Cisco UCS Integrated Management Controller GUI Configuration Guide for S3260 Servers, Release 4.3

First Published: 2023-08-16

Last Modified: 2024-02-15

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

CONTENTS

Preface

This preface includes the following sections:

Audience

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

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

Conventions

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

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

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

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

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

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

Warning IMPORTANT SAFETY INSTRUCTIONS

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

SAVE THESE INSTRUCTIONS

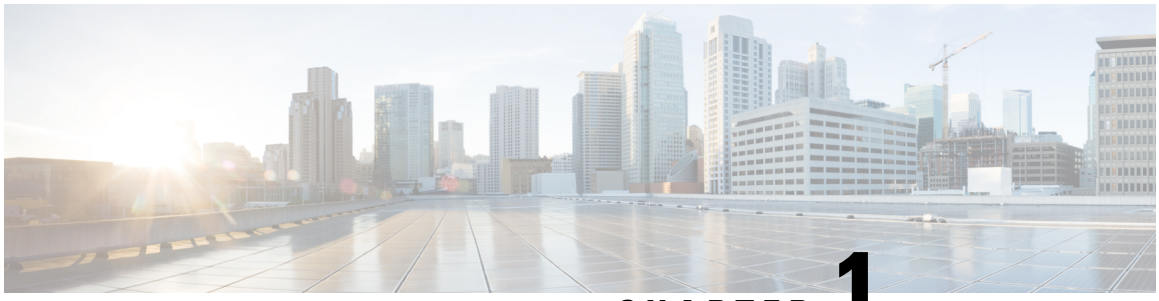
Related Cisco UCS Documentation

Documentation Roadmaps

For a complete list of all B-Series documentation, see the *Cisco UCS B-Series Servers Documentation Roadmap* available at the following URL: https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/overview/guide/UCS_roadmap.html

For a complete list of all C-Series documentation, see the *Cisco UCS C-Series Servers Documentation Roadmap* available at the following URL: https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/overview/guide/ucs_rack_roadmap.html.

For information on supported firmware versions and supported UCS Manager versions for the rack servers that are integrated with the UCS Manager for management, refer to Release Bundle Contents for Cisco UCS Software.



CHAPTER 1

Overview

This chapter includes the following sections:

Overview of the Cisco UCS S-Series Rack-Mount Server S3260

The Cisco UCS S3260 is a modular, dense storage server with dual M3, M4 or M5 server nodes, optimized for large datasets used in environments such as big data, cloud, object storage, and content delivery.

The UCS S3260 chassis is a modular architecture consisting of the following modules:

- Base chassis: contains four redundant, hot-pluggable power supplies, eight redundant, hot-pluggable fans, and a rail kit.
- Server Node: one or two M3, M4 or M5 server nodes, each with two CPUs, 64, 128, 256, or 512 GB of DIMM memory, and a pass-through controller or a RAID card with a 1 GB or 4 GB cache.
- System I/O Controller (SIOC): one or two System I/O Controllers, each of which includes an integrated 1300-series or 1400-series virtual interface capability.
- Optional Drive Expansion Node: Large Form Factor (LFF) 3.5-inch drives in a choice of capacities.
- Solid State Drives: Up to 14 solid-state disks (SSDs) of 400GB, 800 GB, 1.6TB, and 3.2 TB capacities. These replace the previously supported top-loading LFF HDDs.
- Solid-State Boot Drives: up to two SSDs per M3, M4, or M5 server node. On the M4 server node, boot drives support hardware RAID connected to the RAID controller on the server node.
- I/O Expander: provides one storage mezz slot with two PCIe expansion slots and up to two NVMe SSDs.

The enterprise-class UCS S3260 storage server extends the capabilities of Cisco's Unified Computing System portfolio in a 4U form factor that delivers the best combination of performance, flexibility, and efficiency gains.

Note An M3 Server Node has Intel E5-2600 V2 CPUs and DDR-3 DIMMs. An M4 Server Node has Intel E5-2600 v4 CPUs and DDR-4 DIMMs

Overview of the Server Software

The Cisco UCS S-Series Rack-Mount Server ships with the Cisco IMC firmware.

Cisco IMC Firmware

Cisco IMC is a separate management module built into the motherboard. A dedicated ARM-based processor, separate from the main server CPU, runs the Cisco IMC firmware. The system ships with a running version of the Cisco IMC firmware. You can update the Cisco IMC firmware, but no initial installation is needed.

Server OS

The Cisco UCS S-Series rack server supports operating systems such as Windows, Linux, Oracle and so on. For more information on supported operating systems, see the *Hardware and Software Interoperability for Standalone C-series servers* at http://www.cisco.com/en/US/products/ps10477/prod_technical_reference_list.html. You can use Cisco IMC to install an OS on the server using the KVM console and vMedia.

Note You can access the available OS installation documentation from the *Cisco UCS C-Series Servers Documentation Roadmap* at http://www.cisco.com/go/unifiedcomputing/c-series-doc.

Server Ports

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

Table 1: Server Ports

Port Name	Port Number
LDAP Port 1	389
LDAP Port 2	389
LDAP Port 3	389
LDAP Port 4	3268
LDAP Port 5	3268
LDAP Port 6	3268
SSH Port	22

Port Name	Port Number
HTTP Port	80
HTTPS Port	443
SMTP Port	25
KVM Port	2068
Intersight Management Port	8889
Intersight Cloud Port	8888
SOL SSH Port	2400
SNMP Port	161
SNMP Traps	162
External Syslog	514

Cisco Integrated Management Controller

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

Note The Cisco IMC management service is used only when the server is operating in Standalone Mode. If your C-Series server is integrated into a UCS system, you must manage it using UCS Manager. For information about using UCS Manager, see the configuration guides listed in the *Cisco UCS B-Series Servers Documentation Roadmap* at http://www.cisco.com/go/unifiedcomputing/b-series-doc.

Management Interfaces

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

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

Tasks You Can Perform in Cisco IMC

You can use Cisco IMC to perform the following chassis management tasks:

- Power on, power off, power cycle, reset and shut down the server
- Toggle the locator LED

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

You can use Cisco IMC to perform the following server management tasks:

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

No Operating System or Application Provisioning or Management

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

- Deploy an OS, such as Windows or Linux
- Deploy patches for software, such as an OS or an application
- Install base software components, such as anti-virus software, monitoring agents, or backup clients
- Install software applications, such as databases, application server software, or web servers

- Perform operator actions, including restarting an Oracle database, restarting printer queues, or handling non-Cisco IMC user accounts
- Configure or manage external storage on the SAN or NAS storage

Overview of the Cisco IMC User Interface

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

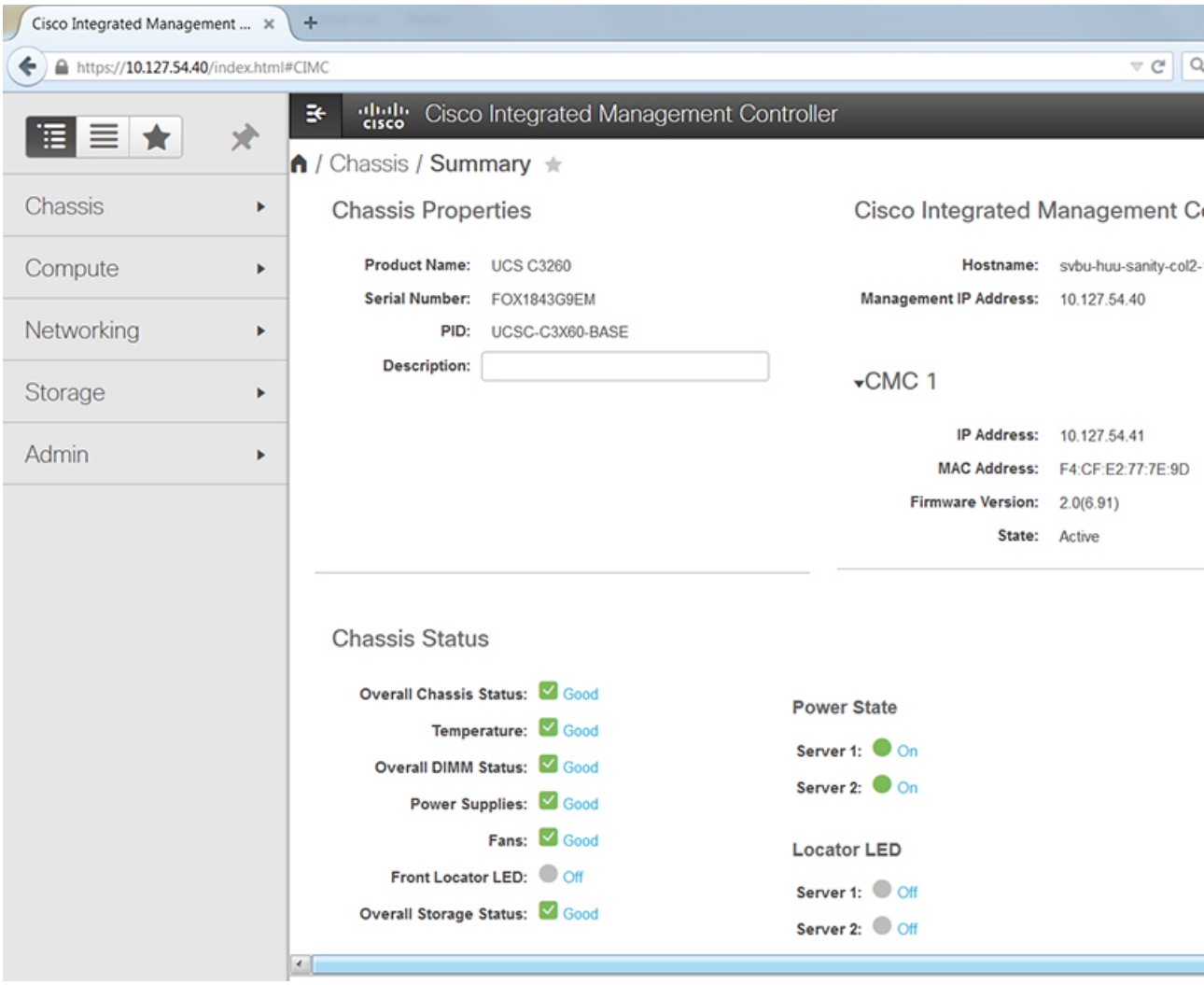
- Microsoft Internet Explorer 6.0 or higher, Mozilla Firefox 3.0 or higher
- Microsoft Windows 7, Microsoft Windows XP, Microsoft Windows Vista, Apple Mac OS X v10.6, Red Hat Enterprise Linux 5.0 or higher operating systems
- Transport Layer Security (TLS) version 1.3

Note In case you lose or forget the password that you use to log in to Cisco IMC, see the password recovery instructions in the Cisco UCS C-Series server installation and service guide for your server. This guide is available from the *Cisco UCS C-Series Servers Documentation Roadmap* at http://www.cisco.com/go/unifiedcomputing/c-series-doc.

Cisco IMC Home Page

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

Note There may be user interface changes, which do not have functionality impact, from release to release.



Navigation and Work Panes

The Cisco Integrated Management Controller GUI comprises the **Navigation** pane on the left hand side of the screen and the **Work** pane on the right hand side of the screen. Clicking links on the **Chassis**, **Compute**, **Networking**, **Storage** or **Admin** menu in the **Navigation** pane displays the associated tabs in the pane on the right.

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

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

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

On the right of the GUI header is a gear icon. Click on the gear icon and the drop-down lists the **Change Password** and **Logout** options. You can use the change password option to change your password.

Note When you change your password you will be logged out of Cisco IMC.

Note **Change Password** option is not available when you login as an admin, you can only change the password of the configured users with read-only user privileges.

When you change your password you will be logged out of Cisco IMC.

The Logout option allows you to log out of Cisco IMC.

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

Note User interface options may vary depending on the server.

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

- **Chassis** Menu
- **Compute** Menu
- **Networking** Menu
- **Storage** Menu
- **Admin** Menu

Chassis Menu

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

Chassis Menu Node Name	Work Pane Provide Information About...
Summary	Chassis properties, Chassis status, Cisco Integrated Management Controller (Cisco IMC) Information, IP and MAC addresses of CMC 1 and CMC 2, Firmware versions, SIOC PIDs, State of CMC 1 and CMC 2, Power Utilization, and Server Utilization.
Inventory	Servers, Power Supplies, Cisco VIC adapters, Dynamic Storage.
Sensors	Power Supply, Fan, Temperature, Voltage, Current, LEDs
Power Management	Power Cap Configuration and Power Monitoring.
Faults and Logs	Fault summary, Fault history, System Event Log, Cisco IMC Log, and logging controls.

Compute Menu

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

Compute Menu Node Name	Work Pane Tabs Provide Information About...
General	Server properties that include product name, serial number, product ID, UUID, BIOS version, hostname, Cisco IMC firmware version, IP address, and MAC address and description.
Inventory	CPU, Memory, PCI Adapters, vNICs, Storage, TPM, IO Expander, Network Adapters, and GPU Inventory.
Sensors	Temperature, Voltage, LEDs, and Storage.
BIOS	The installed BIOS firmware version and BIOS profile configuration, server boot order configuration, I/O, Server management, Security, Processor, Memory, Power or Performance.
Remote Management	Virtual KVM, Virtual Media, and Serial over LAN.
Troubleshooting	Bootstrap Process Recording Actions include Play Recording and Download Recording, and Crash Recording Actions include Play Recording, Capture Recording, and Download Recording.
Power Policies	Power restore policy settings.
PID Catalog	CPU, memory, PCI adapters, and the HDD details.
Secure Key Management	Details of KMIP Servers, KMIP Root CA and Client Certificate details, KMIP login details, KMIP Client Private key status

Networking Menu

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

Networking Menu Node Name	Work Pane Tabs Provide Information About...
General	Adapter card properties, firmware, external ethernet interfaces, and actions to export or import configurations, and reset status.
External Ethernet Interfaces	External ethernet interfaces information such as port, admin speed, MAC address, link state.
vNICs	Host ethernet interfaces information such as name, CDN, MAC address, MTU and individual vNIC properties.
vHBAs	Host fibre channel interfaces information such as name, WWPN, WWNN, boot, uplink, port profile, channel number, and individual vHBA properties.

Storage Menu

Each node in the **Storage** menu corresponds to the LSI MegaRAID controllers or Host Bus Adapters (HBA) that are installed in theCisco UCS C-Series Rack-Mount Servers. Each node leads to one or more tabs that display in the **Work** pane and provide information about the installed controllers.

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

Admin Menu

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

Admin Menu Node Name	Work Pane Tabs Provide Information About...
User Management	Local User Management, LDAP, and Session Management.
Networking	Network, Network Security, and NTP Setting.
Communication Services	Communication Services tab includes HTTP, SSH, XML API, Redfish Properties, IPMI over LAN Properties, SNMP tab includes SNMP Properties, User Settings, and Trap Destinations, and Mail Alert tab includes SNTP Properties and SMTP Recipients.
Security Management	Certificate Management and Security Configuration.
Event Management	List of Platform Event Filters
Firmware Management	Cisco IMC and BIOS firmware information and management.
Utilities	Technical support data collection export to remote and local download, system configuration import and export options, Generate to NMI host, restore factory defaults settings, add or update Cisco IMC Banner, generate inventory data, export hard inventory data to remote, upload PID catalog, enable or disable secure adapter update.
Device Connector	Intersight management and network settings.

Toolbar

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

Button Name	Description
Refresh	Refreshes the current page.
Host Power	Launches the **Server Power Management** pop-up window.
Launch KVM	Launches the **Launch KVM** pop-up window. Launches the **Launch KVM** pop-up window.
Ping	Launches the **Ping Details** pop-up window.
Reboot	Enables you to reboot BMC 1, BMC 2, CIMC 1 or CIMC 2 depending on the option you choose from the drop-down menu.
Locator LED	Launches the **Locator LED** pop-up window.

Cisco Integrated Management Controller Online Help Overview

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

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

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

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

Note For a complete list of all C-Series documentation, see the *Cisco UCS C-Series Servers Documentation Roadmap* available at the following URL: http://www.cisco.com/go/unifiedcomputing/c-series-doc.

Logging into Cisco IMC

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

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

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

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

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

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

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

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

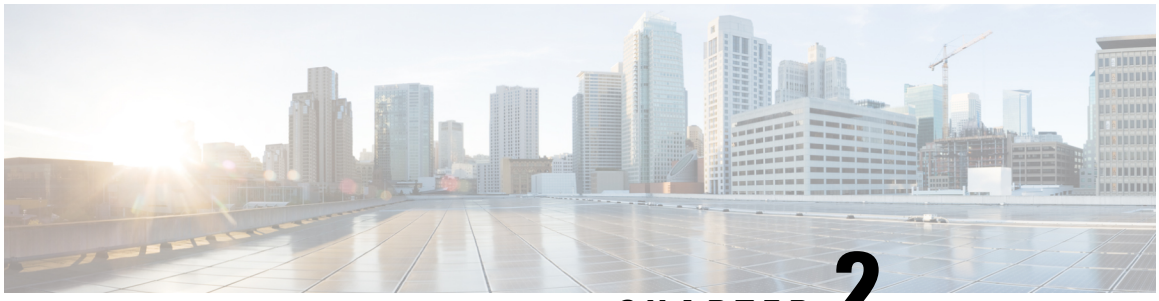
Step 4 Click **Log In**.

Logging out of Cisco IMC

Step 1 In the upper right of Cisco IMC, click the gear icon and click **Log Out** from the drop-down list.

Logging out returns you to the Cisco IMC log in page.

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



CHAPTER 2

Installing the Server OS

This chapter includes the following sections:

OS Installation Methods

C-Series servers support several operating systems. Regardless of the OS being installed, you can install it on your server using one of the following tools:

- KVM console
- PXE installation server

For more information on Cisco UCS Server Configuration Utility, see Cisco UCS Server Configuration Utility Quick Start Guide.

Virtual KVM Console

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

Here are a few major advantages of using Cisco KVM Console:

- The Cisco KVM console provides connection to KVM, SOL, and vMedia whereas the Avocent KVM provides connection only to KVM and vMedia.
- In the KVM Console, the vMedia connection is established at the KVM Launch Manager and is available for all users.
- The KVM console offers you an advanced character replacement options for the unsupported characters while pasting text from the guest to the host.
- The KVM console provides you an ability to store the vMedia mappings on CIMC.

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

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

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

Note To configure the vKVM console successfully for the S3260 Storage Server, you need to configure IP addresses for the Cisco IMC, CMC, and BMC components. You can configure the IP addresses for these components using the CLI interface or Web UI. For the CLI, use the command **scope network**, or view the setting using **scope <chassis/server1/2><cmc/bmc><network>**.

To configure IP addresses for network components on the web interface, see the steps described in the section **Configuring Network-Related Settings**.

Installing an OS Using the KVM Console

Note This procedure describes only the basic installation steps. Detailed guides for installing Linux, VMware, and Windows can be found at this URL: http://www.cisco.com/en/US/products/ps10493/products_installation_and_configuration_guides_list.html.

Before you begin

- Locate the OS installation disk or disk image file.
- You must log in as a user with admin privileges to install an OS.

Step 1 Load the OS installation disk into your CD/DVD drive, or copy the disk image files to your computer.

Step 2 If Cisco IMC is not open, log in.

Step 3 In the **Navigation** pane, click the **Compute** menu.

Step 4 In the **Compute** menu, select a server.

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

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

Step 7 In the **Actions** area, click **Launch KVM Console**.

The **KVM Console** opens in a separate window.

Step 8 From the KVM console, click the **VM** tab.

Step 9 In the **VM** tab, map the virtual media using either of the following methods:

- Check the **Mapped** check box for the CD/DVD drive containing the OS installation disk.
- Click **Add Image**, navigate to and select the OS installation disk image, click **Open** to mount the disk image, and then check the **Mapped** check box for the mounted disk image.

Note You must keep the **VM** tab open during the OS installation process. Closing the tab unmaps all virtual media.

Step 10 Reboot the server and select the virtual CD/DVD drive as the boot device.

When the server reboots, it begins the installation process from the virtual CD/DVD drive. Refer to the installation guide for the OS being installed to guide you through the rest of the installation process.

What to do next

After the OS installation is complete, reset the LAN boot order to its original setting. Always follow your OS vendors recommended configuration, including software interoperability and driver compatibility. For more information on driver recommendations and installation, follow the Cisco UCS Hardware Compatibility list here:

https://ucshcltool.cloudapps.cisco.com/public/

PXE Installation Servers

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

PXE servers can use installation disks, disk images, or scripts to install an OS. Proprietary disk images can also be used to install an OS, additional components, or applications.

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

Installing an OS Using a PXE Installation Server

Before you begin

- Verify that the server can be reached over a VLAN.
- You must log in as a user with admin privileges to install an OS.

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

Step 2 Reboot the server.

If a PXE install server is available on the VLAN, the installation process begins when the server reboots. PXE installations are typically automated and require no additional user input. Refer to the installation guide for the OS being installed to guide you through the rest of the installation process.

What to do next

After the OS installation is complete, reset the LAN boot order to its original setting. Always follow your OS vendors recommended configuration, including software interoperability and driver compatibility. For more information on driver recommendations and installation, follow the Cisco UCS Hardware Compatibility list here:

https://ucshcltool.cloudapps.cisco.com/public/

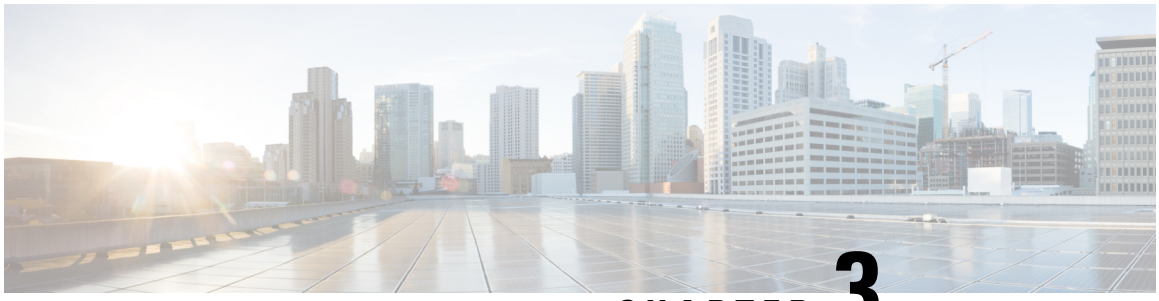
Booting an Operating System from a USB Port

All Cisco UCS C-series servers support booting an operating system from any USB port on the server. However, there are a few guidelines that you must keep in mind, prior to booting an OS from a USB port.

- To maintain the boot order configuration, it is recommended that you use an internal USB port for booting an OS.
- The USB port must be enabled prior to booting an OS from it.

  By default, the USB ports are enabled. If you have disabled a USB port, you must enable it prior to booting an OS from it. For information on enabling a disabled USB ports, see topic *Enabling or Disabling the Internal USB Port* in the server-specific installation and service guide available at the following link:

  http://www.cisco.com/en/US/products/ps10493/prod_installation_guides_list.html.
- After you boot the OS from the USB port, you must set the second-level boot order so that the server boots from that USB source every time.



CHAPTER 3

Managing Chassis

This chapter includes the following sections:

Single Server Dual SIOC Connectivity

The S3260 Storage Server operates either in Single Server Single SIOC mode or Single Server Dual SIOC mode. In single server single SIOC mode, the data path from the second SIOC is unused. The second SIOC is used for management redundancy only, if a VIC installed in the second SIOC.

In single server dual SIOC mode, the data path from both SIOCs is provided to the single server. This allows users to use dual VICs or third party adapters (NIC or HBA) for data, or a combination of both. Only the VIC or dedicated management port can provide server management. When third party adapters are used, they are for the host data path only. In this mode:

Effective with this release, the S3260 storage server supports a single server with dual connectivity, which is based on these two factors:

- The PCIe between the server board and the SIOC card is connected using BIOS.
- The CMC controls the correct association of the server ID with the virtual network interfaces it creates.

This features allows you to configure a new single server dual VIC chassis property on the Cisco IMC by enabling it or disabling it using the web UI or command line interface.

When using a VIC in the SIOC, a specific PCI connectivity is enabled on the VIC. The CMC uses the single server dual VIC property along with the current chassis hardware configuration to identify the server ID property to be specified when you create a virtual network interface in either of the dual SIOC VICs. The VIC configuration page on the web UI displays the read-only attribute of the Server ID to which the VIC is PCIe linked, and this is used by the host server for the virtual network interface traffic.

Configuring Single Server Dual SIOC Connectivity

Before you begin

- You must log in with admin privileges to perform this task.
- The chassis must have a single server and two SIOCs.

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

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

Step 3 In the **Chassis Properties** area of the **Chassis Summary** pane, from the **Server SIOC Connectivity** field, select **Single Server Single SIOC** or **Single Server Dual SIOC**.

If you have a chassis with a single server and dual SIOCs, the **Server SIOC Connectivity** field displays **Single Server Dual SIOC**.

Step 4 Click **Save Changes**.

This configures the server for dual or single connectivity.

Chassis Summary

Viewing Chassis Summary

By default when you log on to the Cisco UCS S-Series storage server, the **Summary** pane of the **Chassis** is displayed in the Web UI. You can also view the Chassis summary when in another tab or working area, by completing the following steps:

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

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

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

Name	Description
Product Name field	The model name of the chassis.
Serial Number field	The serial number for the chassis.
PID field	The product ID.

Name	Description
Description field	A user-defined description for the chassis. Following guidelines should be observed while updating Description field. • Asset Tag can not contain the following special characters: • & • !
Asset Tag field	A user-defined tag for the server. By default, the asset tag for a new server displays **Unknown**. Following guidelines should be observed while updating Asset Tag field. • Asset Tag field can have a maximum of 32 characters. • Asset Tag can not contain the following special characters: • & • !
Server SIOC Connectivity field	**Note** You can edit this field only when you have a chassis with a single server and two SIOCs installed on it. Indicates whether the server is connected to a single SIOC or two SIOCs. The options are: • **Single Server Dual SIOC**—This allows you point two SIOCs to a single available server. This is the default value. **Note** Single server dual SIOC connectivity is possible only when the chassis has an inbuilt single server with two SIOCs. • **Single Server Single SIOC**— This allows you to configure a single SIOC to a particular server.

Step 4 In the **Cisco IMC Information** area of the **Chassis Summary** pane, review the following information:

Name	Description
Hostname field	A user-defined hostname for the Cisco IMC. By default, the hostname appears in CXXX-YYYYYY format, where XXX is the model number and YYYYYY is the serial number of the server.
Management IP Address field	The management IP address for the Cisco IMC.
Single IP Mode	Displays if the single IP mode is enabled or disabled.
Timezone field	Displays the chosen time zone.

Name	Description
Select Timezone button	Allows you to select a time zone. In the **Select Timezone** pop-up screen, mouse over the map and click on the location to select your time zone or choose your time zone from the **Timezone** drop-down menu.
Current Time field	The current date and time according to the Cisco IMC clock. **Note** Cisco IMC gets the current date and time from the server BIOS when the NTP is disabled. When NTP is enabled, BIOS and Cisco IMC gets the current time and date from the NTP server. To change this information, reboot the server and press **F2** when prompted to access the BIOS configuration menu. Then change the date or time using the options on the main BIOS configuration tab.
Local Time field	The local time of the region according to the chosen time zone. You can set your local time by clicking on the calendar icon and choosing the local time on it

Step 5 In the **CMC 1** and **CMC 2** area of the **Chassis Summary** pane, review the following information:

Name	Description
IP Address field	The IP address for CMC.
MAC Address field	The MAC address assigned to the active network interface.
Firmware Version field	The current CMC firmware version.
State field	State of the server. This can be one of the following: • **Active**—CMC is active. • **Standby**—CMC is in standby mode.

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

Name	Description
Overall Chassis Status field	The overall status of the chassis. This can be one of the following: • **Good** • **Moderate Fault** • **Severe Fault**
Temperature field	The temperature status. This can be one of the following: • **Good** • **Fault** • **Severe Fault** You can click the link in this field to view more temperature information.

Name	Description
Overall DIMM Status field	The overall status of the memory modules. This can be one of the following: • **Good** • **Fault** • **Severe Fault** You can click the link in this field to view detailed status information.
Power Supplies field	The overall status of the power supplies. This can be one of the following: • **Good** • **Fault** • **Severe Fault** You can click the link in this field to view detailed status information.
Fans field	The overall status of the power supplies. This can be one of the following: • **Good** • **Fault** • **Severe Fault** You can click the link in this field to view detailed status information.
Front Locator LED field	Whether the front panel locator LED on the chassis is on or off. **Note** This option is available only on some UCS C-Series servers.
Overall Storage Status field	The overall status of all controllers. This can be one of the following: • **Good** • **Moderate Fault** • **Severe Fault**
Power Status field	• **Server 1**—Whether server 1 is powered on or off. • **Server 2**—Whether server 2 is powered on or off.
Locator LED field	• **Server 1**—Whether locator LED on server 1 is on or off. • **Server 2**—Whether locator LED on server 2 is on or off.

Step 7 In the **Power Utilization** area of the **Chassis Summary** pane, review the power utilization of a chassis and servers in a Pie Chart Diagram.

Step 8 In the **Server Utilization** area of the **Chassis Summary** pane, review the following information in a graphical representation.

- **Overall Utilization**
- **CPU Utilization**
- **Memory Utilization**
- **IO Utilization**

Intersight Infrastructure Service License

Chassis Inventory

Viewing the Details of the Servers on the Chassis

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

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

Step 3 In the **Inventory** work pane, the **Servers** tab displays by default. Review the high level details of the server on the chassis:

Name	Description
Name column	The model name of the server.
PID column	Product ID.
UUID column	The UUID assigned to the server.
SysSerialNum column	Serial Number of the server.
Number of Cores column	The number of cores in the CPU.
Memory column	Total memory available.
Power State column	The current power state.

Viewing Power Supply Properties

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

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

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

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

Viewing Cisco VIC Adapter Properties

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

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

Step 3 In the **Inventory** work pane, click the **Cisco VIC Adapters** tab and review the following high level information:

Name	Description
Slot Number column	The PCI slot in which the adapter is installed.
Serial Number column	The serial number for the adapter.
Product ID column	The product ID for the adapter.
Cisco IMC Enabled column	Whether the adapter is able to manage Cisco IMC. This functionality depends on the type of adapter installed and how it is configured. For details, see the hardware installation guide for the type of server you are using.
Description column	Description of the adapter.

Dynamic Storage

Dynamic Storage Support

Effective with this release, The Cisco UCS C-Series rack-mount servers support dynamic storage of Serial Attached SCSI (SAS) drives in the Cisco Management Controller (CMC). This dynamic storage support is provided by the SAS fabric manager located in the CMC.

The fabric manager interacts with the PMC SAS expanders over an Out-of-Band ethernet connection. SAS Expanders allow you to maximize the storage capability of an SAS controller card. Using these expanders,

you can employ SAS controllers support up to 60 hard drives. In CMC, an active SIOC configures the expander zoning, where you can assign the drives to the server nodes through the Web UI, command line interface or Cisco UCS Manager. The standby CMC is updated with the current state, so during a CMC fail-over standby, the CMC can take over the zoning responsibilities. Once the drives are visible to a particular server node, you can manage these using RAID controller.

Note The SAS controller support 56 hard disk drives (HDD) by default. There is also a provision to to replace Server node 2 with an additional four HDDs on Server 2. In that case the total number of HDDs shown in the Zoning page is 60. However, CMC would not support zoning for the additional HDDs 57, 58, 59, 60.

The SAS fabric manager provides an API library for other processes to configure and monitor the expanders and drives. Configuration of the fabric involves zoning the drives, updating the firmware for expanders and drives.

Dynamic Storage supports the following options:

- Assigning physical disks to server 1 and server 2
- Chassis Wide Hot Spare (supported only on RAID controllers)
- Shared mode (supported only in HBAs)
- Unassigning physical disks

Viewing SAS Expander Properties

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

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

Step 3 In the **Inventory** working area, click the **Dynamic Storage** tab.

Step 4 In the **SAS Expander** tab, review the following high level details for SAS Expanders:

Name	Description
ID column	The product ID of the expander.
Name column	The name of the expander.
Firmware Version column	The firmware version the expander uses.
Secondary Firmware Version column	The secondary firmware version of the expander.
Hardware Revision column	The hardware version of the expander.
SAS Address column	The SAS address of the expander.
Server Up Link Speed column	Up link speed received with the LSI RAID Controller. **Note** You can view up to four speed levels for Server 1 and 2 respectively using the **Filter** icon on the top right hand corner of the **SAS Expander** table. Select the Tick mark next to the speed filter to view the individual speed in the table.

Name	Description
Enclosure ID column	The enclosure ID of the expander.

Enabling 6G or 12G Mixed Mode Speed on SAS Expanders

Cisco IMC supports mixed mode speeds of 6 gigabytes or 12 gigabytes for SAS expanders. This support is added because 6 gigabyte solid state drives (SSDs) are now giving way to 12 gigabyte SSDs. Using this feature you can select a SAS expander in the Dynamic Storage tab and enable either modes based on your requirements.

Enabling 6G or 12G Mixed Mode on a SAS Expander

You can enable or disable a 6 gigabyte or 12 gigabyte mixed mode speed support for a card using this option, which is a toggle button.

Step 1 In the **Navigation** pane, click the **Chassis** menu.
Step 2 In the **Chassis** menu, click **Inventory**.
Step 3 In the **Inventory** working area, click the **Dynamic Storage** tab.
Step 4 In the **SAS Expander** area, click **Enable 6G-12G Mixed Mode**.
Step 5 (Optional) Click **Disable 6g-12G Mixed Mode** to disable the feature.

Assigning Physical Drives to Servers

You can assign a physical drive to Server 1 or Server 2, or both, based on your requirements. On the Web UI the **Chassis Front View** area displays the physical drives available on the chassis. You can choose a physical drive individually or an entire row of physical drives by checking the checkbox against the drives.

Before you begin

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

Step 1 In the **Navigation** pane, click the **Chassis** menu.
Step 2 In the **Chassis** menu, click **Inventory**.
Step 3 In the **Inventory** working area, click the **Zoning** tab.

The Chassis Front View is displayed.

Step 4 In the **Chassis Front View** working area, select an individual physical drive or a row of physical drives.
Step 5 Click the **Assign to Server 1** or **Assign to Server 2** link.
A dialog box appears to select the Controller and Path values.

Name	Description
Controller drop-down	Allows you to choose the controller to which you want to assign the chosen physical drive. **Note** Controller option is available for all Dual controllers.

Name	Description
Path drop-down	Allows to choose the SAS Expander path. This could be one of the following: • **Path-0** • **Path-1** • **Both Paths** **Note** Path option is available only for the DHBA controllers.

Step 6 Click **Save Changes**.

Step 7 To assign the physical drive or drives to both servers, click the **Share** link.

A prompt appears informing that the physical drives would be assigned to both servers.

Step 8 Click **OK** to confirm.

Note Shared mode is supported only for HBAs.

What to do next

Move a physical drive as chassis wide hot spare, share, or unassign servers.

