turn the server power on or off.

	Command or Action	Purpose
Step 4	Server /chassis* # **commit**	Commits the changes.
Step 5	Server /chassis # **show detail**	(Optional) Displays server properties, which allows you to determine the current status of the power button (whether it is locked or unlocked).

Example

This example enable the server's physical power button, which is located on the front panel of the physical server:

```
server /chassis # set power-button unlocked
server /chassis *# commit
server /chassis # show detail
Chassis:
    Power: off
    IOS Lockout: unlocked
    Power Button: unlocked
    Reset Button: unlocked
    Serial Number: FOC26285PBW
    Product Name: UCS E1100D M6
    PID : UCS-E1100D-M6
    UUID: 1CD1E026-05DC-0000-88E4-3E11AF0AA302
    Description:
    Asset Tag: Unknown
    FPGA Version: 3.4.2
    Uptime: 4 hours, 22 minutes
    SBFPGA Version: 1.0.2
    MCU Version: 240.9
    AIKIDO Version: 271e-270
    Last Reboot Reason: Flash Reset
server /chassis #
```

Configure the Boot Order

Configure the Server Boot Order Using UEFI Map and UEFIOS

Note Do not change the boot order while the host is performing BIOS power-on self-test (POST).

Before you begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# **scope bios**	Enters BIOS command mode.

	Command or Action	Purpose
Step 2	Server /bios # **set boot-order** {*uefimap, uefios, uefipxeTE0, uefipxeTE1, uefipxeTE3, uefipxeTE4, uefipxeGE2*}	Server/bios # **set boot-order** *uefimap,uefios* Specifies the boot device options and order. **Note** The options are not case sensitive. You can select one or more of the following: • uefimap—UEFI virtual-map boot option • uefios—UEFI Operating System • uefipxe—PXE boot • TE0 • TE1 • TE3 • TE4 • GE2
Step 3	Server /bios # **commit**	Commits the transaction to the system configuration.
Step 4	(Optional) Server /bios # **show detail**	Displays the server boot order.

The new boot order is used on the next BIOS boot.

Example

This example sets the boot order and commits the transaction:

```
server /bios # set boot-order uefimap,uefios
To manage boot-order:
- Reboot server to have your boot-order settings take place
- Do not disable boot options via BIOS screens
- If a specified device type is not seen by the BIOS, it will be removed
from the boot order configured on the BMC
- Your boot order sequence will be applied subject to the previous rule.
The configured list will be appended by the additional device types
seen by the BIOS
- Legacy Boot Order configuration will disable all the active Boot Devices which will
hide them from BIOS

server /bios *# commit
Changes to BIOS set-up parameters will require a reboot.
Do you want to reboot the system?[y|N]y
A system reboot has been initiated.

server /bios # show detail
BIOS:
BIOS Version: UCSEDM6_1.08
BIOS Flash: 1
Backup BIOS Version: UCSEDM6_1.08
Backup BIOS Flash: 0
BIOS Post Complete: 0
```

```
Boot Order: UEFIMAP,UEFIOS
FW Update Status: Done, OK
Password: ******
server /bios #
```

Note When you enable UEFI secure boot, only the UEFI options—uefimap, and uefios are available. Additionally,configure the UEFI secure boot, this reduces their average boot time by approximately 45-50 seconds.

Configuring BIOS Settings

Viewing BIOS Status

Procedure

	Command or Action	Purpose
Step 1	Server # **scope bios**	Enters BIOS command mode.
Step 2	Server /bios # **show detail**	Displays details of the BIOS status.

The BIOS status information contains the following fields:

Name	Description
BIOS Version	The version string of the running BIOS.
Boot Order	The order of bootable target types that the server will attempt to use.
FW Update/Recovery Status	The status of any pending firmware update or recovery action.
FW Update/Recovery Progress	The percentage of completion of the most recent firmware update or recovery action.

Example

This example displays the BIOS status:

```
SERVER /bios # show detail
BIOS:
    BIOS Version: UCSEDM6_1.08
    BIOS Flash: 1
    Backup BIOS Version: UCSEDM6_1.08
    Backup BIOS Flash: 0
    BIOS Post Complete: 0
    Boot Order: (none)
    FW Update Status: Done, OK
    Password: ******
```

Configuring Server Management BIOS Settings

Before you begin

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

Procedure

	Command or Action	Purpose
Step 1	Server # **scope bios**	Enters BIOS command mode.
Step 2	Server /bios # **scope server-management**	Enters the server management BIOS settings command mode.
Step 3	Configure the BIOS settings.	For the CLI commands, descriptions and information about the options for each BIOS setting, see section Server Management BIOS Settings, on page 36.
Step 4	Server /bios/server-management # **commit**	Commits the transaction to the system configuration. Changes are applied on the next server reboot. If server power is on, you are prompted to choose whether to reboot now.

Example

This example shows how to set the BAUD rate to 9.6k :

```
SERVER /bios #
SERVER /bios # scope server-management
SERVER /bios/server-management # set BaudRate
<VALUE> 115.2k* | 19.2k | 38.4k | 57.6k | 9.6k
SERVER /bios/server-management # set BaudRate 9.6k
SERVER /bios/server-management *# commit
Your changes will be reflected in BIOS on next boot.
SERVER /bios/server-management #
```

Clearing the BIOS CMOS

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

Procedure

	Command or Action	Purpose
Step 1	Server# **scope bios**	Enters BIOS command mode.
Step 2	Server /bios # **clear-cmos**	After a prompt to confirm, clears the CMOS memory.

Example

This example clears the BIOS CMOS memory:

```
Server# scope bios
Server /bios # clear-cmos

This operation will clear the BIOS CMOS.
Note: Server should be in powered off state to clear CMOS.
Continue?[y|N] y
```

Setting the BIOS Password

Procedure

	Command or Action	Purpose
Step 1	Server/bios# **set password**	Sets the BIOS password.

Example

This example sets the BIOS password:

```
Server/bios# set password
Warning:

Strong Password Policy is enabled!


For CIMC protection your password must meet the following requirements:
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 (!, @, #, $, %, ^, &, *, -, _, +, =)
```

Clearing the BIOS Password

Procedure

	Command or Action	Purpose
Step 1	Server# **scope bios**	Enters BIOS command mode.
Step 2	Server /bios # **clear-bios-password**	Clears the BIOS password. You must reboot the server for the clear password operation to take effect. You are prompted to create a new password when the server reboots.

Example

This example clears the BIOS password:

```
Server# scope bios
Server /bios # clear-bios-password

This operation will clear the BIOS Password.
Note: Server should be rebooted to clear BIOS password.
Continue?[y|N]y
```

Restoring BIOS Defaults

Before you begin

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

Procedure

	Command or Action	Purpose
Step 1	Server # **scope bios**	Enters BIOS command mode.
Step 2	Server /bios # **bios-setup-default**	Restores BIOS default settings. This command initiates a reboot.

Example

This example restores BIOS default settings:

```
Server# scope bios
Server /bios # bios-setup-default

This operation will reset the BIOS set-up tokens to factory defaults. All your configuration
 will be lost.
Changes to BIOS set-up parameters will initiate a reboot.
Continue?[y|N]y
```

Server BIOS Settings

The tables in the following sections list the server BIOS settings that you can view and configure.

Note We recommend that you verify the support for BIOS settings in your server. Depending on your installed hardware, some settings may not be supported.

Advanced: Processor BIOS Settings

Name	Description
Package C State Limit	The amount of power available to the server components when they are idle. This can be one of the following: • The server provides all server components with full power at all times. This option maintains the highest level of performance and requires the greatest amount of power. • System level coordination is in progress resulting in high power consumption. There might be performance issues until the coordination is complete. • When the CPU is idle, the system reduces the power consumption further than with the C3 option. This option saves more power than C0 or C2, but there might be performance issues until the server returns to full power. • When the CPU is idle, the server makes a minimal amount of power available to the components. This option saves the maximum amount of power but it also requires the longest time for the server to return to high performance mode. • The server may enter any available C state. **Note** This option is used only if **CPU C State** is enabled.

Advanced: USB BIOS Settings

Name	Description
USB Port 0	Status of the USB port 0 (KVM connector). This can be one of the following: • **Disabled**—USB port 0 is disabled. • **Enabled**—USB port 0 is enabled.
USB Port 1	Status of the USB port 1 (physical port). This can be one of the following: • **Disabled**—USB port 1 is disabled. • **Enabled**—USB port 1 is enabled.

Server Management BIOS Settings

Name	Description
FRB2 Enable	Whether the FRB2 timer is used by CIMC to recover the system if it hangs during POST. This can be one of the following: • Disabled—The FRB2 timer is not used. • Enabled—The FRB2 timer is started during POST and used to recover the system if necessary.
Console Redirection	Allows a serial port to be used for console redirection during POST and BIOS booting. After the BIOS has booted and the operating system is responsible for the server, console redirection is irrelevant and has no effect. This can be one of the following: • Disabled—No console redirection occurs during POST. • Enabled —Enables serial port A for console redirection during POST. Note that **Serial Port A** option also requires that you enabled **Serial Port A** in the Advanced menu. **Note** If you enable this option, you also disable the display of the Quiet Boot logo screen during POST.
Flow Control	Whether a handshake protocol is used for flow control. Request to Send/Clear to Send (RTS/CTS) helps to reduce frame collisions that can be introduced by a hidden terminal problem. This can be one of the following: • None—No flow control is used. • RTS-CTS—RTS/CTS is used for flow control. **Note** This setting must match the setting on the remote terminal application.

Name	Description
Baud Rate	What BAUD rate is used for the serial port transmission speed. If you disable Console Redirection, this option is not available. This can be one of the following: • **9.6k**—A 9600 BAUD rate is used. • **19.2k**—A 19200 BAUD rate is used. • **38.4k**—A 38400 BAUD rate is used. • **57.6k**—A 57600 BAUD rate is used. • **115.2k**—A 115200 BAUD rate is used. **Note** This setting must match the setting on the remote terminal application.
Terminal Type	What type of character formatting is used for console redirection. This can be one of the following: • **PC-ANSI**—The PC-ANSI terminal font is used. • **VT100**—A supported VT100 video terminal and its character set are used. • **VT100-PLUS**—A supported VT100-plus video terminal and its character set are used. • **VT-UTF8**—A video terminal with the UTF-8 character set is used. **Note** This setting must match the setting on the remote terminal application.
OS Boot Watchdog Timer	Whether the BIOS programs the watchdog timer with a specified timeout value. If the operating system does not complete booting before the timer expires, the CIMC resets the system and an error is logged. This can be one of the following: • Disabled—The watchdog timer is not used to track how long the server takes to boot. • Enabled—The watchdog timer tracks how long the server takes to boot. If the server does not boot within the length of time specified

Name	Description
OS Boot Watchdog Timer Policy	The action the system takes when the watchdog timer expires. This can be one of the following: • Do Nothing—The state of the server power does not change when the watchdog timer expires during OS boot. • Power Down—The server is powered off if the watchdog timer expires during OS boot. • Reset—The server is reset if the watchdog timer expires during OS boot. **Note** This option is only applicable if you enable the OS Boot Watchdog Timer.

The following example shows the BIOS server management settings:

```
server /bios/server-management # set

BaudRate     Baud rate
BootOrderRules     Boot Order Rules
cli          CLI options
ConsoleRedir       Console redirection
FlowCtrl     Flow Control
FRB-2        FRB 2 Timer
OSBootWatchdogTimer      OS Watchdog Timer
OSBootWatchdogTimerPolicy      OS Watchdog Timer Policy
OSBootWatchdogTimerTimeout     OS Watchdog Timer Timeout
TerminalType       Terminal type

server /bios/server-management # show detail

Set-up parameters:
Baud rate: 115.2k
Boot Order Rules: CIMC-config
Console redirection: Disabled
FRB 2 Timer: Enabled
Flow Control: None
OS Watchdog Timer: Disabled
OS Watchdog Timer Policy: Reset
OS Watchdog Timer Timeout: 10 minutes
Terminal type: PC-ANSI
```

CHAPTER 4

Viewing Server Properties

-

- Viewing Server Properties, on page 39
- Viewing the Actual Boot Order, on page 40
- Viewing CIMC Information, on page 40
- Viewing CPU Properties, on page 41
- Viewing Memory Properties, on page 42
- Viewing Hard Drive Presence, on page 43
- Viewing the MAC Address of an Interface, on page 44
- Viewing the Status of CIMC Network Connections, on page 44

Viewing Server Properties

Before you begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **show detail**	Displays server properties.

Example

This example displays server properties:

```
SERVER# scope chassis
SERVER /chassis # show detail
Power: on
    IOS Lockout: unlocked
    Power Button: unlocked
    Reset Button: unlocked
    Serial Number: FOC26285PD2
    Product Name: UCS E1100D M6
    PID : UCS-E1100D-M6
    UUID: 1CD1E026-05D1-0000-2C68-107B2C231D4A
    Description:
    Asset Tag: Unknown
    FPGA Version: 2.0.2
    Uptime: 3 hours, 15 minutes
    SBFPGA Version: 22.11.8
    MCU Version: 240.10
    AIKIDO Version: 2711-270
    Last Reboot Reason: Flash Reset
SERVER /chassis #
```

Viewing the Actual Boot Order

Procedure

	Command or Action	Purpose
Step 1	Server# **scope bios**	Enters BIOS command mode.
Step 2	Server /bios # **show actual-boot-order**	Displays details of the BIOS status.

Example

The following examples display actual boot order:

```
Server# scope bios
Server /bios # show actual-boot-order
Boot Order   Type     Boot Device
------------  ------------------------- -----------------------------------
1    UEFI Image Map      UEFI Image Map
2    Internal EFI Shell  Internal EFI Shell
3    UEFI PXE TE3 IPv4   UEFI PXE TE3 IPv4
4    UEFI PXE TE4 IPv4   UEFI PXE TE4 IPv4
5    UEFI PXE GE2 IPv4   UEFI PXE GE2 IPv4
6    UEFI PXE TE0 IPv4   UEFI PXE TE0 IPv4
7    UEFI PXE TE1 IPv4   UEFI PXE TE1 IPv4
```

Viewing CIMC Information

Before you begin

Install the CIMC firmware on the server.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters CIMC command mode.

	Command or Action	Purpose
Step 2	Server /cimc # **show** [**detail**]	Displays the CIMC firmware, current time, and boot loader version.

Example

This example shows information about the CIMC:

```
server /cimc # show detail
Cisco IMC:
    Firmware Version: 4.11(0)73
    Current Time: Fri Mar 10 12:22:46 2023
    Boot-loader Version: 4.11(0)73
    Local Time: Fri Mar 10 17:52:46 2023 IST +0530 (NTP)
    Timezone: Asia/Kolkata
    Reset Reason: graceful-rebootE1100D-FOC26071VZY /cimc #
```

Viewing CPU Properties

Before you begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **show cpu** [**detail**]	Displays CPU properties.

Example

This example displays CPU properties:

```
server # scope chassis
server /chassis # show cpu
Name         Cores    Version
------------ -------- --------------------------------------------------
CPU0         10       Intel(R) Xeon(R) D-1749NT CPU @ 3.00GHz

server /chassis #
```

Viewing Memory Properties

Before you begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **show dimm** [**detail**]	Displays memory properties.