Moving Physical Drives as Chassis Wide Hot Spare

You can move the selected physical drive as a chassis wide hot spare. On the Web UI the **Chassis Front View** area displays the physical drives available on the chassis. You can choose a physical drive individually or an entire row of physical drives by checking the checkbox against the drives.

Note Chassis wide hot spare is supported only in Mezz RAID controllers (RAID Controller for UCS C3X60 storage). This option is unavailable if the chassis has an HBA card.

Before you begin

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

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

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

Step 3 In the **Inventory** working area, click the **Zoning** tab.

The Chassis Front View is displayed.

Step 4 In the **Chassis Front View** working area, select an individual server or a row of servers.

Step 5 Click the **Chassis Wide Hot Spare** link.

Step 6 Click **OK**.

What to do next

Assign more physical drives to servers, share, or unassign servers.

Unassigning Physical Drives

You can unassign a physical drive (remove association with) from Server 1 or Server 2, or both, based on your requirements. On the Web UI the **Chassis Front View** area displays the physical drives available on the chassis. You can choose a physical drive individually or an entire row of physical drives by checking the checkbox against the drives.

Before you begin

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

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

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

Step 3 In the **Inventory** working area, click the **Zoning** tab.

The Chassis Front View is displayed.

Step 4 In the **Chassis Front View** working area, select an individual server or a row of servers.

Step 5 Click the **Unassign** link.

Step 6 Click **OK**.

Enabling Dual Enclosure ID

You can enable or disable dual enclosure ID for an expander. For single path functionality, apart from single path drive zoning, expander should have different enclosure ID and SAS paths enabled accordingly.

Before you begin

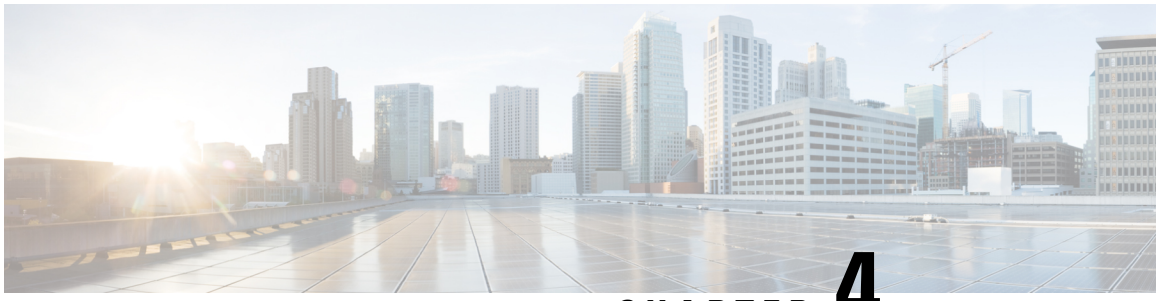
You must log in with admin privileges to perform this task.

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

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

Step 3 In the Inventory working area, click the **SAS Expander** tab.

Step 4 In the **SAS Expander** working area, click **Enable Dual Enclosure ID**.



CHAPTER 4

Managing the Server

This chapter includes the following sections:

Server Boot Order

Using Cisco IMC, you can configure the order in which the server attempts to boot from available boot device types. In the legacy boot order configuration, Cisco IMC allows you to reorder the device types but not the devices within the device types. With the precision boot order configuration, you can have a linear ordering of the devices. In the web UI or CLI you can change the boot order and boot mode, add multiple devices under each device types, rearrange the boot order, set parameters for each device type.

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

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

- BIOS encounters issues while trying to boot using the configured boot order.
- A user changes the boot order directly through BIOS.
- BIOS appends devices that are seen by the host but are not configured from the user.

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

Note During Cisco IMC 2.0(x) upgrade, the legacy boot order is migrated to the precision boot order. The previous boot order configuration is erased and all device types configured before updating to 2.0 version are converted to corresponding precision boot device types and some dummy devices are created for the same device types. you can view these devices in the **Configured Boot Order** area in the web UI. To view these devices in the CLI, enter **show boot-device** command. During this the server's actual boot order is retained and it can be viewed under actual boot order option in web UI and CLI.

When you downgrade Cisco IMC prior to 2.0(x) verison the server's last legacy boot order is retained, and the same can be viewed under **Actual Boot Order** area. For example:

- If you configured the server in a legacy boot order in 2.0(x) version, upon downgrade a legacy boot order configuration is retained.
- If you configured the server in a precision boot order in 2.0(x), upon downgrade the last configured legacy boot order is retained.

Important

- S3260 M4 servers support both Legacy and Precision Boot order configuration through Cisco IMC GUI and CLI interfaces.

  For S3260 M5 servers, you must manually configure the intended boot order through Cisco IMC GUI or CLI interfaces.
- Boot order configuration prior to 2.0(x) is referred as legacy boot order. If your running version is 2.0(x), then you cannot configure legacy boot order through web UI, but you can configure through CLI and XML API. In the CLI, you can configure it by using **set boot-order HDD,PXE** command. Even though, you can configure legacy boot order through CLI or XML API, in the web UI this configured boot order is not displayed.
- Legacy and precision boot order features are mutually exclusive. You can configure either legacy or precision boot order. If you configure legacy boot order, it disables all the precision boot devices configured. If you configure precision boot order, then it erases legacy boot order configuration.

Configuring the Precision Boot Order

Before you begin

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

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

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

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

Step 4 In the **BIOS Properties** area, click **Configure Boot Order** at the bottom of the page.

Configure Boot Order dialog box is displayed.

Step 5 In the **Configure Boot Order** dialog box, update the following properties:

Basic Tab

Name	Description
Device Types table	The server boot options. You can select one or more of the following: • **HDD**—Hard disk drive • **FDD**—Floppy disk drive • **CDROM**—Bootable CD-ROM or DVD • **PXE**—PXE boot • **EFI**—Extensible Firmware Interface
>>	Moves the selected device type to the **Boot Order** table.
<<	Removes the selected device type from the **Boot Order** table.
Boot Order table	Displays the device types from which this server can boot, in the order in which the boot will be attempted.
Down	Moves the selected device type to a higher priority in the **Boot Order** table.
Up	Moves the selected device type to a higher priority in the **Boot Order** table.
Save Changes	Click this button to save the changes made.
Close button	Closes the dialog box without saving any changes and the existing configuration is applied when the server is rebooted.

Advanced Tab

The following list of links are displayed under **Add Boot Device** pane.

- **Add Local HDD**
- **Add PXE Boot**
- **Add SAN Boot**
- **Add iSCSI Boot**
- **Add USB**
- **Add Virtual Media**
- **Add PCHStorage**
- **Add UEFISHELL**

- **Add NVME**
- **Add Local CDD**
- **Add HTTP Boot**

In the **Advanced Boot Order Configuration** pane, the devices are displayed after they are added. You can perform the following actions by selecting the appropriate buttons:

- **Enable or Disable**
- **Modify**
- **Delete**
- **Clone**
- **Re-Apply**
- **Move Up**
- **Move Down**

Step 6 Click **Save Changes**.

Additional device types might be appended to the actual boot order, depending on what devices you have connected to your server.

What to do next

Reboot the server to boot with your new boot order.

Managing a Boot Device

Before you begin

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

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

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

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

Step 4 In the **BIOS Properties** area, click **Configure Boot Order**.

A dialog box with boot order instructions appears.

Step 5 In the **Configure Boot Order** dialog box, from the **Add Boot Device** table, choose the device that you want add to the boot order.

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

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

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

Name	Description
Name field	The name of the device. This name cannot be changed after the device has been created.
State drop-down list	The visibility of the device by BIOS. The state can be one of the following: • **Enabled**—The device is visible to BIOS in a boot order configuration. • **Disabled**—The device is not visible to BIOS in a boot order configuration.
Order field	The order of the device in the available list of devices. Enter between 1 and n, where n is the number of devices.
Slot field	The slot in which the device is installed. Enter the slot number from the available range.
MAC Address	MAC address of the network ethernet interface. **Note** This option is available only on some C-Series servers.
Port field	The port of the slot in which the device is present. Enter a number between 0 and 255.

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

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

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

Name	Description
Name field	The name of the device. This name cannot be changed after the device has been created.
State drop-down list	The visibility of the device by BIOS. The state can be one of the following: • **Enabled**—The device is visible to BIOS in a boot order configuration. • **Disabled**—The device is not visible to BIOS in a boot order configuration.
Order field	The order of the device in the available list of devices. Enter between 1 and n, where n is the number of devices.
Slot field	The slot in which the device is installed. Enter the slot number from the available range.
Port field	The port of the slot in which the device is present. Enter a number between 0 and 255. **Note** In case of a VIC card, use a vNIC instance instead of the port number.
Save Changes button	Adds the device to the **Boot Order** table, and saves the changes.

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

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

Note This option is available only on some UCS C-Series servers.

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

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

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

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

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

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

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

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

Name	Description
LUN field	Logical unit in a slot where the device is present. • Enter a number between 0 and 255 • SATA in AHCI mode—Enter a value between 1 and 10 • SATA in SWRAID mode—Enter 0 for SATA , and enter 1 for SATA **Note** SATA mode is available only on some UCS C-Series servers.
Save Changes button	Adds the device to the **Boot Order** table.
Cancel button	Closes the dialog box without saving any changes made while the dialog box was open.

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

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

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

Note The following OS (ISOs) are supported for HTTP Boot device:

- SLES 12.x
- RHEL 8.2
- ESX 6.5

The following OS (ISOs) are not supported for HTTP Boot device:

- Windows 2016
- Windows 2019

Name	Description
Name field	The name of the device. This name cannot be changed after the device has been created. You can enter between 1 and 30 characters, containing alphanumerics, - (hyphen) and _ (underscore). The name cannot begin with hyphen or underscore.
State drop-down list	The visibility of the device by BIOS. The state can be one of the following: • **Enabled**—The default option. The device is visible to BIOS in a boot order configuration. • **Disabled**—The device is not visible to BIOS in a boot order configuration.
Order field	The order of the device in the available list of devices. The default option is 1.
MAC Address field	MAC address of the network ethernet interface.
IP Type drop-down list	The type of IP. Select any one of the following options displayed in the drop-down list: • None • IPv4 • IPv6 The default value is None.
Slot field	The slot in which the device is installed. Enter the slot number from the available range. Enter the required value from the below list: • SIOC1 • SIOC2 • IOESLOT1 • IOESLOT2 • SBLOM1 • Any number between 1 and 255
Port field	The port of the slot in which the device is present. Enter a number between 0 and 255.

Name	Description
IP Config Type drop-down list	The type of IP configuration. The following options are displayed in the drop-down list: • **None** • **DHCP** • **Static** For **DHCP** IP configuration, the following fields are displayed, depending on the IP type that you have selected: • **MAC Address** • **IP Type** • **Slot** • **Port** For **Static** IP configuration, the following fields are displayed, depending on the IP type that you have selected: • **URI** • **IP Address** • **IPv4 Netmask** or **IPv6 Netmask** • **IPv4 Gateway** or **IPv6 Gateway** • **IPv4 Preferred DNS server** or **IPv6 Preferred DNS server**
URI field	The Uniform Resource Identifier HTTP server path location. You can enter between 1 and 255 characters.
Save Changes button	Saves the changes and adds the device to the **Boot Order** table.
Cancel button	Closes the dialog box without saving any changes made while the dialog box was open.

Overview to UEFI Secure Boot

You can use Unified Extensible Firmware Interface (UEFI) secure boot to ensure that all the EFI drivers, EFI applications, option ROM or operating systems prior to loading and execution are signed and verified for authenticity and integrity, before you load and execute the operating system. You can enable this option using either web UI or CLI. When you enable UEFI secure boot mode, the boot mode is set to UEFI mode and you cannot modify the configured boot mode until the UEFI boot mode is disabled.

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

Important Also, if you use an unsupported adapter, an error log event in Cisco IMC SEL is recorded. The error messages is displayed that says:

System Software event: Post sensor, System Firmware error. EFI Load Image Security Violation. [0x5302] was asserted .

UEFI secure boot is supported on the following components:

Components	Types
Supported OS	• Windows Server 2019 • Windows Server 2016 • ESX 6.7 • ESX 6.5 • ESXi 7.0 • ESXi 8.0 • Linux
QLogic PCI adapters	• 8362 dual port adapter • 2672 dual port adapter
Fusion-io	
LSI	• LSI MegaRAID SAS 9240-8i • LSI MegaRAID SAS 9220-8i • LSI MegaRAID SAS 9265CV-8i • LSI MegaRAID SAS 9285CV-8e • LSI MegaRAID SAS 9285CV-8e • LSI MegaRAID SAS 9266-8i • LSI SAS2008-8i mezz • LSI Nytro card • RAID controller for UCS Storage (SLOT-MEZZ) • Host Bus Adapter (HBA)

Enabling UEFI Secure Boot

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

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

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

Step 4 In the **BIOS Properties** area of the **Configure Boot Order** tab, check **UEFI Secure Boot** checkbox.

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

Note In case of RFD (Reset Factory Default), you must re-enable UEFI Secure Boot.

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

Step 5 Click **Save Changes**.

What to do next

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

Disabling UEFI Secure Boot

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

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

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

Step 4 In the **BIOS Properties** area, uncheck the **UEFI Secure Boot** check box.

Step 5 Click **Save Changes**.

What to do next

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

Viewing the Actual Server Boot Order

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

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

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

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

Step 4 In the **BIOS Properties** area, click **Configure Boot Order**.

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

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

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

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

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

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

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

Configuring a Server to Boot With a One-Time Boot Device

You can configure a server to boot from a particular device only for the next server boot, without disrupting the currently configured boot order. Once the server boots from the one time boot device, all its future reboots occur from the previously configured boot order.

Before you begin

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

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

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

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

Step 4 In the **BIOS Properties** area, select an option from the **Configured One Time Boot Device** drop-down.

Note The host boots to the one time boot device even when configured with a disabled advanced boot device.

Creating a Server Asset Tag

Before you begin

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

Step 1 In the **Navigation** pane, click the **Chassis** menu.
Step 2 In the **Chassis** menu, click **Summary**.
Step 3 In the **Chassis Properties** area, update the **Asset Tag** field.
Step 4 Click **Save Changes**.

Configuring Power Policies

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 admin privileges to perform this task.

Step 1 In the **Navigation** pane, click the **Compute** menu.
Step 2 In the **Compute** menu, select a server.
Step 3 In the work pane, click the **Power Policies** tab.
Step 4 In the **Power Restore Policy** area, update the following fields:

Name	Description
Power Restore Policy drop-down list	The action to be taken when chassis power is restored after an unexpected power loss. This can be one of the following: • **Power Off**—The server remains off until it is manually restarted. • **Power On**—The server is allowed to boot up normally when power is restored. The server can restart immediately or, optionally, after a fixed or random delay. • **Restore Last State**—The server restarts and the system attempts to restore any processes that were running before power was lost.

Name	Description
Power Delay Type drop-down list	If the selected policy is **Power On**, the restart can be delayed with this option. This can be one of the following: • **fixed**—The server restarts after a fixed delay. • **random**—The server restarts after a random delay. **Note** This option is available only for some C-Series servers.
Power Delay Value field	If a fixed delay is selected, once chassis power is restored and the Cisco IMC has finished rebooting, the system waits for the specified number of seconds before restarting the server. Enter an integer between 0 and 240. **Note** This option is available only for some C-Series servers.

Step 5 Click **Save Changes**.

Power Characterization

The chassis power characterization range is calculated and derived from individual server node power characterization status, and from the power requirements of all the unmanageable components of the chassis.

This range varies for each configuration, so you need to run the power characterization every time a configuration changes.

To help you use the power characterization range appropriately for the different power profiles, the system represents the chassis' minimum power as auto profile minimum and custom profile minimum. However, custom power profile minimum is the actual minimum power requirement of the current chassis configuration. For more information see the section Run Power Characterization.

Running Power Characterization

Before you begin

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

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

Step 2 In the **Chassis** menu, click **Power Management**.

Step 3 In the **Power Cap Configuration** tab, click the **Run Power Characterization** link.

A confirmation box appears that says the host is going to be either powered on or rebooted depending on the current power state. Review the message and click **OK** to close the dialog box.

You can verify the progress of the power characterization in the **Status** field. The status can be one of the following:

- **Not Run on One Server**— When the power characterization status is **Not Run** on any one server node.

- **Not Run**— When the power characterization status is **Not Run** on both the server nodes.
- **Failed on One Server**— When the power characterization status is **Failed** on any one server.
- **Completed Successfully**—When the power characterization status is **Completed Successfully** on both the server nodes.
- **Running**— When the power characterization status is **Running** on any one of the server nodes.
- **Failed**— When the power characterization status is **Failed** on both the server nodes.

After power characterization action is performed, the platform power limit range is populated under the **Recommended Power Cap** area as a minimum and maximum power in watts.

Power Profiles

Power capping determines how server power consumption is actively managed. When you enable power capping option, the system monitors power consumption and maintains the power below the allocated power limit. If the server cannot maintain the power limit or cannot bring the platform power back to the specified power limit within the correction time, power capping performs actions that you specify in the Action field under the Power Profile area.

You can configure multiple profiles with the following combinations: automatic and thermal profiles; and custom and thermal profiles. These profiles are configured by using either the web user interface, command line interface, or XML API. In the web UI, the profiles are listed under the Power Capping area. In the CLI, the profiles are configured when you enter the **power-cap-config** command. You can configure the following power profiles for power capping feature:

- Automatic Power Limiting Profile
- Custom Power Limiting Profile
- Thermal Power Limiting Profile

Automatic power limiting profile sets the power limit of the individual server boards based on server priority selected by you, or as detected by the system, based on the server utilization sensor (which is known as manual or dynamic priority selection). The limiting values are calculated within the manageable chassis power budget and applied to the individual server, and the priority server is allocated with its maximum power limiting value, while the other server with the remaining of the manageable power budget. Power limiting occurs at each server board platform level that affects the overall chassis power consumption.

Custom power limiting profile allows you to set an individual server board’s power limit from the Web UI or command line interface within the chassis power budget. In this scenario you can specify an individual server power limit.

Thermal power profile allows you to enable thermal failure power capping, which means you can set a specific platform temperature threshold and it sets P (min-x) as the power limit to be applied on the temperature threshold.

Resetting Power Profiles to Default

Before you begin

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

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

Step 2 In the **Chassis** menu, click **Power Management**.

Step 3 In the **Power Cap Configuration** tab, click the **Reset Profiles to Default** link.

Note This action resets all the power profile settings to factory default values and disables power capping.

Configuring the Power Capping Settings

You can enable power characterization only on some Cisco UCS C-Series servers.

Before you begin

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

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

Step 2 In the **Chassis** menu, click **Power Management**.

Step 3 In the **Chassis Power Characterization Details** area, review the following information:

Name	Description
Chassis Power Characterization Status field	Displays the progress of the power characterization. This can be one of the following: • **Not Run on One Server**— When the power characterization status is **Not Run** on any one server node. • **Not Run**— When the power characterization status is **Not Run** on both the server nodes. • **Failed on One Server**— When the power characterization status is **Failed** on any one server. • **Completed Successfully**—When the power characterization status is **Completed Successfully** on both the server nodes. • **Running**— When the power characterization status is **Running** on any one of the server nodes. • **Failed**— When the power characterization status is **Failed** on both the server nodes.

Name	Description
Chassis Power Characterization Range	It is composed of the following: • **Auto Profile Minimum**— The minimum value to be used for the user allocated chassis power to enable **Auto Profile**. **Note** The **Auto Profile Minimum** option is available only when both server nodes are present. • **Custom Profile Minimum**— The minimum value to be used for the user allocated chassis power to enable **Custom Profile** • **Maximum**— Maximum value for both Auto and Custom profiles.
Server Power Details	When you move the mouse over the Help icon, the server power details are displayed in a table.

Step 4 In the **Power Capping and Profiles Configuration** area, complete the following fields:

Name	Description
Enable Power Capping check box	If checked, this enables the power capping capability of the system, and allows you to select and set the parameters for individual power capping profiles. **Note** If disabled, you cannot configure or modify individual power capping profiles in the **Power Profiles** area.
User Allocated Chassis Power field	Power budget that you allocate to a chassis, in watts.
Chassis Manageable Power field	Maximum power that a chassis can manage, in watts. It is a part of the User Allocated Chassis power that is manageable.

Step 5 Click **Save Changes**.

What to do next

Configure the individual power profiles.

Configuring Auto Power Profile

Note The Auto tab is visible only when both server nodes are present in the chassis.

Before you begin

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

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

Step 2 In the **Chassis** menu, click **Power Management**.

Step 3 In the **Auto** tab of the **Power Cap Configuration** tab, complete the following fields:

Name	Description
Enable Profile check box	If checked, enables the power profile for editing.
Allow Throttle check box	If checked, it forces the processor to use more aggressive power management mechanisms such as CPU throttling states (T-states) and memory bandwidth throttling to maintain the power limit, in addition to the regular internal mechanisms.
Priority Selection drop-down list	This can be one of the following: • **Manual**— When you manually assign priority to a server node. It could be either server 1 or server 2. • **Dynamic**— CMC dynamically decides to assign priority to a server node based on server utilization. The server that is utilized more at any given time is selected as a priority server.
Correction Time field	The time in seconds in which the platform power should be brought back to the specified power limit before taking the action specified in the **Action** field. The valid range is 1 to 600 seconds.
Priority Server drop-down list	Select an option to manually assign priority to a server. This can be one of the following: • **Server 1** • **Server 2** **Note** This option is available when you select **Manual** from the **Priority Selection** drop-down list.
Exception Action drop-down list	The action to be performed if the specified power limit is not maintained within the correction time. • **Alert**—Logs the event to the Cisco IMC SEL. • **Alert and Shutdown**—Logs the event to the Cisco IMC SEL, and gracefully shuts down the host.

Name	Description
Power Limit field **Server 1** **Server 2**	Displays the power cap limit assigned to server 1 and server 2 in auto profile.

Step 4 In the **Suspend Period** area, click the **Configure** link to set the time period in which the power capping profile is not active.

What to do next

Configure the custom power profile.

Configuring Custom Power Profile

Before you begin

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

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

Step 2 In the **Chassis** menu, click **Power Management**.

Step 3 In the **Custom** tab of the **Power Cap Configuration** tab, complete the following fields:

Name	Description
Component field	Component for which you want to enable the **Custom Power** profile.
Enabled check box	If checked, enables the power profile for editing.
Power Limit field	Enter a value in the range suggested by the tooltip.
Exception Action drop-down list	The action to be performed if the specified power limit is not maintained within the correction time. • **Alert**—Logs the event to the Cisco IMC SEL. • **Alert and Shutdown**—Logs the event to the Cisco IMC SEL, and gracefully shuts down the host.
Correction Time field	The time in seconds in which the platform power should be brought back to the specified power limit before taking the action specified in the **Action** field. The valid range is 1 to 600 seconds.
Allow Throttling field	Forces the processor to use more aggressive power management mechanisms such as, CPU the throttling states (T-states) and memory bandwidth throttling to maintain the power limit, in addition to the regular internal mechanisms.

Name	Description
Suspend Period field	Allows you to suspend power capping for a chosen period of time.

What to do next

Configure the thermal power profile.

Configuring Thermal Power Profile

Before you begin

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

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

Step 2 In the **Chassis** menu, click **Power Management**.

Step 3 In the **Thermal** tab of the **Power Cap Configuration** tab, complete the following fields:

Name	Description
Component field	Component for which you want to enable the **Thermal Power** profile.
Enabled field	Enables the power profile for editing.
Temperature field	Enter a temperature value crossing which the thermal profile should be applied. The valid range is 1 to 40.
Power Limit field	Displays the power cap limit that is minimum for the given server.

Viewing Power Monitoring Summary

This option is available only on some Cisco UCS C-Series servers.

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

Step 2 In the **Chassis** menu, click **Power Management**.

Step 3 On the **Work** pane, click the **Power Monitoring** tab.

Step 4 In the **Power Monitoring Summary** area, review the following information:

The following tables display the power consumed by the system and its components since the last time it was rebooted.

Name	Description
Monitoring Period	The time of monitoring the power consumed by the system since the last time it was rebooted. The monitoring period is displayed in Day HH:MM:SS format.

Note **Monitoring Period** is displayed under **Chassis**.

Platform, **CPU**, and **Memory** areas are available under **Server 1** and **Server 2**.

Step 5 In the **Platform** area, review the following information:

Name	Description
Current	The power currently being used by the server, CPU, and memory in watts.
Minimum	The minimum number of watts consumed by the server, CPU, and memory since the last time it was rebooted.
Maximum	The maximum number of watts consumed by the server, CPU, and memory since the last time it was rebooted.
Average	The average amount of power consumed by the server, CPU, and memory in watts over the defined period of time.

Step 6 In the **CPU** area, review the following information:

Name	Description
Current	The power currently being used by the CPU in watts.
Minimum	The minimum number of watts consumed by the CPU since the last time it was rebooted.
Maximum	The maximum number of watts consumed by the CPU since the last time it was rebooted.
Average	The average amount of power consumed by the server, CPU, and memory in watts over the defined period of time.

Step 7 In the **Memory** area, review the following information:

Name	Description
Current	The power currently being used by the memory, in watts.
Minimum	The minimum number of watts consumed by the memory since the last time it was rebooted.
Maximum	The maximum number of watts consumed by the memory since the last time it was rebooted.
Average	The average amount of power consumed by the memory in watts over the defined period of time.

Step 8 In the **Chart Properties** area, review and update the chart, component, and view the power consumption details.

Name	Description
Chart Settings	Enables you to configure the chart properties and the way data is displayed in the chart.
Download Power Statistics and Server Utilization Data	Enables you to download the power statistics and host server utilization information. The files are downloaded to your local download folder. **Note** If the file size of the already downloaded statistics file is less than 256 KB, then when you download, another set of files is downloaded, one for the power statistics and the other for host server utilization. If the size of the existing files exceeds 256 KB, then the next set of files overwrites the existing ones.

Name	Description
Chart drop-down list	Allows you to collect the trends of power consumption from every server for the selected duration. This can be one of the following: • **Last Hour**— Plots the chart for every five minutes • **Last Day**—Plots the chart for every hour from the current time. • **Last Week**—Plots the chart for each day.
Component drop-down list	The component for which you want to view the power consumption over the selected duration. This can be one of the following: • **Chassis** • ***Server 1*** • ***Server 2***
Domain drop-down list	The default value displayed is **Platform**.
Plot button	Displays the power consumed by the selected component for the specified duration.
Chart/Table View (Appears on mouse-over)	Select to view power monitoring summary in either **Chart** or **Table** view.

Name	Description
Chart Type (Appears on mouse-over)	Select the type of chart you wish to view. This could be one of the following: • Line Chart— Power monitoring data appears in lines. • Column Chart— Power monitoring data appears as a column. **Default Chart**: Line Chart. **Note** When the **Chart** drop-down list is selected as **Last Week**, and more than one Component is selected, the Column chart is not displayed, and by default the Line chart is displayed. The following message is displayed in such a scenario: `For the selected Configuration, Column graph cannot be plotted. Reverting to Line Graph.`
Current check box	If checked, the chart displays the current power consumed by the selected component for the selected duration.
Average check box	If checked, the plot displays the average amount of power consumed by the selected component for the selected duration.
Maximum check box	If checked, the plot displays the maximum number of watts consumed by the selected component for the selected duration.
Minimum check box	If checked, the plot displays the minimum number of watts consumed by the selected component for the selected duration.

Configuring the Chart Properties

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

Step 2 In the **Chassis** menu, click **Power Management**.

Step 3 On the **Work** pane, click the **Power Monitoring** tab.

Step 4 In the **Chart Properties** area, click the **Chart Settings** icon to configure the following fields:

Name	Description
Show Range Filter check box	If checked, displays the range filter content.
Show X Axis Labels check box	If checked, displays the X Axis labels for the power monitoring summary.

Name	Description
Show Y Axis Labels check box	If checked, displays the Y Axis labels for the power monitoring summary.
Show Markers check box	If checked, displays the markers for the X and Y axis data.
Y-Axis Interval Value field (1 - 1020)	Select the interval value in wattage. Default value is 20.

The power reading chart plots power consumption values of different components for the selected duration. These power consumption values are captured from the time that the host is powered on. When a power profile is enabled, the power limit is plotted in the chart as a red line. This plot can be used to determine the power consumption trend of the system. To view the configured power limit values of a particular domain, move the mouse over these trend lines.

Note These trend lines are not displayed if the profile is disabled on the **Power Cap Configuration** tab.

Step 5 Click **Save Changes**.

Downloading Power Statistics and Server Utilization Data

This option is available only on some Cisco UCS C-Series servers.

Before you begin

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

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

Step 2 In the **Chassis** menu, click **Power Management**.

Step 3 On the **Work** pane, click the **Power Monitoring** tab.

Step 4 In the **Power Monitoring** tab, click **Download Power Statistics and Server Utilization Data**.

The files are downloaded to your local download folder.

Note If the file size of the already downloaded statistics file is less than 256 KB, then when you download, another set of files is downloaded, one for the power statistics and the other for host server utilization. If the size of the existing files exceeds 256 KB, then the next set of files overwrites the existing ones.

Configuring DIMM Blocklisting

DIMM Block Listing

In Cisco IMC, the state of the Dual In-line Memory Module (DIMM) is based on SEL event records. A DIMM is marked bad if the BIOS encounters a non-correctable memory error or correctable memory error with 16000 error counts during memory test execution during BIOS post. If a DIMM is marked bad, it is considered a non-functional device.

If you enable DIMM blocklisting, Cisco IMC monitors the memory test execution messages and blocklists any DIMM that encounters memory errors at any given point of time in the DIMM SPD data. This allows the host to map out those DIMMs.

DIMMs are mapped out or blocklisted only when Uncorrectable errors occur. When a DIMM gets blocklisted, other DIMMs in the same channel are ignored or disabled, which means that the DIMM is no longer considered bad.

Note DIMMs do not get mapped out or blocklisted for 16000 Correctable errors.

Enabling DIMM Block Listing

Before you begin

- You must log in with admin privileges.

Step 1 In the **Navigation** pane, click the **Compute** menu.
Step 2 In the **Compute** menu, select a server.
Step 3 In the work pane, click the **Inventory** tab.
Step 4 In the **Memory** pane's **DIMM Block Listing** area, click the **Enable DIMM Block List** check box.

Configuring BIOS Settings

Configuring BIOS Settings

Before you begin

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

Step 1 In the **Navigation** pane, click the **Compute** menu.
Step 2 In the **Compute** menu, select a server.
Step 3 In the work pane, click the **BIOS** tab.
Step 4 In the **Actions** area, click **Configure BIOS**.
Step 5 Refer BIOS Parameters by Server Model, on page 383 to update the following tabs:

- I/O
- Server Management
- Security
- Processor

- Memory
- Power/Performance

Note The BIOS parameters available depend on the model of the server that you are using. For descriptions and information about the options for each BIOS setting, see *BIOS Parameters by Server Model* chapter in this guide.

Important A BIOS parameter available in one tab may affect the parameters on all available tabs, not just the parameters on the tab that you are viewing.

Entering BIOS Setup

Before you begin

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

Step 1 In the **Navigation** pane, click the **Compute** menu.
Step 2 In the **Compute** menu, select a server.
Step 3 In the work pane, click the **BIOS** tab.
Step 4 In the **Actions** area, click **Enter BIOS Setup**.
Step 5 Click **OK** at the prompt.
Enables enter BIOS setup. On restart, the server enters the BIOS setup.

Clearing the BIOS CMOS

Before you begin

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

Step 1 In the **Navigation** pane, click the **Compute** menu.
Step 2 In the **Compute** menu, select a server.
Step 3 In the work pane, click the **BIOS** tab.
Step 4 In the **Actions** area, click **Clear BIOS CMOS**.
Step 5 Click **OK** to confirm.
Clears the BIOS CMOS.

Restoring BIOS Manufacturing Custom Settings

Before you begin

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

Step 1 In the **Navigation** pane, click the **Compute** menu.
Step 2 In the **Compute** menu, select a server.
Step 3 In the work pane, click the **BIOS** tab.
Step 4 In the **Actions** area, click **Restore Manufacturing Custom Settings**.
Step 5 Click **Yes** if you wish to reboot the server immediately.
Step 6 Click **OK** to confirm.

Restoring BIOS Defaults

Before you begin

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

Step 1 In the **Navigation** pane, click the **Compute** menu.
Step 2 In the **Compute** menu, select a server.
Step 3 In the work pane, click the **BIOS** tab.
Step 4 In the **Actions** area, click **Restore Defaults**.
Step 5 Click **Yes** if you wish to reboot the server immediately.
Step 6 Click **OK** to confirm.

BIOS Profiles

On the Cisco UCS server, default token files are available for every S3260 server platform, and you can configure the value of these tokens using the Graphic User Interface (GUI), CLI interface, and the XML API interface. To optimize server performance, these token values must be configured in a specific combination.

Configuring a BIOS profile helps you to utilize pre-configured token files with the right combination of the token values. Some of the pre-configured profiles that are available are virtualization, high-performance, low power, and so on. You can download the various options of these pre-configured token files from the Cisco website and apply it on the servers through the BMC.

You can edit the downloaded profile to change the value of the tokens or add new tokens. This allows you to customize the profile to your requirements without having to wait for turnaround time.

Uploading a BIOS Profile

You can upload a BIOS profile either from a remote server location or through a browser client.

Before you begin

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

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

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

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

Step 4 Click the **Configure BIOS Profile** tab.

Step 5 To upload the BIOS profile using a remote server location, in the **BIOS Profile** area, click the **Upload** button.

Step 6 In the **Upload BIOS Profile** dialog box, update the following fields:

Name	Description
Upload BIOS Profile from drop-down list	The remote server type. This can be one of the following: • **TFTP** • **FTP** • **SFTP** • **SCP** • **HTTP**
Server IP/Hostname field	The IP address or hostname of the server on which the BIOS profile information is available. Depending on the setting in the Upload BIOS Profile from drop-down list, the name of the field may vary.
Path and Filename field	The path and filename of the BIOS profile on the remote server.
Username field	Username of the remote server.
Password field	Password of the remote server.

Name	Description
Upload button	Uploads the selected BIOS profile. **Note** If you chose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message *Server (RSA) key fingerprint is <server_finger_print_ID> Do you wish to continue?*. Click Yes or No depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.
Cancel button	Closes the wizard without making any changes to the firmware versions stored on the server.

Step 7 To upload the BIOS profile using a browser client, in the **BIOS Profile** area, click the **Upload** button.

Step 8 In the **Upload BIOS Profile** dialog box, update the following fields:

Name	Description
File field	The BIOS profile that you want to upload.
Browse button	Opens a dialog box that allows you to navigate to the appropriate file.

What to do next

Activate a BIOS profile.

Activating a BIOS Profile

Before you begin

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

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

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

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

Step 4 Click the **Configure BIOS Profile** tab.

Step 5 Select a BIOS profile from the **BIOS Profile** area and click **Activate**.

Step 6 At the prompt, click **Yes** to activate the BIOS profile.

Deleting a BIOS Profile

Before you begin

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

Step 1 In the **Navigation** pane, click the **Compute** menu.
Step 2 In the **Compute** menu, select a server.
Step 3 In the work pane, click the **BIOS** tab.
Step 4 Select a BIOS profile from the **BIOS Profile** area and click **Delete**.
Step 5 At the prompt, click **OK** to delete the BIOS profile.

Backing up a BIOS Profile

Before you begin

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

Step 1 In the **Navigation** pane, click the **Compute** menu.
Step 2 In the **Compute** menu, select a server.
Step 3 In the work pane, click the **BIOS** tab.
Step 4 Select a BIOS profile from the **BIOS Profile** area and click **Take Backup**.
Step 5 At the prompt, click **OK** to take a backup of the BIOS profile.

What to do next

Activate a BIOS profile.

Viewing BIOS Profile Details

Before you begin

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

Step 1 In the **Navigation** pane, click the **Compute** menu.
Step 2 In the **Compute** menu, select a server.
Step 3 In the work pane, click the **BIOS** tab.
Step 4 Select a BIOS profile from the **BIOS Profile** area and click **Details**.
Step 5 Review the following information in the **BIOS Profile Details** window:

Name	Description
Token Name column	Displays the token name of the BIOS profile.
Display Name column	Displays the user name of the BIOS profile.
Profile Value column	Displays the value that was provided in the uploaded file.
Actual Value column	Displays the value of the active BIOS configuration.

Secure Boot Certificate Management

Beginning with 4.2(2a) release, Cisco IMC allows you to upload up to ten certificates for configured secure HTTP Boot device. You can also delete and upload a new certificate for the specific boot device configured. Cisco IMC allows you to upload up to ten root CA Certificates.

Viewing Secure Boot Certificate Details

You can view the details of a secure boot certificate, which is already uploaded.

Before you begin

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

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

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

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

Step 4 Click the **Secure Boot Certificate Management** tab.

Step 5 From the certificates table, select the certificate, which you wish to view.

Step 6 Click the **View Secure Boot Certificate** icon above the table.

Step 7 **View Secure Boot Certificate** dialog box is displayed.

You can view the following information:

Table 2: General Area

Field	Description
Certificate ID field	Displays the certificate ID assigned by Cisco IMC.
Serial Number field	The serial number for the server.
Valid From field	Certificate validity start date.
Valid To field	Certificate expiry date.

Table 3: Subject Area

Field	Description
Country Code field	Country code of the certificate.
Locality field	Locality of the certificate.
State Name field	State of the certificate.
Organization Name field	Organization of the certificate.
Organization Unit field	Organization unit of the certificate.
Common Name field	Certificate name.

Table 4: Issuer Area

Field	Description
Country Code field	Country code of the issuer.
Locality field	Locality of the issuer.
State Name field	State of the issuer.
Organization Name field	Organization of the issuer.
Organization Unit field	Organization unit of the issuer.
Common Name field	Issuer name.

Uploading Secure Boot Certificate

You can upload a boot certificate either from a remote server location or from local location.

Before you begin

- You must log in with admin privileges to perform this task. log in as admin
- If you wish to upload using Local upload, ensure that the certificate file resides on a locally accessible file system.
- Ensure that the generated certificate is of type server.
- The following certificate formats are supported:
  - .crt
  - .cer
  - .pem

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

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

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

Step 4 Click the **Secure Boot Certificate Management** tab.

Step 5 To upload the boot certificate, click the upload button (+).

Step 6 You can upload the certificate using one of the following methods:

- Paste the certificate directly in the paste certificate text field
- Upload from local location
- Upload from remote location

In the **Add Secure Boot Certificate**dialog box, update the fields as per your the method you wish to upload the certificate:

Table 5: Add Secure Boot Certificate

Field	Description
Paste Secure Boot Certificate radio button	Allows you to copy the entire content of the signed certificate and paste it in the Paste certificate content text field. **Note** Ensure the certificate is signed before uploading.
Upload from local radio button	Allows you to browse and navigate to the location of the authorities certificate file that you want to add.

Field	Description

Upload from remote location radio button	Allows you to choose the certificate from a remote location and Upload it. Enter the following details:
	• **Upload Secure Boot Certificate from**—
	  • TFTP Server
	  • FTP Server
	  • SFTP Server
	  • SCP Server
	  • HTTP Server
	• **Server IP/Hostname**—The IP address or hostname of the server on which the certificate file should be stored. Depending on the setting in the Upload Certificate from drop-down list, the name of the field may vary.
	• **Path and Filename**—The path and filename Cisco IMC should use when uploading the file to the remote server.
	• **Username**—The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP.
	• **Password**—The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP.

Upload Secure Boot Certificate button	Allows you to Upload the certificate to the server.

Deleting a Secure Boot Certificate

You can delete a boot certificate which is already uploaded on Cisco IMC.

Before you begin

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

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

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

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

Step 4 Click the **Secure Boot Certificate Management** tab.

Step 5 From the certificates table, select the certificate, which you wish to delete.

Step 6 Click the **Delete Secure Boot Certificate** icon above the table.

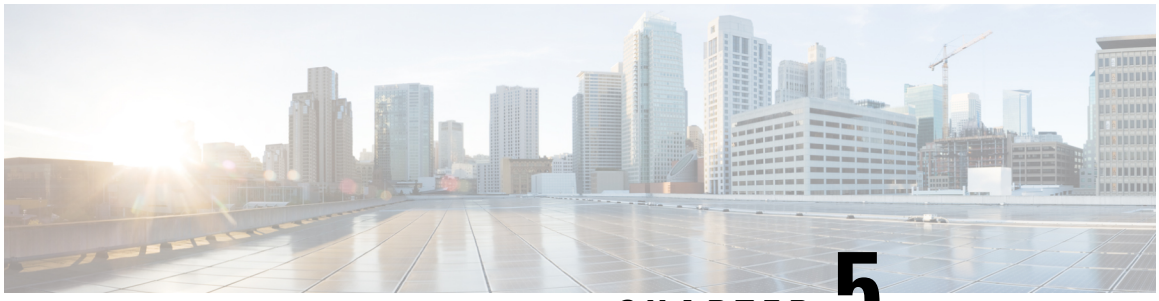
Step 7 Click **Yes** to confirm.

Persistent Memory Modules

Cisco UCS S-Series Release 4.0(4) introduces support for the Intel® Optane™ Data Center persistent memory modules on the UCS M5 servers that are based on the Second Generation Intel® Xeon® Scalable processors. These persistent memory modules can be used only with the Second Generation Intel® Xeon® Scalable processors.

Persistent memory modules are non-volatile memory modules that bring together the low latency of memory and the persistence of storage. Data stored in persistent memory modules can be accessed quickly compared to other storage devices, and is retained across power cycles.

For detailed information about configuring persistent memory modules, see the Cisco UCS: Configuring and Managing Intel® Optane™ Data Center Persistent Memory Modules Guide.



CHAPTER 5

Viewing Server Properties

This chapter includes the following sections:

Viewing Server Properties

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

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

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

Name	Description
Product Name field	The model name of the server.
Serial Number field	The serial number for the server.
PID field	The product ID.
UUID field	The UUID assigned to the server.
BIOS Version field	The version of the BIOS running on the server.
Hostname field	A user-defined hostname for the Cisco IMC. By default, the hostname appears in CXXX-YYYYYY format, where XXX is the model number and YYYYYY is the serial number of the server.
IP Address field	The IP address for the Cisco IMC.

Name	Description
MAC Address field	The MAC address assigned to the active network interface to the Cisco IMC.
Firmware Version field	The current Cisco IMC firmware version.
Description field	A user-defined description for the server.

Viewing Server Utilization

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

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

The **Summary** node provides information on **Chassis Properties**, **Chassis status**, **Cisco IMC Information**, **Power Utilization** and **Server Utilization**.

Real-time monitoring of CPU, memory, and I/O utilization in the system is provided interms of **Compute Usage Per Second (CUPS)** . It is independent of the OS and does not consume CPU resources.

Cisco servers monitors below sensors:

Platform CUPS Sensor - Provides the Computation, Memory, and I/O resource utilization value in the form of a platform CUPS Index.

Core CUPS Sensor - Provides the computation utilization value.

Memory CUPS Sensor - Provides the memory utilization value.

IO CUPS Sensor - Provides the I/O resource utilization value.

Note CUPS sensors are hardware level sensors and the values will not match the values from OS based tools.

These utilization values are obtained by querying the data from a set of dedicated, sideband telemetry counters provided by the platform ingredients (CPU and chipset). These counters are called **Resource Monitoring Counters (RMCs)**.

RMCs provide the real-time information pertaining to the three main domains of platform resources – CPU, memory, and I/O. The utilization information for each of these domains is obtained by aggregating the individual counters at a resource instance level.

Step 3 In the **Server Utilization** area, review the following information:

Name	Description
Overall Utilization (%)	Measured as CUPS Index. This is a composite metric used to provide quick high level assessment of Platform Utilization. The CUPS Index is thus a measure of the compute headroom available on the server. Hence, if the system has a large CUPS Index, then there is limited headroom to place additional workload on that system. As the resource consumption decreases, the system's CUPS Index decreases. A low CUPS Index indicates that there is a large amount of compute headroom and the server is a prime target for receiving new workloads or having the workload migrated off and the server being put into a lower power state in order to reduce power consumption. Such workload monitoring can then be applied throughout the data center to provide a high-level and holistic view of the datacenter's workload.
CPU Utilization (%)	CPU RMC provides CPU utilization metrics. These are individual CPU core counters which are aggregated to provide the cumulative utilization of all the cores in the package.
Memory Utilization (%)	Memory RMC provides memory utilization metrics. These are individual counters to measure memory traffic occurring at each memory channel or memory controller instance. These are then aggregated to measure the cumulative memory traffic across all the memory channels in the package.
IO Utilization (%)	IO RMC provides IO utilization metrics. These are individual counters, one per root port in the PCI Express Root Complex to measure PCI Express traffic emanating from or directed to that root port and the segment below. These counters are then aggregated to measure PCI express traffic for all PCI Express segments emanating from the package. The PCI Express Root Port represents a PCI segment and is hence is the single central component that carries the entire traffic generated by that segment.

Viewing CPU Properties

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

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

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

Step 4 In the **Inventory** pane's **CPU** tab, review the following information for each CPU:

Name	Description
Socket Name field	The socket in which the CPU is installed.
Vendor field	The vendor for the CPU.
Status field	The status of the CPU.
Family field	The family to which this CPU belongs.
Version field	The version information of the CPU.
Speed field	The CPU speed, in megahertz.
Number of Cores field	The number of cores in the CPU.
Signature field	The signature information for the CPU.
Number of Threads field	The maximum number of threads that the CPU can process concurrently.

Viewing Memory Properties

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

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

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

Step 4 In the **Summary** area of the **Memory** tab, review the following summary information about memory:

Name	Description
Memory Speed field	The memory speed, in megahertz.
Total Memory field	The total amount of memory available on the server if all DIMMs are fully functional.
Effective Memory field	The actual amount of memory currently available to the server. When a server has Intel® Optane™ DC persistent memory modules the effective memory is calculated as follows: • **Memory mode or Mixed mode**—It is an approximate sum of all the DCPMM memory. **Note** Memory and Mixed modes are available only on some servers. • **Appdirect mode**—It is an approximate sum of all the DCPMM memory and the DRAMs memory.
Redundant Memory field	The amount of memory used for redundant storage.

Name	Description
Failed Memory field	The amount of memory that is currently failing, in megabytes.
Ignored Memory field	The amount of memory currently not available for use, in megabytes.
Number of Ignored DIMMs field	The number of DIMMs that the server cannot access.
Number of Failed DIMMs field	The number of DIMMs that have failed and cannot be used.
Memory RAS Possible field	Details about the RAS memory configuration that the server supports.
Memory Configuration field	The current memory configuration. This can be one of the following: • **Maximum Performance**—The system automatically optimizes the memory performance. • **Mirroring**—The server maintains two identical copies of the data in memory. This option effectively halves the available memory on the server, as one half is automatically reserved for mirrored copy. • **Lockstep**—If the DIMM pairs in the server have an identical type, size, and organization and are populated across the SMI channels, you can enable lockstep mode to minimize memory access latency and provide better performance.
DIMM location diagram	Displays the DIMM or memory layout for the current server.

Step 5 In the **DIMM Block Listing** area, view the overall status of a DIMM and also enable DIMM block listing.

Name	Description
Overall DIMM Status field	The overall status of a DIMM. This can be one of the following: • **Good**—The DIMM status is available. • **Severe Fault**— The DIMM status when uncorrectable ECC errors are present.
Enable DIMM Block List checkbox	Check this option to enable DIMM block listing.

Step 6 In the **Memory Details** table, review the following detailed information about each DIMM:

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

Name	Description
Name column	The name of the DIMM slot in which the memory module is installed.
Capacity column	The size of the DIMM.
Channel Speed column	The clock speed of the memory channel, in megahertz.
Channel Type column	The type of memory channel.
Memory Type Detail column	The type of memory used in the device.

Name	Description
Bank Locator column	The location of the DIMM within the memory bank.
Manufacturer column	The vendor ID of the manufacturer. This can be one of the following: • **0x2C00**—Micron Technology, Inc. • **0x5105**—Qimonda AG i. In. • **0x802C**—Micron Technology, Inc. • **0x80AD**—Hynix Semiconductor Inc. • **0x80CE**—Samsung Electronics, Inc. • **0x8551**—Qimonda AG i. In. • **0xAD00**—Hynix Semiconductor Inc. • **0xCE00**—Samsung Electronics, Inc.
Serial Number column	The serial number of the DIMM.
Asset Tag column	The asset tag associated with the DIMM, if any.
Part Number column	The part number for the DIMM assigned by the vendor.
Visibility column	Whether the DIMM is available to the server.
Operability column	Whether the DIMM is currently operating correctly.
Data Width column	The amount of data the DIMM supports, in bits.

Viewing PCI Adapter Properties

Before you begin

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

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

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

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

Step 4 In the **PCI Adapters** tab, review the following information for the installed PCI adapters:

Name	Description
Slot ID column	The slot in which the adapter resides.
Product Name column	The name of the adapter.

Name	Description
Option ROM Status column	Indicates the Option ROM status. This can be one of the following: • Loaded—Data is available in the card. • Not Loaded—Data is not available in the card. • Load Error—Card is present and Option ROM is enabled. But Option ROM failed to load due to an error in the card.
Firmware Version column	The firmware versions of the adapters. **Note** The firmware versions are displayed only for adapters that provide versions through the standard UEFI interface. For example, Intel LOM and Emulex Adapters.
Vendor ID column	The adapter ID assigned by the vendor.
Sub Vendor ID column	The secondary adapter ID assigned by the vendor.
Device ID column	The device ID assigned by the vendor.
Sub Device ID column	The secondary device ID assigned by the vendor.

Viewing vNICs Properties

Before you begin

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

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

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

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

Step 4 In the **vNICs** tab's **vNICs** area, review the following information:

Name	Description
Name column	The name of the virtual NIC.
VIC Slot column	VIC slot details.
CDN column	The Consistent Device Name (CDN) that you can assign to the ethernet vNICs on the VIC cards. Assigning a specific CDN to a device helps in identifying it on the host OS. **Note** This feature works only when the **CDN Support for VIC** token is enabled in the BIOS.

Name	Description
MAC Address column	The MAC address for the vNIC.
MTU column	The maximum transmission unit, or packet size, that this vNIC accepts.
usNIC column	The number of usNICs configured on each vNIC device.
Uplink Port column	The uplink port associated with the vNIC. All traffic for this vNIC goes through this uplink port.
CoS column	The Class of Service assigned to the vNIC.
VLAN column	The VLAN associated with the vNIC.
VLAN Mode column	The mode for the associated VLAN.
iSCSI Boot column	Whether iSCSI boot is enabled for this vNIC.
PXE Boot column	Whether PXE boot is enabled for this vNIC.
Channel column	The channel associated with the vNIC, if any. **Note** VNTAG mode is required for this option.
Port Profile column	The port profile associated with the vNIC, if any. **Note** VNTAG mode is required for this option.
Uplink Failover column	Whether traffic on this vNIC will fail over to a secondary interface if the primary interface fails. **Note** VNTAG mode is required for this option.

Viewing Storage Properties

Before you begin

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

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

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

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

Step 4 In the **Storage** tab, review the following information:

Name	Description
Controller field	PCIe slot in which the controller drive is located.

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

Viewing TPM Properties

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

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

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

Step 4 In the **TPM** pane, review the following information:

Name	Description
Version field	The TPM version. This field displays **NA** if the TPM version details are not available.
Presence field	Presence of the TPM module on the host server. • **Equipped**—The TPM is present on the host server. • **Empty**—The TPM does not exist on the host server.
Model field	The model number of the TPM. This field displays **NA** if the TPM does not exist on the host server.
Enabled Status field	Whether or not the TPM is enabled. • **Enabled**—The TPM is enabled. • **Disabled**—The TPM is disabled. • **Unknown**—The TPM does not exist on the host server.
Vendor field	The name of the TPM vendor. This field displays **NA** if the TPM does not exist on the host server.

Name	Description
Active Status field	Activation status of the TPM. • **Activated**—The TPM is activated. • **Deactivated**—The TPM is deactivated. • **Unknown**—The TPM does not exist on the host server. **Note** In some C-series servers that have installed TPM version 2.0, **Active Status** is displayed as **NA**.
Serial field	The serial number of the TPM. This field displays **NA** if the TPM does not exist on the host server.
Ownership field	The ownership status of TPM. • **Owned**—The TPM is owned. • **Unowned**—The TPM is unowned. • **Unknown**—The TPM does not exist on the host server. **Note** In some C-series servers that have installed TPM version 2.0, **Ownership** status is displayed as **NA**.
Revision field	Revision number of the TPM. This field displays **NA** if the TPM does not exist on the host server.
Firmware Version field	Details of the firmware version.

Viewing IO Expander Properties

Before you begin

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

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

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

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

Step 4 In the **IO Expander** tab's **IO Expander** area, review the following information:

Name	Description
Version field	The IO Expander version.

Name	Description
Presence field	Presence of the IO Expander module on the host server. • **Equipped**—The IO Expander is present on the host server. • **Empty**—The IO Expander does not exist on the host server.
Revision field	Revision number of the IO Expander. This field displays **NA** if the IO Expander does not exist on the host server.
Model field	The model number of the IO Expander. This field displays **NA** if the IO Expander does not exist on the host server.
Serial field	The serial number of the IO Expander. This field displays **NA** if the IO Expander does not exist on the host server.

Viewing a PID Catalog

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

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

Step 3 Click the **PID Catalog** tab.

Step 4 Review the following summary information about the PID catalog:

- **Activation Status**: The activation status of the PID catalog.
- **Current Activated Version**: The activated version of the PID catalog.

Step 5 In the **CPUs** table, review the following information about CPU:

Name	Description
Socket Name column	The socket in which the CPU is installed.
Product ID column	The product ID for the CPU.
Model column	The model number of the CPU

Step 6 In the **Memory** table, review the following information about memory:

Name	Description
Name column	The name of the memory slot.
Product ID column	The product ID for the memory slot assigned by the vendor.
Vendor ID column	The ID assigned by the vendor.
Capacity column	The size of the memory.

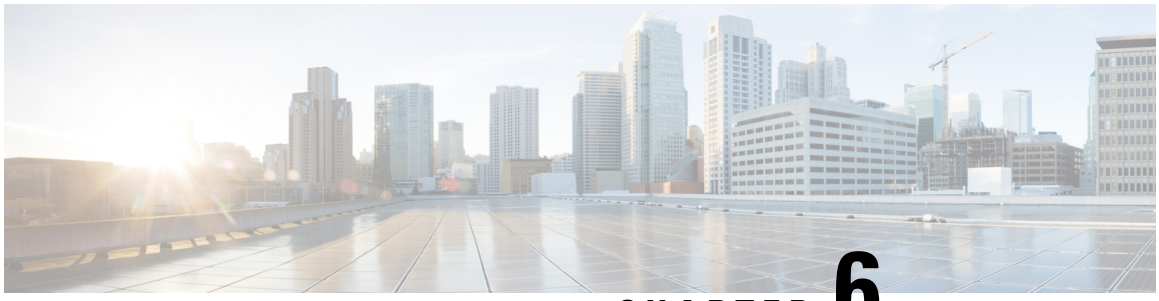
Name	Description
Speed (MHz) column	The memory speed, in megahertz.

Step 7 In the **PCI Adapters** table, review the following information about PCI adapter:

Name	Description
Slot column	The slot in which the adapter resides.
Product ID column	The product ID for the adapter.
Vendor ID column	The adapter ID assigned by the vendor.
Sub Vendor ID column	The secondary adapter ID assigned by the vendor.
Device ID column	The device ID assigned by the vendor.
Sub Device ID column	The secondary device ID assigned by the vendor.

Step 8 In the **HDD** table, review the following information about HDD:

Name	Description
Disk column	The disk of the hard drive.
Product ID column	The product ID for the hard drive.
Controller column	The system-defined name of the selected Cisco Flexible Flash controller. This name cannot be changed.
Vendor column	The vendor for the hard drive.
Model column	The model of the hard drive.



CHAPTER 6

Viewing Sensors

This chapter includes the following sections:

Viewing Server Sensors

Viewing Temperature Sensors

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

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

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

Step 4 Under the **Temperature** tab, view the following statistics for the server in **Temperature Sensors** area:

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

Name	Description
Critical Threshold Min column	The minimum critical threshold.
Critical Threshold Max column	The maximum critical threshold.

Viewing Voltage Sensors

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

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

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

Step 4 Under the **Voltage** tab, view the following statistics for the server in **Voltage Sensors** area:

Name	Description
Sensor Name column	The name of the sensor.
Status column	The status of the sensor. This can be one of the following: • **Unknown** • **Informational** • **Normal** • **Warning** • **Critical** • **Non-Recoverable**
Voltage column	The current voltage, in volts.
Warning Threshold Min column	The minimum warning threshold.
Warning Threshold Max column	The maximum warning threshold.
Critical Threshold Min column	The minimum critical threshold.
Critical Threshold Max column	The maximum critical threshold.

Viewing LED Sensors

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

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

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

Step 4 Under the **LEDs** tab, view the following statistics for the server in **LED Sensors** area:

Name	Description
Sensor Name column	The name of the sensor.
LED State column	Whether the LED is on, blinking, or off.
LED Color column	The current color of the LED. For details about what the colors mean, see the hardware installation guide for the type of server you are using.

Viewing Storage Sensors

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

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

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

Step 4 Under the **Storage** tab, view the following statistics for the server in **Storage Sensors** area:

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

Viewing Chassis Sensors

Viewing Power Supply Sensors

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

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

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

Step 4 Review the following sensor properties for power supply:

Properties Area

Name	Description
Redundancy Status field	The power supply redundancy status.

Threshold Sensors Area

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

Discrete Sensors Area

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

Viewing Fan Sensors

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

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

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

Step 4 Review the following fan sensor properties:

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

Viewing Temperature Sensors

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

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

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

Step 4 Review the following temperature sensor properties:

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

Viewing Voltage Sensors

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

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

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

Step 4 Review the following voltage sensor properties:

Name	Description
Sensor Name column	The name of the sensor

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

Viewing Current Sensors

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

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

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

Step 4 Review the following current sensor properties:

Name	Description
Sensor Name column	The name of the sensor

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

Viewing LED Sensors

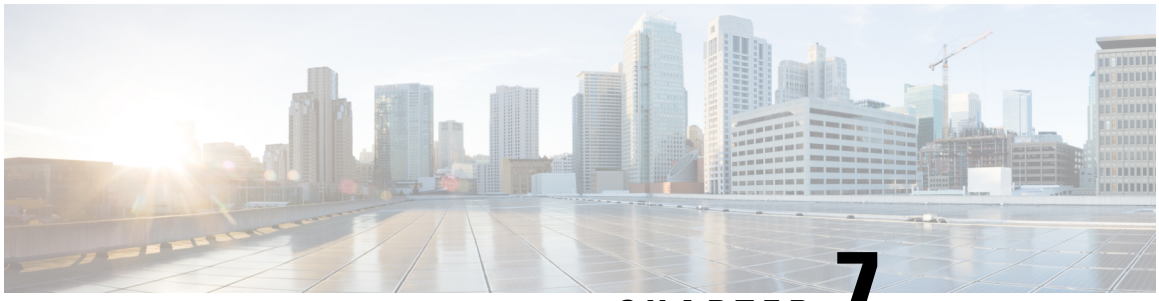
Step 1 In the **Navigation** pane, click the **Chassis** menu.

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

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

Step 4 Review the following LED sensor properties:

Name	Description
Sensor Name column	The name of the sensor
LED Status column	Whether the LED is on, blinking, or off.
LED Color column	The current color of the LED. For details about what the colors mean, see the hardware installation guide for the type of server you are using.



CHAPTER 7

Managing Remote Presence

This chapter includes the following sections:

Configuring Serial Over LAN

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

Important You cannot use native serial redirection and serial over LAN simultaneously.

Before you begin

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

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

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

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

Step 4 In the **Remote Presence** pane, click the **Serial over LAN** tab.

Step 5 In the **Serial over LAN Properties** area, update the following properties:

Name	Description
Enabled check box	If checked, Serial over LAN (SoL) is enabled on this server.

Name	Description
Baud Rate drop-down list	The baud rate the system uses for SoL communication. This can be one of the following: • **9600 bps** • **19.2 kbps** • **38.4 kbps** • **57.6 kbps** • **115.2 kbps**
Com Port drop-down list	The serial port through which the system routes SoL communication. You can select one of the following: • **com0**—SoL communication is routed through COM port 0, an externally accessible serial port that supports either a physical RJ45 connection to an external device or a virtual SoL connection to a network device. If you select this option, the system enables SoL and disables the RJ45 connection, which means that the server can no longer support an external serial device. • **com1**—SoL communication is routed through COM port 1, an internal port accessible only through SoL. If you select this option, you can use SoL on COM port 1 and the physical RJ45 connection on COM port 0. **Note** Changing the Com Port setting disconnects any existing SoL sessions.

Step 6 Click **Save Changes**.

Configuring Virtual Media

Before you begin

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

Step 1 In the **Navigation** pane, click **Compute**.
Step 2 In the **Compute** menu, select a server.
Step 3 Click the **Remote Management** tab.
Step 4 In the **Remote Management** tab, click the **Virtual Media** tab.
Step 5 In the **vKVM Console Based vMedia Properties Area**, update the following properties:

Name	Description
Enabled check box	If checked, virtual media is enabled. **Note** If you clear this check box, all virtual media devices are automatically detached from the host.
Active Sessions field	The number of virtual media sessions that are currently running.
Enable Virtual Media Encryption check box	If checked, all virtual media communications are encrypted.
Low Power USB Enabled check box	If checked, low power USB is enabled. If the low power USB is enabled, after mapping the ISO and rebooting the host, the virtual drives appear on the boot selection menu.

Step 6 Click **Save Changes**.

Creating a Cisco IMC Mapped vMedia Volume

Before you begin

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

Step 1 In the **Navigation** pane, click the **Compute** menu.
Step 2 In the **Compute** menu, select a server.
Step 3 In the work pane, click the **Remote Management** tab.
Step 4 In the **Remote Management** tab, click the **Virtual Media** tab
Step 5 In the **Current Mappings** area, click **Add New Mapping**.
Step 6 In the **Add New Mapping** dialog box, update the following fields:

Name	Description
Volume field	The identity of the image mounted for mapping.

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

Name	Description
Mount Options field	

Name	Description
	Industry-standard mount options entered in a comma separated list. The options vary depending on the selected **Mount Type**. If you are using **NFS**, leave the field blank or enter one or more of the following: • **ro** • **rw** **Note** The folder, which is shared, should have write permissions to use read-write option. Read-write option is available only for .img files. • **nolock** • **noexec** • **soft** • **port=VALUE** • **timeo=VALUE** • **retry=VALUE** • **rsize=VALUE** • **wsize=VALUE** • **vers=VALUE** If you are using **CIFS**, leave the field blank or enter one or more of the following: • **ro** • **rw** **Note** The folder, which is shared, should have write permissions to use read-write option. Read-write option is available only for .img files. • **soft** • **nounix** • **noserverino** • **guest** • **username=VALUE**—ignored if **guest** is entered. • **password=VALUE**—ignored if **guest** is entered. • **sec=VALUE** The protocol to use for authentication when communicating with the remote server. Depending on the configuration of CIFS share, **VALUE** could be

Name	Description
	one of the following: • **None**—No authentication is used • **Ntlm**—NT LAN Manager (NTLM) security protocol. Use this option only with Windows 2008 R2 and Windows 2012 R2. • **Ntlmi**—NTLMi security protocol. Use this option only when you enable Digital Signing in the CIFS Windows server. • **Ntlmssp**—NT LAN Manager Security Support Provider (NTLMSSP) protocol. Use this option only with Windows 2008 R2 and Windows 2012 R2. • **Ntlmsspi**—NTLMSSPi protocol. Use this option only when you enable Digital Signing in the CIFS Windows server. • **Ntlmv2**—NTLMv2 security protocol. Use this option only with Samba Linux. • **Ntlmv2i**—NTLMv2i security protocol. Use this option only with Samba Linux. • `vers=VALUE` **Note** The format of the VALUE should be *x.x* If you are using **WWW(HTTP/HTTPS)**, leave the field blank or enter the following: • `noauto` **Note** Before mounting the virtual media, Cisco IMC tries to verify reachability to the end server by pinging the server. • `username=VALUE` • `password=VALUE`
User Name field	The username for the specified **Mount Type**, if required.
Password field	The password for the selected username, if required.

Step 7 Click **Save**.

Viewing Cisco IMC-Mapped vMedia Volume Properties

Before you begin

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

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

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

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

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

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

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

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

Removing a Cisco IMC-Mapped vMedia Volume

Before you begin

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

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

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

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

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

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

Step 6 Click **Unmap**.

Remapping an Existing Cisco IMC vMedia Image

Before you begin

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

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

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

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

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

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

Step 6 Click **Remap**.

Deleting a Cisco IMC vMedia Image

Before you begin

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

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

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

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

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

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

Step 6 Click **Delete**.

Virtual KVM Console

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

Here are a few major advantages of using Cisco KVM Console:

- The Cisco KVM console provides connection to KVM, SOL, and vMedia whereas the Avocent KVM provides connection only to KVM and vMedia.

- In the KVM Console, the vMedia connection is established at the KVM Launch Manager and is available for all users.
- The KVM console offers you an advanced character replacement options for the unsupported characters while pasting text from the guest to the host.
- The KVM console provides you an ability to store the vMedia mappings on CIMC.

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

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

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

Note To configure the vKVM console successfully for the S3260 Storage Server, you need to configure IP addresses for the Cisco IMC, CMC, and BMC components. You can configure the IP addresses for these components using the CLI interface or Web UI. For the CLI, use the command **scope network**, or view the setting using **scope <chassis/server1/2><cmc/bmc><network>**.

To configure IP addresses for network components on the web interface, see the steps described in the section **Configuring Network-Related Settings**.

Launching KVM Console

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

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

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

Step 3 From the tool bar, click **Launch vKVM**.

Step 4 In the **Servers** drop-down menu, select a server.

Step 5 Alternatively, in the **Navigation** pane, click the **Compute** menu.

Step 6 In the **Compute** menu, select a server.

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

Step 8 In the **Remote Management** pane, click the **Virtual KVM** tab.

Step 9 In the **Virtual vKVM** tab, click **Launch vKVM console**.

Step 10 Required: Click the URL link displayed in the pop-up window to load the client application. You need to click the link every time you launch the vKVM console.

Virtual KVM Console

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

Cisco IMC provides Cisco based vKVM console for S-Series M5 servers with the following options:

File Menu

Menu Item	Description
Paste Text From File / Send Text	Opens the dialog box that allows you to paste content.
Capture to File	Opens the **Save** dialog box that allows you to save the current screen as a JPG image.
Exit	Closes the vKVM console.

View Menu

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

Macros Menu

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

Menu Item	Description
Static Macros menu	Displays a predefined set of macros.
Manage	Opens the **Configure User Defined Macros** dialog box, which allows you to create and manage macros. System-defined macros cannot be deleted.

Tools Menu

Menu Item	Description

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

Session User List	Opens the **Session User List** dialog box that shows all the user IDs that have an active vKVM session.
Chat	Opens the **Chat** box to communicate with other users.
Stats	Opens the **Stats** dialog box, and the **Live vKVM** displays the following: • **Frame Rate**: Frame rate measured in the number of frames per second. • **Bandwidth**: Bandwidth measured in the number of KBs per second. • **Compression**: Compression measured in the percentage of compression being used. • **Packet Rate**: Packet rate measured in number of packets per second. When vMedia is activated, the **Virtual Media** dialog box displays the following: • **Target Device**: The type of local device. • **Mapped to**: The type of local device or image file to which the host server device is mapped. • **Duration**: The elapsed time of the device to map. • **Read Bytes**: The number of bytes sent or received by the server.
Play Controls	Opens **Cisco vKVM Playback** window that allows you to choose a `.dvc` file.

Power Menu

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

Boot Device Menu

Name	Description
No Override	Clicking this option enables the host to boot to the first device configured.
Boot Device list	A list of boot devices that the server uses to boot from only for the next server boot, without disrupting the currently configured boot order. Once the server boots from the one time boot device, all its future reboots occur from the previously configured boot order. A maximum of 15 devices are displayed on the vKVM console.

Virtual Media Menu

Name	Description
Create Image **Note** This option is available only if you use the Google Chrome web browser.	Allows you to create an ISO image. Drag and drop files or folders in the **Create Image** dialog box; these files or folders are converted to an ISO image. You can use the **Download ISO Image** button to save the ISO image to your local machine.
Activate Virtual Devices	Activates a vMedia session that allows you to attach a drive or image file from your local computer or network.

Help Menu

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

Settings

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

Name	Description
Logged in as:	Displays your user role name.
Cisco IMC Host Name	Displays the host name.

Configuring the Virtual KVM

Before you begin

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

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

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

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

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

Step 5 In the **vKVM Properties** area on the **Virtual KVM** tab, complete the following fields:

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

Step 6 Click **Save Changes**.

Enabling the Virtual KVM

Before you begin

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

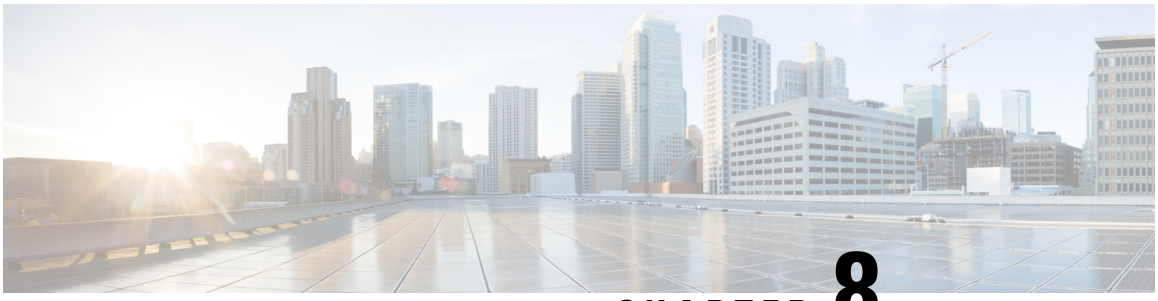
Step 1 In the **Navigation** pane, click the **Compute** menu.
Step 2 In the **Compute** menu, select a server.
Step 3 In the work pane, click the **Remote Management** tab.
Step 4 In the **Remote Management** pane, click the **Virtual KVM** tab.
Step 5 On the **Virtual KVM** tab, check the **Enabled** check box.
Step 6 Click **Save Changes**.