Example

This example displays memory properties:

```
Server# scope chassis
Server /chassis # show dimm
Name                 Capacity        Channel Speed (MHz) Channel Type
-------------------- --------------- ------------------- ---------------
CPU0_DIMM_A1         Not Installed   Unknown             Unknown
CPU0_DIMM_A2         Not Installed   Unknown             Unknown
CPU0_DIMM_B1         32768 MB        2400                DDR4
CPU0_DIMM_B2         32768 MB        2400                DDR4
Server /chassis #
```

This example displays detailed information about memory properties:

```
Server# scope chassis
Server /chassis # show dimm detail

Name CPU0_DIMM_A1:
    Capacity: Not Installed
    Channel Speed (MHz): NA
    Channel Type: NA
    Memory Type Detail: NA
    Bank Locator: NA
    Visibility: NA
    Operability: NA
    Manufacturer: NA
    Part Number: NA
    Serial Number: NA
    Asset Tag: NA
    Data Width: NA

Name CPU0_DIMM_A2:
    Capacity: Not Installed
    Channel Speed (MHz): NA
    Channel Type: NA
    Memory Type Detail: NA
    Bank Locator: NA
    Visibility: NA
    Operability: NA
    Manufacturer: NA
    Part Number: NA
    Serial Number: NA
    Asset Tag: NA
    Data Width: NA

Name CPU0_DIMM_B1:
    Capacity: 32768 MB
    Channel Speed (MHz): 2400
    Channel Type: DDR4
    Memory Type Detail: Synchronous Registered (Buffered)
    Bank Locator: NODE 0
    Visibility: Yes
    Operability: Operable
    Manufacturer: Hynix
    Part Number: HMAA4GR8AMR4N-UH
    Serial Number: 32657137
    Asset Tag: CPU0_DIMM_B1_AssetTag
    Data Width: 64 bits

Name CPU0_DIMM_B2:
    Capacity: 32768 MB
    Channel Speed (MHz): 2400
    Channel Type: DDR4
    Memory Type Detail: Synchronous Registered (Buffered)
    Bank Locator: NODE 0
    Visibility: Yes
    Operability: Operable
    Manufacturer: Hynix
    Part Number: HMAA4GR8AMR4N-UH
    Serial Number: 32657031
    Asset Tag: CPU0_DIMM_B2_AssetTag
    Data Width: 64 bits
```

Viewing Hard Drive Presence

Before you begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **show hdd**	Displays the hard drives.

Example

This example displays power supply properties:

```
Server# scope chassis
Server /chassis # show hdd
Name            Status
-----------          -------
HDD1_STATUS          present
HDD2_STATUS          present
HDD3_STATUS          present
```

```
HDD4_STATUS          present
```

This example displays hard disk presence and details:

```
server /chassis/hdd # show detail
    Name HDD1_STATUS:
    Status :  present
    Name HDD2_STATUS:
    Status :  present
    Name HDD3_STATUS:
    Status :  present
   Name HDD4_STATUS:
    Status :  present
```

Viewing the MAC Address of an Interface

You can view the system defined interface names and the MAC address that is assigned to each host interface.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters CIMC command mode.
Step 2	Server /cimc # **scope network**	Enters network command mode.
Step 3	Server /cimc/network # **show lom-mac-list** [**detail**]	Displays the system defined interface names and the MAC address that is assigned to each host interface.

Example

This example shows how to display the system defined interface names and the MAC address that is assigned to each host interface:

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # show lom-mac-list
Interface                      MAC Address
------------------------------ --------------------
Console                        1C:D1:E0:26:03:12
TE1                            1C:D1:E0:26:03:13
GE2                            1C:D1:E0:26:03:16
TE3                            1C:D1:E0:26:03:14
TE4                            1C:D1:E0:26:03:15
Server /cimc/network #
```

Viewing the Status of CIMC Network Connections

Before you begin

You must log in as a user with admin privileges to view the status of the CIMC network connections.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters CIMC command mode.
Step 2	Server /cimc # **scope network**	Enters CIMC network command mode.
Step 3	Server /cimc/network # **show link state [detail]**	Displays the status of the CIMC network connections; whether the link is detected (physical cable is connected to the network interface) or not detected.

Example

This example displays the status of the CIMC network connections:

```
Server /cimc/network # show link-state detail
Interface                      State
------------------------------ --------------------
Console                        Link Detected
TE1                            No Link Detected
GE2                            Link Detected
TE3                            No Link Detected
TE4                            No Link Detected
Dedicated                      No Link Detected
Server /cimc/network #
```

CHAPTER 5

Viewing Server Sensors

-
- Viewing Temperature Sensors, on page 47
- Viewing Voltage Sensors, on page 48
- Viewing LED Sensors, on page 49

Viewing Temperature Sensors

Procedure

	Command or Action	Purpose
Step 1	Server# **scope sensor**	Enters sensor command mode.
Step 2	Server /sensor # **show temperature** [**detail**]	Displays temperature sensor statistics for the server.

Example

This example displays temperature sensor statistics:

```
Server# scope sensor
Server /sensor # show temperature
Name            Sensor Status  Reading    Units  Critical  Min Critical Max  Non-Recoverable
 Min   Non-Recoverable Max
--------------   -------------- ---------- ------ --------  ----------------
-------------------- ---------------------
TEMP_SENS_FRONT   Normal         23.0       C       N/A          60.0          N/A
          70.0
TEMP_SENS_REAR    Normal         29.0       C       N/A          75.0          N/A
          85.0


Server /sensor #
```

Viewing Voltage Sensors

Procedure

	Command or Action	Purpose
Step 1	Server# **scope sensor**	Enters sensor command mode.
Step 2	Server /sensor # **show voltage** [**detail**]	Displays voltage sensor statistics for the server.

Example

This example displays voltage sensor statistics:

```
Server# scope sensor
Server /sensor # show voltage
Name     Sensor Status   Reading  Units  Critical Min  Critical Max  Non-Recoverable Min
Non-Recoverable Max
------------------------------------------------------------------------------------------
P12V       Normal        12.803      V        11.151       13.806       11.151
   13.806
P0V6_SB_BMC      Normal        0.601      V        0.569        0.632        0.569
        0.632
P5V_SB           Normal        5.031      V        4.493        5.499        4.493
        5.499
P2V5_SB          Normal        2.516      V        2.375        2.621        2.375
        2.621
P3V3_SB          Normal        3.350      V        2.970        3.634        2.970
        3.634
P0V86_SB_C827    Normal        0.858      V        0.819        0.905        0.819
        0.905
P2V5_SB_ABC      Normal        2.492      V        2.375        2.750        2.375
        2.750
P1V8_VCCIN       Normal        1.790      V        1.615        2.071        1.615
        2.071
P1V8_SB          Normal        1.802      V        1.622        1.981        1.622
        1.981
P1V1_SB_BMC      Normal        1.100      V        1.022        1.209        1.022
        1.209
P1V2_DDR4_VDD    Normal        1.225      V        1.076        1.318        1.076
        1.318
P1V8_SB_NACDELAY Normal        1.802      V        1.622        1.981        1.622
        1.981
P1V2_SB          Normal        1.193      V        1.139        1.264        1.139
        1.264
P1V_PCIE4        Normal        0.998      V        0.897        1.100        0.897
        1.100
P1V05_SB         Normal        1.061      V        0.952        1.162        0.952
        1.162
P0V74_SB_VNN     Normal        0.850      V        0.608        1.209        0.608
        1.209
P1V8_SB_PHY      Normal        1.786      V        1.622        1.981        1.622
        1.981
P1V_SB           Normal        0.991      V        0.952        1.053        0.952
        1.053
P0V6_DDR4_ABC    Normal        0.605      V        0.538        0.659        0.538
        0.659
P3V3_SB_MCU      Normal        3.318      V        2.812        3.792        2.812
```

```
        3.792
Server /sensor #
```

Viewing LED Sensors

Before you begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **show led** [**detail**]	Displays the name, state, and color of the external LEDs.

Example

This example displays information about the external LEDs:

```
Server# scope chassis
Server /chassis # show led
LED Name                  LED State  LED Color
------------------------- ---------- --------
LED_PWR_BTN               ON         GREEN
LED_HLTH_STATUS           ON         GREEN
LED_SYS                   ON         GREEN
LED_BMC_ACT               ON         GREEN
OVERALL_DIMM_STATUS       ON         GREEN

Server /chassis # show led detail
LEDs:
    LED Name: LED_PWR_BTN
    LED State: ON
    LED Color: GREEN

LEDs:
    LED Name: LED_HLTH_STATUS
    LED State: ON
    LED Color: GREEN

LEDs:
    LED Name: LED_SYS
    LED State: ON
    LED Color: GREEN

LEDs:
    LED Name: LED_BMC_ACT
    LED State: ON
    LED Color: GREEN

LEDs:
    LED Name: OVERALL_DIMM_STATUS
    LED State: ON
    LED Color: GREEN
```

CHAPTER 6

Managing Remote Presence

-
- Managing the Virtual KVM, on page 51
- Managing Serial over LAN, on page 54

Managing the Virtual KVM

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 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. You can map any of the following to a virtual drive:

- CD/DVD 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 BIOS Boot menu by pressing **F6** during bootup.
- Access the CIMC Configuration Utility by pressing **F8** during bootup.

Configuring the Virtual KVM

Before you begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# **scope kvm**	Enters KVM command mode.
Step 2	Server /kvm # **set enabled** {**yes** | **no**}	Enables or disables the virtual KVM.
Step 3	Server /kvm # **set kvm-port** *port*	Specifies the port used for KVM communications.
Step 4	Server /kvm # **set local-video** {**yes** | **no**}	If local video is **yes**, the KVM session is also displayed on any monitor attached to the server.
Step 5	Server /kvm # **set max-sessions** *sessions*	Specifies the maximum number of concurrent KVM sessions allowed. The value of the *sessions* argument is an integer between 1 and 4.
Step 6	Server /kvm # **commit**	Commits the transaction to the system configuration.
Step 7	Server /kvm # **show** [**detail**]	(Optional) Displays the virtual KVM configuration.

Example

This example configures the virtual KVM and displays the configuration:

```
Server# scope kvm
Server /kvm # set enabled yes
Server /kvm *# set kvm-port 2068
Server /kvm *# set max-sessions 4
Server /kvm *# set local-video yes
Server /kvm *# commit
Server /kvm # show detail
KVM Settings:
    Max Sessions: 4
    Local Video: yes
    Active Sessions: 0
    Enabled: yes
    KVM Port: 2068

Server /kvm #
```

What to do next

Launch the virtual KVM from the GUI.

Enabling the Virtual KVM

Before you begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# **scope kvm**	Enters KVM command mode.
Step 2	Server /kvm # **set enabled yes**	Enables the virtual KVM.
Step 3	Server /kvm # **commit**	Commits the transaction to the system configuration.
Step 4	Server /kvm # **show** [**detail**]	(Optional) Displays the virtual KVM configuration.

Example

This example enables the virtual KVM:

```
Server# scope kvm
Server /kvm # set enabled yes
Server /kvm *# commit
Server /kvm # show
Local Video        Active Sessions    Enabled       VM Port
------------------ ---------------- --------------- -------
yes                 0                 yes           2068

Server /kvm #
```

Disabling the Virtual KVM

Before you begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# **scope kvm**	Enters KVM command mode.
Step 2	Server /kvm # **set enabled no**	Disables the virtual KVM. **Note** Disabling the virtual KVM disables access to the virtual media feature, but does not detach the virtual media devices if virtual media is enabled.
Step 3	Server /kvm # **commit**	Commits the transaction to the system configuration.
Step 4	Server /kvm # **show** [**detail**]	(Optional) Displays the virtual KVM configuration.

Example

This example disables the virtual KVM:

```
Server# scope kvm
Server /kvm # set enabled no
Server /kvm *# commit
Server /kvm # show
Local Video      Active Sessions   Enabled   KVM Port
---------------- ---------------   -------   --------
yes              0                 no        2068

Server /kvm #
```

Managing Serial over LAN

Serial over LAN

Serial over LAN (SoL) is a mechanism that enables the input and output of the serial port of a managed system tobe redirected via an SSH session over IP. SoL provides a means of reaching the host console via the CIMC.

Guidelines and Restrictions for Serial over LAN

For redirection to SoL, the server console must have the following configuration:

- Console redirection to serial port A
- No flow control
- Baud rate the same as configured for SoL
- VT-100 terminal type
- Legacy OS redirection disabled

The SoL session displays line-oriented information, such as boot messages, and character-oriented screen menus, such as BIOS setup menus. If the server boots an operating system or application with a bitmap-oriented display, such as Windows, the SoL session does not display. If the server boots a command-line-oriented operating system (OS), such as Linux, you may need to perform additional configuration of the OS in order to properly display in an SoL session.

In the SoL session, your keystrokes are transmitted to the console except for the function key F2. To send an F2 to the console, press the Escape key, then press 2.

Configuring Serial Over LAN

Before you begin

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

Procedure

	Command or Action	Purpose
Step 1	Server # **scope sol**	Enters SoL command mode.

	Command or Action	Purpose
Step 2	Server /sol # **set enabled** {**yes** | **no**}	Enables or disables SoL on the server.
Step 3	Server /sol # **set baud-rate** {**9600** | **19200** | **38400** | **57600** | **115200**}	Sets the serial baud rate the system uses for SoL communication. **Note** The baud rate must match the baud rate configured in the server serial console.
Step 4	Server /sol # **commit**	Commits the transaction to the system configuration.
Step 5	Server /sol # **show** [**detail**]	(Optional) Displays the SoL settings.

Example

This example configures SoL:

```
Server# scope sol
Server /sol # set enabled yes
Server /sol *# set baud-rate 115200
Server /sol *# commit
Server /sol # show
Enabled     Baud Rate(bps)   Com Port  SOL SSH Port
-------     ---------------  --------  -------------
yes         115200           com0      2400

Server /sol #
```

Launching Serial over LAN

Procedure

	Command or Action	Purpose
Step 1	Server# **connect host**	Opens an SoL connection to the redirected server console port. You can enter this command in any command mode.

What to do next

Press the **Ctrl** and **X** keys to disconnect from SoL and return to the CLI session.

Note When you enable SoL, the output from the serial port is redirected; therefore, when you try to session into the host from Cisco IOS CLI, you will not see any output.

CHAPTER 7

Managing User Accounts

-

- Configuring Local Users, on page 57
- LDAP Servers (Active Directory), on page 58
- TACACS+ Server, on page 63
- Viewing User Sessions, on page 65
- Terminating a User Session, on page 66

Configuring Local Users

Before you begin

You must log in as a user with admin privileges to configure or modify local user accounts.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope user** *usernumber*	Enters user command mode for the user number.
Step 2	Server /user # **set enabled** {**yes** | **no**}	Enables or disables the user account on the CIMC.
Step 3	Server /user # **set name** *username*	Specifies the username for the user.
Step 4	Server /user # **set password**	Specifies the password for the user. You are prompted to enter the password twice.
Step 5	Server /user # **set role** {**readonly** | **user** | **admin**}	Specifies the role assigned to the user. The role can be one of the following: • readonly—This user can view information but cannot make any changes. • user—This user can do the following: • View all information • Manage the power control options such as power on, power cycle, and power off

	Command or Action	Purpose
		• Launch the KVM console and virtual media • Clear all logs • Toggle the locator LED • admin—This user can perform all actions available through the GUI, CLI, and IPMI.
Step 6	Server /user # **commit**	Commits the transaction to the system configuration.

Example

This example configures user 5 as an admin:

```
Server# scope user 5
Server /user # set enabled yes
Server /user *# set name john
Server /user *# set password
Please enter password:
Please confirm password:
Server /user *# set role readonly
Server /user *# commit
Server /user #  show
User   Name             Role      Enabled   SSH Key Count
------ --------------- --------  ---------  --------------
5      user             readonly  yes       (n/a)
```

LDAP Servers (Active Directory)

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

When LDAP is enabled in the CIMC, 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.

By checking the Enable Encryption check box in the **LDAP Settings** area, you can require the server to encrypt data sent to the LDAP server.

Configuring the LDAP Server

The CIMC can be configured to use LDAP for user authentication and authorization. To use LDAP, configure users with an attribute that holds the user role and locale information for the CIMC. You can use an existing LDAP attribute that is mapped to the CIMC user roles and locales, or you can modify the LDAP schema to add a new custom attribute, such as the Cisco AV Pair 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 Cisco AV Pair, but you can also use an existing LDAP attribute that is mapped to the CIMC user roles and locales.

The following steps must be performed on the LDAP server:

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

Step 2 Using the schema snap-in, add a new attribute with the following properties:

Properties	**Value**
Common Name	`CiscoAVPair`
LDAP Display Name	`CiscoAVPair`
Unique X500 Object ID	`1.3.6.1.4.1.9.287247.1`
Description	`CiscoAVPair`
Syntax	`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 CIMC:

Role	**Cisco AVPair Attribute Value**
admin	`shell:roles="admin"`
user	`shell:roles="user"`
read-only	`shell:roles="read-only"`

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

What to do next

Use the CIMC to configure the LDAP server.

Configuring LDAP in CIMC

Configure LDAP in CIMC when you want to use an LDAP server for local user authentication and authorization.

Before you begin

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

Procedure

	Command or Action	Purpose
Step 1	Server # **scope ldap**	Enters LDAP command mode.
Step 2	Server /ldap # **set enabled** {**yes** | **no**}	Enables or disables LDAP security. When enabled, user authentication and role authorization is performed by LDAP for user accounts not found in the local user database.
Step 3	Server /ldap # **set domain** *LDAP domain name*	Specifies an LDAP domain name.
Step 4	Server /ldap # **set timeout** *seconds*	Specifies the number of seconds the CIMC waits until the LDAP search operation times out. The value must be between 0 and 1800 seconds.
Step 5	Server /ldap # **set encrypted** {**yes** | **no**}	If encryption is enabled, the server encrypts all information sent to AD.
Step 6	Server /ldap # **set base-dn** *domain-name*	Specifies the Base DN that is searched on the LDAP server.
Step 7	Server /ldap # **set attribute** *name*	Specifies 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. You can use an existing LDAP attribute that is mapped to the CIMC user roles and locales or you can create a custom attribute, such as the CiscoAVPair attribute, which has the following attribute ID: `1.3.6.1.4.1.9.287247.1` **Note** If you do not specify this property, user access is denied.

	Command or Action	Purpose
Step 8	Server /ldap # **set filter-attribute**	Specifies the account name attribute. If Active Directory is used, then specify **sAMAccountName** for this field.
Step 9	Server /ldap # **commit**	Commits the transaction to the system configuration.
Step 10	Server /ldap # **show** [**detail**]	(Optional) Displays the LDAP configuration.

Example

This example configures LDAP using the CiscoAVPair attribute:

```
Server# scope ldap
Server /ldap # set enabled yes
Server /ldap *# set domain sample-domain
Server /ldap *# set timeout 60
Server /ldap *# set base-dn example.com
Server /ldap *# set attribute CiscoAVPair
Server /ldap *# set filter-attribute sAMAccountName
Server /ldap *# commit
Server /ldap # show detail
LDAP Settings:
    Enabled: yes
    Domain: sample-domain
    BaseDN: example.com
    Timeout (for each server): 60
    Filter-Attribute: sAMAccountName
    Attribute: CiscoAvPair
Server /ldap #
```

What to do next

To use LDAP groups for group authorization, see section Configuring LDAP Groups in CIMC.

Configuring LDAP Groups in CIMC

Note When Active Directory (AD) group authorization is enabled and configured, user authentication is also done on the group level for users that are not found in the local user database or who are not individually authorized to use CIMC in the Active Directory.

Before you begin

- You must log in as a user with admin privileges to perform this task.
- Active Directory (or LDAP) must be enabled and configured.

Procedure

	Command or Action	Purpose
Step 1	Server # **scope ldap**	Enters the LDAP command mode for AD configuration.
Step 2	Server /ldap# **scope ldap-group-rule**	Enters the LDAP group rules command mode for AD configuration.
Step 3	Server /ldap/ldap-group-rule # **set group-auth** {**yes** | **no**}	Enables or disables LDAP group authorization.
Step 4	Server /ldap # **scope role-group** *index*	Selects one of the available group profiles for configuration, where *index* is a number between 1 and 28.
Step 5	Server /ldap/role-group # **set name** *group-name*	Specifies the name of the group in the AD database that is authorized to access the server.
Step 6	Server /ldap/role-group # **set domain** *domain-name*	Specifies the AD domain the group must reside in.
Step 7	Server /ldap/role-group # **set role** {**admin** | **user** | **readonly**}	Specifies the permission level (role) assigned to all users in this AD group. This can be one of the following: • **admin**—The user can perform all actions available. • **user**—The user 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 • **readonly**—The user can view information but cannot make any changes.
Step 8	Server /ldap/role-group # **commit**	Commits the transaction to the system configuration.

Example

This example shows how to configure LDAP group authorization:

```
Server# scope ldap
Server /ldap # scope ldap-group-rule
Server /ldap/ldap-group-rule # set group-auth yes
Server /ldap *# scope role-group 5
Server /ldap/role-group # set name Training
Server /ldap/role-group* # set domain example.com
Server /ldap/role-group* # set role readonly
Server /ldap/role-group* # commit
ucs-c250-M2 /ldap # show role-group
Group  Group Name       Domain Name      Assigned Role
------ -----------     --------------   --------------
```

```
1       (n/a)           (n/a)           admin
2       (n/a)           (n/a)           user
3       (n/a)           (n/a)           readonly
4       (n/a)           (n/a)           (n/a)
5      Training        example.com      readonly

Server /ldap/role-group #
```

TACACS+ Server

TACACS+ is a security protocol 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. 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.

Restrictions for TACACS+ Support for CIMC

- CIMC supports connection to up to 6 TACACS+ servers.
- Users must first successfully complete TACACS+ authentication before proceeding to TACACS+ authorization.
- 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.
- Only IPv4 is supported.
- Pre-shared key (PSK) size is 32 characters.
- Supported special characters in shared secret key are: **! @% ^ * - _ .**

TACACS+ Operation

Before you begin

When a user attempts a simple ASCII login by authenticating to CIMC using TACACS+, the following options are provided:

CIMC eventually receives one of the following responses from the TACACS+ server:

- ACCEPT—The user is authenticated and service may begin. If CIMC is configured to require authorization, authorization begins at this time.

- REJECT—The user has failed to authenticate. The user may be denied further access, or will be prompted to retry the login sequence depending on the TACACS+ server.
- CONTINUE—The user is prompted for additional authentication information.

What to do next

After authentication, CIMC sends authorization request to the TACACS+ server. Based on authorization result, CIMC assigns the user's role.

Configure TACACS+ Server

Procedure

	Command or Action	Purpose
Step 1	Server # **scope tacacs+**	Enters TACACS+ configuration mode.
Step 2	Server /tacacs+ # **set enabled** [**yes** | **no**]	Enables or disables TACACS+ based authentication.
Step 3	Server /tacacs+ # **fallback-only-on-no-connectivity** [**yes** | **no**]	Enables or disables fallback to other authentication precedence.
Step 4	Server /tacacs+/tacacs-server # **scope tacacs-server 1**	Enters tacacs-server 1 configuration mode.
Step 5	Server /tacacs+/tacacs-server # **set tacacs-server** *ip-address*	Sets the TACACS server IP address.
Step 6	Server / tacacs+/tacacs-server # **set tacacs-port** *port*	Sets the TACACS port.
Step 7	Server /tacacs+/tacacs-server # **set tacacs-key** *key-string*	Sets the pre-shared key to initiate authentication with the server. The maximum length of the key is 32 characters.
Step 8	Server /tacacs+/tacacs-server # **scope tacacs-server 1**	Enters tacacs-server 1 configuration mode.
Step 9	Server /tacacs+/tacacs-server # **set tacacs-server** *ip-address*	Sets the TACACS server IP address.
Step 10	Server /tacacs+/tacacs-server # **set tacacs-port** *port*	Sets the TACACS port.
Step 11	Server /tacacs+/tacacs-server # **set tacacs-key***key-string*	Sets the pre-shared key to initiate authentication with the server. The maximum length of the key is 32 characters.
Step 12	Server /tacacs # **commit**	Commits the transaction to the system configuration.
Step 13	Server /tacacs # **show** [**detail**]	(Optional) Displays the TACACS configuration.

Example

This example shows how to configure a TACACS server:

```
Server /# scope tacacs+
Server /tacacs+ #set enabled yes
Server /tacacs+ *#set fallback-only-on-no-connectivity no
Server /tacacs+ *#commit
Server /tacacs+ #scope tacacs-server 1
Server /tacacs+/tacacs-server #set tacacs-server 10.126.254.174
Server /tacacs+/tacacs-server *#set tacacs-port 49
Server /tacacs+/tacacs-server *#set tacacs-key
Please enter tacacs-key: _Abcded_abcde_123_abcd12_zxy123_
Please confirm tacacs-key: _Abcded_abcde_123_abcd12_zxy123_
Server /tacacs+/tacacs-server #commit
```

This example shows how to verify a TACACS+ server configuration:

```
Server /tacacs+/tacacs-server #show  detail
Server Id 1:
Server IP address/Hostname: 10.126.254.174
Server Key: ******
Server Port: 49
```

Viewing User Sessions

Procedure

	Command or Action	Purpose
Step 1	Server# **show user-session**	Displays information about current user sessions.

The command output displays the following information about current user sessions:

Name	Description
Session ID column	The unique identifier for the session.
Username column	The username for the user.
IP Address column	The IP address from which the user accessed the server.
Type column	The method by which the user accessed the server. For example, CLI, vKVM, and so on.
Action column	If your user account is assigned the **admin** user role, this column displays **Terminate** if you can force the associated user session to end. Otherwise it displays **N/A**. **Note** You cannot terminate your current session from this tab.

Example

This example displays information about current user sessions:

```
Server# show user-session
ID     Name             IP Address        Type         Killable
------ ---------------- ----------------- ------------ --------
15     admin            10.20.30.138      CLI          yes

Server /user #
```

Terminating a User Session

Before you begin

You must log in as a user with admin privileges to terminate a user session.

Procedure

	Command or Action	Purpose
Step 1	Server # **show user-session**	Displays information about current user sessions. The user session to be terminated must be eligible to be terminated (killable) and must not be your own session.
Step 2	Server /user-session # **scope user-session** *session-number*	Enters user session command mode for the numbered user session that you want to terminate.
Step 3	Server /user-session # **terminate**	Terminates the user session.

Example

This example shows how the admin at user session 10 terminates user session 15:

```
Server# show user-session
ID     Name             IP Address        Type         Killable
------ ---------------- ----------------- ------------ --------
10     admin            10.20.41.234      CLI          yes
15     admin            10.20.30.138      CLI          yes

Server# scope user-session 15
Server /user-session # terminate
User session 15 terminated.

Server /user-session #
```

CHAPTER 8

Configuring Network-Related Settings

-
- CIMC NIC Configuration, on page 67
- Configuring Common Properties, on page 69
- Configuring IPv4, on page 70
- Configuring IPv6, on page 72
- Configuring the Server VLAN, on page 74
- Network Security Configuration, on page 75
- NTP Settings Configuration, on page 78

CIMC NIC Configuration

CIMC NICs

Two NIC modes are available for connection to the CIMC.

NIC Mode

- Dedicated—A connection to the CIMC is available through the management Ethernet port or ports.
- Shared LOM—A connection to the CIMC is available through the LAN On Motherboard (LOM) Ethernet host ports and through the router's PCIe and MGF interfaces.

Note In shared LOM mode, all host ports must belong to the same subnet.

The following example shows the link state:

```
server /cimc/network # show link-state detail
Interface                      State
------------------------------ --------------------
Console                        Link Detected
TE1                            No Link Detected
GE2                            No Link Detected
TE3                            No Link Detected
```

```
TE4                            No Link Detected
Dedicated                      Link Detected
```

The following example shows the LOM MAC list:

```
Server /cimc/network # show lom-mac-list
Interface                      MAC Address
------------------------------ --------------------
Console                        1C:D1:E0:26:05:A6
TE1                            1C:D1:E0:26:05:A7
GE2                            1C:D1:E0:26:05:AA
TE3                            1C:D1:E0:26:05:A8
TE4                            1C:D1:E0:26:05:A9
```

Configuring CIMC NICs

Use this procedure to set the NIC mode and Interface.

Before you begin

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

Procedure

	Command or Action	Purpose
Step 1	Server # **scope cimc**	Enters CIMC command mode.
Step 2	Server /cimc # **scope network**	Enters CIMC network command mode.
Step 3	Server /cimc/network # **set mode** {**dedicated** | **shared_lom**}	Sets the NIC mode to one of the following: • **dedicated**: The management Ethernet port is used to access the CIMC. • **shared LOM mode**: The LAN On Motherboard (LOM) Ethernet host ports are used to access the CIMC. **Note** In shared LOM mode, all host ports must belong to the same subnet.
Step 4	Server /cimc/network # **set interface** {**console** | **te1** | **ge2** | **te3** | **te4**}	Sets the NIC interface to one of the following: • **console**: Internal interface, which is used to connect either the router's PCIe interface to the E-Series server. • **te1**: Internal interface, which is used to access the CIMC over a high-speed backplane switch. • **ge2**: External interface, which can be used as a primary interface or as a backup interface. • **te3**: External interface, which can be used as a primary interface or as a backup interface.

	Command or Action	Purpose
		- **te4**: External interface, which can be used as a primary interface or as a backup interface.
Step 5	Server /cimc/network # **commit**	Commits the transaction to the system configuration. **Note** The available NIC mode and NIC redundancy mode options may vary depending on your platform. If you select a mode not supported by your server, an error message displays when you save your changes.

Example

This example configures the CIMC network interface:

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set mode shared_lom
WARNING: Changing this configuration may cause the Router network configuration to be out
of sync.
You may still commit your changes, but it is recommended that changes be done on the Router.
Server /cimc/network *# set interface ge2
WARNING: Changing this configuration may cause the Router network configuration to be out
of sync.
You may still commit your changes, but it is recommended that changes be done on the Router.
Server /cimc/network *# commit
Changes to the network settings will be applied immediately.
You may lose connectivity to the Cisco IMC and may have to log in again.
Do you wish to continue? [y/N] y
Server /cimc/network #
```

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

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters CIMC command mode.
Step 2	Server /cimc # **scope network**	Enters CIMC network command mode.
Step 3	Server /cimc/network # **set hostname** *host-name*	Specifies the name of the host.
Step 4	Server /cimc/network # **commit**	Commits the transaction to the system configuration.

Example

This example configures the common properties:

```
Server# scope cimc
Server /cimc # scope network
server /cimc/network # set hostname Server
WARNING: Changing this configuration may cause the Router network configuration to be out
of sync.
You may still commit your changes, but it is recommended that changes be done on the Router.
server /cimc/network *# commit
Changes to the network settings will be applied immediately.
You may lose connectivity to the Cisco IMC and may have to log in again.
Do you wish to continue? [y/N] y
Server /cimc/network #
```

Configuring IPv4

Before you begin

You must log in as a user with admin privileges to configure IPv4 network settings.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters CIMC command mode.
Step 2	Server /cimc # **scope network**	Enters CIMC network command mode.
Step 3	Server /cimc/network # **set dhcp-enabled** {**yes** | **no**}	Selects whether the CIMC uses DHCP. **Note** If DHCP is enabled, it is recommended that the DHCP server be configured to reserve a single IP address for the CIMC. If the CIMC is reachable through multiple ports on the server, the single IP address must be reserved for the full range of MAC addresses of those ports.
Step 4	Server /cimc/network # **set v4-addr** *ipv4-address*	Specifies the IP address for the CIMC.
Step 5	Server /cimc/network # **set v4-netmask** *ipv4-netmask*	Specifies the subnet mask for the IP address.
Step 6	Server /cimc/network # **set v4-gateway** *gateway-ipv4-address*	Specifies the gateway for the IP address.
Step 7	Server /cimc/network # **set dns-use-dhcp** {**yes** | **no**}	Selects whether the CIMC retrieves the DNS server addresses from DHCP.
Step 8	Server /cimc/network # **set preferred-dns-server** *dns1-ipv4-address*	Specifies the IP address of the primary DNS server.