Disabling the Virtual KVM

Before you begin

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

Step 1 In the **Navigation** pane, click the **Compute** menu.
Step 2 In the **Compute** menu, select a server.
Step 3 In the work pane, click the **Remote Management** tab.
Step 4 In the **Remote Management** pane, click the **Virtual KVM** tab.
Step 5 On the **Virtual KVM** tab, uncheck the **Enabled** check box.
Step 6 Click **Save Changes**.



CHAPTER 8

Modifying or Adding Local Users for Cisco UCS C-Series M6 and Earlier Servers

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

Before you begin

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

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

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

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

Step 4 To add a local user account, click **Add User**.

To modify a local user account, click a row in the **Local User Management** pane and click **Modify User**.

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

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

Name	Description

Role Played field	The role assigned to the user. This can be one of the following:
	• **read-only**—A user with this role can view information but cannot make any changes.
	• **user**—A user with this role can perform the following tasks:
	  • View all information
	  • Manage the power control options such as power on, power cycle, and power off
	  • Launch the vKVM console and virtual media
	  • Clear all logs
	  • Ping
	• **admin**—A user with this role can perform all actions available through the GUI, CLI, and IPMI.
	Note Any user with admin role will not have the option of **Change Password** from the right top corner in **Settings** drop-down menu.
	To change password as a non-admin user, select **read-only** or **user** role and not the **admin** role.

Enabled check box	If checked, the user is enabled on Cisco IMC.
Change Password check box	Enable this check box if you want to change the password.

Name	Description
New Password field	The password for this user name. Click the **Suggest** button to get a system generated password that you may want to use. When you move the mouse over the help icon beside the field, the following guidelines to set the password are displayed: • The password must have a minimum of 8 and a maximum of 20 characters. The password can have a maximum of 127 characters for non IPMI users. • The password must not contain the user's name. • The password must contain characters from three of the following four categories: • English uppercase characters (A through Z). • English lowercase characters (a through z). • Base 10 digits (0 through 9). • Non-alphabetic characters (!, @, #, $, %, ^, &, *, -, _,+ , =). These guidelines are meant to define a strong password for the user, for security reasons. However, if you want to set a password of your choice ignoring these guidelines, click the **Disable Strong Password** button on the **Local User Management** tab. While setting a password when the strong password option is disabled, you can use between 1- 20 characters.
Confirm Password field	The password repeated for confirmation.

Step 6 Enter password information.

Step 7 Click **Save Changes**.

- Adding Local Users for Cisco UCS C-Series M7 and Later Servers, on page 106
- Modifying Local Users for Cisco UCS C-Series M7 and Later Servers, on page 109
- Managing SSH Keys in User Accounts, on page 112
- Non-IPMI User Mode, on page 116
- Changing Password as a Non-Admin User, on page 117
- Password Expiry, on page 120
- Configuring Password Expiry Duration, on page 120
- Enabling Password Expiry, on page 121
- Configuring Account Lockout Details, on page 122
- Configuring User Authentication Precedence, on page 122
- Resetting User Credentials to Factory Default Values, on page 122
- LDAP Servers, on page 123
- TACACS+ Authentication, on page 134
- Viewing User Sessions, on page 136

Adding Local Users for Cisco UCS C-Series M7 and Later Servers

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

Before you begin

You must log in as a user with admin privileges to add local user accounts.

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

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

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

Step 4

Step 5 To add a local user account, click **Add User**.

To modify a local user account, click a row in the **Local User Management** pane and click **Modify User**.

Step 6 In the **Modify User Details** or **Local User Details** dialog box, update the following properties:

Name	Description
ID field	The unique identifier for the user. ID is not user configurable. ID is assigned automatically.
Username field	The username for the user. Username can be maximum of 32 characters for **CIMC** and **SNMP** user type (any combination) and maximum 16 characters for **IPMI** user type (any combination). For more information on **User Type** see **User Type** check box description.

Name	Description

Role Played field	The role assigned to the user. This can be one of the following:
	• **read-only**—A user with this role can view information but cannot make any changes.
	• **user**—A user with this role can perform the following tasks:
	  • View all information
	  • Manage the power control options such as power on, power cycle, and power off
	  • Launch the vKVM console and virtual media
	  • Clear all logs
	  • Ping
	• **admin**—A user with this role can perform all actions available through the GUI, CLI, and IPMI.
	• **snmponly**—A user with only SNMP role.
	Note Any user with admin role will not have the option of **Change Password** from the right top corner in **Settings** drop-down menu.
	To change password as a non-admin user, select **read-only** or **user** role and not the **admin** role.

User Type check box	You may create the following types of users: • CIMC • SNMP • IPMI You may assign multiple types to one single user.
Enabled check box	If checked, the user is enabled on Cisco IMC.

Table 6: CIMC User Type

Name	Description
Password field	Enter a suitable password. To know more about password requirements, hover the cursor over **?** icon beside the **Suggest** button.
Confirm Password field	The password repeated for confirmation.
Suggest button	You may use this option for a system generated password.

Table 7: SNMP User Type

Name	Description
Security Level drop-down list	The security level for this user. This can be one of the following: • **no auth, no priv**—The user does not require an authorization or privacy password. • **auth, no priv**—The user requires an authorization password but not a privacy password. If you select this option, Cisco IMC enables the Auth fields described below. • **auth, priv**—The user requires both an authorization password and a privacy password. If you select this option, Cisco IMC enables the Auth and Privacy fields.
Auth Type drop-down	The authorization type. This can be one of the following: • **HMAC_SHA96** • **HMAC128_SHA224** • **HMAC192_SHA256** • **HMAC256_SHA384** • **HMAC384_SHA512**
Auth Password field	The authorization password for this SNMP user. Enter between 8 and 64 characters or spaces. **Note** Cisco IMC automatically trims leading or trailing spaces.
Confirm Auth Password field	The authorization password again for confirmation purposes.
Privacy Type drop-down	The privacy type. This can be one of the following:
Privacy Password field	The privacy password for this SNMP user. Enter between 8 and 64 characters or spaces. **Note** Cisco IMC automatically trims leading or trailing spaces.
Confirm Privacy Password field	The authorization password again for confirmation purposes.

Table 8: IPMI User Type

Name	Description
Password field	Enter a suitable password. To know more about password requirements, hover the cursor over **?** icon beside the **Suggest** button.
Confirm Password field	The password repeated for confirmation.
Suggest button	You may use this option for a system generated password.

Step 7 Click **Save**.

Modifying Local Users for Cisco UCS C-Series M7 and Later Servers

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

Before you begin

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

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

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

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

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

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

Name	Description
ID field	The unique identifier for the user. This is not user configurable.
Username field	The username for the user. Enter between 1 and 16 characters.

Name	Description

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

User Type	You may update the user type to: • CIMC • SNMP • IPMI You may assign multiple types to one single user.
Enabled check box	If checked, the user is enabled on the Cisco IMC.
Change Password check box	If checked, when you save the changes the password for this user will be changed. You must check this box if you want the change the password. **Change Password** check box also opens all the checked **User Type** options.

Table 9: CIMC User Type

Name	Description
Password field	Enter a suitable password. To know more about password requirements, hover the cursor over **?** icon beside the **Suggest** button.
Confirm Password field	The password repeated for confirmation.
Suggest button	You may use this option for a system generated password.

Table 10: SNMP User Type

Name	Description
Security Level drop-down list	The security level for this user. This can be one of the following: • **no auth, no priv**—The user does not require an authorization or privacy password. • **auth, no priv**—The user requires an authorization password but not a privacy password. If you select this option, Cisco IMC enables the Auth fields described below. • **auth, priv**—The user requires both an authorization password and a privacy password. If you select this option, Cisco IMC enables the Auth and Privacy fields.
Auth Type drop-down	The authorization type. This can be one of the following: • **HMAC_SHA96** • **HMAC128_SHA224** • **HMAC192_SHA256** • **HMAC256_SHA384** • **HMAC384_SHA512**
Auth Password field	The authorization password for this SNMP user. Enter between 8 and 64 characters or spaces. **Note** Cisco IMC automatically trims leading or trailing spaces.
Confirm Auth Password field	The authorization password again for confirmation purposes.
Privacy Type drop-down	The privacy type. This can be one of the following:
Privacy Password field	The privacy password for this SNMP user. Enter between 8 and 64 characters or spaces. **Note** Cisco IMC automatically trims leading or trailing spaces.
Confirm Privacy Password field	The authorization password again for confirmation purposes.

Table 11: IPMI User Type

Name	Description
Password field	Enter a suitable password. To know more about password requirements, hover the cursor over **?** icon beside the **Suggest** button.
Confirm Password field	The password repeated for confirmation.
Suggest button	You may use this option for a system generated password.

Step 6 Enter password information.

Managing SSH Keys in User Accounts

Configuring SSH Keys

You must log in as a user with admin privileges to view the SSH keys for all the users. If you are a non-admin user, you can view the SSH keys only for your account.

The Cisco IMC sessions authenticated using public SSH keys will be active even if the password has expired. You can also start new sessions using the public SSH key even after the password has expired.

Account lockout option does not apply to the accounts that use public key authentication.

Before you begin

- You must log in as a user with admin privileges to configure SSH keys for all the users.
- Ensure that you have created a pair of SSH RSA keys, public and private.
- Ensure that the SSH keys are in .pem or .pub format.

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

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

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

Step 4 To view the number of SSH keys configured for an account, view the details in the **SSH Key Count** field.

Step 5 To view the details of the SSH keys for an account, click a row in the **Local User Management** pane and click **SSH Keys**.

The **SSH Keys** window is displayed.

Step 6 In the **SSH Keys** window, view the following properties:

Name	Description
ID field	The unique identifier for the SSH key.

Name	Description
Comment	User name and remote server host name in the format *username@hostname*
Key	Details of the public SSH key configured for a specific user.

What to do next

Add or modify the SSH keys.

Adding SSH Keys

Before you begin

- You must log in as a user with admin privileges to add SSH keys for all users.
- If you are a non-admin user, you can add SSH keys only for your account.

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

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

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

Step 4 To add the SSH keys for an account, click a row in the **Local User Management** pane and click **SSH Keys**.

The **SSH Keys** window is displayed.

Step 5 Click any of the radio buttons near the **ID** column.

Step 6 Click **Add Keys** icon in the **SSH Keys** window to add the SSH key.

Step 7 Select any of the following radio buttons to add the SSH key.

a) Select **Paste SSH key**.

Copy the public SSH key from the host and paste the key in the text field.

b) Select **Upload from local**.

Click **Browse** and navigate to the public SSH key file that you want to add.

c) Select **Upload from remote location**.

Enter the following details to upload the public key file from the remote location.

Name	Description
Upload SSH key from drop-down list	The remote server type. This can be one of the following: • TFTP • FTP • SCP • SFTP • HTTP **Note** If you choose FTP, SCP or SFTP, you will be prompted to enter your username and password.
Server IP/Hostname field	The IP address or hostname of the server on which the SSH key file is available
Path and Filename field	The path and filename of the public SSH key file on the remote server.

Step 8 Click **Upload SSH Key**.

What to do next

Modify or delete the SSH keys.

Modifying SSH Keys

Before you begin

- You must log in as a user with admin privileges to modify the SSH keys for all the users.
- If you are a non-admin user, you can modify the SSH keys only for your account.

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

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

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

Step 4 To view and modify the SSH keys, click a row in the **Local User Management** pane and click **SSH Keys**.

The **SSH Keys** window is displayed.

Step 5 To modify the SSH key, review the list of SSH keys and select the desired row in the **SSH Keys** window.

Step 6 Click the **Modify Key** icon.

Step 7 Select any of the following radio buttons to modify the SSH key.

a) Select **Paste SSH key**.

Copy the updated public SSH key from the host and paste the key in the text field.

b) Select **Upload from local**.

Click **Browse** and navigate to the updated public key file that you want to upload.

c) Select **Upload from remote location**.

Enter the following details to upload the updated public key file from the remote location.

Name	Description
Upload SSH key from drop-down list	The remote server type. This can be one of the following: • TFTP • FTP • SCP • SFTP • HTTP **Note** If you choose FTP, SCP or SFTP, you will be prompted to enter your username and password.
Server IP/Hostname field	The IP address or hostname of the server on which the updated SSH key file is available
Path and Filename field	The path and filename of the updated public SSH key file on the remote server.

Step 8 Click **Upload SSH Key**.

What to do next

Delete an SSH key.

Deleting SSH Keys

Before you begin

- You must log in as a user with admin privileges to delete the SSH keys for all the users.
- If you are a non-admin user, you can delete the SSH keys only for your account.

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

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

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

Step 4 To view and delete the SSH keys for a user account, click a row in the **Local User Management** pane and click **SSH Keys**.

The **SSH Keys** window is displayed.

Step 5 To delete the SSH key, review the list of SSH keys and select the desired row in the **SSH Keys** window.

Step 6 Click the **Delete Key** icon.

A pop-up window is displayed with the message *Do you want to delete the selected SSH key?*

Step 7 Click **Yes** to confirm the deletion.

Non-IPMI User Mode

Release 4.1 introduces a new user configuration option called **User Mode** that allows you to switch between IPMI and non-IPMI user modes. Introduction of the non-IPMI user mode provides enhanced password security for users and security enhancements to the BMC database that were restricted in earlier releases due to the constraints posed by the IPMI 2.0 standards. Non-IPMI user mode allows you to use 127 characters to set user passwords whereas users in IPMI mode are restricted to a password length of 20 characters. Non-IPMI user mode enables you to set stronger passwords for users configured in this mode.

You must consider the following configuration changes that occur while switching between user modes, when you:

- Switch to the non-IPMI mode, IPMI over LAN will not be supported.
- Switch from the non-IPMI to IPMI mode, deletes all the local users and reverts user credentials to default username and password. On subsequent login, you will be prompted to change the password.

  User data is not affected when you switch from IPMI to non-IPMI mode.
- Downgrade the firmware to a versions lower than 4.1 and if the user mode is non-IPMI, deletes all the local users and reverts user credentials to default username and password. On subsequent login, you will be prompted to change the default password.

Note When you reset to factory defaults, the user mode reverts to IPMI mode.

Switching between IPMI and Non-IPMI User Modes

Caution Performing this procedure restarts SSH, KVM, Webserver, XML API, and REST API services. It also removes the IPMI user support when you switch to Non-IPMI user mode.

Before you begin

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

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

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

Step 3 Click the **Disable IPMI User Mode** or **Enable IPMI User Mode** button and click **OK** to confirm.

Changing Password as a Non-Admin User

Note To perform this task, you must first login as admin and add a user with read-only or user privileges. Only then, you will be able to login as a non-admin user to change the password.

Step 1 Login as an admin user.

Step 2 In the **Navigation** pane, click the **Admin** menu.

Step 3 In the **Admin** menu, click **User Management**.

Step 4 In the **User Management** pane, click the **Local User Management** tab.

Step 5 To configure or add a local user account, click a row in the **Local User Management** pane and click **Add User**.

Step 6 In the **Add User** dialog box, update the following properties by adding a user with read-only or user privileges:

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

Name	Description

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

Enabled check box	If checked, the user is enabled on the Cisco IMC.
Change Password check box	If checked, the user is enabled to change the password.

Name	Description
New Password	Enter the new password for this username. Click the **Suggest** button to get a system generated password that you may want to use. When you move the mouse over the help icon beside the field, the following guidelines to set the password are displayed: • The password must have a minimum of 8 and a maximum of 14 characters. For Non IPMI users, the password can have maximum of 127 characters. • The password must not contain the User's Name. • The password must contain characters from three of the following four categories: • English uppercase characters (A through Z). • English lowercase characters (a through z). • Base 10 digits (0 through 9). • Non-alphabetic characters (!, @, #, $, %, ^, &, *, -, _, , =, "). These guidelines are meant to define a strong password for the user, for security reasons. However, if you want to set a password of your choice ignoring these guidelines, click the **Disable Strong Password** button on the **Local User Management** tab. While setting a password when the strong password option is disabled, you can use between 1- 20 characters.
Confirm Password field	The password repeated for confirmation.

Step 7 Click **Save Changes**.

Note On changing the password, you will be logged out of Cisco IMC.

Step 8 After creating a new user with read-only or user privileges, logout as admin.

Step 9 Now, login with the newly created read-only or user role. **Change Password** option is available in the right top corner in **Settings** drop-down menu.

When you click on the **Settings** icon, the drop-down lists the **Change Password** option. This option is visible only if you are logged in as a non-admin user.

If you do not see the **Change Password** option in the drop-down list, login as a non-admin user with read-only or user privileges.

You can now use the **Change Password** option to change your password. As soon as the password is changed, you will be logged out automatically and will be prompted to login with the new password.

Password Expiry

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

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

Password Set Time

A 'Password set time' is configured for every existing user, to the time when the migration or upgrade occurred. For new users (users created after an upgrade), the Password Set time is configured to the time when the user was created, and the password is set. For users in general (new and existing), the Password Set Time is updated whenever the password is changed.

Configuring Password Expiry Duration

Before you begin

- You must enable password expiry.

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

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

Step 3 In the **Local User Management** pane (opens by default), click **Password Expiration Details**.

Step 4 In the **Password Expiration Details** dialog box, update the following fields:

Name	Description
Enable Password Expiry check box	Checking this box allows you to configure the **Password Expiry Duration**. Uncheck the check box to disable it.
Password Expiry Duration field	The time period that you can set for the existing password to expire (from the time you set a new password or modify an existing one). The range is between 1 to 3650 days. **Note** Password expiry once set by the admin is applicable for all users that are subsequently created.

Name	Description
Password History field	The number of occurrences when a password was entered. When this is enabled, you cannot repeat a password. Enter a value between 0 to 5. Entering 0 disables this field.
Notification Period field	Notifies the time by when the password expires. Enter a value between 0 to 15 days. Entering 0 disables this field. **Note** The notification period time must be lesser than the password expiry duration.
Grace Period field	Time period till when the existing password can still be used, after it expires. Enter a value between 0 to 5 days. Entering 0 disables this field. **Note** The grace period time must be lesser than the password expiry duration.

Note The valid **Password Expiry Duration** must be greater than the **Notification Period** and the **Grace Period**. If otherwise, you will see an **User Password Expiry Policy configuration error**.

Step 5 Click **Save Changes**.

Step 6 Optionally, click **Reset Values** to clear the text fields and reset the values you entered. Click **Restore Defaults** to revert to the default settings.

Enabling Password Expiry

Before you begin

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

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

Step 3 In the **Local User Management** pane (opens by default), click **Password Expiration Details**.

Step 4 In the **Password Expiration Details** dialog box, check the **Enable Password Expiry** check box.

The **Password Expiry Duration** text field becomes editable and you can configure the duration by entering a number in days.

What to do next

Configure password expiry duration.

Configuring Account Lockout Details

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

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

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

Step 4 In the **Local User Management** pane, click **Account Lockout Details**.

Step 5 In the **Account Lockout Details** dialog box, complete the following:

Name	Description
Allowed Attempts (0-20) field	Number of unsuccessful log in attempts allowed for a user before which it is locked out for the duration defined in **Lockout Period**.
Lockout Period (0-60 Minutes) field	The time duration, in minutes, for which the user account is locked out after the allowed attempts.
Disable User on Lockout check box	Disables the user ID up on lockout.

Configuring User Authentication Precedence

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

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

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

Step 4 In the **Local User Management** pane, click **Configure User Authentication Precedence**.

Step 5 In the **Configure User Authentication Precedence** dialog box, select the database for which you wish to update the priority.

Step 6 Use the Up or the Down arrow to change the priority of the database.

Resetting User Credentials to Factory Default Values

Caution You may lose current IP address settings, NIC port settings, NIC redundancy after performing this procedure. Cisco recommends that you make a note of your current server settings before performing this procedure.

Before you begin

Ensure that your management Ethernet cable is plugged into the dedicated management port.

Step 1 Login as an admin user.

Step 2 In the **Navigation** pane, click the **Chassis** menu.

Step 3 In the **Chassis** menu, click **Summary**.

Step 4 From the tool bar, click **Launch KVM**.

Step 5 Alternatively, in the **Navigation** pane, click the **Compute** menu.

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

b. In the work pane, click the **Remote Management** tab.

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

d. In the **Virtual KVM** tab, click **Launch HTML based KVM console**.

Step 6 From the **Power** menu, select **Reset System**.

Step 7 When prompted, press **F8** to enter the Cisco IMC Configuration Utility. This utility opens in the KVM console window.

Step 8 Check the **Factory Default** check box, the server reverts to the factory defaults.

Step 9 Press **F5** to refresh the settings that you made. You might have to wait about 45 seconds until the new settings appear and the message **Network settings configured** is displayed before you reboot the server in the next step.

Step 10 Press **F10** to save your settings and reboot the server.

LDAP Servers

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

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

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 Cisco IMC 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 Cisco IMC. You can use an existing LDAP attribute that is mapped to the Cisco IMC user roles and locales or you can modify the LDAP schema to add a new custom attribute, such as the CiscoAVPair attribute, which has an attribute ID of 1.3.6.1.4.1.9.287247.1.

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

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

If you are using Group Authorization on the Cisco IMC LDAP configuration, then you can skip Steps 1-4 and perform the steps listed in the *Configuring LDAP Settings and Group Authorization in Cisco IMC* section.

The following steps must be performed on the LDAP server.

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

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

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

Step 4 Ensure that the LDAP schema snap-in is installed.

Step 5 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 6 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 7 Add the following user role values to the CiscoAVPair attribute, for the users that you want to have access to Cisco IMC:

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

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

What to do next

Use the Cisco IMC to configure the LDAP server.

Configuring LDAP Settings and Group Authorization in Cisco IMC

Before you begin

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

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

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

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

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

Name	Description
Enable LDAP check box	If checked, user authentication and role authorization is performed first by the LDAP server, followed by user accounts that are not found in the local user database.
Base DN field	Base Distinguished Name. This field describes where to load users and groups from. It must be in the `dc=domain,dc=com` format for Active Directory servers.
Domain field	The IPv4 domain that all users must be in. This field is required unless you specify at least one Global Catalog server address.
Enable Secure LDAP check box	If checked, the server enables secure LDAP and prompts you to download LDAP CA certificate. Refer Downloading an LDAP CA Certificate, on page 132 to download LDAP CA certificate. To delete an existing secure LDAP certificate, un-check this option. Follow the system prompts to confirm deletion.

Name	Description
Timeout (0 - 180) seconds	The number of seconds the Cisco IMC waits until the LDAP search operation times out. If the search operation times out, Cisco IMC tries to connect to the next server listed on this tab, if one is available. **Note** The value you specify for this field could impact the overall time.

Note If you check the **Enable Secure LDAP**check box, enter the fully qualified domain name (FQDN) of the LDAP server in the **LDAP Server** field. To resolve the FQDN of the LDAP server, configure the preferred DNS of Cisco IMC network with the appropriate DNS IP address.

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

Name	Description
Pre-Configure LDAP Servers radio button	If checked, the Active Directory uses the pre-configured LDAP servers.
LDAP Servers fields	
Server	The IP address of the 6 LDAP servers. If you are using Active Directory for LDAP, then servers 1, 2 and 3 are domain controllers, while servers 4, 5 and 6 are Global Catalogs. If you are not Active Directory for LDAP, then you can configure a maximum of 6 LDAP servers. **Note** You can provide the IP address of the host name as well.
Port	The port numbers for the servers. If you are using Active Directory for LDAP, then for servers 1, 2 and 3, which are domain controllers, the default port number is 389. For servers 4, 5 and 6, which are Global Catalogs, the default port number is 3268. LDAPS communication occurs over the TCP 636 port. LDAPS communication to a global catalog server occurs over TCP 3269 port.
Use DNS to Configure LDAP Servers radio button	If checked, you can use DNS to configure access to the LDAP servers.
DNS Parameters fields	

Name	Description
Source drop-down list	Specifies how to obtain the domain name used for the DNS SRV request. It can be one of the following: • **Extracted**—specifies using domain name extracted-domain from the login ID • **Configured**—specifies using the configured-search domain. • **Configured-Extracted**—specifies using the domain name extracted from the login ID than the configured-search domain.
Domain to Search	A configured domain name that acts as a source for a DNS query. This field is disabled if the source is specified as **Extracted**.
Forest to Search	A configured forest name that acts as a source for a DNS query. This field is disabled if the source is specified as **Extracted**.

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

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

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

Name	Description
Filter Attribute	This field must match the configured attribute in the schema on the LDAP server. By default, this field displays **sAMAccountName**.
Group Attribute	This field must match the configured attribute in the schema on the LDAP server. By default, this field displays **memberOf**.
Attribute	An LDAP attribute that contains the role and locale information for the user. This property is always a name-value pair. The system queries the user record for the value that matches this attribute name. The LDAP attribute can use an existing LDAP attribute that is mapped to the Cisco IMC user roles and locales, or can modify the schema such that a new LDAP attribute can be created. For example, **CiscoAvPair**.
Nested Group Search Depth (1-128)	Parameter to search for an LDAP group nested within another defined group in an LDAP group map. The parameter defines the depth of a nested group search.

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

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

Name	Description

Role column	The role assigned to all users in this LDAP server group. This can be one of the following:
	• **read-only**—A user with this role can view information but cannot make any changes.
	• **user**—A user with this role can perform the following tasks:
	  • View all information
	  • Manage the power control options such as power on, power cycle, and power off
	  • Launch the KVM console and virtual media
	  • Clear all logs
	  • Ping
	• **admin**—A user with this role can perform all actions available through the GUI, CLI, and IPMI.

Configure button	Opens the **Configure LDAP Group** window for an active directory group with the same **Group Name**, **Group Domain**, and **Role** options listed above. Once configured, click **Save Changes**.
Delete button	Deletes an existing LDAP group.

Step 9 Click **Save Changes**.

LDAP Certificates Overview

Cisco S3260 C-series servers allow an LDAP client to validate a directory server certificate against an installed CA certificate or chained CA certificate during an LDAP binding step. This feature is introduced in the event where anyone can duplicate a directory server for user authentication and cause a security breach due to the inability to enter a trusted point or chained certificate into the Cisco IMC for remote user authentication.

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

Viewing LDAP CA Certificate Status

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

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

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

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

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

Exporting an LDAP CA Certificate

Before you begin

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

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

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

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

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

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

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

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

Step 5 Click **Export Certificate**.

Downloading an LDAP CA Certificate

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

Steps

1. In the **Navigation** pane, click the **Admin** tab.
2. In the **Admin** menu, click **User Management**.
3. In the **User Management** pane, click the **LDAP** tab.
4. Click the **Download LDAP CA Certificate** link.

   The **Download LDAP CA Certificate** dialog box appears.
5. Fill the required information in the **Download LDAP CA Certificate** dialog box.

Name	Description
Upload **from remote location** radio button	Selecting this option allows you to choose the certificate from a remote location and Upload it. Enter the following details: • • **TFTP Server** • **FTP Server** • **SFTP Server** • **SCP Server** • **HTTP Server** **Note** If you chose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message *Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*. Click Yes or No depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to. • **Server IP/Hostname** field — The IP address or hostname of the server on which the LDAP CA certificate file should be stored. Depending on the setting in the Upload **Certificate from** drop-down list, the name of the field may vary. • **Path and Filename** field — The path and filename Cisco IMC should use when uploading the file to the remote server. • **Username** field — The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP. • **Password** field — The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP.
Upload **through browser client** radio button	Selecting this option allows you to navigate to the certificate stored on a drive that is local to the computer running the Cisco IMC GUI. When you select this option, Cisco IMC GUI displays a **Browse** button that lets you navigate to the file you want to import.
Paste Certificate content radio button	Selecting this option allows you to copy the entire content of the signed certificate and paste it in the **Paste certificate content** text field. **Note** Ensure the certificate is signed before uploading.
Upload **Certificate** button	Allows you to Upload the certificate to the server.

Testing LDAP Binding

Before you begin

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

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

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

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

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

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

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

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

Step 5 Click **Test**.

TACACS+ Authentication

Beginning with 4.1(3b) release, Cisco IMC supports Terminal Access Controller Access-Control System Plus (TACACS+) user authentication. Cisco IMC supports up to six TACACS+ remote servers. Once a user is successfully authenticated, the username is appended with **(TACACS+)**. This is also displayed in the Cisco IMC interfaces.

Refer Enabling TACACS+ Authentication, on page 135 to enable TACACS+ Authentication. Cisco IMC also supports user authentication precedence in case TACACS+ remote servers are inaccessible. User authentication precedence can be configured using Configuring User Authentication Precedence, on page 122.

TACACS+ Server Configuration

Privilege level of a user is calculated based on the **cisco-av-pair** value configured for that user. A **cisco-av-pair** should be created on the TACACS+ server. Users cannot use any existing TACACS+ attributes.

Following three syntax are supported for the **cisco-av-pair** attribute:

- For `admin` privilege: **cisco-av-pair=shell:roles="admin"**
- For `user` privilege: **cisco-av-pair=shell:roles="user"**

- For `read-only` privilege: **cisco-av-pair=shell:roles="read-only"**

More roles, if required, can be added by using **comma** as a separator.

Note If **cisco-av-pair** is not configured on the TACACS+ server, then a user with that server has **read-only** privilege.

Enabling TACACS+ Authentication

Before you begin

Before configuring Terminal Access Controller Access-Control System (TACACS+) based user authentication, ensure that privilege level of a user is configured on TACACS+ server based on the **cisco-av-pair** value.

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

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

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

Step 4 Under the **TACACS+ Properties** area perform the following:

Name	Description
Enabled check box	Check this box to enable TACACS+ based user authentication.
Fallback only on no connectivity check box	If checked, the authentication falls back to the next precedence database only in-case Cisco IMC is not able to connect to any of the configured TACACS+ servers. Ensure to configure user authentication precedence. Refer Configuring User Authentication Precedence, on page 122.
Timeout (for each server): (5 - 30) seconds field	Time duration, in seconds, for which Cisco IMC waits for a response from each of the TACACS+ servers

Configuring TACACS+ Remote Server Settings

You can configure up to six TACACS+ remote servers.

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

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

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

Step 4 Under the **Server List** area, click the radio button for the server ID which you wish to configure and click the **Edit** button.

Step 5 Update the following fields:

Name	Description
ID	This is unique identifier of the server and is not user editable.
IP Address or Host Name	The IP address at which the TACACS+ server is running.
Port	The port on which TACACS+ server is running.
Server key	The same key that is configured on the TACACS+ server. Repeat the same key for **Confirm Server Key**.

Viewing User Sessions

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

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

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

Step 4 In the **Sessions** pane, view the following information about current user sessions:

Name	Description
Terminate Session button	If your user account is assigned the **admin** user role, this option enables you to force the associated user session to end. **Note** You cannot terminate your current session from this tab.
Session ID column	The unique identifier for the session.
BMC Session ID	The identifier for the BMC session.
User Name column	The username for the user.
IP Address column	The IP address from which the user accessed the server. If this is a serial connection, it displays **N/A**.

Name	Description
Session Type column	The type of session the user chose to access the server. This can be one of the following: • **webgui**— indicates the user is connected to the server using the web UI. • **CLI**— indicates the user is connected to the server using CLI. • **serial**— indicates the user is connected to the server using the serial port. • — indicates the user is connected to the server using XML API. • — indicates the user is connected to the server using Redfish API.

Adding Local Users for Cisco UCS C-Series M7 and Later Servers

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

Before you begin

You must log in as a user with admin privileges to add local user accounts.

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

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

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

Step 4

Step 5 To add a local user account, click **Add User**.

To modify a local user account, click a row in the **Local User Management** pane and click **Modify User**.

Step 6 In the **Modify User Details** or **Local User Details** dialog box, update the following properties:

Name	Description
ID field	The unique identifier for the user. ID is not user configurable. ID is assigned automatically.
Username field	The username for the user. Username can be maximum of 32 characters for **CIMC** and **SNMP** user type (any combination) and maximum 16 characters for **IPMI** user type (any combination). For more information on **User Type** see **User Type** check box description.

Name	Description

Role Played field	The role assigned to the user. This can be one of the following:
	• **read-only**—A user with this role can view information but cannot make any changes.
	• **user**—A user with this role can perform the following tasks:
	  • View all information
	  • Manage the power control options such as power on, power cycle, and power off
	  • Launch the vKVM console and virtual media
	  • Clear all logs
	  • Ping
	• **admin**—A user with this role can perform all actions available through the GUI, CLI, and IPMI.
	• **snmponly**—A user with only SNMP role.
	Note Any user with admin role will not have the option of **Change Password** from the right top corner in **Settings** drop-down menu.
	To change password as a non-admin user, select **read-only** or **user** role and not the **admin** role.

User Type check box	You may create the following types of users: • CIMC • SNMP • IPMI You may assign multiple types to one single user.
Enabled check box	If checked, the user is enabled on Cisco IMC.

Table 12: CIMC User Type

Name	Description
Password field	Enter a suitable password. To know more about password requirements, hover the cursor over **?** icon beside the **Suggest** button.
Confirm Password field	The password repeated for confirmation.
Suggest button	You may use this option for a system generated password.

Table 13: SNMP User Type

Name	Description
Security Level drop-down list	The security level for this user. This can be one of the following: • **no auth, no priv**—The user does not require an authorization or privacy password. • **auth, no priv**—The user requires an authorization password but not a privacy password. If you select this option, Cisco IMC enables the Auth fields described below. • **auth, priv**—The user requires both an authorization password and a privacy password. If you select this option, Cisco IMC enables the Auth and Privacy fields.
Auth Type drop-down	The authorization type. This can be one of the following: • **HMAC_SHA96** • **HMAC128_SHA224** • **HMAC192_SHA256** • **HMAC256_SHA384** • **HMAC384_SHA512**
Auth Password field	The authorization password for this SNMP user. Enter between 8 and 64 characters or spaces. **Note** Cisco IMC automatically trims leading or trailing spaces.
Confirm Auth Password field	The authorization password again for confirmation purposes.
Privacy Type drop-down	The privacy type. This can be one of the following:
Privacy Password field	The privacy password for this SNMP user. Enter between 8 and 64 characters or spaces. **Note** Cisco IMC automatically trims leading or trailing spaces.
Confirm Privacy Password field	The authorization password again for confirmation purposes.

Table 14: IPMI User Type

Name	Description
Password field	Enter a suitable password. To know more about password requirements, hover the cursor over **?** icon beside the **Suggest** button.
Confirm Password field	The password repeated for confirmation.
Suggest button	You may use this option for a system generated password.

Step 7 Click **Save**.

Modifying Local Users for Cisco UCS C-Series M7 and Later Servers

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

Before you begin

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

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

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

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

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

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

Name	Description
ID field	The unique identifier for the user. This is not user configurable.
Username field	The username for the user. Enter between 1 and 16 characters.

Name	Description

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

User Type	You may update the user type to: • CIMC • SNMP • IPMI You may assign multiple types to one single user.
Enabled check box	If checked, the user is enabled on the Cisco IMC.
Change Password check box	If checked, when you save the changes the password for this user will be changed. You must check this box if you want the change the password. **Change Password** check box also opens all the checked **User Type** options.

Table 15: CIMC User Type

Name	Description
Password field	Enter a suitable password. To know more about password requirements, hover the cursor over **?** icon beside the **Suggest** button.
Confirm Password field	The password repeated for confirmation.
Suggest button	You may use this option for a system generated password.

Table 16: SNMP User Type

Name	Description
Security Level drop-down list	The security level for this user. This can be one of the following: • **no auth, no priv**—The user does not require an authorization or privacy password. • **auth, no priv**—The user requires an authorization password but not a privacy password. If you select this option, Cisco IMC enables the Auth fields described below. • **auth, priv**—The user requires both an authorization password and a privacy password. If you select this option, Cisco IMC enables the Auth and Privacy fields.
Auth Type drop-down	The authorization type. This can be one of the following: • **HMAC_SHA96** • **HMAC128_SHA224** • **HMAC192_SHA256** • **HMAC256_SHA384** • **HMAC384_SHA512**
Auth Password field	The authorization password for this SNMP user. Enter between 8 and 64 characters or spaces. **Note** Cisco IMC automatically trims leading or trailing spaces.
Confirm Auth Password field	The authorization password again for confirmation purposes.
Privacy Type drop-down	The privacy type. This can be one of the following:
Privacy Password field	The privacy password for this SNMP user. Enter between 8 and 64 characters or spaces. **Note** Cisco IMC automatically trims leading or trailing spaces.
Confirm Privacy Password field	The authorization password again for confirmation purposes.

Table 17: IPMI User Type

Name	Description
Password field	Enter a suitable password. To know more about password requirements, hover the cursor over **?** icon beside the **Suggest** button.
Confirm Password field	The password repeated for confirmation.
Suggest button	You may use this option for a system generated password.

Step 6 Enter password information.

Managing SSH Keys in User Accounts

Configuring SSH Keys

You must log in as a user with admin privileges to view the SSH keys for all the users. If you are a non-admin user, you can view the SSH keys only for your account.

The Cisco IMC sessions authenticated using public SSH keys will be active even if the password has expired. You can also start new sessions using the public SSH key even after the password has expired.

Account lockout option does not apply to the accounts that use public key authentication.

Before you begin

- You must log in as a user with admin privileges to configure SSH keys for all the users.
- Ensure that you have created a pair of SSH RSA keys, public and private.
- Ensure that the SSH keys are in .pem or .pub format.

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

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

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

Step 4 To view the number of SSH keys configured for an account, view the details in the **SSH Key Count** field.

Step 5 To view the details of the SSH keys for an account, click a row in the **Local User Management** pane and click **SSH Keys**.

The **SSH Keys** window is displayed.

Step 6 In the **SSH Keys** window, view the following properties:

Name	Description
ID field	The unique identifier for the SSH key.

Name	Description
Comment	User name and remote server host name in the format *username@hostname*
Key	Details of the public SSH key configured for a specific user.

What to do next

Add or modify the SSH keys.

Adding SSH Keys

Before you begin

- You must log in as a user with admin privileges to add SSH keys for all users.
- If you are a non-admin user, you can add SSH keys only for your account.

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

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

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

Step 4 To add the SSH keys for an account, click a row in the **Local User Management** pane and click **SSH Keys**.

The **SSH Keys** window is displayed.

Step 5 Click any of the radio buttons near the **ID** column.

Step 6 Click **Add Keys** icon in the **SSH Keys** window to add the SSH key.

Step 7 Select any of the following radio buttons to add the SSH key.

a) Select **Paste SSH key**.

Copy the public SSH key from the host and paste the key in the text field.

b) Select **Upload from local**.

Click **Browse** and navigate to the public SSH key file that you want to add.

c) Select **Upload from remote location**.

Enter the following details to upload the public key file from the remote location.

Name	Description
Upload SSH key from drop-down list	The remote server type. This can be one of the following: • TFTP • FTP • SCP • SFTP • HTTP **Note** If you choose FTP, SCP or SFTP, you will be prompted to enter your username and password.
Server IP/Hostname field	The IP address or hostname of the server on which the SSH key file is available
Path and Filename field	The path and filename of the public SSH key file on the remote server.

Step 8 Click **Upload SSH Key**.

What to do next

Modify or delete the SSH keys.

Modifying SSH Keys

Before you begin

- You must log in as a user with admin privileges to modify the SSH keys for all the users.
- If you are a non-admin user, you can modify the SSH keys only for your account.

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

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

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

Step 4 To view and modify the SSH keys, click a row in the **Local User Management** pane and click **SSH Keys**.

The **SSH Keys** window is displayed.

Step 5 To modify the SSH key, review the list of SSH keys and select the desired row in the **SSH Keys** window.

Step 6 Click the **Modify Key** icon.

Step 7 Select any of the following radio buttons to modify the SSH key.

a) Select **Paste SSH key**.

Copy the updated public SSH key from the host and paste the key in the text field.

b) Select **Upload from local**.

Click **Browse** and navigate to the updated public key file that you want to upload.

c) Select **Upload from remote location**.

Enter the following details to upload the updated public key file from the remote location.

Name	Description
Upload SSH key from drop-down list	The remote server type. This can be one of the following: • TFTP • FTP • SCP • SFTP • HTTP **Note** If you choose FTP, SCP or SFTP, you will be prompted to enter your username and password.
Server IP/Hostname field	The IP address or hostname of the server on which the updated SSH key file is available
Path and Filename field	The path and filename of the updated public SSH key file on the remote server.

Step 8 Click **Upload SSH Key**.

What to do next

Delete an SSH key.

Deleting SSH Keys

Before you begin

- You must log in as a user with admin privileges to delete the SSH keys for all the users.
- If you are a non-admin user, you can delete the SSH keys only for your account.

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

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

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

Step 4 To view and delete the SSH keys for a user account, click a row in the **Local User Management** pane and click **SSH Keys**.

The **SSH Keys** window is displayed.

Step 5 To delete the SSH key, review the list of SSH keys and select the desired row in the **SSH Keys** window.

Step 6 Click the **Delete Key** icon.

A pop-up window is displayed with the message *Do you want to delete the selected SSH key?*

Step 7 Click **Yes** to confirm the deletion.

Non-IPMI User Mode

Release 4.1 introduces a new user configuration option called **User Mode** that allows you to switch between IPMI and non-IPMI user modes. Introduction of the non-IPMI user mode provides enhanced password security for users and security enhancements to the BMC database that were restricted in earlier releases due to the constraints posed by the IPMI 2.0 standards. Non-IPMI user mode allows you to use 127 characters to set user passwords whereas users in IPMI mode are restricted to a password length of 20 characters. Non-IPMI user mode enables you to set stronger passwords for users configured in this mode.

You must consider the following configuration changes that occur while switching between user modes, when you:

- Switch to the non-IPMI mode, IPMI over LAN will not be supported.
- Switch from the non-IPMI to IPMI mode, deletes all the local users and reverts user credentials to default username and password. On subsequent login, you will be prompted to change the password.

  User data is not affected when you switch from IPMI to non-IPMI mode.
- Downgrade the firmware to a versions lower than 4.1 and if the user mode is non-IPMI, deletes all the local users and reverts user credentials to default username and password. On subsequent login, you will be prompted to change the default password.

Note When you reset to factory defaults, the user mode reverts to IPMI mode.

Switching between IPMI and Non-IPMI User Modes

Caution Performing this procedure restarts SSH, KVM, Webserver, XML API, and REST API services. It also removes the IPMI user support when you switch to Non-IPMI user mode.

Before you begin

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

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

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

Step 3 Click the **Disable IPMI User Mode** or **Enable IPMI User Mode** button and click **OK** to confirm.

Changing Password as a Non-Admin User

Note To perform this task, you must first login as admin and add a user with read-only or user privileges. Only then, you will be able to login as a non-admin user to change the password.

Step 1 Login as an admin user.

Step 2 In the **Navigation** pane, click the **Admin** menu.

Step 3 In the **Admin** menu, click **User Management**.

Step 4 In the **User Management** pane, click the **Local User Management** tab.

Step 5 To configure or add a local user account, click a row in the **Local User Management** pane and click **Add User**.

Step 6 In the **Add User** dialog box, update the following properties by adding a user with read-only or user privileges:

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

Name	Description

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

Enabled check box	If checked, the user is enabled on the Cisco IMC.
Change Password check box	If checked, the user is enabled to change the password.

Name	Description
New Password	Enter the new password for this username. Click the **Suggest** button to get a system generated password that you may want to use. When you move the mouse over the help icon beside the field, the following guidelines to set the password are displayed: • The password must have a minimum of 8 and a maximum of 14 characters. For Non IPMI users, the password can have maximum of 127 characters. • The password must not contain the User's Name. • The password must contain characters from three of the following four categories: • English uppercase characters (A through Z). • English lowercase characters (a through z). • Base 10 digits (0 through 9). • Non-alphabetic characters (!, @, #, $, %, ^, &, *, -, _, , =, "). These guidelines are meant to define a strong password for the user, for security reasons. However, if you want to set a password of your choice ignoring these guidelines, click the **Disable Strong Password** button on the **Local User Management** tab. While setting a password when the strong password option is disabled, you can use between 1- 20 characters.
Confirm Password field	The password repeated for confirmation.

Step 7 Click **Save Changes**.

Note On changing the password, you will be logged out of Cisco IMC.

Step 8 After creating a new user with read-only or user privileges, logout as admin.

Step 9 Now, login with the newly created read-only or user role. **Change Password** option is available in the right top corner in **Settings** drop-down menu.

When you click on the **Settings** icon, the drop-down lists the **Change Password** option. This option is visible only if you are logged in as a non-admin user.

If you do not see the **Change Password** option in the drop-down list, login as a non-admin user with read-only or user privileges.

You can now use the **Change Password** option to change your password. As soon as the password is changed, you will be logged out automatically and will be prompted to login with the new password.

Password Expiry

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

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

Password Set Time

A 'Password set time' is configured for every existing user, to the time when the migration or upgrade occurred. For new users (users created after an upgrade), the Password Set time is configured to the time when the user was created, and the password is set. For users in general (new and existing), the Password Set Time is updated whenever the password is changed.

Configuring Password Expiry Duration

Before you begin

- You must enable password expiry.

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

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

Step 3 In the **Local User Management** pane (opens by default), click **Password Expiration Details**.

Step 4 In the **Password Expiration Details** dialog box, update the following fields:

Name	Description
Enable Password Expiry check box	Checking this box allows you to configure the **Password Expiry Duration**. Uncheck the check box to disable it.
Password Expiry Duration field	The time period that you can set for the existing password to expire (from the time you set a new password or modify an existing one). The range is between 1 to 3650 days. **Note** Password expiry once set by the admin is applicable for all users that are subsequently created.

Name	Description
Password History field	The number of occurrences when a password was entered. When this is enabled, you cannot repeat a password. Enter a value between 0 to 5. Entering 0 disables this field.
Notification Period field	Notifies the time by when the password expires. Enter a value between 0 to 15 days. Entering 0 disables this field. **Note** The notification period time must be lesser than the password expiry duration.
Grace Period field	Time period till when the existing password can still be used, after it expires. Enter a value between 0 to 5 days. Entering 0 disables this field. **Note** The grace period time must be lesser than the password expiry duration.

Note The valid **Password Expiry Duration** must be greater than the **Notification Period** and the **Grace Period**. If otherwise, you will see an **User Password Expiry Policy configuration error**.

Step 5 Click **Save Changes**.

Step 6 Optionally, click **Reset Values** to clear the text fields and reset the values you entered. Click **Restore Defaults** to revert to the default settings.

Enabling Password Expiry

Before you begin

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

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

Step 3 In the **Local User Management** pane (opens by default), click **Password Expiration Details**.

Step 4 In the **Password Expiration Details** dialog box, check the **Enable Password Expiry** check box.

The **Password Expiry Duration** text field becomes editable and you can configure the duration by entering a number in days.

What to do next

Configure password expiry duration.

Configuring Account Lockout Details

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

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

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

Step 4 In the **Local User Management** pane, click **Account Lockout Details**.

Step 5 In the **Account Lockout Details** dialog box, complete the following:

Name	Description
Allowed Attempts (0-20) field	Number of unsuccessful log in attempts allowed for a user before which it is locked out for the duration defined in **Lockout Period**.
Lockout Period (0-60 Minutes) field	The time duration, in minutes, for which the user account is locked out after the allowed attempts.
Disable User on Lockout check box	Disables the user ID up on lockout.

Configuring User Authentication Precedence

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

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

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

Step 4 In the **Local User Management** pane, click **Configure User Authentication Precedence**.

Step 5 In the **Configure User Authentication Precedence** dialog box, select the database for which you wish to update the priority.

Step 6 Use the Up or the Down arrow to change the priority of the database.

Resetting User Credentials to Factory Default Values

Caution You may lose current IP address settings, NIC port settings, NIC redundancy after performing this procedure. Cisco recommends that you make a note of your current server settings before performing this procedure.

Before you begin

Ensure that your management Ethernet cable is plugged into the dedicated management port.

Step 1 Login as an admin user.

Step 2 In the **Navigation** pane, click the **Chassis** menu.

Step 3 In the **Chassis** menu, click **Summary**.

Step 4 From the tool bar, click **Launch KVM**.

Step 5 Alternatively, in the **Navigation** pane, click the **Compute** menu.

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

b. In the work pane, click the **Remote Management** tab.

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

d. In the **Virtual KVM** tab, click **Launch HTML based KVM console**.

Step 6 From the **Power** menu, select **Reset System**.

Step 7 When prompted, press **F8** to enter the Cisco IMC Configuration Utility. This utility opens in the KVM console window.

Step 8 Check the **Factory Default** check box, the server reverts to the factory defaults.

Step 9 Press **F5** to refresh the settings that you made. You might have to wait about 45 seconds until the new settings appear and the message **Network settings configured** is displayed before you reboot the server in the next step.

Step 10 Press **F10** to save your settings and reboot the server.

LDAP Servers

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

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

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 Cisco IMC 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 Cisco IMC. You can use an existing LDAP attribute that is mapped to the Cisco IMC user roles and locales or you can modify the LDAP schema to add a new custom attribute, such as the CiscoAVPair attribute, which has an attribute ID of 1.3.6.1.4.1.9.287247.1.

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

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

If you are using Group Authorization on the Cisco IMC LDAP configuration, then you can skip Steps 1-4 and perform the steps listed in the *Configuring LDAP Settings and Group Authorization in Cisco IMC* section.

The following steps must be performed on the LDAP server.

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

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

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

Step 4 Ensure that the LDAP schema snap-in is installed.

Step 5 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 6 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 7 Add the following user role values to the CiscoAVPair attribute, for the users that you want to have access to Cisco IMC:

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

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

What to do next

Use the Cisco IMC to configure the LDAP server.

Configuring LDAP Settings and Group Authorization in Cisco IMC

Before you begin

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

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

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

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

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

Name	Description
Enable LDAP check box	If checked, user authentication and role authorization is performed first by the LDAP server, followed by user accounts that are not found in the local user database.
Base DN field	Base Distinguished Name. This field describes where to load users and groups from. It must be in the **`dc=domain,dc=com`** format for Active Directory servers.
Domain field	The IPv4 domain that all users must be in. This field is required unless you specify at least one Global Catalog server address.
Enable Secure LDAP check box	If checked, the server enables secure LDAP and prompts you to download LDAP CA certificate. Refer Downloading an LDAP CA Certificate, on page 132 to download LDAP CA certificate. To delete an existing secure LDAP certificate, un-check this option. Follow the system prompts to confirm deletion.

Name	Description
Timeout (0 - 180) seconds	The number of seconds the Cisco IMC waits until the LDAP search operation times out. If the search operation times out, Cisco IMC tries to connect to the next server listed on this tab, if one is available. **Note** The value you specify for this field could impact the overall time.

Note If you check the **Enable Secure LDAP**check box, enter the fully qualified domain name (FQDN) of the LDAP server in the **LDAP Server** field. To resolve the FQDN of the LDAP server, configure the preferred DNS of Cisco IMC network with the appropriate DNS IP address.

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

Name	Description
Pre-Configure LDAP Servers radio button	If checked, the Active Directory uses the pre-configured LDAP servers.
LDAP Servers fields	
Server	The IP address of the 6 LDAP servers. If you are using Active Directory for LDAP, then servers 1, 2 and 3 are domain controllers, while servers 4, 5 and 6 are Global Catalogs. If you are not Active Directory for LDAP, then you can configure a maximum of 6 LDAP servers. **Note** You can provide the IP address of the host name as well.
Port	The port numbers for the servers. If you are using Active Directory for LDAP, then for servers 1, 2 and 3, which are domain controllers, the default port number is 389. For servers 4, 5 and 6, which are Global Catalogs, the default port number is 3268. LDAPS communication occurs over the TCP 636 port. LDAPS communication to a global catalog server occurs over TCP 3269 port.
Use DNS to Configure LDAP Servers radio button	If checked, you can use DNS to configure access to the LDAP servers.
DNS Parameters fields	

Name	Description
Source drop-down list	Specifies how to obtain the domain name used for the DNS SRV request. It can be one of the following: • **Extracted**—specifies using domain name extracted-domain from the login ID • **Configured**—specifies using the configured-search domain. • **Configured-Extracted**—specifies using the domain name extracted from the login ID than the configured-search domain.
Domain to Search	A configured domain name that acts as a source for a DNS query. This field is disabled if the source is specified as **Extracted**.
Forest to Search	A configured forest name that acts as a source for a DNS query. This field is disabled if the source is specified as **Extracted**.

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

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

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

Name	Description
Filter Attribute	This field must match the configured attribute in the schema on the LDAP server. By default, this field displays **sAMAccountName**.
Group Attribute	This field must match the configured attribute in the schema on the LDAP server. By default, this field displays **memberOf**.
Attribute	An LDAP attribute that contains the role and locale information for the user. This property is always a name-value pair. The system queries the user record for the value that matches this attribute name. The LDAP attribute can use an existing LDAP attribute that is mapped to the Cisco IMC user roles and locales, or can modify the schema such that a new LDAP attribute can be created. For example, **CiscoAvPair**.
Nested Group Search Depth (1-128)	Parameter to search for an LDAP group nested within another defined group in an LDAP group map. The parameter defines the depth of a nested group search.

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

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

Name	Description

Role column	The role assigned to all users in this LDAP server group. This can be one of the following:
	• **read-only**—A user with this role can view information but cannot make any changes.
	• **user**—A user with this role can perform the following tasks:
	  • View all information
	  • Manage the power control options such as power on, power cycle, and power off
	  • Launch the KVM console and virtual media
	  • Clear all logs
	  • Ping
	• **admin**—A user with this role can perform all actions available through the GUI, CLI, and IPMI.

Configure button	Opens the **Configure LDAP Group** window for an active directory group with the same **Group Name**, **Group Domain**, and **Role** options listed above. Once configured, click **Save Changes**.
Delete button	Deletes an existing LDAP group.

Step 9 Click **Save Changes**.

LDAP Certificates Overview

Cisco S3260 C-series servers allow an LDAP client to validate a directory server certificate against an installed CA certificate or chained CA certificate during an LDAP binding step. This feature is introduced in the event where anyone can duplicate a directory server for user authentication and cause a security breach due to the inability to enter a trusted point or chained certificate into the Cisco IMC for remote user authentication.

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

Viewing LDAP CA Certificate Status

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

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

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

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

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

Exporting an LDAP CA Certificate

Before you begin

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

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

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

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

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

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

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

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

Step 5 Click **Export Certificate**.

Downloading an LDAP CA Certificate

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

Steps

1. In the **Navigation** pane, click the **Admin** tab.
2. In the **Admin** menu, click **User Management**.
3. In the **User Management** pane, click the **LDAP** tab.
4. Click the **Download LDAP CA Certificate** link.

   The **Download LDAP CA Certificate** dialog box appears.
5. Fill the required information in the **Download LDAP CA Certificate** dialog box.

Name	Description
Upload **from remote location** radio button	Selecting this option allows you to choose the certificate from a remote location and Upload it. Enter the following details: • **TFTP Server** • **FTP Server** • **SFTP Server** • **SCP Server** • **HTTP Server** **Note** If you chose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message *Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*. Click Yes or No depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to. • **Server IP/Hostname** field — The IP address or hostname of the server on which the LDAP CA certificate file should be stored. Depending on the setting in the Upload **Certificate from** drop-down list, the name of the field may vary. • **Path and Filename** field — The path and filename Cisco IMC should use when uploading the file to the remote server. • **Username** field — The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP. • **Password** field — The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP.
Upload **through browser client** radio button	Selecting this option allows you to navigate to the certificate stored on a drive that is local to the computer running the Cisco IMC GUI. When you select this option, Cisco IMC GUI displays a **Browse** button that lets you navigate to the file you want to import.
Paste Certificate content radio button	Selecting this option allows you to copy the entire content of the signed certificate and paste it in the **Paste certificate content** text field. **Note** Ensure the certificate is signed before uploading.
Upload **Certificate** button	Allows you to Upload the certificate to the server.

Testing LDAP Binding

Before you begin

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

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

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

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

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

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

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

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

Step 5 Click **Test**.

TACACS+ Authentication

Beginning with 4.1(3b) release, Cisco IMC supports Terminal Access Controller Access-Control System Plus (TACACS+) user authentication. Cisco IMC supports up to six TACACS+ remote servers. Once a user is successfully authenticated, the username is appended with **(TACACS+)**. This is also displayed in the Cisco IMC interfaces.

Refer Enabling TACACS+ Authentication, on page 135 to enable TACACS+ Authentication. Cisco IMC also supports user authentication precedence in case TACACS+ remote servers are inaccessible. User authentication precedence can be configured using Configuring User Authentication Precedence, on page 122.

TACACS+ Server Configuration

Privilege level of a user is calculated based on the **cisco-av-pair** value configured for that user. A **cisco-av-pair** should be created on the TACACS+ server. Users cannot use any existing TACACS+ attributes.

Following three syntax are supported for the **cisco-av-pair** attribute:

- For `admin` privilege: **cisco-av-pair=shell:roles="admin"**
- For `user` privilege: **cisco-av-pair=shell:roles="user"**

- For `read-only` privilege: **cisco-av-pair=shell:roles="read-only"**

More roles, if required, can be added by using **comma** as a separator.

Note If **cisco-av-pair** is not configured on the TACACS+ server, then a user with that server has **read-only** privilege.

Enabling TACACS+ Authentication

Before you begin

Before configuring Terminal Access Controller Access-Control System (TACACS+) based user authentication, ensure that privilege level of a user is configured on TACACS+ server based on the **cisco-av-pair** value.

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

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

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

Step 4 Under the **TACACS+ Properties** area perform the following:

Name	Description
Enabled check box	Check this box to enable TACACS+ based user authentication.
Fallback only on no connectivity check box	If checked, the authentication falls back to the next precedence database only in-case Cisco IMC is not able to connect to any of the configured TACACS+ servers. Ensure to configure user authentication precedence. Refer Configuring User Authentication Precedence, on page 122.
Timeout (for each server): (5 - 30) seconds field	Time duration, in seconds, for which Cisco IMC waits for a response from each of the TACACS+ servers

Configuring TACACS+ Remote Server Settings

You can configure up to six TACACS+ remote servers.

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

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

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

Step 4 Under the **Server List** area, click the radio button for the server ID which you wish to configure and click the **Edit** button.

Step 5 Update the following fields:

Name	Description
ID	This is unique identifier of the server and is not user editable.
IP Address or Host Name	The IP address at which the TACACS+ server is running.
Port	The port on which TACACS+ server is running.
Server key	The same key that is configured on the TACACS+ server. Repeat the same key for **Confirm Server Key**.

Viewing User Sessions

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

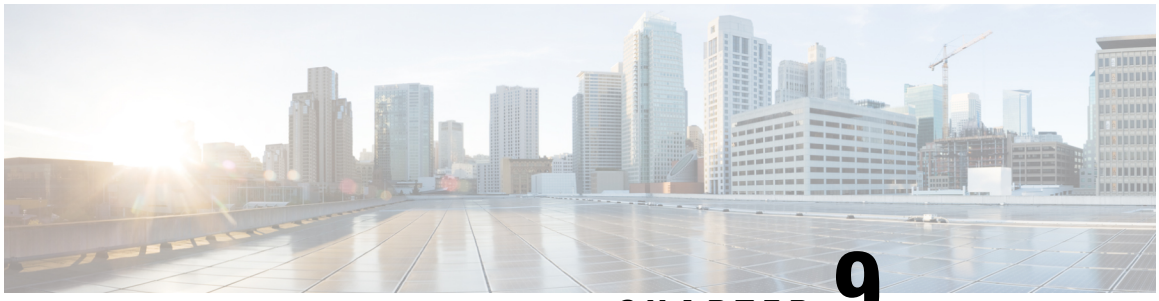
Step 2 In the **Admin** menu, click **User Management**.

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

Step 4 In the **Sessions** pane, view the following information about current user sessions:

Name	Description
Terminate Session button	If your user account is assigned the **admin** user role, this option enables you to force the associated user session to end. **Note** You cannot terminate your current session from this tab.
Session ID column	The unique identifier for the session.
BMC Session ID	The identifier for the BMC session.
User Name column	The username for the user.
IP Address column	The IP address from which the user accessed the server. If this is a serial connection, it displays **N/A**.

Name	Description
Session Type column	The type of session the user chose to access the server. This can be one of the following: • **webgui**— indicates the user is connected to the server using the web UI. • **CLI**— indicates the user is connected to the server using CLI. • **serial**— indicates the user is connected to the server using the serial port. • — indicates the user is connected to the server using XML API. • — indicates the user is connected to the server using Redfish API.



CHAPTER 9

Configuring Chassis Related Settings

This chapter includes the following sections:

Managing Server Power

Before you begin

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

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

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

Step 3 In the toolbar above the work pane, click the **Host Power** link.

Step 4 In the **Server Power Management** dialog box, review the following information and select the relevant radio buttons (highlighted radio buttons indicate the current power state of the server or servers) to manage power for server 1 or server 2.

Actions	Description
Power On	Powers on the chosen server.
Power Off	Powers off the chosen server, even if tasks are running on that server. **Important** If any firmware or BIOS updates are in progress, do not power off or reset the server until those tasks are complete.
Power Cycle	Powers off and powers on chosen server.
Hard Reset	Reboots the chosen server.

Actions	Description
Shut Down	Shuts down the chosen server if the operating system supports that feature.

Pinging a Hostname/IP Address from the Web UI

Before you begin

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

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

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

Actions	Description
***Hostname/IP Address** field	Hostname or IP address you want to reach out to.
***Number of Retries** field	The maximum number of retries allowed to ping the IP address. The default value is 3. The valid range is from 1 to 10.
***Timeout** field	The maximum response time for a pinging activity. The default value is 10 seconds. The valid range is from 1 to 20 seconds.
***Component** drop-down list	The controller that you can ping. This can be one of the following: • **CMC 1** • **CMC 2** • **BMC 1** • **BMC 2**
Ping Status field	Displays results of the pinging activity.
Details button	Displays details of the pinging activity.
Ping button	Pings the IP address.
Cancel button	Closes the dialog box without pinging.

Step 3 Click **Ping**.

Toggling the Locator LEDs

Before you begin

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

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

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

Step 3 In the toolbar above the work pane, click the **Locator LED** link.

Step 4 In the **Locator LED** dialog box, update the following information:

Action	Description
Turn On Server 1 Locator LED button	Turns on the locator LED of the server 1 module.
Turn On Server 2 Locator LED button	Turns on the locator LED of the server 2 module.
Turn On Front Locator LED button	Turns on the locator LED on the front panel of the chassis.

Depending on your actions, the LED indicator in the **Chassis Status** area lights up and the physical locator LED on the server turns on or off and blinks.

Selecting a Time Zone

Before you begin

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

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

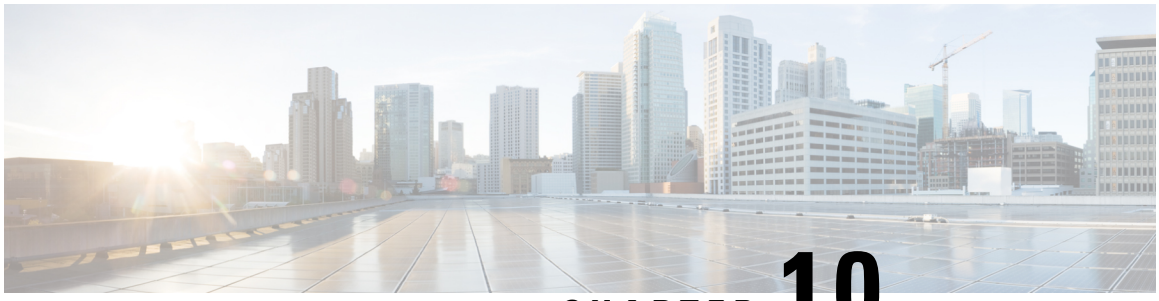
Step 2 In the **Chassis** menu, click **Summary**.

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

Select Timezone screen appears.

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

Step 5 Click **OK**.



CHAPTER 10

Configuring Network-Related Settings

This chapter includes the following sections:

Server NIC Configuration

Server NICs

NIC Mode

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

- **Dedicated**—The management port that is used to access the Cisco IMC.
- **Cisco Card**—Any port on the adapter card that can be used to access the Cisco IMC. The Cisco adapter card has to be installed in a slot with Network the Communications Services Interface protocol support (NCSI).
- **Shared LOM**—Any LOM (LAN on Motherboard) port that can be used to access Cisco IMC.
- **Shared LOM Extended**—Any LOM port or adapter card port that can be used to access Cisco IMC. The Cisco adapter card has to be installed in a slot with NCSI support.

Note **Shared LOM** and **Shared LOM Extended** ports are available only on some C-series servers.

Note For other UCS C-Series M4 and M5 servers, the NIC mode is set to **Shared LOM Extended** by default.

Default NIC Mode Setting:

- For UCS C-Series C125 M5 servers and S3260 servers, the **NIC Mode** is set to **Cisco Card** by default.

NIC Redundancy

The following NIC redundancy options are available, depending on the selected NIC mode and your platform:

- **active-active**—If supported, all ports that are associated with the configured NIC mode operate simultaneously. This feature increases throughput and provides multiple paths to the Cisco IMC.
- **active-standby**—If a port that is associated with the configured NIC mode fails, traffic fails over to one of the other ports associated with the NIC mode.

Note If you choose this option, make sure that all ports associated with the configured NIC mode are connected to the same subnet to ensure that traffic is secure regardless of which port is used.

- **None**—In *Dedicated* mode, NIC redundancy is set to *None*.

The available redundancy modes vary depending on the selected network mode and your platform. For the available modes, see the *Hardware Installation Guide* (HIG) for the type of server you are using. The C-Series HIGs are available at the following URL:
http://www.cisco.com/en/US/products/ps10493/prod_installation_guides_list.html

VIC Slots

The VIC slot that can be used for management functions in Cisco card mode.

The following options are available only on some UCS C-Series servers:

- **4**
- **5**
- **9**
- **10**

Note This option is available only on some UCS C-Series servers.

Configuring Server NICs

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

Before you begin

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

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

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

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

Name	Description
NIC Mode drop-down list	The ports that can be used to access Cisco IMC. This can be one of the following: • **Dedicated**—The management port that is used to access the Cisco IMC. • **Cisco Card**—Any port on the adapter card that can be used to access Cisco IMC. The Cisco adapter card has to be installed in a slot with Network the Communications Services Interface protocol support (NCSI). **Default NIC Mode Setting**: • For UCS C-Series C125 M5 servers and S3260 servers, the **NIC Mode** is set to **Cisco Card** by default.
SIOC Slot drop-down list	Configures Cisco IMC network mode. Based on the card present in the System IO Controller (SIOC1), network mode can be changed to either 1 or 2. **Note** This option is available only on some UCS S-Series servers.

Name	Description
NIC Redundancy drop-down list	The available NIC redundancy options depend on the selected NIC mode and the model of the server that you are using. If you do not see a particular option, it is not available for the selected mode or server model. This can be one of the following: • **active-active**—If supported, all ports that are associated with the configured NIC mode operate simultaneously. This feature increases throughput and provides multiple paths to Cisco IMC. • **active-standby**—If a port that is associated with the configured NIC mode fails, traffic fails over to one of the other ports associated with the NIC mode. **Note** • If you choose this option, make sure that all ports associated with the configured NIC mode are connected to the same VLAN to ensure that traffic is secure regardless of which port is used. • When using **active-active**, do not configure a port-channel in the upstream switch for the member interfaces. A port-channel can be configured when using **active-standby**. • **None**—In *Dedicated* mode, NIC redundancy is set to *None*.
MAC Address field	The MAC address of the Cisco IMC network interface that is selected in the **NIC Mode** field.

Step 4 Click **Save Changes**.

Single IP Configuration

Single IP is an optional method to assign IPv4 for Cisco IMC management.

Note When **Single IP Mode** is enabled following IPv4 addressess will not be available for configuration:

CMC and BMC.

Since **Single IP Mode** is applicable only for IPv4, IPv6 can be configured irrespective of **Single IP Mode**. IPv6 address can assign for individual components like CMC1, CMC2, BMC1 and BMC2.

Note Disable single IP configuration before downgrade to 4.0.1x or below.

Configuring Single IP Properties

Configure Single IP when you want to assign IP for Cisco IMC management.

Before you begin

You must log in as a user with admin privileges to configure the Single IP Properties.

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

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

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

Name	Description
Single IP Mode	Single IP is an optional method to assign IPv4 for Cisco IMC management. **Note** When **Single IP Mode** is enabled following IPv4 addresses will not be available for configuration: CMC and BMC. Since **Single IP Mode** is applicable only for IPv4, IPv6 can be configured irrespective of **Single IP Mode**. IPv6 address can assign for individual components like CMC1, CMC2, BMC1 and BMC2. Default mode: **Disabled**
Starting Port	When **Single IP Mode** is enabled, the port range available is 9000-65529. **Note** Click on the help icon next to the **Starting Port** to get the table listing of the component with the port numbers used by Cisco IMC to access KVM, SOL, and IPMI Over LAN of each component.

Note In **Single IP Mode**, vkvm port is not configurable and will be changed from default **2068** to the user-assigned port.

Step 4 Click **Save Changes**.

Common Properties Configuration

Overview to Common Properties Configuration

Hostname

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

The default hostname of the server is changed from ucs-c2XX to CXXX-YYYYYY, where XXX is the model number and YYYYYY is the serial number of the server. This unique string acts as a client identifier, allows you to track and map the IP addresses that are leased out to Cisco IMC from the DHCP server. The default serial number is provided by the manufacturer as a sticker or label on the server to help you identify the server.