	Command or Action	Purpose
Step 9	Server /cimc/network # **set alternate-dns-server** *dns2-ipv4-address*	Specifies the IP address of the secondary DNS server.
Step 10	Server /cimc/network # **commit**	Commits the transaction to the system configuration.
Step 11	Server /cimc/network # **show** [**detail**]	(Optional) Displays the IPv4 network settings.

Example

This example configures and displays the IPv4 network settings:

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set dns-use-dhcp no
WARNING: Changing this configuration may cause the Router network configuration to be out
of sync.
You may still commit your changes, but it is recommended that changes be done on the Router.
Server /cimc/network *# set dhcp-enabled no
WARNING: Changing this configuration may cause the Router network configuration to be out
of sync.
You may still commit your changes, but it is recommended that changes be done on the Router.
Server /cimc/network *# set v4-addr 10.20.30.11
WARNING: Changing this configuration may cause the Router network configuration to be out
of sync.
You may still commit your changes, but it is recommended that changes be done on the Router.
Server /cimc/network *# set v4-gateway 10.20.30.1
WARNING: Changing this configuration may cause the Router network configuration to be out
of sync.
You may still commit your changes, but it is recommended that changes be done on the Router.
Server /cimc/network *# set v4-netmask 255.255.248.0
WARNING: Changing this configuration may cause the Router network configuration to be out
of sync.
You may still commit your changes, but it is recommended that changes be done on the Router.
Server /cimc/network *# set preferred-dns-server 192.168.30.31
WARNING: Changing this configuration may cause the Router network configuration to be out
of sync.
You may still commit your changes, but it is recommended that changes be done on the Router.
Server /cimc/network *# set alternate-dns-server 192.168.30.32
WARNING: Changing this configuration may cause the Router network configuration to be out
of sync.
You may still commit your changes, but it is recommended that changes be done on the Router.
Server /cimc/network *# commit
Changes to the network settings will be applied immediately.
You may lose connectivity to the Cisco IMC and may have to log in again.
Do you wish to continue? [y/N] y
Server /cimc/network #

Server /cimc/network # show detail
Network Setting:
IPv4 Enabled: yes
IPv4 Address: 10.20.30.11
IPv4 Netmask: 255.255.248.0
IPv4 Gateway: 10.20.30.1
DHCP Enabled: no
DDNS Enabled: yes
DDNS Update Domain:
DDNS Refresh Interval(0-8736 Hr): 0
Obtain DNS Server by DHCP: no
Preferred DNS: 192.168.30.31
```

```
Alternate DNS: 192.168.30.32
IPv6 Enabled: no
IPv6 Address: ::
IPv6 Prefix: 64
IPv6 Gateway: ::
IPv6 Link Local: ::
IPv6 SLAAC Address: ::
IPV6 DHCP Enabled: no
IPV6 Obtain DNS Server by DHCP: no
IPV6 Preferred DNS: ::
IPV6 Alternate DNS: ::
VLAN Enabled: no
VLAN ID: 1
VLAN Priority: 0
Port Profile:
Hostname: Server
MAC Address: 1C:D1:E0:26:0F:81
NIC Mode: shared_lom
NIC Redundancy: none
NIC Interface: ge2
VIC Slot: 0
```

Note This configuration can take a few minutes to reflect in the **show detail** command.

Configuring IPv6

Before you begin

You must log in as a user with admin privileges to configure IPv6 network settings.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters CIMC command mode.
Step 2	Server /cimc # **scope network**	Enters CIMC network command mode.
Step 3	Server /cimc/network # **set v6-dhcp no**	Disables DHCP.
Step 4	Server /cimc/network # **set v6-enabled yes**	Enables the IPv6 addressing.
Step 5	Server /cimc/network # **set v6-addr** *ipv6-address*	Specifies the IP address for the CIMC.
Step 6	Server /cimc/network # **set v6-gateway** *gateway-ipv6address*	Specifies the gateway for the IP address.
Step 7	Server /cimc/network # **commit**	Commits the transaction to the system configuration.
Step 8	Server /cimc/network # **show** [**detail**]	(Optional) Displays the IPv4 and IPv6 network settings.

Example

This example configures and displays the IPv6 network settings:

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set v6-dhcp-enabled no
WARNING: Changing this configuration may cause the Router network configuration to be out
of sync.
You may still commit your changes, but it is recommended that changes be done on the Router.
Please set "v6-enabled" to "yes" before you commit
Otherwise your setting for "v6-dhcp-enabled" will not be reflected
Server /cimc/network *# set v6-enabled yes
WARNING: Changing this configuration may cause the Router network configuration to be out
of sync.
You may still commit your changes, but it is recommended that changes be done on the Router.
Warning: You have chosen to change IPv6 property without a valid IPv6 address.
Server /cimc/network *# set v6-addr 2001:db8:101:f101:f2f7::14
WARNING: Changing this configuration may cause the Router network configuration to be out
of sync.
You may still commit your changes, but it is recommended that changes be done on the Router.
Server /cimc/network *# set v6-gateway 2001:db8:101:f101:f2f7::1
WARNING: Changing this configuration may cause the Router network configuration to be out
of sync.
You may still commit your changes, but it is recommended that changes be done on the Router.
Server /cimc/network *# commit
Changes to the network settings will be applied immediately.
You may lose connectivity to the Cisco IMC and may have to log in again.
Do you wish to continue? [y/N] y
Server /cimc/network #

Server /cimc/network # show detail
Network Setting:
IPv4 Enabled: yes
IPv4 Address: 10.20.30.11
IPv4 Netmask: 255.255.248.0
IPv4 Gateway: 10.20.30.1
DHCP Enabled: no
DDNS Enabled: yes
DDNS Update Domain:
DDNS Refresh Interval(0-8736 Hr): 0
Obtain DNS Server by DHCP: no
Preferred DNS: 192.168.30.31
Alternate DNS: 192.168.30.32
IPv6 Enabled: yes
IPv6 Address: 2001:db8:101:f101:f2f7::14
IPv6 Prefix: 64
IPv6 Gateway: 2001:db8:101:f101:f2f7::1
IPv6 Link Local: fe80::1ed1:e0ff:fe26:f81
IPv6 SLAAC Address: 6666:1000::1ed1:e0ff:fe26:f81
IPV6 DHCP Enabled: no
IPV6 Obtain DNS Server by DHCP: no
IPV6 Preferred DNS: ::
IPV6 Alternate DNS: ::
VLAN Enabled: no
VLAN ID: 1
VLAN Priority: 0
Port Profile:
Hostname: Server
MAC Address: 1C:D1:E0:26:0F:81
NIC Mode: shared_lom
NIC Redundancy: none
NIC Interface: ge2
```

```
VIC Slot: 0
Server /cimc/network #
```

Configuring the Server VLAN

Before you begin

You must be logged in as admin to configure the server VLAN.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters CIMC command mode.
Step 2	Server /cimc # **scope network**	Enters CIMC network command mode.
Step 3	Server /cimc/network # **set vlan-enabled** {**yes** | **no**}	Selects whether the CIMC is connected to a VLAN.
Step 4	Server /cimc/network # **set vlan-id** *id*	Specifies the VLAN number.
Step 5	Server /cimc/network # **set vlan-priority** *priority*	Specifies the priority of this system on the VLAN.
Step 6	Server /cimc/network # **commit**	Commits the transaction to the system configuration.
Step 7	Server /cimc/network # **show** [**detail**]	(Optional) Displays the network settings.

Example

This example configures the server VLAN:

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set vlan-enabled yes Server /cimc/network *# set vlan-id 10 Server
/cimc/network *# set vlan-priority 32 Server /cimc/network *# commit
Server /cimc/network # show detail
Network Setting:
    IPv4 Enabled: yes
     IPv4 Address: 10.20.30.11
     IPv4 Netmask: 255.255.248.0
     IPv4 Gateway: 10.20.30.1
     DHCP Enabled: no
     DDNS Enabled: yes
     DDNS Update Domain:
     DDNS Refresh Interval(0-8736 Hr): 0
     Obtain DNS Server by DHCP: no
     Preferred DNS: 0.0.0.0
     Alternate DNS: 0.0.0.0
     IPv6 Enabled: no
     IPv6 Address: ::
     IPv6 Prefix: 64
     IPv6 Gateway: ::
     IPv6 Link Local: ::
     IPv6 SLAAC Address: ::
     IPV6 DHCP Enabled: no
     IPV6 Obtain DNS Server by DHCP: no
     IPV6 Preferred DNS: ::
     IPV6 Alternate DNS: ::
     VLAN Enabled: yes
     VLAN ID: 10
     VLAN Priority: 32
     Port Profile:
     Hostname: Server
     MAC Address: 1C:D1:E0:26:05:A5
     NIC Mode: dedicated
     NIC Redundancy: none
     NIC Interface:
     VIC Slot: 0
Server /cimc/network #
```

Network Security Configuration

Network Security

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

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

Configuring Network Security

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

Before you begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters CIMC command mode.
Step 2	Server /cimc # **scope network**	Enters CIMC network command mode.
Step 3	Server /cimc/network # **scope ipblocking**	Enters IP blocking command mode.
Step 4	Server /cimc/network/ipblocking # **set enabled** {**yes** | **no**}	Enables or disables IP blocking.
Step 5	Server /cimc/network/ipblocking # **set fail-count** *fail-count*	Sets 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.

	Command or Action	Purpose
		Enter an integer between 3 and 10.
Step 6	Server /cimc/network/ipblocking # **set fail-window** *fail-seconds*	Sets 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.
Step 7	Server /cimc/network/ipblocking # **set penalty-time** *penalty-seconds*	Sets 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 8	Server /cimc/network/ipblocking # **commit**	Commits the transaction to the system configuration.

Example

This example configures IP blocking:

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # scope ipblocking
Server /cimc/network/ipblocking # set enabled yes
Server /cimc/network/ipblocking *# set fail-count 5
Server /cimc/network/ipblocking *# set fail-window 90
Server /cimc/network/ipblocking *# set penalty-time 600
Server /cimc/network/ipblocking *# commit
Server /cimc/network/ipblocking #
```

Configuring IP Filtering

Before you begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters CIMC command mode.
Step 2	Server /cimc # **scope network**	Enters CIMC network command mode.
Step 3	Server /cimc/network # **scope ipfiltering**	Enters the IP filtering command mode.
Step 4	Server /cimc/network/ipfiltering # **set enabled** {**yes** | **no**}	Enables or disables IP filtering. At the prompt, enter **y** to enable IP filtering.
Step 5	Server /cimc/network/ipfiltering # **set filter-1** *IPv4 or IPv6 address or a range of IP addresses*	You can set up to 20 IP filters. You can assign an IPv4 or IPv6 IP address, or a range of IP addresses.

	Command or Action	Purpose
Step 6	Server /cimc/network/ipfiltering # **commit**	Commits the transaction to the system configuration.
Step 7	Server /cimc/network/nam # **showdetail**	(Optional) Displays the status of IP filtering.

Example

This example configures IP filtering:

```
Server /cimc/network # scope ipfiltering
Server /cimc/network/ipfiltering # set enabled yes
This will enable IP Filtering
Do you wish to continue? [y/N] y
Server /cimc/network/ipfiltering *# commit
Changes to the ipfiltering will be applied immediately.
You may lose connectivity to the Cisco IMC and may have to log in again.
Do you wish to continue? [y/N] y
Server /cimc/network/ipfiltering # set filter-1 1.1.1.1-255.255.255.255
Server /cimc/network/ipfiltering *# set filter-2 10.10.10.10
Server /cimc/network/ipfiltering *# set filter-3 2001:db8:101:f101:f2f7::15
Server /cimc/network/ipfiltering *# commit
Changes to the ipfiltering will be applied immediately.
You may lose connectivity to the Cisco IMC and may have to log in again.
Do you wish to continue? [y/N] y
Server /cimc/network/ipfiltering #

Server /cimc/network/ipfiltering # show detail
IP Filter Service Settings:
Enabled: yes
Filter 1: 1.1.1.1-255.255.255.255
Filter 2: 10.10.10.10
Filter 3: 2001:db8:101:f101:f2f7::15
Filter 4:
Filter 5:
Filter 6:
Filter 7:
Filter 8:
Filter 9:
Filter 10:
Filter 11:
Filter 12:
Filter 13:
Filter 14:
Filter 15:
Filter 16:
Filter 17:
Filter 18:
Filter 19:
Filter 20:
Server /cimc/network/ipfiltering #
```

NTP Settings Configuration

NTP Settings

By default, when CIMC is reset, it synchronizes the time with the host. With the introduction of the Network Time Protocol (NTP) service, you can configure CIMC to synchronize the time with an NTP server. The NTP server does not run in CIMC by default. You must enable and configure the NTP service by specifying the IP or DNS address of at least one server, or a maximum of four servers, that function as NTP servers or time source servers. When you enable the NTP service, CIMC synchronizes the time with the configured NTP server. The NTP service can be modified only through CIMC.

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

Configuring NTP Settings

Before you begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters CIMC command mode.
Step 2	Server /cimc # **scope network**	Enters CIMC network command mode.
Step 3	Server /cimc/network # **scope ntp**	Enters NTP command mode.
Step 4	Server /cimc/network/ntp # **set enabled** {**yes** | **no**}	Enables or disables the NTP service.
Step 5	Server /cimc/network/ntp # **set** [**server-1** | **server-2** | **server-3** | **server-4**] *ip-address or domain-name*	Configures the IP address or domain name for the specified server to act as an NTP server or the time source server. You can configure a maximum of four servers.
Step 6	Server /cimc/network/ntp # **show detail**	(Optional) Displays whether the NTP service is enabled and the IP address or domain name of the NTP servers.

Example

This example configures NTP settings:

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # scope ntp
Server /cimc/network/ntp # set enabled yes
Warning: IPMI Set SEL Time command will be disabled if NTP is enabled.
Do you wish to continue? [y/N] y
Server /cimc/network/ntp *# set server-1 10.50.171.9
Server /cimc/network/ntp *# set server-2 time.cisco.com
Server /cimc/network/ntp *# commit
Server /cimc/network/ntp #

Server /cimc/network/ntp # show detail
NTP Service Settings:
Enabled: yes
Server 1: 10.50.171.9
Server 2: time.cisco.com
Server 3:
Server 4:
Status: unsynchronised
Server /cimc/network/ntp #
```

CHAPTER 9

Configuring Communication Services

-
- Configuring HTTP, on page 81
- Configuring SSH, on page 82
- Enabling Redfish, on page 83
- Configuring the XML API, on page 84
- Configuring IPMI, on page 84
- Configuring SNMP, on page 86

Configuring HTTP

Before you begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# **scope http**	Enters HTTP command mode.
Step 2	Server /http # **set enabled** {**yes** | **no**}	Enables or disables HTTP and HTTPS service on the CIMC.
Step 3	Server /http # **set http-port** *number*	Sets the port to use for HTTP communication. The default is 80.
Step 4	Server /http # **set https-port** *number*	Sets the port to use for HTTPS communication. The default is 443.
Step 5	Server /http # **set timeout** *seconds*	Sets the number of seconds to wait between HTTP requests before the CIMC times out and terminates the session. Enter an integer between 60 and 10,800. The default is 1,800 seconds.
Step 6	Server /http # **commit**	Commits the transaction to the system configuration.

Example

This example configures HTTP for the CIMC:

```
Server#
Server# scope http
Server /http # set http-enabled yes
Server /http *# set http-port 80
Server /http *# set http-redirect yes
Server /http *# set https-enabled yes
Server /http *# set https-port 443
Server /http *# set timeout 1800
Server /http *# commit
Server /http # show
HTTP Port  HTTPS Port Timeout  Active Sessions HTTPS Enabled HTTP Redirected  HTTP Enabled
---------- ---------- -------- --------------- ------------- ---------------- ----------------
80         443        1800     0               yes           yes              yes

Server /http #
```

Configuring SSH

Before you begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# **scope ssh**	Enters SSH command mode.
Step 2	Server /ssh # **set enabled** {**yes** | **no**}	Enables or disables SSH on the CIMC.
Step 3	Server /ssh # **set ssh-port** *number*	Sets the port to use for secure shell access. The default is 22.
Step 4	Server /ssh # **set timeout** *seconds*	Sets the number of seconds to wait before the system considers an SSH request to have timed out. Enter an integer between 60 and 10,800. The default is 300 seconds.
Step 5	Server /ssh # **commit**	Commits the transaction to the system configuration.
Step 6	Server /ssh # **show** [**detail**]	(Optional) Displays the SSH configuration.

Example

This example configures SSH for the CIMC:

```
Server# scope ssh
Server /ssh # set enabled yes
Server /ssh *# set ssh-port 22
Server /ssh *# set timeout 600
Server /ssh *# commit
Server /ssh # show detail

SSH Port Timeout   Active Sessions   Enabled
---------      --------   ---------------   ---------
22       600  1           yes

Server /ssh #
```

Enabling Redfish

Before you begin

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

SUMMARY STEPS

1. Server # **scope redfish**
2. Server /redfish # **set enabled** {**yes** | **no**}
3. Server /redfish* # **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server # **scope redfish**	Enters redfish command mode.
Step 2	Server /redfish # **set enabled** {**yes** | **no**}	Enables or disables redfish control of Cisco IMC.
Step 3	Server /redfish* # **commit**	Commits the transaction to the system configuration.

Example

This example enables redfish control of Cisco IMC and commits the transaction:

```
Server# scope redfish
Server /redfish # set enabled yes
Server /redfish *# commit
Server /redfish # show detail
REDFISH Settings:
 Enabled: yes
 Active Sessions: 0
 Max Sessions: 4

Server /redfish #
```

For more information, see Cisco UCS C-Series Servers REST API Programmer's Guide, Release 3.0

Configuring the XML API

XML API for the CIMC

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

For detailed information about the XML API, see the CIMC XML API Programmer's Guide for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine.

Enabling the XML API

Before you begin

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

Procedure

	Command or Action	Purpose
Step 1	Server # **scope xmlapi**	Enters XML API command mode.
Step 2	Server /xmlapi # **set enabled** {**yes** | **no**}	Enables or disables XML API control of the CIMC.
Step 3	Server /xmlapi *# **commit**	Commits the transaction to the system configuration.

Example

This example enables XML API control of the CIMC and commits the transaction:

```
Server# scope xmlapi
Server /xmlapi # set enabled yes
Server /xmlapi *# commit
Server /xmlapi # show detail
XMLAPI Settings:
    Enabled: yes
    Active Sessions: 0
    Max Sessions: 4
```

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 the server temperature rises above specified levels, the server operating system can direct the BMC to increase fan speed or reduce processor speed to address the problem.

Configuring IPMI over LAN

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

Before you begin

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

Procedure

	Command or Action	Purpose
Step 1	Server # **scope ipmi**	Enters the IPMI command mode.
Step 2	Server /ipmi # **set enabled** {**yes** | **no**}	Enables or disables IPMI access on this server.
Step 3	Server /ipmi # **set privilege-level** {**readonly** | **user** | **admin**}	Specifies the highest privilege level that can be assigned to an IPMI session on this server. This can be: • **readonly** —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.
Step 4	Server /ipmi # **set encryption-key** *key*	Sets the IPMI encryption key to use for IPMI communications. The key value must be 40 hexadecimal numbers.
Step 5	Server /ipmi # **commit**	Commits the transaction to the system configuration.

Example

This example configures IPMI over LAN for the CIMC:

```
Server# scope ipmi
Server /ipmi # set enabled yes
Server /ipmi *# set privilege-level admin
Server /ipmi *# set encryption-key abcdef01234567890abcdef01234567890abcdef
Server /ipmi *# commit
Server /ipmi # show

Enabled     Encryption Key                         Privilege Level Limit
--------    ----------------------------------------    ------------------------
yes   abcdef01234567890abcdef01234567890abcdef     admin

Server /ipmi #
```

Configuring SNMP

SNMP

The Cisco UCS E-Series M6 Servers support the Simple Network Management Protocol (SNMP) for viewing server configuration and status and for sending fault and alert information by SNMP traps. For information on Management Information Base (MIB) files supported by CIMC, see the MIB Quick Reference for Cisco UCS.

Configuring SNMP Properties

Before you begin

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

Procedure

	Command or Action	Purpose
Step 1	Server # **scope snmp**	Enters SNMP command mode.
Step 2	Server /snmp # **set enabled** {**yes** | **no**}	Enables or disables SNMP. **Note** SNMP must be enabled and saved before additional SNMP configuration commands are accepted.
Step 3	Server /snmp # **commit**	Commits the transaction to the system configuration.
Step 4	Server /snmp # **set community-str** *community*	Specifies the default SNMP v1 or v2c community name that CIMC includes on any trap messages it sends to the SNMP host. The name can be up to 18 characters.
Step 5	Server /snmp # **setcommunity-access**	This can be one of the following: • Disabled • Limited

	Command or Action	Purpose
		• Full
Step 6	Server /snmp # **settrap-community-str**	Specifies the SNMP community group to which trap information should be sent. The name can be up to 18 characters.
Step 7	Server /snmp # **set sys-contact** *contact*	Specifies the system contact person responsible for the SNMP implementation. The contact information can be up to 254 characters, such as an email address or a name and telephone number. To enter a value that contains spaces, you must enclose the entry with quotation marks.
Step 8	Server /snmp # **set sys-location** *location*	Specifies the location of the host on which the SNMP agent (server) runs. The location information can be up to 254 characters. To enter a value that contains spaces, you must enclose the entry with quotation marks.
Step 9	Server /snmp # **commit**	Commits the transaction to the system configuration.

Example

This example configures the SNMP properties and commits the transaction:

```
Server# scope snmp
Server /snmp # set enabled yes
Server /snmp *# commit
Server /snmp # set community-str cimcpublic
Server /snmp # set community-access Full

Server /snmp # set trap-community-str public
Server /snmp *# set sys-contact "User Name <username@example.com> +1-408-555-1212"
Server /snmp *# set sys-location "San Jose, California"
Server /snmp *# commit Server /snmp # show detail

SNMP Settings:
 Enabled: yes
 SNMP Port: 161
 System Contact: User Name <username@example.com> +1-408-555-1212
 System Location: unknown
 SNMP v2 Enabled: yes
 Access Community String: cimcpublic
 Trap Community String: public
 SNMP Community access: full
 SNMP v3 Enabled: no
 User Input EngineID:
 SNMP Engine ID: 80 00 1F 88 80 40 EB F5 32 B7 C9 EC 63
 Serial Number Enabled: no

Server /snmp #
```

What to do next

Configure SNMP trap settings as described in section Configuring SNMP Trap Settings, on page 88.

Configuring SNMP Trap Settings

Before you begin

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

SNMP must be enabled and saved before trap settings can be configured.

Procedure

	Command or Action	Purpose
Step 1	Server # **scope snmp**	Enters SNMP command mode.
Step 2	Server /snmp # **scope trap-destinations** *number*	Enters the SNMP trap destination command mode for the specified destination. Four SNMP trap destinations are available. The destination *number* is an integer between 1 and 15.
Step 3	Server /snmp/trap-destinations # **set enabled** {**yes** | **no**}	Enables or disables the SNMP trap destination.
Step 4	Server /snmp/trap-destinations # **set version** {**1** | **2** | **3**}	Specify the desired SNMP version of the trap message. **Note** SNMPv3 traps will be delivered only to locations where the SNMPv3 user and key values are configured correctly.
Step 5	Server /snmp/trap-destinations # **set type** {**trap** | **inform**}	Specifies whether SNMP notification messages are sent as simple traps or as inform requests requiring acknowledgment by the receiver. **Note** The inform option can be chosen only for V2 users.
Step 6	Server /snmp/trap-destinations # **set user** *user*	
Step 7	Server /snmp/trap-destination # **set v4-addr** *ip-address*	Specifies the destination IP address to which SNMP trap information is sent.
Step 8	Server /snmp/trap-destination # **commit**	Commits the transaction to the system configuration.

Example

This example configures general SNMP trap settings and trap destination number 1, and commits the transaction:

```
Server# scope snmp
Server /snmp # Scope trap-destinations 1
Server /snmp/trap-destination *# set enabled yes
Server /snmp/trap-destination *# set version 2
Server /snmp/trap-destination *# set type inform
Server /snmp/trap-destination *# set user user1
Server /snmp/trap-destination *# set trap-addr 192.2.3.4
Server /snmp/trap-destination *# commit
Server /snmp/trap-destination # show detail
```

```
Trap Destination 1:
    Enabled: yes
    SNMP version: 2
    Trap type: inform
    SNMP user: unknown
    Trap Address(IPv4/IPv6/FQDN): 10.197.82.5
    Trap Port: 162
    Delete Trap: no
    Trap Community String: public
```

Sending a Test SNMP Trap Message

Before you begin

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

Procedure

	Command or Action	Purpose
Step 1	Server # **scope snmp**	Enters SNMP command mode.
Step 2	Server /snmp # **sendSNMPtrap**	Sends an SNMP test trap to the configured SNMP trap destination that are enabled. **Note** The trap must be configured and enabled in order to send a test message.

Example

This example sends a test message to all the enabled SNMP trap destinations:

```
Server# scope snmp
Server /snmp # sendSNMPtrap
SNMP Test Trap sent to the destination.
Server /snmp #
```

Configuring SNMPv3 Users

Before you begin

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

SNMP must be enabled and saved before these configuration commands are accepted.

Procedure

	Command or Action	Purpose
Step 1	Server # **scope snmp**	Enters SNMP command mode.

	Command or Action	Purpose
Step 2	Server /snmp # **scope v3users** *number*	Enters the SNMPv3 users command mode for the specified user number.
Step 3	Server /snmp/v3users # **set v3add** {**yes** | **no**}	Adds or deletes an SNMPv3 user. • **yes**—This user is enabled as an SNMPv3 user and is allowed to access the SNMP OID tree. **Note** The security name and security level must also be configured at this time or the user addition will fail. • **no**—This user configuration is deleted.
Step 4	Server /snmp/v3users # **set v3security-name** *security-name*	Enter an SNMP username for this user.
Step 5	Server /snmp/v3users # **set v3security-level** {**noauthnopriv** | **authnopriv** | **authpriv**}	Select a security level for this user. This can be one of the following: • **noauthnopriv**—The user does not require an authorization or privacy password. • **authnopriv**—The user requires an authorization password but not a privacy password. If you select this option, you must configure an authentication key. • **authpriv**—The user requires both an authorization password and a privacy password. If you select this option, you must configure an authentication key and a private encryption key.
Step 6	Server /snmp/v3users # **set v3proto** {**MD5** | **SHA**}	Select an authentication protocol for this user.
Step 7	Server /snmp/v3users # **set v3auth-key** *auth-key*	Enter an authorization password for this user.
Step 8	Server /snmp/v3users # **set v3priv-proto** {**DES** | **AES**}	Select an encryption protocol for this user.
Step 9	Server /snmp/v3users # **set v3priv-auth-key** *priv-auth-key*	Enter a private encryption key (privacy password) for this user.
Step 10	Server /snmp/v3users # **commit**	Commits the transaction to the system configuration.

Example

This example configures SNMPv3 user number 2 and commits the transaction:

```
Server# scope snmp
Server /snmp # scope v3users 2
Server /snmp/v3users # set v3add yes
Server /snmp/v3users *# set v3security-name ucsSNMPV3user
Server /snmp/v3users *# set v3security-level authpriv
Server /snmp/v3users *# set v3proto SHA
Server /snmp/v3users *# set v3auth-key
Please enter v3auth-key:ex4mp1ek3y
Please confirm v3auth-key:ex4mp1ek3y
Server /snmp/v3users *# set v3priv-proto AES
Server /snmp/v3users *# set v3priv-auth-key
Please enter v3priv-auth-key:!1@2#3$4%5^6&7*8
Please confirm v3priv-auth-key:!1@2#3$4%5^6&7*8
Server /snmp/v3users *# commit
Settings are being applied ... allow a few minutes for the process to complete
Server /snmp/v3users # show detail
User 2:
 Add User: yes
 Security Name: ucsSNMPV3user
 Security Level: authpriv
 Auth Type: SHA
 Auth Key: ******
 Encryption: AES
 Private Key: ******

Server /snmp/v3users #
```

CHAPTER 10

Managing Certificates

-
- Managing the Server Certificate, on page 93
- Generating a Certificate Signing Request, on page 93
- Creating a Self-Signed Certificate, on page 95
- Uploading a Server Certificate, on page 97

Managing the Server Certificate

Step 1 Generate the CSR from the CIMC.

Step 2 Submit the CSR file to a certificate authority that will issue and sign your certificate. If your organization generates its own self-signed certificates, you can use the CSR file to generate a self-signed certificate.

Step 3 Upload the new certificate to the CIMC.

Note The uploaded certificate must be created from a CSR generated by the CIMC. Do not upload a certificate that was not created by this method.

Generating a Certificate Signing Request

Before you begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# **scope certificate**	Enters the certificate command mode.
Step 2	Server /certificate # **generate-csr**	Launches a dialog for the generation of a certificate signing request (CSR).

You will be prompted to enter the following information for the certificate signing request:

Common Name (CN)	The fully qualified hostname of the CIMC.
Organization Name (O)	The organization requesting the certificate.
Organization Unit (OU)	The organizational unit.
Locality (L)	The city or town in which the company requesting the certificate is headquartered.
StateName (S)	The state or province in which the company requesting the certificate is headquartered.
Country Code (CC)	The two-letter ISO country code for the country in which the company is headquartered.
Email	The administrative email contact at the company.

After you have entered the requested information, the system will generate and display a certificate signing request in the console output. A CSR file will not be created, but you can copy the CSR information from the console output and paste the information into a text file.

Example

This example generates a certificate signing request:

```
Server /certificate # generate-csr
Common Name (CN): test.example.com
Organization Name (O): Example, Inc.
Organization Unit (OU): Test Department
Locality (L): San Jose
StateName (S): CA
Country Code (CC): US
Email: user@example.com
[Supported Algorithms: sha1, sha256, sha384, sha512 (Default sha384)]
Signature Algorithm: sha384
Do you want to set Challenge Password ? [y|n] (Default y)n
String Encoding utf8only/nombstr/pkix/default (Enter to skip):
Do you want to enter Subject Alternative Name parameters?[y|n]n
Continue to generate CSR?[y|N]y
Do you want self sign CSR and overwrite the current certificate?
All HTTPS and SSH sessions will be disconnected. [y|N]y