Dynamic DNS

Dynamic DNS (DDNS) is used to add or update the resource records on the DNS server from Cisco IMC. You can enable Dynamic DNS by using either the web UI or CLI. When you enable the DDNS option, the DDNS service records the current hostname, domain name, and the management IP address and updates the resource records in the DNS server from Cisco IMC.

Note The DDNS server deletes the prior resource records (if any) and adds the new resource records to the DNS server if any one of the following DNS configuration is changed:

- Hostname
- Domain name in the LDAP settings
- When DDNS and DHCP are enabled, if the DHCP gets a new IP address or DNS IP or domain name due to a change in a network or a subnet.
- When DHCP is disabled and if you set the static IP address by using CLI or web UI.
- When you enter the **dns-use-dhcp** command.

Dynamic DNS Update Domain— You can specify the domain. The domain could be either main domain or any sub-domain. This domain name is appended to the hostname of the Cisco IMC for the DDNS update.

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.

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

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

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

Name	Description
Management Hostname field	The user-defined management hostname of the system that manages the various components of Cisco IMC.
Dynamic DNS check box	If checked, updates the resource records to the DNS from Cisco IMC.
Dynamic DNS Update Domain field	The domain name that is appended to a hostname for a Dynamic DNS (DDNS) update. If left blank, only a hostname is sent to the DDNS update request.
Dynamic DNS Refresh Interval field	The time set to refresh the DNS. Set a value between 0 and 8736 hours. If set to 0, it is disabled.

Step 4 Click **Save Changes**.

Configuring IPv4

Before you begin

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

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

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

Step 3 In the **IPv4 Properties** area, update the following properties:

Name	Description
Enable IPv4 check box	If checked, IPv4 is enabled.
Use DHCP check box	If checked, Cisco IMC uses DHCP.
Management IP Address field	The management IP address. An external virtual IP address that helps manage the CMCs and BMCs.
Subnet Mask field	The subnet mask for the IP address.
Gateway field	The gateway for the IP address.

Name	Description
Obtain DNS Server Addresses from DHCP check box	If checked, Cisco IMC retrieves the DNS server addresses from DHCP.
Preferred DNS Server field	The IP address of the primary DNS server.
Alternate DNS Server field	The IP address of the secondary DNS server.

Step 4 Click **Save Changes**.

Configuring IPv6

Before you begin

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

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

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

Step 3 In the **IPv6 Properties** area, update the following properties:

Name	Description
Enable IPv6 check box	If checked, IPv6 is enabled.
Use DHCP check box	If checked, the Cisco IMC uses DHCP. **Note** Only stateful DHCP is supported.
Management IP Address field	Management IPv6 address. **Note** Only global unicast addresses are supported.
Prefix Length field	The prefix length for the IPv6 address. Enter a value within the range 1 to 127. The default value is 64.
Gateway field	The gateway for the IPv6 address. **Note** Only global unicast addresses are supported.
Obtain DNS Server Addresses from DHCP check box	If checked, the Cisco IMC retrieves the DNS server addresses from DHCP. **Note** You can use this option only when the **Use DHCP** option is enabled.
Preferred DNS Server field	The IPv6 address of the primary DNS server.
Alternate DNS Server field	The IPv6 address of the secondary DNS server.

Name	Description
Link Local Address field	The link local address for the IPv6 address.
SLAAC Address field	The Stateless Address Auto Configuration (SLAAC) depends on the Router Advertisement (RA) of the network.

Step 4 Click **Save Changes**.

Connecting to a VLAN

Before you begin

You must be logged in as admin to connect to a VLAN.

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

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

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

Name	Description
Enable VLAN check box	If checked, the Cisco IMC is connected to a virtual LAN. **Note** You can configure a VLAN or a port profile, but you cannot use both. If you want to use a port profile, make sure that this check box is not checked.
VLAN ID field	The VLAN ID.
Priority field	The priority of this system on the VLAN.

Step 4 Click **Save Changes**.

Connecting to a Port Profile

Before you begin

You must be logged in as admin to connect to a port profile.

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

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

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

Name	Description
Port Profile field	Details of the **Port Profile** field.
Auto Negotiation check box	Using this option, you can either set the network port speed and duplex values for the switch, or allow the system to automatically derive the values from the switch. This option is available for dedicated mode only. • If checked, the network port speed and duplex settings are ignored by the system and Cisco IMC retains the speed at which the switch is configured. • If unchecked, you can configure the network port speed and duplex values.
Admin Mode Area	**Network Port Speed** field The network speed of the port. This can be one of the following: • 10 Mbps • 100 Mbps • 1 Gbps The default value is 100 Mbps. In the **Dedicated** mode, if you disable **Auto Negotiation**, you can configure the network speed and duplex values. **Note** • Before changing the port speed, ensure that the switch you connected to has the same port speed. **Duplex** drop-down list The duplex mode for the Cisco IMC management port. This can be one of the following: • **Half** • **Full** By default, the duplex mode is set to **Full**.
Operation Mode Area	Displays the operation network port speed and duplex values. If you checked the **Auto Negotiation** check box, the network port speed and duplex details of the switch are displayed. If unchecked, the network port speed and duplex values that you set at the **Admin Mode** are displayed.

Step 4 Click **Save Changes**.

Configuring Individual Settings

This functionality is applicable only for Cisco UCS S-Series servers.

Before you begin

You must be logged in as admin to configure the settings.

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

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

Step 3 In the Individual Settings area, review and update the following fields for **CMC 1**, **CMC 2**, **BMC 1** and **BMC 2** in their respective areas:

Name	Description
Hostname field	The user-defined hostname. By default, the hostname appears in CXXX-YYYYYY format, where XXX is the model number and YYYYYY is the serial number of the server.
MAC Address field	The MAC address of the component.
IPv4 Address field	The IPv4 address of the component.
IPv6 Address field	The IPv6 address of the component.
Link Local Address field	The link local address for the component's IPv6 address.

Step 4 Click **Save Changes**.

Network Security Configuration

Network Security

The Cisco IMC 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. Cisco IMC 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.

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

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

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

Name	Description
Enable IP Blocking check box	Check this box to enable IP blocking.
IP Blocking Fail Count field	The number of times a user can attempt to log in unsuccessfully before the system locks that user out for a specified length of time. The number of unsuccessful login attempts must occur within the time frame specified in the **IP Blocking Fail Window** field. Enter an integer between 3 and 10.
IP Blocking Fail Window field	The length of time, in seconds, in which the unsuccessful login attempts must occur in order for the user to be locked out. Enter an integer between 60 and 280.
IP Blocking Penalty Time field	The number of seconds the user remains locked out if they exceed the maximum number of login attempts within the specified time window. Enter an integer between 300 and 900.

Step 4 In the **IP Filtering (Allow listing)** area, update the following properties:

Name	Description
Enable IP Filtering check box	Check this box to enable IP filtering.
IP Filter fields	To provide secure access to the server, you can now set a filter to allow only a selected set of IPs to access it. This option provides four slots for storing IP addresses (IP Filter 1, 2, 3, and 4). You can either assign a single IP address or a range of IP addresses while setting the IP filters. Once you set the IP filter, you would be unable to access the server using any other IP address.

Step 5 Click **Save Changes**.

Network Time Protocol Settings

Network Time Protocol Service Setting

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

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

Configuring Network Time Protocol Settings

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

Before you begin

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

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

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

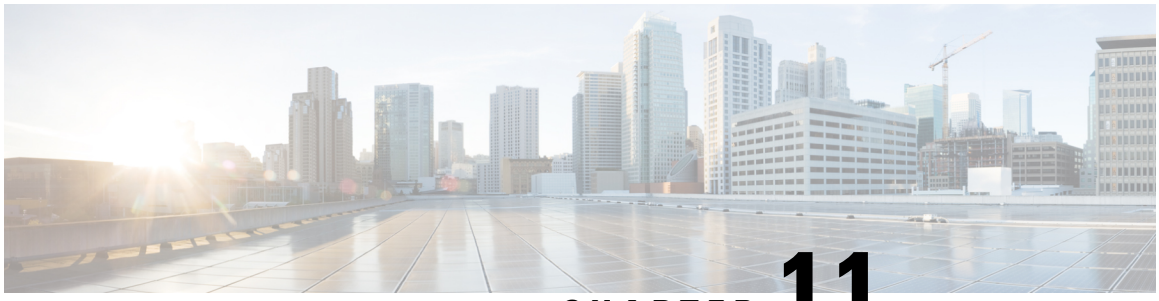
Step 3 In the **Networking** pane, click **NTP Setting**.

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

Name	Description
NTP Enabled check box	Check this box to enable the NTP service.
Server 1 field	The IP/DNS address of one of the four servers that act as an NTP server or the time source server.
Server 2 field	The IP/DNS address of one of the four servers that act as an NTP server or the time source server.
Server 3 field	The IP/DNS address of one of the four servers that act as an NTP server or the time source server.
Server 4 field	The IP/DNS address of one of the four servers that act as an NTP server or the time source server.

Name	Description
Status message	Indicates whether or not the server is able to synchronize its time with the remote NTP server. It is an eight bit integer indicating the stratum level of the local clock. This can be one of the following: • 0—Unspecified or invalid • 1—Primary server • 2-15—Secondary server (via NTP) • 16—Unsynchronized • 17-255—Reserved

Step 5 Click **Save Changes**.



CHAPTER 11

Managing Network Adapters

This chapter includes the following sections:

Overview of the Cisco UCS C-Series Network Adapters

Note The procedures in this chapter are available only when a Cisco UCS C-Series network adapter is installed in the chassis.

A Cisco UCS C-Series network adapter can be installed to provide options for I/O consolidation and virtualization support. The following adapters are available:

- Cisco UCS VIC 15238 Virtual Interface Card
- Cisco UCS VIC 15428 Virtual Interface Card
- Cisco UCS VIC 1497 Virtual Interface Card
- Cisco UCS VIC 1495 Virtual Interface Card
- Cisco UCS VIC 1457 Virtual Interface Card
- Cisco UCS VIC 1455 Virtual Interface Card
- Cisco UCS VIC 1387 Virtual Interface Card
- Cisco UCS VIC 1385 Virtual Interface Card
- Cisco UCS VIC 1227T Virtual Interface Card
- Cisco UCS VIC 1225 Virtual Interface Card

Note You must have same generation VIC cards on a server. For example, you cannot have a combination of 3rd generation and 4th generation VIC cards on a single server.

The interactive *UCS Hardware and Software Interoperability Utility* lets you view the supported components and configurations for a selected server model and software release. The utility is available at the following URL: http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html

Cisco UCS VIC 1497 Virtual Interface Card

The Cisco VIC 1497 is a dual-port Small Form-Factor (QSFP28) mLOM card designed for the M5 generation of Cisco UCS C-Series Rack Servers. The card supports 40/100-Gbps Ethernet and FCoE. The card can present PCIe standards-compliant interfaces to the host, and these can be dynamically configured as NICs and HBAs.

Cisco UCS VIC 1495 Virtual Interface Card

The Cisco UCS VIC 1495 is a dual-port Small Form-Factor (QSFP28) PCIe card designed for the M5 generation of Cisco UCS C-Series Rack Servers. The card supports 40/100-Gbps Ethernet and FCoE. The card can present PCIe standards-compliant interfaces to the host, and these can be dynamically configured as NICs and HBAs.

Cisco UCS VIC 1457 Virtual Interface Card

The Cisco UCS VIC 1457 is a quad-port Small Form-Factor Pluggable (SFP28) mLOM card designed for M5 generation of Cisco UCS C-Series rack servers. The card supports 10/25-Gbps Ethernet or FCoE. It incorporates Cisco's next-generation CNA technology and offers a comprehensive feature set, providing investment protection for future feature software releases. The card can present PCIe standards-compliant interfaces to the host, and these can be dynamically configured as NICs and HBAs.

Cisco UCS VIC 1455 Virtual Interface Card

The Cisco UCS VIC 1455 is a quad-port Small Form-Factor Pluggable (SFP28) half-height PCIe card designed for M5 generation of Cisco UCS C-Series rack servers. The card supports 10/25-Gbps Ethernet or FCoE. It incorporates Cisco's next-generation CNA technology and offers a comprehensive feature set, providing investment protection for future feature software releases. The card can present PCIe standards-compliant interfaces to the host, and these can be dynamically configured as NICs and HBAs.

Cisco UCS VIC 1387 Virtual Interface Card

The Cisco UCS VIC 1387 Virtual Interface Card is a dual-port Enhanced Quad Small Form-Factor Pluggable (QSFP) 40 Gigabit Ethernet and Fibre Channel over Ethernet (FCoE)-capable half-height PCI Express (PCIe) card designed exclusively for Cisco UCS C-Series Rack Servers. It incorporates Cisco's next-generation converged network adapter (CNA) technology, with a comprehensive feature set, providing investment protection for future feature software releases.

Cisco UCS VIC 1385 Virtual Interface Card

The Cisco UCS VIC 1385 Virtual Interface Cardis a dual-port Enhanced Quad Small Form-Factor Pluggable (QSFP) 40 Gigabit Ethernet and Fibre Channel over Ethernet (FCoE)-capable half-height PCI Express (PCIe) card designed exclusively for Cisco UCS C-Series Rack Servers. It incorporates Cisco's next-generation converged network adapter (CNA) technology, with a comprehensive feature set, providing investment protection for future feature software releases.

Cisco UCS VIC 1227T Virtual Interface Card

The Cisco UCS VIC 1227T Virtual Interface Card is a dual-port 10GBASE-T (RJ-45) 10-Gbps Ethernet and Fibre Channel over Ethernet (FCoE)–capable PCI Express (PCIe) modular LAN-on-motherboard (mLOM) adapter designed exclusively for Cisco UCS C-Series Rack Servers. New to Cisco rack servers, the mLOM slot can be used to install a Cisco VIC without consuming a PCIe slot, which provides greater I/O expandability. It incorporates next-generation converged network adapter (CNA) technology from Cisco, providing Fibre Channel connectivity over low-cost twisted pair cabling with a bit error rate (BER) of 10 to 15 up to 30 meters and investment protection for future feature releases.

Cisco UCS VIC 1225 Virtual Interface Card

The Cisco UCS VIC 1225 Virtual Interface Card is a high-performance, converged network adapter that provides acceleration for the various new operational modes introduced by server virtualization. It brings superior flexibility, performance, and bandwidth to the new generation of Cisco UCS C-Series Rack-Mount Servers.

Configuring Network Adapter Properties

Before you begin

- You must log in as a user with admin privileges to perform this task.
- The server must be powered on, or the properties will not display.

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

Step 2 In the **Networking** menu, click **Adapter Card SIOC1** or **Adapter Card SIOC2**.

Step 3 In the **Adapter Card Properties** area under the **General** tab, review the following information:

Name	Description
PCI Slot field	The PCI slot in which the adapter is installed.
Vendor field	The vendor for the adapter.
Product Name field	The product name for the adapter.
Product ID field	The product ID for the adapter.
Serial Number field	The serial number for the adapter.
Version ID field	The version ID for the adapter.
PCI Link field	The server to which the PCIe link is established.
Hardware Revision field	The hardware revision for the adapter.
Cisco IMC Management Enabled field	If this field displays **yes**, then the adapter is functioning in Cisco Card Mode and passing Cisco IMC management traffic through to the server Cisco IMC.

Name	Description
Configuration Pending field	If this field displays **yes**, the adapter configuration has changed in Cisco IMC but these changes have not been communicated to the host operating system. To activate the changes, an administrator must reboot the adapter.
ISCSI Boot Capable field	Whether iSCSI boot is supported on the adapter.
CDN Capable field	Whether CDN is supported on the adapter.
usNIC Capable field	Whether the adapter and the firmware running on the adapter support the usNIC.
Port Channel Capable field	Indicates whether Port Channel is supported on the adapter. **Note** This option is available only on some of the adapters and servers.
Description field	A user-defined description for the adapter. You can enter between 1 and 63 characters.
Enable FIP Mode check box	If checked, then FCoE Initialization Protocol (FIP) mode is enabled. FIP mode ensures that the adapter is compatible with current FCoE standards. **Note** We recommend that you use this option only when explicitly directed to do so by a technical support representative.
Enable LLDP check box	**Note** For LLDP change to be effective, it is required that you reboot the server. In case of S3260 chassis with two nodes, ensure to reboot the secondary node after making LLDP changes in the primary node. If checked, then Link Layer Discovery Protocol (LLDP) enables all the Data Center Bridging Capability Exchange protocol (DCBX) functionality, which includes FCoE, priority based flow control. By default, LLDP option is enabled. **Note** We recommend that you do not disable LLDP option, as it disables all the DCBX functionality.

Name	Description
Enable VNTAG Mode check box	If VNTAG mode is enabled: • vNICs and vHBAs can be assigned to a specific channel. • vNICs and vHBAs can be associated to a port profile. • vNICs can fail over to another vNIC if there are communication problems.
Port Channel check box	This option is enabled by default. When Port channel is enabled, two vNICs and two vHBAs are available for use on the adapter card. When disabled, four vNICs and four vHBAs are available for use on the adapter card. **Note** This option is available only on some of the adapters and servers.

Name	Description
Physical NIC Mode check box	This option is disabled by default. When Physical NIC Mode is enabled, up-link ports of the VIC are set to pass-through mode. This allows the host to transmit packets without any modification. VIC ASIC does not rewrite the VLAN tag of the packets based on the VLAN and CoS settings for the vNIC. **Note** • This option is available for Cisco UCS VIC 14xx series and 15xxx series adapters. • For the VIC configuration changes to be effective, you must reboot the host. • This option cannot be enabled on an adapter that has: • **Port Channel mode** enabled • **VNTAG mode** enabled • **LLDP** enabled • **FIP mode** enabled • **Cisco IMC Management Enabled** value set to **Yes** • Multiple user created vNICs When Physical NIC Mode is enabled, the following message is displayed in a pop-up window: **After physical nic-mode mode switch, vNIC configurations will be lost and new default vNICs will be created.** Click **OK**.

Step 4 In the **Firmware** area, review the following information:

Name	Description
Running Version field	The firmware version that is currently active.

Name	Description
Backup Version field	The alternate firmware version installed on the adapter, if any. The backup version is not currently running. To activate it, administrators can click **Activate Firmware** in the **Actions** area. **Note** When you install new firmware on the adapter, any existing backup version is deleted and the new firmware becomes the backup version. You must manually activate the new firmware if you want the adapter to run the new version.
Startup Version field	The firmware version that will become active the next time the adapter is rebooted.
Bootloader Version field	The bootloader version associated with the adapter card.
Status field	The status of the last firmware activation that was performed on this adapter. **Note** The status is reset each time the adapter is rebooted.

Step 5 Click the **External Ethernet Interfaces** link to review the following information:

Note **External Ethernet Interfaces** opens in a different tab.

Name	Description
Port column	The uplink port ID.
Admin Speed column	The data transfer rate for the port. This can be one of the following: • **Auto** • **40 Gbps** • **4 x 10 Gbps** **Note** You can edit the **Admin Speed** column if Cisco UCS S3260 server SIOC is equipped with Cisco UCS VIC 1385. Select the port for which you want to edit the Admin Speed and click on the icon above the Port column. Click on save to save your changes. You need to choose 40 Gbps as the port speed if you are using a 40 Gbps switch.
Admin Link Training column	Indicates if admin link training is enabled on the port. Select any of the below options for Admin Link Training: • Auto • Off • On Admin Link Training is set to **Auto**, by default. **Note** This option is available only on some of the adapters and servers.

Name	Description
Admin FEC Mode drop-down list	Admin Forward Error Correction (FEC) apply only to Cisco UCS VIC 14xx adapters at speed 25/100G and Cisco UCS VIC 15xxx adapters at speeds 25G/50G. Following Admin Forward Error Correction (FEC) mode options are available for configuration: • cl108 (RS-IEEE, clause 108) • cl91-cons16 (RS-FEC, clause 91, consortium version 1.6) • cl91 (RS-FEC, clause 91, consortium version 1.5) • cl74 (FC-FEC, clause 74), 25G only • Off Admin FEC Mode is set to **cl91**, by default. **Note** • This option is available only on some of the adapters and servers. • Any changes in the **Admin FEC Mode** settings leads to the reset of the port, even when the value for **Operating FEC mode** remains the same.
Operating FEC Mode column	The value of **Operating FEC Mode** is the same as **Admin FEC mode** with these exceptions: • The value is Off when the speed is 10 Gbps or 40 Gbps. This is because FEC is not supported. • The value is Off for QSFP-100G-LR4-S transceiver. • The value is Off for QSFP-40/100-SRBD transceiver. **Note** This option is available only on some of the adapters and servers.

Name	Description
Oper Link Training column	**Oper Link Training** values are fetched from the values set in the **Admin Link Training** drop-down list. Beginning from 4.2(2a), the below different settings apply only to Cisco UCS VIC 15xxx adapters and Copper cables at speeds 10G/25G/50G only. • If Admin Link Training is set to Auto, Adapter firmware sets Oper Link Training value (AutoNeg) as on or off, depending upon the transceivers. • AutoNeg disabled with 25G copper • AutoNeg enabled with 50G copper • If Admin Link Training is set to on, Adapter firmware sets Oper Link Training value as on. • AutoNeg enabled with 25G copper • AutoNeg enabled with 50G copper • If Admin Link Training is **off**, Adapter firmware sets **Oper Link Training** as **off**. • AutoNeg disabled with 25G copper • AutoNeg disabled with 50G copper **Note** For all non-passive copper cables, **Oper Link Training** (AN) mode is set to Off, irrespective of the **Admin Link Training** mode. Any changes in the **Admin Link Training** settings leads to the reset of the Series for that port, even if the **Oper Link Training** value remains the same.
MAC Address column	The MAC address of the uplink port.

Name	Description
Link State column	The current operational state of the uplink port. This can be one of the following: • **Fault** • **Link Up** • **Link Down** • **SFP ID Error** • **SFP Not Installed** • **SFP Security Check Failed** • **Unsupported SFP** **Note** • A Serdes reset causes the **Link State** field to change from **Link-Up** to **Link-down**. If the **Oper Link Training** setting is valid, Link-Partners determine a **Link-Up** or **Link-down** after the reset. • You might require to refresh the Web UI several times to view **Link State** field change.
Encap column	The mode in which adapter operates. This can be one of the following: • **CE**—Classical Ethernet mode. • **NIV**—Network Interface Virtualization mode.
Operating Speed column	The operating rate for the port. This can be one of the following: • **40 Gbps** • **4 x 10 Gbps** • **100 Gbps**
Connector Present column	Indicated whether or not the connector is present. This can be one of the following: • **Yes**—Connector is present. • **No**—Connector not present. **Note** This option is only available for some adapter cards.
Connector Supported column	Indicates whether or not the connector is supported by Cisco. This can be one of the following: • **Yes**—The connector is supported by Cisco. • **No**—The connector is not supported by Cisco. If the connector is not supported then the link will not be up. **Note** This option is only available for some adapter cards.

Name	Description
Connector Type column	The Cisco Product ID (PID) of the transceiver/cable that is present. **Note** This option is only available for some adapter cards.
Connector Vendor column	The vendor for the connector. **Note** This option is only available for some adapter cards.
Connector Part Number column	The Connector Vendor part number. **Note** This option is only available for some adapter cards.
Connector Part Revision column	The part revision of the Connector Vendor part number. **Note** This option is only available for some adapter cards.

Managing vHBAs

Guidelines for Managing vHBAs

When managing vHBAs, consider the following guidelines and restrictions:

- The SIOCs with the Cisco UCS Virtual Interface Cards provide two vHBAs and two vNICs by default. You can create up to 14 additional vHBAs or vNICs on these adapter cards.

  The Cisco UCS 1455 and 1457 Virtual Interface Cards, in non-port channel mode, provide four vHBAs and four vNICs by default. You can create up to 10 additional vHBAs or vNICs on these adapter cards in VNTAG mode.

Note If VNTAG mode is enabled for the adapter, you must assign a channel number to a vHBA when you create it.

- When using the Cisco UCS Virtual Interface Cards in an FCoE application, you must associate the vHBA with the FCoE VLAN. Follow the instructions in the **Modifying vHBA Properties** section to assign the VLAN.
- After making configuration changes, you must reboot the host for settings to take effect.

Viewing vHBA Properties

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

Step 2 In the **Networking** pane, select the Adapter Card SIOC1 or Adapter Card SIOC2 that you want to view.

Step 3 In the **Adapter Card SIOC1 or Adapter Card SIOC2** area, click the **vHBAs** tab.

Step 4 In the **vHBAs** pane, click **fc0** or **fc1**.

Step 5 In the **General** area of vHBA Properties, review the information in the following fields:

Name	Description
Name field	The name of the virtual HBA. This name cannot be changed after the vHBA has been created.
Initiator WWNN field	The WWNN associated with the vHBA. To let the system generate the WWNN, select **AUTO**. To specify a WWNN, click the second radio button and enter the WWNN in the corresponding field.
Initiator WWPN field	The WWPN associated with the vHBA. To let the system generate the WWPN, select **AUTO**. To specify a WWPN, click the second radio button and enter the WWPN in the corresponding field.
FC SAN Boot check box	If checked, the vHBA can be used to perform a SAN boot.
Persistent LUN Binding check box	If checked, any LUN ID associations are retained in memory until they are manually cleared.
Uplink Port drop-down list	The uplink port associated with the vHBA. **Note** This value cannot be changed for the system-defined vHBAs fc0 and fc1.
MAC Address field	The MAC address associated with the vHBA. To let the system generate the MAC address, select **AUTO**. To specify an address, click the second radio button and enter the MAC address in the corresponding field.
Default VLAN field	If there is no default VLAN for this vHBA, click **NONE**. Otherwise, click the second radio button and enter a VLAN ID between 1 and 4094 in the field.
PCI Order field	The order in which this vHBA will be used. To let the system set the order, select **ANY**. To specify an order, select the second radio button and enter an integer between 0 and 17.

Name	Description
vHBA Type drop-down list	**Note** This option is available only with 14xx series and VIC 15428 adapters. The vHBA type used in this policy. vHBAs supporting FC and FC-NVMe can now be created on the same adapter. The vHBA type used in this policy can be one of the following: • fc-initiator—Legacy SCSI FC vHBA initiator • fc-target—vHBA that supports SCSI FC target functionality **Note** This option is available as a Tech Preview. • fc-nvme-initiator—vHBA that is an FC NVME initiator, which discovers FC NVME targets and connects to them. • fc-nvme-target—vHBA that acts as an FC NVME target and provides connectivity to the NVME storage.
Class of Service field	The CoS for the vHBA. Select an integer between 0 and 6, with 0 being lowest priority and 6 being the highest priority. **Note** This option cannot be used in VNTAG mode.
Rate Limit field	The data rate limit for traffic on this vHBA, in Mbps. If you want this vHBA to have an unlimited data rate, select **OFF**. Otherwise, click the second radio button and enter an integer between 1 and 10,000. **Note** This option cannot be used in VNTAG mode.
EDTOV field	The error detect timeout value (EDTOV), which is the number of milliseconds to wait before the system assumes that an error has occurred. Enter an integer between 1,000 and 100,000. The default is 2,000 milliseconds.
RATOV field	The resource allocation timeout value (RATOV), which is the number of milliseconds to wait before the system assumes that a resource cannot be properly allocated. Enter an integer between 5,000 and 100,000. The default is 10,000 milliseconds.
Max Data Field Size field	The maximum size of the Fibre Channel frame payload bytes that the vHBA supports. Enter an integer between 256 and 2112.
Channel Number field	The channel number that will be assigned to this vHBA. Enter an integer between 1 and 1,000. **Note** VNTAG mode is required for this option.

Name	Description
PCI Link	It is read-only field.
Port Profile drop-down list	The port profile that should be associated with the vHBA, if any. This field displays the port profiles defined on the switch to which this server is connected. **Note** VNTAG mode is required for this option.

Step 6 In the **Error Recovery** area, review the information in the following fields:

Name	Description
FCP Error Recovery check box	If checked, the system uses FCP Sequence Level Error Recovery protocol (FC-TAPE).
Link Down Timeout field	The number of milliseconds the uplink port should be offline before it informs the system that the uplink port is down and fabric connectivity has been lost. Enter an integer between 0 and 240,000.
Port Down I/O Retry Count field	The number of times an I/O request to a port is returned because the port is busy before the system decides the port is unavailable. Enter an integer between 0 and 255.
IO Timeout Retry field	The time period till which the system waits for timeout before retrying. When a disk does not respond for I/O within the defined timeout period, the driver aborts the pending command, and resends the same I/O after the timer expires. Enter an integer between 1 and 59.
Port Down Timeout field	The number of milliseconds a remote Fibre Channel port should be offline before informing the SCSI upper layer that the port is unavailable. Enter an integer between 0 and 240,000.

Step 7 In the **Fibre Channel Interrupt** area, review the information in the following fields:

Name	Description
Interrupt Mode drop-down list	The preferred driver interrupt mode. This can be one of the following: • **MSIx**—Message Signaled Interrupts (MSI) with the optional extension. This is the recommended option. • **MSI**—MSI only. • **INTx**—PCI INTx interrupts.

Step 8 In the **Fibre Channel Port** area, review the information in the following fields:

Name	Description
I/O Throttle Count field	The number of I/O operations that can be pending in the vHBA at one time. Enter an integer between 1 and 1,024.
LUNs per Target field	The maximum number of LUNs that the driver will export. This is usually an operating system platform limitation. Enter an integer between 1 and 4,096.
LUN Queue Depth field	The number of commands that the HBA can send or receive in a single chunk per LUN. This parameter adjusts the initial queue depth for all LUNs on the adapter. Default value is 20 for physical miniports and 250 for virtual miniports.

Step 9 In the **Fibre Channel Port FLOGI** area, review the information in the following fields:

Name	Description
FLOGI Retries field	The number of times that the system tries to log in to the fabric after the first failure. To specify an unlimited number of retries, select the **INFINITE** radio button. Otherwise select the second radio button and enter an integer into the corresponding field.
FLOGI Timeout field	The number of milliseconds that the system waits before it tries to log in again. Enter an integer between 1,000 and 255,000.

Step 10 In the **Fibre Channel Port PLOGI** area, review the information in the following fields:

Name	Description
PLOGI Retries field	The number of times that the system tries to log in to a port after the first failure. Enter an integer between 0 and 255.
PLOGI Timeout field	The number of milliseconds that the system waits before it tries to log in again. Enter an integer between 1,000 and 255,000.

Step 11 In the **I/O** area, review the information in the following fields:

Name	Description
CDB Transmit Queue Count field	The number of SCSI I/O queue resources the system should allocate. For Cisco UCS VIC 14xx series adapters, enter an integer between 1 and 64. For any other VIC adapter, enter an integer between 1 and 245.
CDB Transmit Queue Ring Size field	The number of descriptors in each SCSI I/O queue. Enter an integer between 64 and 512.

Step 12 In the **Receive/Transmit Queues** area, review the information in the following fields:

Name	Description
FC Work Queue Ring Size field	The number of descriptors in each transmit queue. Enter an integer between 64 and 128.
FC Receive Queue Ring Size field	The number of descriptors in each receive queue. Enter an integer between 64 and 2048.

Step 13 **Note** **Boot Table** is available as a separate tab for Cisco UCS C-Series M7 and later servers. Click **Add Boot Entry** to create a new boot entry or select an existing entry and click **Edit Boot Entry**.

In the **Boot Table** area, review the information in the following fields:

Name	Description
Index column	The unique identifier for the boot target.
Target WWPN column	The World Wide Port Name (WWPN) that corresponds to the location of the boot image.
LUN column	The LUN ID that corresponds to the location of the boot image.
Add Boot Entry button	Opens a dialog box that allows you to specify a new WWPN and LUN ID.
Edit Boot Entry button	Opens a dialog box that allows you to change the WWPN and LUN ID for the selected boot target.
Delete Boot Entry button	Deletes the selected boot target after you confirm the deletion.

Step 14 **Note** **Persistent Bindings** is available as a separate tab for Cisco UCS C-Series M7 and later servers. You may click **Rebuild Persistent Binding** to clear the bindings and create a new one.

In the **Persistent Bindings** area, review the information in the following fields:

Name	Description
Index column	The unique identifier for the binding.
Target WWPN column	The target World Wide Port Name with which the binding is associated.
Host WWPN column	The host World Wide Port Name with which the binding is associated.
Bus ID column	The bus ID with which the binding is associated.
Target ID column	The target ID on the host system with which the binding is associated.
Rebuild Persistent Bindings button	Clears all unused bindings and resets the ones that are in use.

Modifying vHBA Properties

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

Step 2 In the **Networking** pane, select the Adapter Card SIOC1 or Adapter Card SIOC2 that you want to modify.

Step 3 In the **Adapter Card SIOC1 or Adapter Card SIOC2** pane, click the **vHBAs** tab.

Step 4 In the **vHBAs** pane, click **fc0** or **fc1**.

Step 5 In the **General** area, update the following fields:

Name	Description
Name field	The name of the virtual HBA. This name cannot be changed after the vHBA has been created.
Initiator WWNN field	The WWNN associated with the vHBA. To let the system generate the WWNN, select **AUTO**. To specify a WWNN, click the second radio button and enter the WWNN in the corresponding field.
Initiator WWPN field	The WWPN associated with the vHBA. To let the system generate the WWPN, select **AUTO**. To specify a WWPN, click the second radio button and enter the WWPN in the corresponding field.
FC SAN Boot check box	If checked, the vHBA can be used to perform a SAN boot.
Persistent LUN Binding check box	If checked, any LUN ID associations are retained in memory until they are manually cleared.
Uplink Port drop-down list	The uplink port associated with the vHBA. **Note** This value cannot be changed for the system-defined vHBAs fc0 and fc1.
MAC Address field	The MAC address associated with the vHBA. To let the system generate the MAC address, select **AUTO**. To specify an address, click the second radio button and enter the MAC address in the corresponding field.
Default VLAN field	If there is no default VLAN for this vHBA, click **NONE**. Otherwise, click the second radio button and enter a VLAN ID between 1 and 4094 in the field.
PCI Order field	The order in which this vHBA will be used. To let the system set the order, select **ANY**. To specify an order, select the second radio button and enter an integer between 0 and 17.

Name	Description
vHBA Type drop-down list	**Note** This option is available only with 14xx series and VIC 15428 adapters. The vHBA type used in this policy. vHBAs supporting FC and FC-NVMe can now be created on the same adapter. The vHBA type used in this policy can be one of the following: • fc-initiator—Legacy SCSI FC vHBA initiator • fc-target—vHBA that supports SCSI FC target functionality **Note** This option is available as a Tech Preview. • fc-nvme-initiator—vHBA that is an FC NVME initiator, which discovers FC NVME targets and connects to them. • fc-nvme-target—vHBA that acts as an FC NVME target and provides connectivity to the NVME storage.
Class of Service field	The CoS for the vHBA. Select an integer between 0 and 6, with 0 being lowest priority and 6 being the highest priority. **Note** This option cannot be used in VNTAG mode.
Rate Limit field	The data rate limit for traffic on this vHBA, in Mbps. If you want this vHBA to have an unlimited data rate, select **OFF**. Otherwise, click the second radio button and enter an integer between 1 and 10,000. **Note** This option cannot be used in VNTAG mode.
EDTOV field	The error detect timeout value (EDTOV), which is the number of milliseconds to wait before the system assumes that an error has occurred. Enter an integer between 1,000 and 100,000. The default is 2,000 milliseconds.
RATOV field	The resource allocation timeout value (RATOV), which is the number of milliseconds to wait before the system assumes that a resource cannot be properly allocated. Enter an integer between 5,000 and 100,000. The default is 10,000 milliseconds.
Max Data Field Size field	The maximum size of the Fibre Channel frame payload bytes that the vHBA supports. Enter an integer between 256 and 2112.
Channel Number field	The channel number that will be assigned to this vHBA. Enter an integer between 1 and 1,000. **Note** VNTAG mode is required for this option.

Name	Description
PCI Link	It is read-only field.
Port Profile drop-down list	The port profile that should be associated with the vHBA, if any. This field displays the port profiles defined on the switch to which this server is connected. **Note** VNTAG mode is required for this option.

Step 6 In the **Error Recovery** area, update the following fields:

Name	Description
FCP Error Recovery check box	If checked, the system uses FCP Sequence Level Error Recovery protocol (FC-TAPE).
Link Down Timeout field	The number of milliseconds the uplink port should be offline before it informs the system that the uplink port is down and fabric connectivity has been lost. Enter an integer between 0 and 240,000.
Port Down I/O Retry Count field	The number of times an I/O request to a port is returned because the port is busy before the system decides the port is unavailable. Enter an integer between 0 and 255.
IO Timeout Retry field	The time period till which the system waits for timeout before retrying. When a disk does not respond for I/O within the defined timeout period, the driver aborts the pending command, and resends the same I/O after the timer expires. Enter an integer between 1 and 59.
Port Down Timeout field	The number of milliseconds a remote Fibre Channel port should be offline before informing the SCSI upper layer that the port is unavailable. Enter an integer between 0 and 240,000.

Step 7 In the **Fibre Channel Interrupt** area, update the following fields:

Name	Description
Interrupt Mode drop-down list	The preferred driver interrupt mode. This can be one of the following: • **MSIx**—Message Signaled Interrupts (MSI) with the optional extension. This is the recommended option. • **MSI**—MSI only. • **INTx**—PCI INTx interrupts.

Step 8 In the **Fibre Channel Port** area, update the following fields:

Name	Description
I/O Throttle Count field	The number of I/O operations that can be pending in the vHBA at one time. Enter an integer between 1 and 1,024.
LUNs per Target field	The maximum number of LUNs that the driver will export. This is usually an operating system platform limitation. Enter an integer between 1 and 4,096.
LUN Queue Depth field	The number of commands that the HBA can send or receive in a single chunk per LUN. This parameter adjusts the initial queue depth for all LUNs on the adapter. Default value is 20 for physical miniports and 250 for virtual miniports.

Step 9 In the **Fibre Channel Port FLOGI** area, update the following fields:

Name	Description
FLOGI Retries field	The number of times that the system tries to log in to the fabric after the first failure. To specify an unlimited number of retries, select the **INFINITE** radio button. Otherwise select the second radio button and enter an integer into the corresponding field.
FLOGI Timeout field	The number of milliseconds that the system waits before it tries to log in again. Enter an integer between 1,000 and 255,000.

Step 10 In the **Fibre Channel Port PLOGI** area, update the following fields:

Name	Description
PLOGI Retries field	The number of times that the system tries to log in to a port after the first failure. Enter an integer between 0 and 255.
PLOGI Timeout field	The number of milliseconds that the system waits before it tries to log in again. Enter an integer between 1,000 and 255,000.

Step 11 In the **SCSI I/O** area, update the following fields:

Name	Description
CDB Transmit Queue Count field	The number of SCSI I/O queue resources the system should allocate. For Cisco UCS VIC 14xx series adapters, enter an integer between 1 and 64. For any other VIC adapter, enter an integer between 1 and 245.
CDB Transmit Queue Ring Size field	The number of descriptors in each SCSI I/O queue. Enter an integer between 64 and 512.

Step 12 In the **Receive/Transmit Queues** area, update the following fields:

Name	Description
FC Work Queue Ring Size field	The number of descriptors in each transmit queue. Enter an integer between 64 and 128.
FC Receive Queue Ring Size field	The number of descriptors in each receive queue. Enter an integer between 64 and 2048.

Step 13 Click **Save Changes**.

Step 14 **Note** **Boot Table** is available as a separate tab for Cisco UCS C-Series M7 and later servers. Click **Add Boot Entry** to create a new boot entry or select an existing entry and click **Edit Boot Entry**.

In the **Boot Table** area, update the following fields or add a new entry:

Name	Description
Index column	The unique identifier for the boot target.
Target WWPN column	The World Wide Port Name (WWPN) that corresponds to the location of the boot image.
LUN column	The LUN ID that corresponds to the location of the boot image.
Add Boot Entry button	Opens a dialog box that allows you to specify a new WWPN and LUN ID.
Edit Boot Entry button	Opens a dialog box that allows you to change the WWPN and LUN ID for the selected boot target.
Delete Boot Entry button	Deletes the selected boot target after you confirm the deletion.

Step 15 **Note** **Persistent Bindings** is available as a separate tab for Cisco UCS C-Series M7 and later servers. You may click **Rebuild Persistent Binding** to clear the bindings and create a new one.

In the **Persistent Bindings** area, update the following fields or add a new entry:

Name	Description
Index column	The unique identifier for the binding.
Target WWPN column	The target World Wide Port Name with which the binding is associated.
Host WWPN column	The host World Wide Port Name with which the binding is associated.
Bus ID column	The bus ID with which the binding is associated.
Target ID column	The target ID on the host system with which the binding is associated.
Rebuild Persistent Bindings button	Clears all unused bindings and resets the ones that are in use.

Creating a vHBA

The Cisco UCS Virtual Interface Cards provide two vHBAs and two vNICs by default. You can create up to 14 additional vHBAs or vNICs on these adapter cards.

Cisco UCS 1455 and 1457 Virtual Interface Cards, in non-port channel mode, provide four vHBAs and four vNICs by default. You can create up to 10 additional vHBAs or vNICs on these adapter cards.

Before you begin

Ensure that **Enable VNTAG Mode** under **Adapter Card Properties** in the **General** tab is checked.

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

Step 2 In the **Networking** pane, select the Adapter Card SIOC1 or Adapter Card SIOC2 that you want to modify.

Step 3 In the **Adapter Card SIOC1 or Adapter Card SIOC2** pane, click the **vHBAs** tab.

Step 4 In the **Host Fibre Channel Interfaces** area, choose one of these actions:

- To create a vHBA using default configuration settings, click **Add vHBA**.
- To create a vHBA using the same configuration settings as an existing vHBA, select that vHBA and click **Clone vHBA**.

The **Add vHBA** dialog box appears.

Step 5 In the **Add vHBA** dialog box, enter a name for the vHBA in the **Name** entry box.

Step 6 Configure the new vHBA as described in Modifying vHBA Properties, on page 203.

Step 7 Click **Add vHBA**.

What to do next

- Reboot the server to create the vHBA.

Deleting a vHBA

Default vHBAs cannot be deleted. You can delete any other vHBAs created using VNTAG mode.

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

Step 2 In the **Networking** pane, select the Adapter Card SIOC1 or Adapter Card SIOC2 that you want to modify.

Step 3 In the **Adapter Card SIOC1 or Adapter Card SIOC2** pane, click the **vHBAs** tab.

Step 4 In the **Host Fibre Channel Interfaces** area, select a vHBA or vHBAs from the table.

Note You cannot delete either of the two default vHBAs, **fc0** or **fc1**.

Step 5 Click **Delete vHBAs** and click **OK** to confirm.

What to do next

Reboot the server to delete the vHBA.

vHBA Boot Table

In the vHBA boot table, you can specify up to four LUNs from which the server can boot.

Creating a Boot Table Entry

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

Step 2 In the **Networking** pane, select the Adapter Card SIOC1 or Adapter Card SIOC2 that you want to modify.

Step 3 In the **Adapter Card SIOC1 or Adapter Card SIOC2** pane, click the **vHBAs** tab.

Step 4 Select a vHBA from the list of available vHBAs under **vHBAs** in the **vHBAs** tab.

The related **vHBA Properties** pane is displayed in the right hand side of the window.

Step 5 For:

- Cisco UCS C-Series M7 and later servers, select the **Boot Table** tab.
- Cisco UCS C-Series M6 and earlier servers, scroll down to view **Boot Table**.

Step 6 Click the **Add Boot Entry** button to open the **Add Boot Entry** dialog box.

Step 7 In the **Add Boot Entry** dialog box, review the following information and perform the actions specified:

Name	Description
Index field	The default value for this field is **0**.
Target WWPN field	The World Wide Port Name (WWPN) that corresponds to the location of the boot image. Enter the WWPN in the format **hh:hh:hh:hh:hh:hh:hh:hh**.
LUN ID field	The LUN ID that corresponds to the location of the boot image. Enter an ID between 0 and 255.
Add Boot Entry button	Adds the specified location to the boot table.
Reset Values button	Clears the values currently entered in the fields.
Cancel button	Closes the dialog box without saving any changes made while the dialog box was open.

Deleting a Boot Table Entry

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

Step 2 In the **Networking** pane, select the Adapter Card SIOC1 or Adapter Card SIOC2 that you want to modify.

Step 3 In the **Adapter Card SIOC1 or Adapter Card SIOC2** pane, click the **vHBAs** tab.

Step 4 Select a vHBA from the list of available vHBAs under **vHBAs** in the **vHBAs** tab.

The related **vHBA Properties** pane is displayed in the right hand side of the window.

Step 5 For:

- Cisco UCS C-Series M7 and later servers, select the **Boot Table** tab.
- Cisco UCS C-Series M6 and earlier servers, scroll down to view **Boot Table**.

Step 6 In the **Boot Table** area, click the entry to be deleted.

Step 7 Click **Delete Boot Entry** and click **OK** to confirm.

vHBA Persistent Binding

Persistent binding ensures that the system-assigned mapping of Fibre Channel targets is maintained after a reboot.

Viewing Persistent Bindings

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

Step 2 In the **Networking** pane, select the Adapter Card SIOC1 or Adapter Card SIOC2 that you want to modify.

Step 3 In the **Adapter Card SIOC1 or Adapter Card SIOC2** pane, click the **vHBAs** tab.

Step 4 In the **vHBAs** pane, click **fc0** or **fc1**.

Step 5 For:

- Cisco UCS C-Series M7 and later servers, select the **Persistent Bindings** tab.
- Cisco UCS C-Series M6 and earlier servers, scroll down to view **Persistent Bindings**.

Step 6 In the **Persistent Bindings** area, review the following information:

Name	Description
Index column	The unique identifier for the binding.
Target WWPN column	The target World Wide Port Name with which the binding is associated.
Host WWPN column	The host World Wide Port Name with which the binding is associated.
Bus ID column	The bus ID with which the binding is associated.
Target ID column	The target ID on the host system with which the binding is associated.
Rebuild Persistent Bindings button	Clears all unused bindings and resets the ones that are in use.

Rebuilding Persistent Bindings

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

Step 2 In the **Networking** pane, select the Adapter Card SIOC1 or Adapter Card SIOC2 that you want to modify.

Step 3 In the **Adapter Card SIOC1 or Adapter Card SIOC2** pane, click the **vHBAs** tab.

Step 4 In the **vHBAs** pane, click **fc0** or **fc1**.

Step 5 For:

- Cisco UCS C-Series M7 and later servers, select the **Persistent Bindings** tab.
- Cisco UCS C-Series M6 and earlier servers, scroll down to view **Persistent Bindings** area.

Step 6 Click the **Rebuild Persistent Bindings** button.

Step 7 Click **OK** to confirm.

Managing vNICs

Guidelines for Managing vNICs

When managing vNICs, consider the following guidelines and restrictions:

- The Cisco UCS Virtual Interface Cards provide two vHBAs and two vNICs by default. You can create up to 14 additional vHBAs or vNICs on these adapter cards.

  Additional vHBAs can be created using VNTAG mode.

  The Cisco UCS 1455 and 1457 Virtual Interface Cards, in non-port channel mode, provide four vHBAs and four vNICs by default. You can create up to 10 additional vHBAs or vNICs on these adapter cards.

Note If VNTAG mode is enabled for the adapter, you must assign a channel number to a vNIC when you create it.

- After making configuration changes, you must reboot the host for settings to take effect.

Viewing vNIC Properties

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

Step 2 In the **Networking** pane, select the Adapter Card SIOC1 or Adapter Card SIOC2 that you want to view.

Step 3 In the **Adapter Card SIOC1 or Adapter Card SIOC2** pane, click the **vNICs** tab.

Step 4 In the **vNICs** pane, click **eth0** or **eth1**.

Step 5 In the **General** area under **vNIC Properties** area, review the following fields:

General Area

Name	Description
Name field	The name for the virtual NIC. This name cannot be changed after the vNIC has been created.
CDN field	The Consistent Device Name (CDN) that you can assign to the ethernet vNICs on the VIC cards. Assigning a specific CDN to a device helps in identifying it on the host OS. **Note** This feature works only when the **CDN Support for VIC** token is enabled in the BIOS.
MTU field	The maximum transmission unit, or packet size, that this vNIC accepts. Enter an integer between 1500 and 9000.
Uplink Port drop-down list	The uplink port associated with this vNIC. All traffic for this vNIC goes through this uplink port.
MAC Address field	The MAC address associated with the vNIC. To let the adapter select an available MAC address from its internal pool, select **Auto**. To specify an address, click the second radio button and enter the MAC address in the corresponding field.
Class of Service field	The class of service to associate with traffic from this vNIC. Select an integer between 0 and 6, with 0 being lowest priority and 6 being the highest priority. **Note** This option cannot be used in VNTAG mode.
Trust Host CoS check box	Check this box if you want the vNIC to use the class of service provided by the host operating system.
PCI Order field	The order in which this vNIC will be used. To specify an order, enter an integer within the displayed range.
Default VLAN radio button	If there is no default VLAN for this vNIC, select **NONE**. Otherwise, select the second radio button and enter a VLAN ID between 1 and 4094 in the field. **Note** This option cannot be used in VNTAG mode.
VLAN Mode drop-down list	If you want to use VLAN trunking, select **TRUNK**. Otherwise, select **ACCESS**. **Note** This option cannot be used in VNTAG mode.

Name	Description
Enable PTP check box	Check this box to enable Precision Time Protocol (PTP). Precision Time Protocol (PTP) precisely synchronizes the server clock with other devices and peripherals on Linux operating systems. Clocks managed by PTP follow a client-worker hierarchy, with workers sychronized to a master client. The hierarchy is updated by the best master clock (BMC) algorithm, which runs on every clock. One PTP interface per adapter must be enabled to sychronize it to the grand master clock. **Note** • This option is supported only with Linux operating system. • This option is available only for Cisco UCS VIC 15xxx series adapters. This option is available only on some Cisco UCS C-Series servers. • For the PTP enabling to be effective, it is required that you reboot the server.
Rate Limit radio button	If you want this vNIC to have an unlimited data rate, select OFF. Otherwise, click the second radio button and enter a rate limit in the associated field. Enter an integer between 1 and 10,000 Mbps. For VIC 13xx controllers, you can enter an integer between 1 and 40,000 Mbps. For VIC 1455 and 1457 controllers: • If the adapter is connected to 25 Gbps link on a Switch, then you can enter an integer between 1 to 25,000 Mbps for the **Rate Limit** field. • If the adapter is connected to 10 Gbps link on a Switch, then you can enter an integer between 1 to 10,000 Mbps for the **Rate Limit** field. For VIC 1495 and 1497 controllers: • If the adapter is connected to 40 Gbps link on a switch, then you can enter an integer between 1 to 40,000 Mbps for the **Rate Limit** field. • If the adapter is connected to 100 Gbps link on a switch, then you can enter an integer between 1 to 100,000 Mbps for the **Rate Limit** field. **Note** This option cannot be used in VNTAG mode.
Channel Number field	Select the channel number that will be assigned to this vNIC. **Note** VNTAG mode is required for this option.

Name	Description
PCI Link field	The link through which vNICs can be connected. These are the following values: • **0** - The first cross-edged link where the vNIC is placed. • **1** - The second cross-edged link where the vNIC is placed. **Note** • This option is available only on some Cisco UCS C-Series servers.
Enable NVGRE check box	Check this box to enable Network Virtualization using Generic Routing Encapsulation. • This option is available only on some Cisco UCS C-Series servers. • This option is available only on C-Series servers with Cisco VIC 1385 cards.
Enable VXLAN check box	Check this box to enable Virtual Extensible LAN. • This option is available only on some Cisco UCS C-Series servers. • This option is available only on C-Series servers with Cisco VIC 1385, VIC 14xx, and VIC 15xxx.

Name	Description
Geneve Offload check box	Beginning with release 4.1(2a), Cisco IMC supports Generic Network Virtualization Encapsulation (Geneve) Offload feature with Cisco VIC 14xx series and VIC 15xxx adapters in ESX 7.0 (NSX-T 3.0) and ESX 6.7U3(NSX-T 2.5) OS. Geneve is a tunnel encapsulation functionality for network traffic . Check this box if you want to enable Geneve Offload encapsulation in Cisco VIC 14xx series adapters. Un-check this box to disable Geneve Offload, in order to prevent non-encapsulated UDP packets whose destination port numbers match with the Geneve destination port from being treated as tunneled packets. If you enable **Geneve Offload** feature, then Cisco recommends the following settings: • Transmit Queue Count—1 • Transmit Queue Ring Size—4096 • Receive Queue Count—8 • Receive Queue Ring Size—4096 • Completion Queue Count—9 • Interrupt Count—11 **Note** You cannot enable the following when **Geneve Offload** is enabled in a setup with Cisco VIC 14xx series: • RDMA on the same vNIC • usNIC on the same vNIC • Non-Port Channel Mode on Cisco VIC 145x adapters • aRFS • Advanced Filters • NetQueue • Physical NIC Mode **Note** You cannot enable the following when **Geneve Offload** is enabled in a setup with Cisco VIC 15xxx: • aRFS • RoCEv2 Outer IPV6 is not supported with GENEVE Offload feature. Downgrade Limitation—If **Geneve Offload** is enabled, you cannot downgrade to any release earlier than 4.1(2a).

Name	Description
Advanced Filter check box	Check this box to enable advanced filter options in vNICs.
Port Profile drop-down list	Select the port profile that should be associated with the vNIC. This field displays the port profiles defined on the switch to which this server is connected. **Note** VNTAG mode is required for this option.
Enable PXE Boot check box	Check this box if the vNIC can be used to perform a PXE boot.
Enable VMQ check box	Check this box to enable Virtual Machine Queue (VMQ).
Enable Multi Queue check box	Check this box to enable the Multi Queue option on vNICs. When enabled multi queue vNICs will be available to the host. By default this is disabled. **Note** • Multi queue is supported only on C-Series servers with 14xx and VIC 15xxx adapters. • VMQ must be in enabled state to enable this option. • When you enable this option on one of the vNICs, configuring only VMQ (without choosing multi-queue) on other vNICs is not supported. • When this option is enabled usNIC configuration will be disabled.
No. of Sub vNICs field	Number of sub vNICs available to the host when the multi queue option is enabled.
Enable aRFS check box	Check this box to enable Accelerated Receive Flow steering (aRFS). This option is available only on some Cisco UCS C-Series servers.
Enable Uplink Failover check box	Check this box if traffic on this vNIC should fail over to the secondary interface if there are communication problems. **Note** VNTAG mode is required for this option.
Failback Timeout field	After a vNIC has started using its secondary interface, this setting controls how long the primary interface must be available before the system resumes using the primary interface for the vNIC. Enter a number of seconds between 0 and 600. **Note** VNTAG mode is required for this option.

Name	Description
Enable VIC QinQ Tunneling check box	Beginning with release 4.3.2.230207, Cisco IMC provides **VIC QinQ Tunneling** support for Cisco UCS M5 servers with Cisco UCS VIC 14xx series and 15xxx series VIC adapters. Check this box to enable the **VIC QinQ Tunneling** option on the specified vNIC. **Note** • VIC QinQ Tunneling is not supported on 13xx adapters. • Default vLAN should not be none when VIC QinQ Tunneling is configured and vLAN mode is trunk. You cannot enable the following when **VIC QinQ Tunneling** is enabled in a setup with Cisco VIC 14xx: • usNIC on the same vNIC • Geneve offload on the same vNIC • VMMQ on the same vNIC • RDMA v2 on the same vNIC • SR-IOV on the same vNIC • iSCSI boot on the same vNIC • PXE boot on the same vNIC You cannot enable the following when **VIC QinQ Tunneling** is enabled in a setup with Cisco VIC 15xxx: • usNIC on the same vNIC • VMMQ on the same vNIC • RDMA v2 on the same vNIC • SR-IOV on the same vNIC • iSCSI boot on the same vNIC • PXE boot on the same vNIC
QinQ VLAN field	Enter a QinQ VLAN ID between 2 and 4094 in the field.

Step 6 In the **Ethernet Interrupt** area, review the information in the following fields:

Name	Description
Interrupt Count field	The number of interrupt resources to allocate. In general, this value should be equal to the number of completion queue resources. Enter an integer between 1 and 1024.

Name	Description
Interrupt Mode drop-down list	The preferred driver interrupt mode. This can be one of the following: • **MSI-X**—Message Signaled Interrupts (MSI) with the optional extension. This is the recommended option. • **MSI**—MSI only. • **INTx**—PCI INTx interrupts.
Coalescing Time field	The time to wait between interrupts or the idle period that must be encountered before an interrupt is sent. Enter an integer between 1 and 65535. To turn off interrupt coalescing, enter 0 (zero) in this field.
Coalescing Type drop-down list	This can be one of the following: • **MIN**—The system waits for the time specified in the **Coalescing Time** field before sending another interrupt event. • **IDLE**—The system does not send an interrupt until there is a period of no activity lasting as least as long as the time specified in the **Coalescing Time** field.

Step 7 In the **TCP Offload** area, review the information in the following fields:

Name	Description
Enable Large Receive check box	If checked, the hardware reassembles all segmented packets before sending them to the CPU. This option may reduce CPU utilization and increase inbound throughput. If cleared, the CPU processes all large packets.
Enable TCP Rx Offload Checksum Validation check box	If checked, the CPU sends all packet checksums to the hardware for validation. This option may reduce CPU overhead. If cleared, the CPU validates all packet checksums.
Enable TCP Segmentation Offload check box	If checked, the CPU sends large TCP packets to the hardware to be segmented. This option may reduce CPU overhead and increase throughput rate. If cleared, the CPU segments large packets. **Note** This option is also known as Large Send Offload (LSO).
Enable TCP Tx Offload Checksum Generation check box	If checked, the CPU sends all packets to the hardware so that the checksum can be calculated. This option may reduce CPU overhead. If cleared, the CPU calculates all packet checksums.

Step 8 In the **Receive Side Scaling** area, review the information in the following fields:

Name	Description
Enable TCP Receive Side Scaling check box	Receive Side Scaling (RSS) distributes network receive processing across multiple CPUs in multiprocessor systems. If checked, network receive processing is shared across processors whenever possible. If cleared, network receive processing is always handled by a single processor even if additional processors are available.
Enable IPv4 RSS check box	If checked, RSS is enabled on IPv4 networks.
Enable TCP-IPv4 RSS check box	If checked, RSS is enabled for TCP transmissions across IPv4 networks.
Enable IPv6 RSS check box	If checked, RSS is enabled on IPv6 networks.
Enable TCP-IPv6 RSS check box	If checked, RSS is enabled for TCP transmissions across IPv6 networks.
Enable IPv6 Extension RSS check box	If checked, RSS is enabled for IPv6 extensions.
Enable TCP-IPv6 Extension RSS check box	If checked, RSS is enabled for TCP transmissions across IPv6 networks.

Step 9

Note Cisco UCS C-Series M7 and later servers have a **Queues** tab.

Review the following

Name	Description
Enable VMQ check box	Check this box to enable Virtual Machine Queue (VMQ).
Enable Multi Queue check box	Check this box to enable the Multi Queue option on vNICs. When enabled multi queue vNICs will be available to the host. By default this is disabled. • Multi queue is supported only on C-Series servers with 14xx and VIC 15xxx adapters. • VMQ must be in enabled state to enable this option. • When you enable this option on one of the vNICs, configuring only VMQ (without choosing multi-queue) on other vNICs is not supported. • When this option is enabled usNIC configuration will be disabled
Trust Host CoS check box	Check this box if you want the vNIC to use the class of service provided by the host operating system.
No. of Sub vNICs field	Number of sub vNICs available to the host when the multi queue option is enabled.

Step 10 **Note** **Ethernet Receive Queue** is available under **Queues** tab for Cisco UCS C-Series M7 and later servers.

In the **Ethernet Receive Queue** area, review the information in the following fields:

Name	Description
Count field	The number of receive queue resources to allocate. Enter an integer between 1 and 256.
Ring Size field	The number of descriptors in each receive queue. Enter an integer between 64 and 4096.

Step 11 **Note** **Ethernet Transmit Queue** is available under **Queues** tab for Cisco UCS C-Series M7 and later servers.

In the **Ethernet Transmit Queue** area, review the information in the following fields:

Name	Description
Count field	The number of transmit queue resources to allocate. Enter an integer between 1 and 256.
Ring Size field	The number of descriptors in each transmit queue. Enter an integer between 64 and 4096.

Step 12 **Note** **Completion Queue** is available under **Queues** tab for Cisco UCS C-Series M7 and later servers.

In the **Completion Queue** area, review the information in the following fields:

Name	Description
Count field	The number of completion queue resources to allocate. In general, the number of completion queue resources you should allocate is equal to the number of transmit queue resources plus the number of receive queue resources. Enter an integer between 1 and 512.
Ring Size	The number of descriptors in each completion queue. This value cannot be changed.

Step 13 **Note** **Multi Queue** is available under **Queues** tab for Cisco UCS C-Series M7 and later servers.

In the **Multi Queue** area, review the information in the following fields:

Name	Description
Receive Queue Count field	The number of receive queue resources to allocate. Enter an integer between 1 and 1000.
Transmit Queue Count field	The number of transmit queue resources to allocate. Enter an integer between 1 and 1000.

Name	Description
Completion Queue Count field	The number of completion queue resources to allocate. In general, the number of completion queue resources you should allocate is equal to the number of transmit queue resources plus the number of receive queue resources. Enter an integer between 1 and 2000.
RoCE check box	Check the check box to change the RoCE Properties. **Note** If **Multi Queue** RoCE is enabled, ensure that VMQ RoCE is also enabled.
Queue Pairs field	The number of queue pairs per adapter. Enter an integer between 1 and 2048. We recommend that this number be an integer power of 2.
Memory Regions field	The number of memory regions per adapter. Enter an integer between 1 and 524288. We recommend that this number be an integer power of 2.
Resource Groups field	The number of resource groups per adapter. Enter an integer between 1 and 128. We recommend that this number be an integer power of 2 greater than or equal to the number of CPU cores on the system for optimum performance.
Class of Service field	This field is read-only and is set to 5. **Note** This option is available only on some of the adapters.

Step 14

Note **RoCE Properties** is available under **Queues** tab for Cisco UCS C-Series M7 and later servers.

In the **RoCE Properties** area, review the information in the following fields:

Name	Description
RoCE checkbox	Check the check box to change the RoCE Properties.
Queue Pairs field	The number of queue pairs per adapter. Enter an integer between 1 and 2048. We recommend that this number be an integer power of 2. The recommended value for queue pairs per vNIC is 2048.
Memory Regions field	The number of memory regions per adapter. Enter an integer between 1 and 524288. We recommend that this number be an integer power of 2. The recommended value is 131072. The number of memory regions supported should be enough to meet application requirements as the regions are primarily used to send operation channel semantics.

Name	Description
Resource Groups field	The number of resource groups per adapter. Enter an integer between 1 and 128. We recommend that this number be an integer power of 2 greater than or equal to the number of CPU cores on the system for optimum performance. The resource group defines the total number of hardware resources such as WQ, RQ, CQ, and interrupts required to support the RDMA functionality, and is based on the total number of processor cores available with the host. The host chooses to dedicate a particular resource group to a core to maximize performance and get a better non-uniform memory access.
Class of Service drop-down list	NO Drop QOS COS to be specified. This same value should be configured at the up link switch. Default No Drop QOS COS is 5. **Note** This option is available only on some adapters.

Step 15 **Note** **SR-IOV Properties** is available under **Queues** tab for Cisco UCS C-Series M7 and later servers.

In the **SR-IOV Properties** area, review the information in the following fields:

Name	Description
No. of VFs field	Enter an integer between 1 and 64. **Note** Other SR-IOV properties are enabled only when you enter an integer between 1 and 64.
Receive Queue Count Per VF field	The number of receive queue resources to allocate. Enter an integer between 1 and 8.
Transmit Queue Count Per VF field	The number of descriptors in each transmit queue. Enter an integer between 1 and 8.
Completion Queue Count Per VF field	The number of completion queue resources to allocate. In general, the number of completion queue resources you should allocate is equal to the number of transmit queue resources plus the number of receive queue resources. Enter an integer between 1 and 16.
Interrupt Count field	The number of interrupt resources to allocate. In general, this value should be equal to the number of completion queue resources. Enter an integer between 1 and 16.

What to do next

Reboot the server to create the vHBA.

Modifying vNIC Properties

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

Step 2 In the **Networking** pane, select the Adapter Card SIOC1 or Adapter Card SIOC2 that you want to modify.

Step 3 In the **Adapter Card SIOC1 or Adapter Card SIOC2** pane, click the **vNICs** tab.

Step 4 In the **vNICs** pane, click **eth0** or **eth1**.

Step 5 In the **General** area under **vNIC Properties** in the **vNICs** pane, update the following fields:

Name	Description
Name field	The name for the virtual NIC. This name cannot be changed after the vNIC has been created.
CDN field	The Consistent Device Name (CDN) that you can assign to the ethernet vNICs on the VIC cards. Assigning a specific CDN to a device helps in identifying it on the host OS. **Note** This feature works only when the **CDN Support for VIC** token is enabled in the BIOS.
MTU field	The maximum transmission unit, or packet size, that this vNIC accepts. Enter an integer between 1500 and 9000.
Uplink Port drop-down list	The uplink port associated with this vNIC. All traffic for this vNIC goes through this uplink port.
MAC Address field	The MAC address associated with the vNIC. To let the adapter select an available MAC address from its internal pool, select **Auto**. To specify an address, click the second radio button and enter the MAC address in the corresponding field.
Class of Service field	The class of service to associate with traffic from this vNIC. Select an integer between 0 and 6, with 0 being lowest priority and 6 being the highest priority. **Note** This option cannot be used in VNTAG mode.
Trust Host CoS check box	Check this box if you want the vNIC to use the class of service provided by the host operating system.
PCI Order field	The order in which this vNIC will be used. To specify an order, enter an integer within the displayed range.
Default VLAN radio button	If there is no default VLAN for this vNIC, select **NONE**. Otherwise, select the second radio button and enter a VLAN ID between 1 and 4094 in the field. **Note** This option cannot be used in VNTAG mode.

Name	Description
VLAN Mode drop-down list	If you want to use VLAN trunking, select **TRUNK**. Otherwise, select **ACCESS**. **Note** This option cannot be used in VNTAG mode.
Enable PTP check box	Check this box to enable Precision Time Protocol (PTP). Precision Time Protocol (PTP) precisely synchronizes the server clock with other devices and peripherals on Linux operating systems. Clocks managed by PTP follow a client-worker hierarchy, with workers sychronized to a master client. The hierarchy is updated by the best master clock (BMC) algorithm, which runs on every clock. One PTP interface per adapter must be enabled to sychronize it to the grand master clock. **Note** • This option is supported only with Linux operating system. • This option is available only for Cisco UCS VIC 15xxx series adapters. This option is available only on some Cisco UCS C-Series servers. • For the PTP enabling to be effective, it is required that you reboot the server.
Rate Limit radio button	If you want this vNIC to have an unlimited data rate, select OFF. Otherwise, click the second radio button and enter a rate limit in the associated field. Enter an integer between 1 and 10,000 Mbps. For VIC 13xx controllers, you can enter an integer between 1 and 40,000 Mbps. For VIC 1455 and 1457 controllers: • If the adapter is connected to 25 Gbps link on a Switch, then you can enter an integer between 1 to 25,000 Mbps for the **Rate Limit** field. • If the adapter is connected to 10 Gbps link on a Switch, then you can enter an integer between 1 to 10,000 Mbps for the **Rate Limit** field. For VIC 1495 and 1497 controllers: • If the adapter is connected to 40 Gbps link on a switch, then you can enter an integer between 1 to 40,000 Mbps for the **Rate Limit** field. • If the adapter is connected to 100 Gbps link on a switch, then you can enter an integer between 1 to 100,000 Mbps for the **Rate Limit** field. **Note** This option cannot be used in VNTAG mode.
Channel Number field	Select the channel number that will be assigned to this vNIC. **Note** VNTAG mode is required for this option.

Name	Description
PCI Link field	The link through which vNICs can be connected. These are the following values: • **0** - The first cross-edged link where the vNIC is placed. • **1** - The second cross-edged link where the vNIC is placed. **Note** • This option is available only on some Cisco UCS C-Series servers.
Enable NVGRE check box	Check this box to enable Network Virtualization using Generic Routing Encapsulation. • This option is available only on some Cisco UCS C-Series servers. • This option is available only on C-Series servers with Cisco VIC 1385 cards.
Enable VXLAN check box	Check this box to enable Virtual Extensible LAN. • This option is available only on some Cisco UCS C-Series servers. • This option is available only on C-Series servers with Cisco VIC 1385, VIC 14xx, and VIC 15xxx.

Name	Description
Geneve Offload check box	Beginning with release 4.1(2a), Cisco IMC supports Generic Network Virtualization Encapsulation (Geneve) Offload feature with Cisco VIC 14xx series and VIC 15xxx adapters in ESX 7.0 (NSX-T 3.0) and ESX 6.7U3(NSX-T 2.5) OS. Geneve is a tunnel encapsulation functionality for network traffic . Check this box if you want to enable Geneve Offload encapsulation in Cisco VIC 14xx series adapters. Un-check this box to disable Geneve Offload, in order to prevent non-encapsulated UDP packets whose destination port numbers match with the Geneve destination port from being treated as tunneled packets. If you enable **Geneve Offload** feature, then Cisco recommends the following settings: • Transmit Queue Count—1 • Transmit Queue Ring Size—4096 • Receive Queue Count—8 • Receive Queue Ring Size—4096 • Completion Queue Count—9 • Interrupt Count—11 **Note** You cannot enable the following when **Geneve Offload** is enabled in a setup with Cisco VIC 14xx series: • RDMA on the same vNIC • usNIC on the same vNIC • Non-Port Channel Mode on Cisco VIC 145x adapters • aRFS • Advanced Filters • NetQueue • Physical NIC Mode **Note** You cannot enable the following when **Geneve Offload** is enabled in a setup with Cisco VIC 15xxx: • aRFS • RoCEv2 Outer IPV6 is not supported with GENEVE Offload feature. Downgrade Limitation—If **Geneve Offload** is enabled, you cannot downgrade to any release earlier than 4.1(2a).