Server /certificate # show detail
Certificate Information:
    Serial Number: 3FA8AF325A18359FAFB29C518838A542D945F0EB
    Subject Country Code (CC): US
    Subject State (S): CA
    Subject Locality (L): San Jose
    Subject Organization (O): "Example
    Subject Organizational Unit (OU): Test Department
    Subject Common Name (CN): test.example.com
    Issuer Country Code (CC): US
    Issuer State (S): CA
    Issuer Locality (L): San Jose
    Issuer Organization (O): "Example
    Issuer Organizational Unit (OU): Test Department
    Issuer Common Name (CN): test.example.com
    Valid From: Mar 24 04:32:34 2023 GMT
    Valid To: Jun 26 04:32:34 2025 GMT
```

What to do next

Perform one of the following tasks:

- If you do not want to obtain a certificate from a public certificate authority, and if your organization does not operate its own certificate authority, you can allow the CIMC to internally generate a self-signed certificate from the CSR and upload it immediately to the server. Type **y** after the final prompt in the example to perform this action.
- If your organization operates its own certificate server for generating self-signed certificates, copy the command output from "-----BEGIN ..." to "END CERTIFICATE REQUEST-----" and paste to a file named csr.txt. Input the CSR file to your certificate server to generate a self-signed certificate.
- If you will obtain a certificate from a public certificate authority, copy the command output from "-----BEGIN ..." to "END CERTIFICATE REQUEST-----" and paste to a file named csr.txt. Submit the CSR file to the certificate authority to obtain a signed certificate.

If you did not use the first option, in which the CIMC internally generates and uploads a self-signed certificate, you must upload the new certificate using the **upload** command in certificate command mode.

Creating a Self-Signed Certificate

As an alternative to using a public Certificate Authority (CA) to generate and sign a server certificate, you can operate your own CA and sign your own certificates. This section shows commands for creating a CA and generating a server certificate using the OpenSSL certificate server running on Linux. For detailed information about OpenSSL, see http://www.openssl.org.

Note These commands are to be entered on a Linux server with the OpenSSL package, not in the CIMC CLI.

Before you begin

Obtain and install a certificate server software package on a server within your organization.

Procedure

	Command or Action	Purpose
Step 1	**opensslgenrsa-out***CA_keyfilenamekeysize* **Example:** `# openssl genrsa -out ca.key 1024`	This command generates an RSA private key that is used by the CA. **Note** To allow the CA to access the key without user input, do not use the -des3 option for this command. The specified file name contains an RSA key of the specified key size.

	Command or Action	Purpose
Step 2	**opensslreq-new -x509 -days** *numdays*-**key***CA_keyfilename*-**out***CA_certfilename* **Example:** `# openssl req -new -x509 -days 365 -key ca.key -out ca.crt`	This command generates a new self-signed certificatefor the CA using the specified key. The certificate is valid for the specified period. The command prompts the user for additional certificate information. The certificate server is an active CA.
Step 3	**echo"nsCertType = server" > openssl.conf** **Example:** `# echo "nsCertType = server" > openssl.conf`	This command adds a line to the OpenSSL configuration fileto designate the certificate as a server-only certificate. This designation is a defense against a man-in-the-middle attack, in which an authorized client attempts to impersonate the server. The OpenSSL configuration file openssl.conf contains the statement "nsCertType = server".
Step 4	**opensslx509-text -noout -in ca.crt** **Example:** `# openssl x509 -text -noout -in ca.crt`	This command displays the certificate.

Example

This example shows how to create a CA and to generate a server certificate signed by the new CA. These commands are entered on a Linux server running OpenSSL.

```
[root@localhost ~]# openssl genrsa -out ca.key 1024
Generating RSA private key, 1024 bit long modulus (2 primes)
...........+++++
......+++++
e is 65537 (0x010001)
[root@localhost ~]# openssl req -new -x509 -days 365 -key ca.key -out ca.crt
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:US
State or Province Name (full name) []:CA
Locality Name (eg, city) [Default City]:San Jose
Organization Name (eg, company) [Default Company Ltd]:Example
Organizational Unit Name (eg, section) []:Test Department
Common Name (eg, your name or your server's hostname) []:test.example.com
Email Address []:user@example.com
[root@localhost ~]#
[root@localhost ~]# echo "nsCertType = server" > openssl.conf
[root@localhost ~]# openssl x509 -text -noout -in ca.crt
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            33:52:14:5a:12:8d:12:9c:c1:fa:77:13:a5:0c:eb:af:83:bd:6b:68
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, ST = CA, L = San Jose, O = Example, OU = Test Department, CN =
test.example.com, emailAddress = user@example.com
```

```
        Validity
            Not Before: Mar 28 23:15:11 2023 GMT
            Not After : Mar 27 23:15:11 2024 GMT
        Subject: C = US, ST = CA, L = San Jose, O = Example, OU = Test Department, CN =
test.example.com, emailAddress = user@example.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (1024 bit)
                Modulus:
                    00:b9:a6:16:7d:bf:74:d0:10:e2:61:af:56:55:ee:
                    60:e6:57:c0:74:bd:b0:0b:7d:64:54:75:74:d8:f8:
                    7b:3e:1a:5b:cf:d4:76:6d:fb:01:92:07:d0:3b:45:
                    9c:49:22:7d:22:55:75:05:d9:94:d2:f2:7d:4b:14:
                    96:5e:fc:26:12:30:6f:1f:54:a8:40:25:e2:1a:62:
                    f8:ec:f8:be:e2:b0:fc:85:21:9b:cb:78:f7:6d:0e:
                    00:01:50:a9:07:e8:de:c2:b5:44:c5:41:c1:3a:0b:
                    93:4f:e9:94:c6:82:df:76:15:de:42:1f:b3:86:de:
                    96:0c:52:27:10:25:25:75:8d
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                71:84:61:C4:AF:E7:57:2C:B4:BB:19:22:D7:DC:7A:7F:80:E8:58:A3
            X509v3 Authority Key Identifier:
                keyid:71:84:61:C4:AF:E7:57:2C:B4:BB:19:22:D7:DC:7A:7F:80:E8:58:A3

            X509v3 Basic Constraints: critical
                CA:TRUE
    Signature Algorithm: sha256WithRSAEncryption
         89:6d:7f:72:89:29:4e:8b:da:74:ec:8b:10:78:ca:86:68:be:
         88:c2:25:79:cd:a1:dc:7d:ac:32:18:be:7d:54:6e:12:c9:53:
         de:c3:dc:b3:e7:52:1e:14:c5:1c:10:95:3f:e3:df:04:82:27:
         19:56:55:c6:96:e1:0c:cc:0a:81:05:aa:3f:a3:29:52:b3:bb:
         66:78:55:2b:b0:c5:f9:f7:bc:fb:e4:fd:30:f2:16:73:65:88:
         38:ea:6f:dc:34:44:50:ef:3b:a8:ac:22:98:34:11:bb:e8:27:
         6d:da:5d:ff:18:b9:e4:4f:22:54:b9:ab:51:1f:41:51:00:4e:
         25:f6
[root@localhost ~]#
```

What to do next

Upload the new certificate to the CIMC.

Uploading a Server Certificate

Before you begin

You must log in as a user with admin privileges to upload a certificate.

The certificate to be uploaded must be available as readable text. During the upload procedure, you will copy the certificate text and paste it into the CLI.

Note You must first generate a CSR using the CIMC certificate management CSR generation procedure, and you must use that CSR to obtain the certificate for uploading. Do not upload a certificate that was not obtained by this method.

Note All current HTTPS and SSH sessions are disconnected when the new server certificate is uploaded.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope certificate**	Enters the certificate command mode.
Step 2	Server /certificate # **upload**	Launches a dialog for entering and uploading the new server certificate.

Copy the certificate text, paste it into the console when prompted, and type CTRL+D to upload the certificate.

Example

This example uploads a new certificate to the server:

```
Server# scope certificate
Server /certificate # upload
Please paste your certificate here, when finished, press CTRL+D.
-----BEGIN CERTIFICATE-----
MIIB/zCCAWgCAQAwgZkxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJDQTEVMBMGA1UE
BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
ZgAMivyCsKgb/6CjQtsofvzxmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKONDl
GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
mK3Ku+YiORnv6DhxrOoqau8r/hyI/L43l7IPN1HhOi3oha4=
-----END CERTIFICATE-----
<CTRL+D>
```

CHAPTER 11

Configuring Platform Event Filters

•

- Platform Event Filters, on page 99
- Enabling Platform Event Alerts, on page 99
- Disabling Platform Event Alerts, on page 100
- Configuring Platform Event Filters, on page 100
- Interpreting Platform Event Traps, on page 102

Platform Event Filters

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

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

Enabling Platform Event Alerts

Procedure

	Command or Action	Purpose
Step 1	Server# **scope fault**	Enters the fault command mode.
Step 2	Server /fault # **set platform-event-enabled** {**yes** | **no**}	Enables or disables platform event alerts. At the prompt, enter **y** to enable platform event alerts.
Step 3	Server /fault # **commit**	Commits the transaction to the system configuration.
Step 4	Server /fault # **show** [**detail**]	(Optional) Displays the platform event alert configuration.

Example

This example enables platform event alerts:

```
Server# scope fault
Server /fault # set platform-event-enabled yes
Server /fault *# commit
Server /fault # show Platform Event
Enabled
yes

Server /fault #
```

Disabling Platform Event Alerts

Procedure

	Command or Action	Purpose
Step 1	Server# **scope fault**	Enters the fault command mode.
Step 2	Server /fault # **set platform-event-enabled** {**yes** | **no**}	Enables or disables platform event alerts. At the prompt, enter **n** to disable platform event alerts.
Step 3	Server /fault # **commit**	Commits the transaction to the system configuration.
Step 4	Server /fault # **show** [**detail**]	(Optional) Displays the platform event alert configuration.

Example

This example disables platform event alerts:

```
Server# scope fault
Server /fault # set platform-event-enabled no
Server /fault *# commit
Server /fault # show Platform Event
Enabled
no

Server /fault #
```

Configuring Platform Event Filters

You can configure actions and alerts for the following platform event filters:

ID	Platform Event Filter
1	Temperature Critical Assert Filter
2	Temperature Warning Assert Filter

ID	Platform Event Filter
3	Voltage Critical Assert Filter
4	Processor Assert Filter
5	Memory Critical Assert Filter
6	Drive Slot Assert Filter
7	LSI Critical Assert Filter
8	LSI Warning Assert Filter

Procedure

	Command or Action	Purpose
Step 1	Server# **scope fault**	Enters the fault command mode.
Step 2	Server /fault # **scope pef** *id*	Enters the platform event filter command mode for the specified event. See the Platform Event Filter table for event ID numbers.
Step 3	Server /fault/pef # **set action** {**none** | **reboot** | **power-cycle** | **power-off**}	Selects the desired system action when this event occurs. The action can be one of the following: • **none** —No system action is taken. • **reboot** —The server is rebooted. • **power-cycle** —The server is power cycled. • **power-off** —The server is powered off.
Step 4	Server /fault/pef # **commit**	Commits the transaction to the system configuration.

Example

This example configures the platform event alert for an event:

```
Server# scope fault
Server /fault # scope pef 1
Server /fault/pef # set action reboot Server /fault/pef *# commit
Server /fault/pef # show

Platform Event Filter      Event                            Action
----------------------    ---------------------------------    ---------
  1                   Temperature Critical Assert Filter    reboot
Server /fault/pef #
```

What to do next

If you configure any PEFs to send an alert, complete the following tasks:

- Enable platform event alerts
- Configure SNMP trap settings

Interpreting Platform Event Traps

A CIMC platform event alert sent as an SNMP trap contains an enterprise object identifier (OID) in the form `1.3.6.1.4.1.3183.1.1.0.`*`event`*. The first ten fields of the OID represent the following information: `iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).wired_for_management(3183).PET(1).version(1).version(0)`, indicating an IPMI platform event trap (PET) version 1.0 message. The last field is an event number, indicating the specific condition or alert being notified.

Platform Event Trap Descriptions

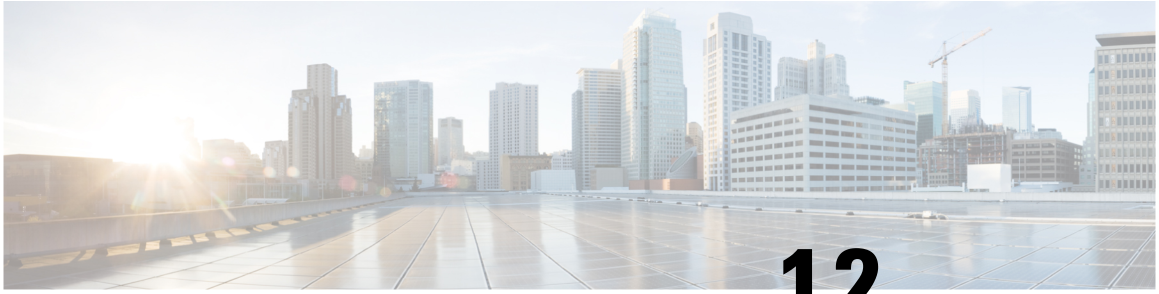
The following table provides a description of the event being notified in a platform event trap message, based on the event number in the trap OID.

Event Number		Platform Event Description
0	0h	Test Trap
65799	010107h	Temperature Warning
65801	010109h	Temperature Critical
131330	020102h	Under Voltage, Critical
131337	020109h	Voltage Critical
196871	030107h	Current Warning
262402	040102h	Fan Critical
459776	070400h	Processor related (IOH-Thermalert/Caterr sensor) – predictive failure deasserted
459777	070401h	Processor related (IOH-Thermalert/Caterr sensor) – predictive failure asserted
460032	070500h	Processor Power Warning – limit not exceeded
460033	070501h	Processor Power Warning – limit exceeded
524533	0800F5h	Power Supply Critical
524551	080107h	Power Supply Warning
525313	080401h	Discrete Power Supply Warning

Event Number		Platform Event Description
527105	080B01h	Power Supply Redundancy Lost
527106	080B02h	Power Supply Redundancy Restored
552704	086F00h	Power Supply Inserted
552705	086F01h	Power Supply Failure
552707	086F03h	Power Supply AC Lost
786433	0C0001h	Correctable ECC Memory Errors, Release 1.3(1) and later releases, filter set to accept all reading types
786439	0C0007h	DDR3_INFO sensor LED - RED bit asserted (Probable ECC error on a DIMM), Generic Sensor
786689	0C0101h	Correctable ECC Memory Errors, Release 1.3(1) and later releases
818945	0C7F01h	Correctable ECC Memory Errors, Release 1.2(x) and earlier releases
818951	0C7F07h	DDR3_INFO sensor LED - RED bit asserted (Probable ECC error on a DIMM), 1.2(x) and earlier releases
851968	0D0000h	HDD sensor indicates no fault, Generic Sensor
851972	0D0004h	HDD sensor indicates a fault, Generic Sensor
854016	0D0800h	HDD Absent, Generic Sensor
854017	0D0801h	HDD Present, Generic Sensor
880384	0D6F00h	HDD Present, no fault indicated
880385	0D6F01h	HDD Fault
880512	0D6F80h	HDD Not Present
880513	0D6F81h	HDD is deasserted but not in a fault state
884480	0D7F00h	Drive Slot LED Off
884481	0D7F01h	Drive Slot LED On

Event Number		Platform Event Description
884482	0D7F02h	Drive Slot LED fast blink
884483	0D7F03h	Drive Slot LED slow blink
884484	0D7F04h	Drive Slot LED green
884485	0D7F05h	Drive Slot LED amber
884486	0D7F01h	Drive Slot LED blue
884487	0D7F01h	Drive Slot LED read
884488	0D7F08h	Drive Slot Online
884489	0D7F09h	Drive Slot Degraded

Note When the event filter is set to accept all reading types, bits 15:8 of the hex event number are masked to 0. For example, event number 786689 (0C0101h) becomes 786433 (0C0001h).



CHAPTER 12

Firmware Management

-
- Overview of CIMC Firmware, on page 105
- Options for Upgrading Firmware, on page 106
- Obtaining Software from Cisco Systems, on page 106
- Installing CIMC Firmware from a Remote Server, on page 107
- Activating Installed CIMC Firmware, on page 108
- Changing Password Storage Format, on page 109
- Installing BIOS Firmware from the TFTP Server, on page 110
- Troubleshooting the UCS E-Series M6 Server Access Issues, on page 111

Overview of CIMC Firmware

The UCS E-Series M6 Servers use Cisco-certified firmware specific to the server model that you are using. You can download new releases of the firmware for all supported server models from Cisco.com.

To avoid potential problems, it is strongly recommended that you use the Host Upgrade Utility (HUU), which upgrades the CIMC, BIOS, and other firmware components to compatible levels.

Note Do not install the new BIOS firmware until after you have activated the compatible CIMC firmware, or the server will not boot.

The CIMC firmware update process is divided into the following stages to minimize the amount of time the server will be offline:

- **Installation**—During this stage, CIMC installs the selected CIMC firmware in the non-active, or backup, slot on the server.
- **Activation**—During this stage, CIMC sets the non-active firmware version as active and reboots the server, causing a disruption in service. When the server reboots, the firmware in the new active slot becomes the running version.

After you activate the CIMC firmware, you can update the BIOS firmware. The server must be powered off during the entire BIOS update process. Once the CIMC finishes rebooting, the server can be powered on and returned to service.

Note You can either upgrade an older firmware version to a newer one, or downgrade a newer firmware version to an older one.

Options for Upgrading Firmware

You can use the Cisco Host Upgrade Utility (HUU) to upgrade the firmware components.

HUU—We recommend that you use the HUU ISO file to upgrade all firmware components, which include the CIMC, BIOS and FPGA firmware. It is recommended to upgrade all firmware with the HUU ISO package.

Note Using the latest versions of CIMC or BIOS firmware with older versions of other firmware may result in unexpected behavior.

Obtaining Software from Cisco Systems

Use this procedure to download BIOS and CIMC firmware.

Step 1 Navigate to http://www.cisco.com/.

Step 2 If you are not already logged in, click **Log In** at the top right-hand edge of the page and log in using your Cisco.com credentials.

Step 3 In the menu bar at the top, click **Support**.

A roll-down menu appears.

Step 4 From the Downloads (center) pane, click **All Downloads** (located at the bottom right corner).

The **Download Software** page appears.

Step 5 From the left pane, click **Products**.

Step 6 From the center pane, click **Unified Computing and Servers**.

Step 7 From the right pane, click **Cisco UCS E-Series Software**.

Step 8 From the right pane, click the name of the server model for which you want to download the software.

The **Download Software** page appears with the following categories.

- **Unified Computing System (UCSE) Server Firmware**—Contains the Host Upgrade Utility.

Step 9 Click the appropriate software category link.

Step 10 Click the **Download** button associated with software image that you want to download.

The **End User License Agreement** dialog box appears.

Step 11 (Optional) To download multiple software images, do the following:

a) Click the **Add to cart** button associated with the software images that you want to download.

b) Click the **Download Cart** button located on the top right .

All the images that you added to the cart display.

c) Click the **Download All** button located at the bottom right corner to download all the images.

The **End User License Agreement** dialog box appears.

Step 12 Click **Accept License Agreement**.

Step 13 Do one of the following as appropriate:

- Save the software image file to a local drive.
- If you plan to install the software image from a TFTP server, copy the file to the TFTP server that you want to use.

  The server must have read permission for the destination folder on the TFTP server.

What to do next

Install the software image.

Installing CIMC Firmware from a Remote Server

To avoid potential problems, it is strongly recommended that you use the Host Upgrade Utility (HUU), which upgrades the CIMC, BIOS, and other firmware components to compatible levels.

Note Do not install the new BIOS firmware until after you have activated the compatible CIMC firmware or the server will not boot.

Before you begin

- Log into CIMC as a user with admin privileges.
- Obtain the CIMC firmware file from Cisco Systems.

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

Procedure

	Command or Action	Purpose
Step 1	Server # **scope cimc**	Enters CIMC command mode.
Step 2	Server /cimc # **scope firmware**	Enters CIMC firmware command mode.

	Command or Action	Purpose
Step 3	Server /cimc/firmware # **update** *protocol ip-address path*	Specifies the protocol, IP address of the remote server, and the file path to the firmware file on the server. The protocol can be one of the following: • **tftp** • **ftp** • **sftp** • **scp** • **http**
Step 4	Server /cimc # **show detail**	(Optional) Displays the progress of the firmware update.

Example

This example updates the firmware:

```
Server# scope cimc
Server /cimc # scope firmware
Server /cimc/firmware # update tftp 10.20.34.56 test/dnld-ucs-k9-bundle.1.0.2h.bin
<CR> Press Enter key Firmware update has started.

Please check the status using "show detail"

Server /cimc #
```

What to do next

Activate the new firmware.

Activating Installed CIMC Firmware

Before you begin

Install the CIMC firmware on the server.

Important While the activation is in progress, do not:

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

Note If you start an activation while an update is in process, the activation will fail.

Procedure

	Command or Action	Purpose
Step 1	Server # **scope cimc**	Enters CIMC command mode.
Step 2	Server /cimc # **scope firmware**	Enters CIMC firmware command mode.
Step 3	Server /cimc/firmware # **show** [**detail**]	Displays the available firmware images and status.
Step 4	Server /cimc # **activate**	Activates the selected image. If no image number is specified, the server activates the currently inactive image.

Example

This example activates the firmware image:

```
Server /cimc/firmware # show detail
Firmware Image Information:
    Update Stage: NONE
    Update Progress: 0%
    Current FW Version: 4.11(0)73
    FW Image 1 Version: 4.1-suthandy-030223-111138
    FW Image 1 State: BACKUP INACTIVATED
    FW Image 2 Version: 4.11(0)73
    FW Image 2 State: RUNNING ACTIVATED
    Boot-loader Version: 4.11(0)73
    Secure Boot: ENABLED

Server /cimc #
Server /cimc # activate
```

Changing Password Storage Format

This procedure explains how to change the format of the password storage.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters CIMC command mode.
Step 2	Server /cimc # **change-password-storage**	Changes the format of the password storage. You will be prompted before changing the format.

Example

This example changes the format:

```
Server# scope cimc
Server /cimc # change-password-storage

This operation will change the user password storage form to be SHA512 with salt.
Note that, once you start this operation:
1. You cannot change the password storage format back.
2. The IPMI over LAN feature will stop working.
3. You need to change the passwords of all local users to have them stored in the new format.
Are you sure you want to continue?[y|N]

Press Y to change the format.
```

Installing BIOS Firmware from the TFTP Server

To avoid potential problems, it is strongly recommended that you use the Host Upgrade Utility (HUU), which upgrades the CIMC, BIOS, and other firmware components to compatible levels.

If you choose to upgrade the CIMC and BIOS firmware manually—instead of using the HUU—you must update the CIMC firmware first, and then the BIOS firmware. Do not install the new BIOS firmware until after you have activated the compatible CIMC firmware or the server will not boot.

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

Note Before you update the BIOS firmware, power off the server and put the module in maintenance mode.

Before you begin

Obtain the CIMC firmware file from Cisco Systems.

Procedure

	Command or Action	Purpose
Step 1	Server # **scope bios**	Enters BIOS command mode.
Step 2	Server /bios # **update protocol** *ip-address path-and-filename*	Starts the BIOS firmware update. The server will obtain the update firmware at the specified path and file name from the TFTP server at the specified IP address.
Step 3	Server /bios # **show detail**	(Optional) Displays the progress of the BIOS firmware update.
Step 4	Server /bios # **activate**	Activates the installed BIOS firmware.

Example

This example updates the BIOS firmware:

```
Server# scope bios
Server /bios # update 10.20.34.56 //test/dnld-ucs-k9-bundle.1.0.2h.bin
<CR> Press Enter key
Firmware update has started.
Please check the status using "show detail"
Server /bios #
```

Troubleshooting the UCS E-Series M6 Server Access Issues

If you have problems accessing the E-Series M6 Server, it could be that the CIMC firmware image is corrupted, or the file system is corrupted, or the CIMC firmware installation did not complete successfully. Do one of the following as appropriate:

- If the CIMC firmware image is corrupted, see Recovering from a Corrupted CIMC Firmware Image, on page 111.
- If the file system is corrupted, see Recovering from a Corrupted File System, on page 113.
- If the CIMC firmware installation did not complete successfully, reinstall the CIMC firmware.

Important Due to security considerations, the **boot backup** command is disabled.

Recovering from a Corrupted CIMC Firmware Image

Before you begin

- Connect the server to your PC. Connect one end of the serial cable to the E-Series Server serial port and the other end to your PC.
- Depending on the interface option that you specify, do one of the following:
  - Dedicated—Attach an Ethernet cable to the Management (dedicated) port of the E-Series M6 Server.
  - Shared-Lom-GE2—Attach an Ethernet cable to the E-Series M6 Server’s external GE2 interface.
  - Shared-Lom-Console—Use the Cisco IOS CLI to configure the E-Series M6 Server’s internal console interface.
- To view the serial output, start the Minicom.
- Make sure that the communications settings are configured as: 9600 baud, 8 bits, No parity, and 1 stop bit.

Procedure

	Command or Action	Purpose
Step 1	Router # **hw-module subslot** *slot* **stop**	Shuts down the power to the specified E-Series M6 Server.
Step 2	Router # **hw-module subslot** *slot* **start**	Restarts the power to the specified E-Series M6 Server.
Step 3	***	From the Minicom, enter the *** command to enter the bootloader prompt.
Step 4	ucse-cimc > boot current recovery	Boots the E-Series M6 Server from the current image.
Step 5	Recovery-shell # **interface** [**dedicated** | **shared-lom-console** | **shared-lom-ge1** | **shared-lom-ge2** | **shared-lom-ge3**] *interface-ip-address* **netmask** *gateway-ip-address*	Specifies the IP address, subnet mask, and the gateway IP address of the specified interface.
Step 6	Recovery-shell # **ping** *tftp-ip-address*	Pings the remote TFTP server in which the CIMC firmware is located to verify network connectivity.
Step 7	Recovery-shell # **update** *tftp-ip-address image-filename*	Installs the CIMC firmware image, which is located on a remote TFTP server.
Step 8	Recovery-shell # **reboot**	Reboots CIMC.

Example

This example recovers the CIMC firmware image in an E-Series M6 Server:

```
Router# hw-module subslot 2/0 stop
Router# hw-module subslot 2/0 start

***

ucse-cimc > boot current recovery
recovery-shell# interface shared-lom-ge2 192.168.0.138 255.255.255.0 192.168.0.1
Network configuration:
IP config: addr: 192.168.0.138 Mask: 255.255.255.0
Gateway: 192.168.0.1
recovery-shell# ping 10.20.34.56
PING 10.20.34.56 (10.20.34.56): 56 data bytes
64 bytes from 10.20.34.56: seq=0 ttl=60 time=10.000 ms
64 bytes from 10.20.34.56: seq=1 ttl=60 time=0.000 ms
--- 10.20.34.56 ping statistics ---
10 packets transmitted, 10 packets received, 0% packet loss round-trip min/avg/max =
0.000/1.000/10.000 ms
recovery-shell# update 10.20.34.56 update_pkg-cimc.combined.bin
downloading firmware image "update_pkg-cimc.combined.bin" from " 10.20.34.56 "
download firmware image done, size in bytes: 22384144
installing firmware image, please wait ... activating installed image
done
Stage: NONE
Status: SUCCESS

Error: Success
recovery-shell# reboot
```

Recovering from a Corrupted File System

Use this procedure if you see the following error message in the CIMC boot log files.

```
UNEXPECTED INCONSISTENCY; RUN fsck MANUALLY
```

Before you begin

- Connect the server to your PC. Connect one end of the serial cable to the E-Series Server serial port and the other end to your PC.
- Depending on the interface option that you specify, do one of the following:
  - Dedicated—Attach an Ethernet cable to the Management (dedicated) port of the E-Series M6 Server.
  - Shared-Lom-GE2—Attach an Ethernet cable to the E-Series M6 Server's external GE2 interface.
  - Shared-Lom-Console—Use the Cisco IOS CLI to configure the E-Series M6 Server's internal console interface.
- To view the serial output, start the Minicom.
- Make sure that the communications settings are configured as: 9600 baud, 8 bits, No parity, and 1 stop bit.

Procedure

	Command or Action	Purpose
Step 1	Router # **hw-module subslot** *slot* **stop**	Shuts down the power to the specified E-Series M6 Server.
Step 2	Router # **hw-module subslot** *slot* **start**	Restarts the power to the specified E-Series M6 Server.
Step 3	***	From the Minicom, enter the *** command to enter the bootloader prompt.
Step 4	ucse-cimc > boot current recovery	Boots the E-Series M6 Server from the current image.
Step 5	Recovery-shell # **fs-check** [**p3** | **p4**]	Checks the file system of the specified partition and recovers the corrupted file system **Note** You can only use p3 and p4 partitions with this command. Use this command on the partition that is corrupted. The corrupted partition is the one that displays the **run fsk** error message during CIMC bootup. • If the command output displays **clean**, it indicates that the corrupted files are recovered. Enter the **reboot** command to reboot CIMC. Skip the steps that follow. • If the command output does not display **clean**, proceed to Step 6.

	Command or Action	Purpose
Step 6	Recovery-shell # **reboot**	(Optional) If the **fs-check [p3 | p4]**command does not recover the corrupted file system, and the output does not display **clean**, enter the **reboot** command to format the partitions. Skip the steps that follow. **Note** When the p3 partition is formatted, the CIMC configuration is lost.
Step 7	Recovery-shell # **interface** [**dedicated** | **shared-lom-console** | **shared-lom-ge1** | **shared-lom-ge2** | **shared-lom-ge3**] *interface-ip-address* **netmask** *gateway-ip-address*	Specifies the IP address, subnet mask, and the gateway IP address of the specified interface.
Step 8	Recovery-shell # **ping** *tftp-ip-address*	Pings the remote TFTP server in which the CIMC firmware is located to verify network connectivity.
Step 9	Recovery-shell # **update** *tftp-ip-address image-filename*	Installs the CIMC firmware image, which is located on a remote TFTP server.
Step 10	Recovery-shell # **reboot**	Reboots CIMC.

Example

This example recovers the CIMC firmware from the current image using the **fs-checkp3** command in an E-Series M6 Server:

```
Router# hw-module subslot 1/0 stop
Router# hw-module subslot 1/0 start

***

ucse-cimc > boot current recovery
recovery-shell# fs-check p3
e2fsck 1.41.14 (22-Dec-2010)
/dev/mmcblk0p3: recovering journal
/dev/mmcblk0p3: clean, 429/7840 files, 3331/31296 blocks
recovery-shell# fs-check p4
e2fsck 1.41.14 (22-Dec-2010)
/dev/mmcblk0p4: clean, 51/506912 files, 1880262/2025296 blocks
recovery-shell# reboot
```

Recovery Shell Commands

Recovery Shell Commands	Description
Recovery-shell # **dedicated-interface** *interface-ip-address netmask gateway-ip-address*	Specifies the IP address, subnet mask, and the gateway IP address of the dedicated interface.
Recovery-shell # **dedicated-interface (DEPRECATED)**	Shows the current configuration of the dedicated port.

Recovery-shell # **interface [dedicated | shared-lom-console | shared-lom-ge1 | shared-lom-ge2 | shared-lom-ge3]** *interface-ip-address netmask gateway-ip-address*	Specifies the IP address, subnet mask, and the gateway IP address of the specified interface.
Recovery-shell # **interface**	Shows the configuration on the interface.
Recovery-shell # **ping** *tftp-ip-address*	Pings the remote TFTP server in which the CIMC firmware is located to verify network connectivity.
Recovery-shell # **update** *tftp-ip-address image-filename*	Installs the CIMC firmware image, which is located on a remote TFTP server.
Recovery-shell # **fs-check [p3 | p4]**	Checks the file system of the specified partition and recover the corrupted file system.
Recovery-shell # **active image**	Shows the current active image that CIMC is running, which can be image 1 or image 2.
Recovery-shell # **active image [1 | 2]**	Changes the active image to 1 or 2. If the specified image is already active, a message is displayed. Otherwise, the specified image is made active. After you use the active image command, use the **reboot** command for the newly configured image to take effect.
Recovery-shell # **reboot**	Reboots the CIMC firmware.

Recovering Password

Before you begin

- Connect the server to your PC. Connect one end of the serial cable to the E-Series Server serial port and the other end to your PC.
- Depending on the interface option that you specify, do one of the following:
  - Dedicated—Attach an Ethernet cable to the Management (dedicated) port of the E-Series M6 Server.
  - Shared-Lom-GE2—Attach an Ethernet cable to the E-Series M6 Server's external GE2 interface.
  - Shared-Lom-Console—Use the Cisco IOS CLI to configure the E-Series M6 Server's internal console interface.
- To view the serial output, start the Minicom.
- Make sure that the communications settings are configured as: 9600 baud, 8 bits, No parity, and 1 stop bit.

Step 1 Router # **hw-module subslot** *1/0* **oir power-cycle**

Power-cycles the E-Series M6 Server.

Step 2 Type '***' to Stop Autoboot: 0”

At this prompt, type ****.

Step 3 ucse-cimc > **boot current recovery**

Type **`boot current recovery`** to boot up into recovery mode.

Step 4 Recovery-shell #

```
Recovery-shell is a menu-driven limited functionality interface
```

```
main options:
```

```
1. configure interface
   2. show interfaces
   3. ping
   4. cimc image options
   5. emmc options
   6. admin password reset
   7. enter debug shell
   8. exit and reboot
```

Step 5 Recovery-shell (enter your choice) # **emmc format p3**

Formats the p3 partition on the EMMC card that will clear the configuration, including the password.

Note When you partition EMMC, the contents of the EMMC card, such as the CIMC configuration, ISO file and password, are either lost or cleared.

```
ACT2 Reset Completed. Kindly reboot the system and login with default password. Recovery-shell is a
menu-driven limited functionality interface main options:
```

```
1. configure interface
  2. show interfaces
  3. ping
  4. cimc image options
  5. emmc options
  6. admin password reset
  7. enter debug shell
  8. exit and reboot
```

Step 6 Recovery shell (enter your choice) # **8**

```
Press 8 to exit and reboot the device
```

Example

This example recovers the password if you do not remember the CMIC password:

```
server # login: admin
Password:
***************WARNING!*****************
Default credentials were used for login.
   Administrator password needs to be
     changed for security purposes.
****************************************
Enter current password: password
Please change the password...
```

```
Enter new password: <strong-password>
Re-enter new password: <strong-password>
Updating password...
Password updated successfully.
```

CHAPTER 13

Viewing Faults and Logs

-
- Faults, on page 119
- System Event Log, on page 120
- Cisco IMC Log, on page 121

Faults

Viewing the Fault Summary

Procedure

	Command or Action	Purpose
Step 1	Server# **scope fault**	Enters fault command mode.
Step 2	Server /fault # **show discrete-alarm** [**detail**]	Displays a summary of faults from discrete sensors.
Step 3	Server /fault # **show threshold-alarm** [**detail**]	Displays a summary of faults from threshold sensors.
Step 4	Server /fault # **show pef** [**detail**]	(Optional) Displays a summary of platform event filters.

Example

This example displays a summary of faults from discrete sensors:

```
Server# scope fault
Server /fault # show discrete-alarm
Name              Reading          Sensor Status
-------------    ------------     ----------------
PSU2_STATUS       absent           Critical

Server /fault #
```

System Event Log

Viewing the System Event Log

Procedure

	Command or Action	Purpose
Step 1	Server# **scope sel**	Enters the system event log (SEL) command mode.
Step 2	Server /sel # **show entries** [**details**]	(Optional) For system events, displays timestamp, the severity of the event, and a description of the event. The **`detail`** keyword displays the information in a list format instead of a table format.

Example

This example displays the system event log:

```
Server# scope sel
Server /sel # show entries
Time                        Severity          Description
-----------------------     -------------     ----------------------------------------
2023-06-30 21:17:53 UTC     Informational     "LED_BMC_ACT: Platform sensor, "
2023-06-30 21:17:53 UTC     Informational     "LED_BMC_ACT: Platform sensor, "
2023-06-30 21:17:52 UTC     Informational     "LED_SYS: Platform sensor, "
2023-06-30 21:17:52 UTC     Informational     "LED_SYS: Platform sensor, "
2023-06-30 21:17:51 UTC     Informational     "LED_HLTH_STATUS: Platform sensor, "
2023-06-30 21:17:51 UTC     Informational     "LED_HLTH_STATUS: Platform sensor, "
2023-06-30 21:17:50 UTC     Informational     "LED_PWR_BTN: Platform sensor, "
2023-06-30 21:17:50 UTC     Informational     "LED_PWR_BTN: Platform sensor, "
2023-06-30 21:17:50 UTC     Normal            "P1_PRESENT: Presence sensor, Device Removed
 / Device Absent was asserted"
2023-06-30 21:17:50 UTC     Normal            "BIOS_POST_CMPLT: Presence sensor, Device
Removed / Device Absent was asserted"
2023-06-30 21:17:50 UTC     Normal            "MINI_STORAGE_PRS: Presence sensor, Device
Removed / Device Absent was asserted"
2023-06-30 21:17:50 UTC     Normal            "MAIN_POWER_PRS: Presence sensor, Device
Inserted / Device Present was asserted"
2023-06-30 21:17:50 UTC    Normal           "HDD4_STATUS: Drive Slot sensor, Drive Presence
 was asserted"
sence was asserted" UTC     Normal            "HDD3_STATUS: Drive Slot sensor, Drive
Pre--More--
2023-06-30 21:17:50 UTC    Normal           "HDD2_STATUS: Drive Slot sensor, Drive Presence
 was asserted"
2023-06-30 21:17:50 UTC    Normal           "HDD1_STATUS: Drive Slot sensor, Drive Presence
 was asserted"
2023-06-30 21:17:50 UTC     Normal            "RISER3_PRESENT: Presence sensor, Device
Removed / Device Absent was asserted"
2023-06-30 21:17:50 UTC     Normal            "RISER2_PRESENT: Presence sensor, Device
Removed / Device Absent was asserted"
2023-06-30 21:17:50 UTC     Normal            "RISER1_PRESENT: Presence sensor, Device
Removed / Device Absent was asserted"
```

Clearing the System Event Log

Procedure

	Command or Action	Purpose
Step 1	Server# **scope sel**	Enters the system event log command mode.
Step 2	Server /sel # **clear**	You are prompted to confirm the action. If you enter **y** at the prompt, the system event log is cleared.

Example

This example clears the system event log:

```
Server# scope sel
Server /sel # clear
This operation will clear the whole sel.
Continue?[y|N]y
```

Cisco IMC Log

Viewing the CIMC Log

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters CIMC command mode.
Step 2	Server /cimc # **scope log**	Enters CIMC log command mode.
Step 3	Server /cimc/log # **show entries** [**detail**]	(Optional) Displays CIMC events, including timestamp, the software module that logged the event, and a description of the event.

Example

This example displays the log of CIMC events:

Recovery-shell# **`fs-check [p3| p4]`**	Checks the file system of the specified partition and recover the corrupted file system.
Recovery-shell# **`active image`**	Shows the current active image that CIMC is running, which can be image 1 or image 2.

Recovery-shell# **`active image [1 | 2]`**	Changes the active image to 1 or 2. If the specified image is already active, a message is displayed. Otherwise,the specified image is made active. After you use the active image command, use the **reboot** command for the newly configured image to take effect.
Recovery-shell# **`reboot`**	Reboots the CIMC firmware.

CHAPTER 14

Server Utilities

-

- Exporting Technical Support Data to a Remote Server, on page 123
- Rebooting the CIMC, on page 125
- Resetting the CIMC to Factory Defaults, on page 125
- Exporting and Importing the CIMC Configuration, on page 126

Exporting Technical Support Data to a Remote Server

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

Procedure

	Command or Action	Purpose
Step 1	Server # **scope cimc**	Enters CIMC command mode.
Step 2	Server /cimc # **scope tech-support**	Enters tech-support command mode.
Step 3	Server /cimc/tech-support # **set remote-ip** *ip-address*	Specifies the IP address of the remote server on which the support data file should be stored.
Step 4	Server /cimc/tech-support # **set remote-path** *path/filename*	Specifies the filename for the support data to be stored on the server. When you enter this name, include the relative path for the file from the top of the server tree to the desired location.
Step 5	Server /cimc/tech-support # **set remote-protocol** *protocol-type*	Specifies the remote server protocol. The remote server protocol can be one of the following: • **tftp** • **ftp** • **sftp** • **scp**

	Command or Action	Purpose
		• **http**
Step 6	Server /cimc/tech-support # **set remote-username** *username*	(Optional) The username that the system should use to log in to the remote server. **Note** The username is not applicable if the remote server is TFTP or HTTP.
Step 7	Server /cimc/tech-support # **set remote-password** *password*	(Optional) The password for the remote username. **Note** The password is not applicable if the remote server is TFTP or HTTP.
Step 8	Server /cimc/tech-support # **commit**	Commits the transaction to the system configuration.
Step 9	Server /cimc/tech-support # **start**	Begins the transfer of the support data file to the remote server.
Step 10	Server /cimc/tech-support # **show detail**	Displays the status of the file upload.
Step 11	Server /cimc/tech-support # **cancel**	(Optional) Cancels the transfer of the support data file to the remote server.

Example

This example creates a support data file and transfers the file to a TFTP server:

```
Server# scope cimc
Server /cimc # scope tech-support
Server /cimc/tech-support # set remote-ip 10.20.30.41
Server /cimc/tech-support *# set remote-path /user/user1/supportfile
Server /cimc/tech-support *# set remote-protocol tftp
Server /cimc/tech-support *# commit
Server /cimc/tech-support # start
 Tech Support upload started.
Server /cimc/tech-support # show detail
Tech Support:
    Server Address: 10.20.30.41
    Path: /user/user1/supportfile Protocol: tftp
    Username:
    Password: ******
    Progress(%): 0
    Status: COLLECTING

Server /cimc/tech-support # show detail
Tech Support:
    Server Address: 10.20.30.41
    Path: /user/user1/supportfile
    Protocol: tftp
    Username:
    Password: ******
    Progress(%): 85
    Status: COLLECTING

Server /cimc/tech-support # show detail
Tech Support:
```

```
Server Address: 10.20.30.41
Path: /user/user1/supportfile
Protocol: tftp
Username:
Password: ******
Progress(%): 100
Status: COMPLETED
```

What to do next

Provide the generated report file to Cisco TAC.

Rebooting the CIMC

On rare occasions, such as an issue with the current running firmware, troubleshooting a server may require you to reboot the CIMC. This procedure is not part of the normal maintenance of a server. After you reboot the CIMC, you are logged off and the CIMC will be unavailable for a few minutes.

Note If you reboot the CIMC while the server is performing power-on self test (POST) or is operating in the Extensible Firmware Interface (EFI) shell, the server will be powered down until the CIMC reboot is complete.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters CIMC command mode.
Step 2	Server /cimc # **reboot**	After the prompt to confirm, reboots the CIMC.

Example

This example reboots the CIMC:

```
Server# scope cimc
Server /cimc # reboot
This operation will reboot the CIMC.
Continue?[y|N]y
```

Resetting the CIMC to Factory Defaults

On rare occasions, such as an issue with the current running firmware, troubleshooting a server may require you to reset the CIMC to the factory default. When this happens, all user-configurable settings are reset.

This procedure is not part of the normal server maintenance. After you reset the CIMC, you are logged off and must log in again. You may also lose connectivity and may need to reconfigure the network settings.

Procedure

	Command or Action	Purpose
Step 1	Server # **scope cimc**	Enters CIMC command mode.
Step 2	Server /cimc # **factory-default**	After a prompt to confirm, the CIMC resets to factory defaults.

The CIMC factory defaults include the following conditions:

- SSH is enabled for access to the CIMC CLI.
- HTTPS is enabled for access to the CIMC GUI.
- A single user account exists (username is **admin**, and the password is **password**).
- DHCP is enabled on the management port.
- The boot order is CDROM, PXE (using LoM), FDD, HDD.
- KVM and vMedia are enabled.
- USB is enabled.
- SoL is disabled.

Example

This example resets the CIMC to factory defaults:

```
Server# scope cimc
Server /cimc # factory-default
This operation will reset the CIMC configuration to factory default.
All your configuration will be lost.
Continue?[y|N]
```

Exporting and Importing the CIMC Configuration

Exporting and Importing the CIMC Configuration

To perform a backup of the CIMC configuration, you can take a snapshot of the system configuration and export the resulting CIMC 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 CIMC configuration file to the same system or you can import it to another CIMC system, provided that the software version of the importing system is the same as or is configuration-compatible with the software version of the exporting system. When you import a configuration file to another system as a configuration template, you must modify system-specific settings such as IP addresses and host names. An import operation modifies information on the management plane only.

The CIMC configuration file is an XML text file whose structure and elements correspond to the CIMC command modes.

When performing 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.

Exporting the CIMC Configuration

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

Before you begin

- Obtain the backup TFTP server IP address.
- If you want the option to restore the SNMP configuration information when you import the configuration file, make sure thatSNMP is enabled on this server before you create the configuration file. If SNMP is disabled when you export the configuration, the CIMC will not apply the SNMP values when the file is imported.

Procedure

	Command or Action	Purpose
Step 1	Server # **scope cimc**	Enters CIMC command mode.
Step 2	Server /cimc # **scope import-export**	Enters import-export command mode.
Step 3	Server /cimc/import-export # **export-config** *tftp-ip-address path-and-filename*	Starts the backup operation. The configuration file will be stored at the specified path and file name on the TFTP server at the specified IP address.

To determine whether the export operation has completed successfully, use the **show detail** command. To abort the operation, type CTRL+C.

Example

This example shows how to back up the CIMC configuration:

```
Server# scope cimc
Server /cimc # scope import-export
Server /cimc/import-export # export-config 192.0.2.34 /ucs/backups/cimc5.xml
Export config started. Please check the status using "show detail".
Server /cimc/import-export # show detail
Import Export: Operation: EXPORT Status: COMPLETED
Error Code: 100 (No Error) Diagnostic Message: NONE

Server /cimc/import-export #
```

Importing a CIMC Configuration

Before you begin

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

Procedure

	Command or Action	Purpose
Step 1	Server # **scope cimc**	Enters CIMC command mode.
Step 2	Server /cimc # **scope import-export**	Enters import-export command mode.
Step 3	Server /cimc/import-export # **import-config** *tftp-ip-address path-and-filename*	Starts the import operation. The configuration file at the specified path and file name on the TFTP server at the specified IP address will be imported.

To determine whether the import operation has completed successfully, use the **show detail** command. To abort the operation, type CTRL+C.

Example

This example shows how to import a CIMC configuration:

```
Server /cimc/import-export # import-config tftp 192.0.2.34 /ucs/backups/cimc5.xml
Passphrase:
Import config started. Please check the status using "show detail".

Server /cimc/import-export # show detail
Import Export:
Operation: IMPORT
Status: TRANSFERING
Error Code: 0 (No Error)
Diagnostic Message: NONE
Server /cimc/import-export #
```