Name	Description
Advanced Filter check box	Check this box to enable advanced filter options in vNICs.
Port Profile drop-down list	Select the port profile that should be associated with the vNIC. This field displays the port profiles defined on the switch to which this server is connected. **Note** VNTAG mode is required for this option.
Enable PXE Boot check box	Check this box if the vNIC can be used to perform a PXE boot.
Enable VMQ check box	Check this box to enable Virtual Machine Queue (VMQ).
Enable Multi Queue check box	Check this box to enable the Multi Queue option on vNICs. When enabled multi queue vNICs will be available to the host. By default this is disabled. **Note** • Multi queue is supported only on C-Series servers with 14xx and VIC 15xxx adapters. • VMQ must be in enabled state to enable this option. • When you enable this option on one of the vNICs, configuring only VMQ (without choosing multi-queue) on other vNICs is not supported. • When this option is enabled usNIC configuration will be disabled.
No. of Sub vNICs field	Number of sub vNICs available to the host when the multi queue option is enabled.
Enable aRFS check box	Check this box to enable Accelerated Receive Flow steering (aRFS). This option is available only on some Cisco UCS C-Series servers.
Enable Uplink Failover check box	Check this box if traffic on this vNIC should fail over to the secondary interface if there are communication problems. **Note** VNTAG mode is required for this option.
Failback Timeout field	After a vNIC has started using its secondary interface, this setting controls how long the primary interface must be available before the system resumes using the primary interface for the vNIC. Enter a number of seconds between 0 and 600. **Note** VNTAG mode is required for this option.

Name	Description
Enable VIC QinQ Tunneling check box	Beginning with release 4.3.2.230207, Cisco IMC provides **VIC QinQ Tunneling** support for Cisco UCS M5 servers with Cisco UCS VIC 14xx series and 15xxx series VIC adapters. Check this box to enable the **VIC QinQ Tunneling** option on the specified vNIC. **Note** • VIC QinQ Tunneling is not supported on 13xx adapters. • Default vLAN should not be none when VIC QinQ Tunneling is configured and vLAN mode is trunk. You cannot enable the following when **VIC QinQ Tunneling** is enabled in a setup with Cisco VIC 14xx: • usNIC on the same vNIC • Geneve offload on the same vNIC • VMMQ on the same vNIC • RDMA v2 on the same vNIC • SR-IOV on the same vNIC • iSCSI boot on the same vNIC • PXE boot on the same vNIC You cannot enable the following when **VIC QinQ Tunneling** is enabled in a setup with Cisco VIC 15xxx: • usNIC on the same vNIC • VMMQ on the same vNIC • RDMA v2 on the same vNIC • SR-IOV on the same vNIC • iSCSI boot on the same vNIC • PXE boot on the same vNIC
QinQ VLAN field	Enter a QinQ VLAN ID between 2 and 4094 in the field.

Step 6 In the **Ethernet Interrupt** area, update the following fields:

Name	Description
Interrupt Count field	The number of interrupt resources to allocate. In general, this value should be equal to the number of completion queue resources. Enter an integer between 1 and 1024.

Name	Description
Coalescing Time field	The time to wait between interrupts or the idle period that must be encountered before an interrupt is sent. Enter an integer between 1 and 65535. To turn off interrupt coalescing, enter 0 (zero) in this field.
Coalescing Type drop-down list	This can be one of the following: • **MIN**—The system waits for the time specified in the **Coalescing Time** field before sending another interrupt event. • **IDLE**—The system does not send an interrupt until there is a period of no activity lasting as least as long as the time specified in the **Coalescing Time** field.
Interrupt Mode drop-down list	The preferred driver interrupt mode. This can be one of the following: • **MSI-X**—Message Signaled Interrupts (MSI) with the optional extension. This is the recommended option. • **MSI**—MSI only. • **INTx**—PCI INTx interrupts.

Step 7 In the **TCP Offload** area, update the following fields:

Name	Description
Enable Large Receive check box	If checked, the hardware reassembles all segmented packets before sending them to the CPU. This option may reduce CPU utilization and increase inbound throughput. If cleared, the CPU processes all large packets.
Enable TCP Segmentation Offload check box	If checked, the CPU sends large TCP packets to the hardware to be segmented. This option may reduce CPU overhead and increase throughput rate. If cleared, the CPU segments large packets. **Note** This option is also known as Large Send Offload (LSO).
Enable TCP Rx Offload Checksum Validation check box	If checked, the CPU sends all packet checksums to the hardware for validation. This option may reduce CPU overhead. If cleared, the CPU validates all packet checksums.
Enable TCP Tx Offload Checksum Generation check box	If checked, the CPU sends all packets to the hardware so that the checksum can be calculated. This option may reduce CPU overhead. If cleared, the CPU calculates all packet checksums.

Step 8 In the **Receive Side Scaling** area, update the following fields:

Name	Description
Enable TCP Receive Side Scaling check box	Receive Side Scaling (RSS) distributes network receive processing across multiple CPUs in multiprocessor systems. If checked, network receive processing is shared across processors whenever possible. If cleared, network receive processing is always handled by a single processor even if additional processors are available.
Enable IPv4 RSS check box	If checked, RSS is enabled on IPv4 networks.
Enable TCP-IPv4 RSS check box	If checked, RSS is enabled for TCP transmissions across IPv4 networks.
Enable IPv6 RSS check box	If checked, RSS is enabled on IPv6 networks.
Enable TCP-IPv6 RSS check box	If checked, RSS is enabled for TCP transmissions across IPv6 networks.
Enable IPv6 Extension RSS check box	If checked, RSS is enabled for IPv6 extensions.
Enable TCP-IPv6 Extension RSS check box	If checked, RSS is enabled for TCP transmissions across IPv6 networks.

Step 9

Note Cisco UCS C-Series M7 and later servers have a **Queues** tab.

Review the following:

Name	Description
Enable VMQ check box	Check this box to enable Virtual Machine Queue (VMQ).
Enable Multi Queue check box	Check this box to enable the Multi Queue option on vNICs. When enabled multi queue vNICs will be available to the host. By default this is disabled. • Multi queue is supported only on C-Series servers with 14xx and VIC 15xxx adapters. • VMQ must be in enabled state to enable this option. • When you enable this option on one of the vNICs, configuring only VMQ (without choosing multi-queue) on other vNICs is not supported. • When this option is enabled usNIC configuration will be disabled
Trust Host CoS check box	Check this box if you want the vNIC to use the class of service provided by the host operating system.
No. of Sub vNICs field	Number of sub vNICs available to the host when the multi queue option is enabled.

Step 10 **Note** **Ethernet Receive Queue** is available under **Queues** tab for Cisco UCS C-Series M7 and later servers.

In the **Ethernet Receive Queue** area, update the following fields:

Name	Description
Count field	The number of receive queue resources to allocate. Enter an integer between 1 and 256.
Ring Size field	The number of descriptors in each receive queue. Enter an integer between 64 and 16384. VIC 14xx Series adapters support a 4K (4096) maximum Ring Size VIC15xxx Series adapters support up to 16K Ring Size.

Step 11 **Note** **Ethernet Transmit Queue** is available under **Queues** tab for Cisco UCS C-Series M7 and later servers.

In the **Ethernet Transmit Queue** area, update the following fields:

Name	Description
Count field	The number of transmit queue resources to allocate. Enter an integer between 1 and 256.
Ring Size field	The number of descriptors in each transmit queue. Enter an integer between 64 and 16384. VIC 14xx Series adapters support a 4K (4096) maximum Ring Size VIC15xxx Series adapters support up to 16K Ring Size.

Step 12 **Note** **Completion Queue** is available under **Queues** tab for Cisco UCS C-Series M7 and later servers.

In the **Completion Queue** area, update the following fields:

Name	Description
Count field	The number of completion queue resources to allocate. In general, the number of completion queue resources you should allocate is equal to the number of transmit queue resources plus the number of receive queue resources. Enter an integer between 1 and 512.
Ring Size	The number of descriptors in each completion queue. This value cannot be changed.

Step 13 **Note** **Multi Queue** is available under **Queues** tab for Cisco UCS C-Series M7 and later servers.

In the **Multi Queue** area, update the following details:

Name	Description
Receive Queue Count field	The number of receive queue resources to allocate. Enter an integer between 1 and 1000.
Transmit Queue Count field	The number of transmit queue resources to allocate. Enter an integer between 1 and 1000.
Completion Queue Count field	The number of completion queue resources to allocate. In general, the number of completion queue resources you should allocate is equal to the number of transmit queue resources plus the number of receive queue resources. Enter an integer between 1 and 2000.
RoCE check box	Check the check box to change the RoCE Properties. **Note** If **Multi Queue** RoCE is enabled, ensure that VMQ RoCE is also enabled.
Queue Pairs field	The number of queue pairs per adapter. Enter an integer between 1 and 2048. We recommend that this number be an integer power of 2.
Memory Regions field	The number of memory regions per adapter. Enter an integer between 1 and 524288. We recommend that this number be an integer power of 2.
Resource Groups field	The number of resource groups per adapter. Enter an integer between 1 and 128. We recommend that this number be an integer power of 2 greater than or equal to the number of CPU cores on the system for optimum performance.
Class of Service field	This field is read-only and is set to 5. **Note** This option is available only on some of the adapters.

Step 14

Note **RoCE Properties** is available under **Queues** tab for Cisco UCS C-Series M7 and later servers.

In the **RoCE Properties** area, update the following fields:

Name	Description
RoCE check box	Check the check box to change the RoCE Properties. **Note** If **Multi Queue** RoCE is enabled, ensure that VMQ RoCE is also enabled.
Queue Pairs field	The number of queue pairs per adapter. Enter an integer between 1 and 2048. We recommend that this number be an integer power of 2.
Memory Regions field	The number of memory regions per adapter. Enter an integer between 1 and 524288. We recommend that this number be an integer power of 2.
Resource Groups field	The number of resource groups per adapter. Enter an integer between 1 and 128. We recommend that this number be an integer power of 2 greater than or equal to the number of CPU cores on the system for optimum performance.

Name	Description
Class of Service field	This field is read-only and is set to 5. **Note** This option is available only on some of the adapters.

Step 15 **Note** **SR-IOV Properties** is available under **Queues** tab for Cisco UCS C-Series M7 and later servers.

In the **SR-IOV Properties** area, review the information in the following fields:

Name	Description
No. of VFs field	Enter an integer between 1 and 64. **Note** Other SR-IOV properties are enabled only when you enter an integer between 1 and 64.
Receive Queue Count Per VF field	The number of receive queue resources to allocate. Enter an integer between 1 and 8.
Transmit Queue Count Per VF field	The number of descriptors in each transmit queue. Enter an integer between 1 and 8.
Completion Queue Count Per VF field	The number of completion queue resources to allocate. In general, the number of completion queue resources you should allocate is equal to the number of transmit queue resources plus the number of receive queue resources. Enter an integer between 1 and 16.
Interrupt Count field	The number of interrupt resources to allocate. In general, this value should be equal to the number of completion queue resources. Enter an integer between 1 and 16.

Step 16 Click **Save Changes**.

What to do next

Reboot the server to modify the vNIC.

Creating a vNIC

The Cisco UCS Virtual Interface Cards provide two vHBAs and two vNICs by default. You can create up to 14 additional vHBAs or vNICs on these adapter cards.

The Cisco UCS 1455 and 1457 Virtual Interface Cards, in non-port channel mode, provide four vHBAs and four vNICs by default. You can create up to 10 additional vHBAs or vNICs on these adapter cards.

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

Step 2 In the **Networking** pane, select the Adapter Card SIOC1 or Adapter Card SIOC2 that you want to modify.

Step 3 In the **Adapter Card SIOC1 or Adapter Card SIOC2** pane, click the **vNICs** tab.

Step 4 In the **Host Ethernet Interfaces** area, choose one of these actions:

- To create a vNIC using default configuration settings, click **Add vNIC**.
- To create a vNIC using the same configuration settings as an existing vNIC, select that vNIC and click **Clone vNIC**.

The **Add vNIC** dialog box appears.

Step 5 In the **Add vNIC** dialog box, enter a name for the vNIC in the **Name** entry box.

Step 6 In the **Add vNIC** dialog box, enter a channel number for the vNIC in the **Channel Number** entry box.

Note If VNTAG is enabled on the adapter, you must assign a channel number for the vNIC when you create it.

Step 7 Click **Add vNIC**.

What to do next

If configuration changes are required, configure the new vNIC as described in Modifying vNIC Properties, on page 223.

Deleting a vNIC

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

Step 2 In the **Networking** pane, select the Adapter Card SIOC1 or Adapter Card SIOC2 that you want to modify.

Step 3 In the **Adapter Card SIOC1 or Adapter Card SIOC2** pane, click the **vNICs** tab.

Step 4 In the **Host Ethernet Interfaces** area, select a vNIC from the table.

Note You cannot delete either of the two default vNICs, **eth0** or **eth1**.

Step 5 Click **Delete vNIC** and click **OK** to confirm.

Configuring iSCSI Boot Capability

Configuring iSCSI Boot Capability for vNICs

To configure the iSCSI boot capability on a vNIC:

- You must log in with admin privileges to perform this task.
- To configure a vNIC to boot a server remotely from an iSCSI storage target, you must enable the PXE boot option on the vNIC.

Note You can configure a maximum of 2 iSCSI vNICs for each host.

Configuring iSCSI Boot Capability on a vNIC

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

Step 2 In the **Networking** pane, select the Adapter Card SIOC1 or Adapter Card SIOC2 that you want to modify.

Step 3 In the **Adapter Card SIOC1 or Adapter Card SIOC2** pane, click the **vNICs** tab.

Step 4 In the **vNICs** pane, click **eth0** or **eth1**.

Step 5 Select the **iSCSI Boot Properties** area.

Step 6 In the **General** area, update the following fields:

Name	Description
Name field	The name of the vNIC.
DHCP Network check box	Whether DHCP Network is enabled for the vNIC. If enabled, the initiator network configuration is obtained from the DHCP server.
DHCP iSCSI check box	Whether DHCP iSCSI is enabled for the vNIC. If enabled and the DHCP ID is set, the initiator IQN and target information are obtained from the DHCP server. **Note** If DHCP iSCSI is enabled without a DHCP ID, only the target information is obtained.
DHCP ID field	The vendor identifier string used by the adapter to obtain the initiator IQN and target information from the DHCP server. Enter a string up to 64 characters.
DHCP Timeout field	The number of seconds to wait before the initiator assumes that the DHCP server is unavailable. Enter an integer between 60 and 300 (default: 60 seconds)
Link Timeout field	The number of seconds to wait before the initiator assumes that the link is unavailable. Enter an integer between 0 and 255 (default: 15 seconds)
LUN Busy Retry Count field	The number of times to retry the connection in case of a failure during iSCSI LUN discovery. Enter an integer between 0 and 255. The default is 15.
IP Version field	The IP version to use during iSCSI boot.

Step 7 In the **Initiator** area, update the following fields:

Name	Description
Name field	A regular expression that defines the name of the iSCSI initiator. You can enter any alphanumeric string as well as the following special characters: • . (period) • : (colon) • - (dash) **Note** The name is in the IQN format.
IP Address field	The IP address of the iSCSI initiator.
Subnet Mask field	The subnet mask for the iSCSI initiator.
Gateway field	The default gateway.
Primary DNS field	The primary DNS server address.
Initiator Priority drop-down list	The initiator priority drop-down list.
Secondary DNS field	The secondary DNS server address.
TCP Timeout field	The number of seconds to wait before the initiator assumes that TCP is unavailable. Enter an integer between 0 and 255 (default: 15 seconds)
CHAP Name field	The Challenge-Handshake Authentication Protocol (CHAP) name of the initiator.
CHAP Secret field	The Challenge-Handshake Authentication Protocol (CHAP) shared secret of the initiator.

Step 8 In the **Primary Target** area, update the following fields:

Name	Description
Name field	The name of the primary target in the IQN format.
IP Address field	The IP address of the target.
TCP Port field	The TCP port associated with the target.
Boot LUN field	The Boot LUN associated with the target.
CHAP Name field	The Challenge-Handshake Authentication Protocol (CHAP) name of the initiator.
CHAP Secret field	The Challenge-Handshake Authentication Protocol (CHAP) shared secret of the initiator.

Step 9 In the **Secondary Target** area, update the following fields:

Name	Description
Name field	The name of the secondary target in the IQN format.
IP Address field	The IP address of the target.
TCP Port field	The TCP port associated with the target.
Boot LUN field	The Boot LUN associated with the target.
CHAP Name field	The Challenge-Handshake Authentication Protocol (CHAP) name of the initiator.
CHAP Secret field	The Challenge-Handshake Authentication Protocol (CHAP) shared secret of the initiator.

Name	Description
Configure ISCSI button	Configures iSCSI boot on the selected vNIC.
Unconfigure ISCSI button	Removes the configuration from the selected vNIC.
Reset Values button	Restores the values for the vNIC to the settings that were in effect when this dialog box was first opened.
Cancel button	Closes the dialog box without making any changes.

Step 10 Click **Save Changes**.

Removing iSCSI Boot Configuration from a vNIC

Before you begin

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

Step 1 In the **Navigation** pane, click the **Networking** menu.
Step 2 In the **Networking** pane, select the Adapter Card SIOC1 or Adapter Card SIOC2 that you want to modify.
Step 3 In the **Adapter Card SIOC1 or Adapter Card SIOC2** pane, click the **vNICs** tab.
Step 4 In the **vNICs** pane, click **eth0** or **eth1**.
Step 5 Select the **iSCSI Boot Properties** area.
Step 6 Click the **Unconfigure ISCSI Boot** button at the bottom of the **iSCSI Boot Properties** area.

What to do next

Reboot the server to remove the iSCSI Boot Configuration.

Managing Cisco usNIC

Overview of Cisco usNIC

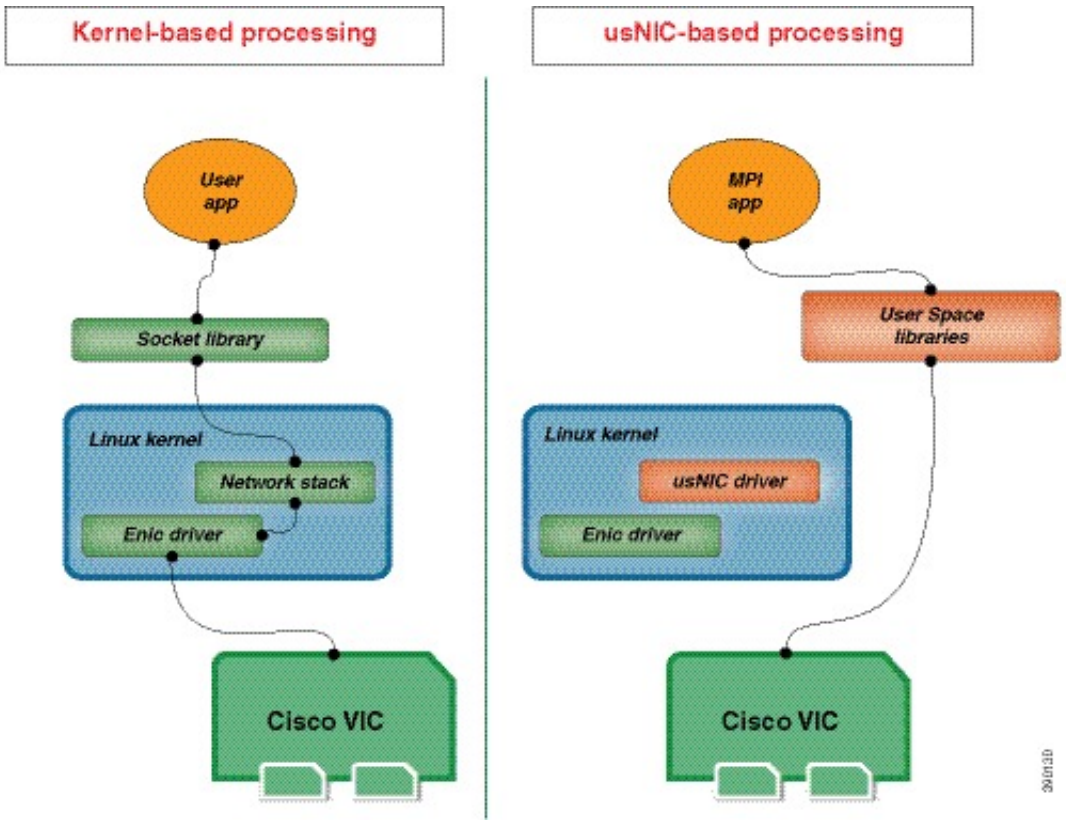
The Cisco user-space NIC (Cisco usNIC) feature improves the performance of software applications that run on the Cisco UCS servers in your data center by bypassing the kernel when sending and receiving networking packets. The applications interact directly with a Cisco UCS VIC second generation or later generation adapter, such as the , which improves the networking performance of your high-performance computing cluster. To benefit from Cisco usNIC, your applications must use the Message Passing Interface (MPI) instead of sockets or other communication APIs.

Cisco usNIC offers the following benefits for your MPI applications:

- Provides a low-latency and high-throughput communication transport.
- Employs the standard and application-independent Ethernet protocol.
- Takes advantage of lowlatency forwarding, Unified Fabric, and integrated management support in the following Cisco data center platforms:
  - Cisco UCS server
  - Cisco UCS VIC second generation or later generation adapter
  - 10 or 40GbE networks

Standard Ethernet applications use user-space socket libraries, which invoke the networking stack in the Linux kernel. The networking stack then uses the Cisco eNIC driver to communicate with the Cisco VIC hardware. The following figure shows the contrast between a regular software application and an MPI application that uses Cisco usNIC.

Figure 1: Kernel-Based Network Communication versus Cisco usNIC-Based Communication



Viewing and Configuring Cisco usNIC using the Cisco IMC GUI

Before you begin

You must log in to the Cisco IMC GUI with admin privileges to perform this task. Click Play on this video to watch how to configure Cisco usNIC in Cisco IMC.

Step 1 Log into the Cisco IMC GUI.

For more information about how to log into Cisco IMC, see Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide.

Step 2 In the **Navigation** pane, click the **Networking** menu.

Step 3 In the **Networking** pane, select the Adapter Card SIOC1 or Adapter Card SIOC2 that you want to modify.

Step 4 In the **Adapter Card SIOC1 or Adapter Card SIOC2** pane, click the **vNICs** tab.

Step 5 In the **vNICs** pane, click **eth0** or **eth1**.

Step 6 In the **usNIC** area, review and update the following fields.

Name	Description
Name	The name for the vNIC that is the parent of the usNIC. **Note** This field is read-only.

Name	Description
usNIC field	The number of usNICs assigned to the specific vNIC. Enter an integer between 0 and 225. To assign additional usNICs to a specified vNIC, enter value higher than the existing value. To delete usNICs from a specified vNIC, enter value smaller than the existing value. To delete all the usNICs assigned to a vNIC, enter zero.
Transmit Queue Count field	The number of transmit queue resources to allocate. Enter an integer between 1 and 256.
Receive Queue Count field	The number of receive queue resources to allocate. Enter an integer between 1 and 256.
Completion Queue Count field	The number of completion queue resources to allocate. In general, the number of completion queue resources you should allocate is equal to the number of transmit queue resources plus the number of receive queue resources. Enter an integer between 1 and 512.
Transmit Queue Ring Size field	The number of descriptors in each transmit queue. Enter an integer between 64 and 4096.
Receive Queue Ring Size field	The number of descriptors in each receive queue. Enter an integer between 64 and 4096.
Interrupt Count field	The number of interrupt resources to allocate. In general, this value should be equal to the number of completion queue resources. Enter an integer between 1 and 514.
Interrupt Coalescing Type drop-down list	This can be one of the following: • **MIN**—The system waits for the time specified in the **Coalescing Time** field before sending another interrupt event. • **IDLE**—The system does not send an interrupt until there is a period of no activity lasting as least as long as the time specified in the **Coalescing Time** field.
Interrupt Coalescing Timer Time field	The time to wait between interrupts or the idle period that must be encountered before an interrupt is sent. Enter an integer between 1 and 65535. To turn off interrupt coalescing, enter 0 (zero) in this field.

Name	Description
Class of Service field	The class of service to associate with traffic from this usNIC. Select an integer between 0 and 6, with 0 being lowest priority and 6 being the highest priority. **Note** This option cannot be used in VNTAG mode.
TCP Segment Offload check box	If checked, the CPU sends large TCP packets to the hardware to be segmented. This option may reduce CPU overhead and increase throughput rate. If cleared, the CPU segments large packets. **Note** This option is also known as Large Send Offload (LSO).
Large Receive check box	If checked, the hardware reassembles all segmented packets before sending them to the CPU. This option may reduce CPU utilization and increase inbound throughput. If cleared, the CPU processes all large packets.
TCP Tx Checksum check box	If checked, the CPU sends all packets to the hardware so that the checksum can be calculated. This option may reduce CPU overhead. If cleared, the CPU calculates all packet checksums.
TCP Rx Checksum check box	If checked, the CPU sends all packet checksums to the hardware for validation. This option may reduce CPU overhead. If cleared, the CPU validates all packet checksums.

Step 7 Click **Save Changes**.

The changes take effect upon the next server reboot.

Viewing usNIC Properties

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

Step 2 In the **Networking** pane, select the Adapter Card SIOC1 or Adapter Card SIOC2 that you want to view.

Step 3 In the **Adapter Card SIOC1 or Adapter Card SIOC2** pane, click the **vNICs** tab.

Step 4 In the **vNICs** pane, click **eth0** or **eth1**.

Step 5 In the **Host Ethernet Interfaces** pane's **usNIC Properties** area, review the information in the following fields:

Name	Description
Name	The name for the vNIC that is the parent of the usNIC. **Note** This field is read-only.
usNIC field	The number of usNICs assigned to the specific vNIC. Enter an integer between 0 and 225. To assign additional usNICs to a specified vNIC, enter value higher than the existing value. To delete usNICs from a specified vNIC, enter value smaller than the existing value. To delete all the usNICs assigned to a vNIC, enter zero.
Transmit Queue Count field	The number of transmit queue resources to allocate. Enter an integer between 1 and 256.
Receive Queue Count field	The number of receive queue resources to allocate. Enter an integer between 1 and 256.
Completion Queue Count field	The number of completion queue resources to allocate. In general, the number of completion queue resources you should allocate is equal to the number of transmit queue resources plus the number of receive queue resources. Enter an integer between 1 and 512.
Transmit Queue Ring Size field	The number of descriptors in each transmit queue. Enter an integer between 64 and 4096.
Receive Queue Ring Size field	The number of descriptors in each receive queue. Enter an integer between 64 and 4096.
Interrupt Count field	The number of interrupt resources to allocate. In general, this value should be equal to the number of completion queue resources. Enter an integer between 1 and 514.
Interrupt Coalescing Type drop-down list	This can be one of the following: • **MIN**—The system waits for the time specified in the **Coalescing Time** field before sending another interrupt event. • **IDLE**—The system does not send an interrupt until there is a period of no activity lasting as least as long as the time specified in the **Coalescing Time** field.

Name	Description
Interrupt Coalescing Timer Time field	The time to wait between interrupts or the idle period that must be encountered before an interrupt is sent. Enter an integer between 1 and 65535. To turn off interrupt coalescing, enter 0 (zero) in this field.
Class of Service field	The class of service to associate with traffic from this usNIC. Select an integer between 0 and 6, with 0 being lowest priority and 6 being the highest priority. **Note** This option cannot be used in VNTAG mode.
TCP Segment Offload check box	If checked, the CPU sends large TCP packets to the hardware to be segmented. This option may reduce CPU overhead and increase throughput rate. If cleared, the CPU segments large packets. **Note** This option is also known as Large Send Offload (LSO).
Large Receive check box	If checked, the hardware reassembles all segmented packets before sending them to the CPU. This option may reduce CPU utilization and increase inbound throughput. If cleared, the CPU processes all large packets.
TCP Tx Checksum check box	If checked, the CPU sends all packets to the hardware so that the checksum can be calculated. This option may reduce CPU overhead. If cleared, the CPU calculates all packet checksums.
TCP Rx Checksum check box	If checked, the CPU sends all packet checksums to the hardware for validation. This option may reduce CPU overhead. If cleared, the CPU validates all packet checksums.

Backing Up and Restoring the Adapter Configuration

Exporting the Adapter Configuration

The adapter configuration can be exported as an XML file to a remote server which can be one of the following:

- TFTP

- FTP
- SFTP
- SCP
- HTTP

Before you begin

Obtain the remote server IP address.

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

Step 2 In the **Networking** pane, select the Adapter Card SIOC1 or Adapter Card SIOC2 that you want to modify.

Step 3 In the **Adapter Card SIOC1 or Adapter Card SIOC2** pane, click the **General** tab.

Step 4 In the **Actions** area of the **General** tab, click **Export vNIC**.

The **Export vNIC** dialog box opens.

Step 5 In the **Export Adapter Configuration** dialog box, update the following fields:

Name	Description
Export To drop-down list	The remote server type. This can be one of the following: • **TFTP Server** • **FTP Server** • **SFTP Server** • **SCP Server** • **HTTP Server** **Note** If you chose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message *Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*. Click Yes or No depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.
IP Address or Host Name field	The IPv4 or IPv6 address, or hostname of the server to which the adapter configuration file will be exported. Depending on the setting in the **Export to** drop-down list, the name of the field may vary.
Path and Filename field	The path and filename Cisco IMC should use when exporting the file to the remote server.
Username	The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP.

Name	Description
Password	The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP.

Step 6 Click **Export vNIC**.

Importing the Adapter Configuration

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

Step 2 In the **Networking** pane, select the Adapter Card SIOC1 or Adapter Card SIOC2 that you want to modify.

Step 3 Select the **General** tab.

Step 4 In the **Actions** area of the **General** tab, click **Import vNIC**.

The **Import vNIC** dialog box is displayed.

Step 5 In the **Import vNIC** dialog box, update the following fields:

Name	Description
Import from drop-down list	The remote server type. This can be one of the following: • **TFTP Server** • **FTP Server** • **SFTP Server** • **SCP Server** • **HTTP Server** **Note** If you chose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message *Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*. Click Yes or No depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.
IP Address or Host Name field	The IPv4 or IPv6 address, or hostname of the server on which the adapter configuration file resides. Depending on the setting in the **Import from** drop-down list, the name of the field may vary.
Path and Filename field	The path and filename of the configuration file on the remote server.
Username	The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP.

Name	Description
Password	The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP.

Step 6 Click **Import vNIC**.

What to do next

Reboot the server to apply the imported configuration.

Restoring Adapter Defaults

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

Step 2 In the **Networking** pane, select the Adapter Card SIOC1 or Adapter Card SIOC2 that you want to restore to default settings.

Step 3 Select the **General** tab.

Step 4 In the **Actions** area of the **General** tab, click **Reset To Defaults** and click **OK** to confirm.

Resetting the Adapter

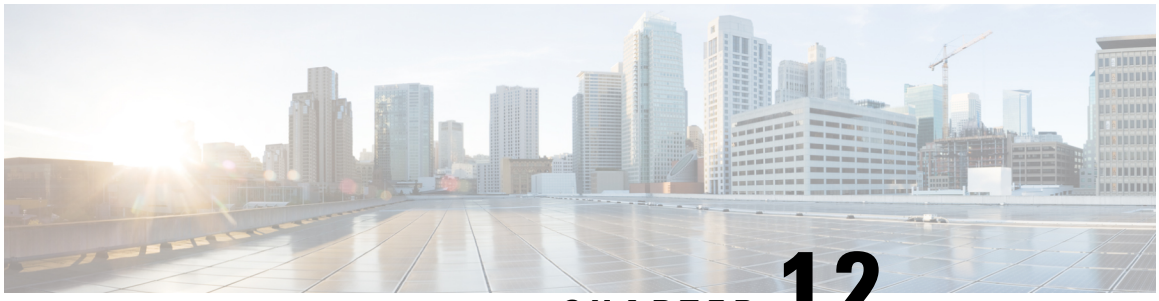
Step 1 In the **Navigation** pane, click the **Networking** menu.

Step 2 In the **Networking** pane, select the Adapter Card SIOC1 or Adapter Card SIOC2 that you want to reset.

Step 3 Select the **General** tab.

Step 4 In the **Actions** area of the **General** tab, click **Reset** and click **OK** to confirm.

Note Resetting the adapter also resets the host.



CHAPTER 12

Managing Storage Adapters

This chapter includes the following sections:

Managing Storage Adapters

Self Encrypting Drives (Full Disk Encryption)

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

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

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

The FDE feature supports the following operations:

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

Scenarios to consider While Configuring Controller Security in a Dual or Multiple Controllers Environment

Note Dual or Multiple controllers connectivity is available only on some servers.

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

Consider the following two scenarios:

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

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

Enabling Controller Security

This option is available only on some C-series servers.

Before you begin

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

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

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

Step 3 In the **Controller Info** area, click **Enable Drive Security**.

Step 4 In the **Enable Drive Security** dialog box, update the following fields:

Name	Description
Controller Security field	Indicates that the controller is disabled.
Key Management field	Indicates whether the key is remotely managed or locally managed. This can be one of the following: • **Remote Key Management** radio button— Controller security key is configured or managed using the remote KMIP server. **Note** If you choose this option, you do not have to specify the existing security key but you have to provide the key ID and the security key for local management. • **Local Key Management** radio button— Controller security is configured locally.

Name	Description
Security Key Identifier field	The current key ID.
Security Key field	Security key used to enable controller security. If you wish to change the current security key, enter the new key here. **Note** Once you change the security key, a **Secure Key Verification** pop-up window appears where you need to enter the current security key to verify it.
Confirm Security Key field	Re-enter the security key.
Suggest button	Suggests the security key or key ID that can be assigned.

Step 5 Click **Save**.

This enables controller security.

Modifying Controller Security

This option is available only on some C-series servers.

Before you begin

- You must log in with admin privileges to perform this task.
- You must have first enabled controller security to modify it.

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

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

Step 3 In the **Controller Info** area, click **Modify Drive Security**.

Step 4 In the **Modify Drive Security** dialog box, update the following fields:

Name	Description
Controller Security field	Indicates whether or not controller security is enabled. This can be one of the following: • **Enabled**— Controller security is enabled. • **Disabled**— Controller security is disabled.
Security Key Identifier field	The current key ID.
Security Key field	Security key used to enable controller security. If you wish to change the current security key, enter the new key here. **Note** Once you change the security key, a **Secure Key Verification** pop-up window appears where you need to enter the current security key to verify it.

Name	Description
Confirm Security Key field	Re-enter the security key.
Modify Security Key check box	**Note** This option appears only for remote key management. If you select this option the security key on the KMIP server is modified.
Suggest button	Suggests the security key or key ID that can be assigned.
Save button	Saves the data.
Cancel button	Cancels the action.

Step 5 Click **Save**.

This modifies the controller security settings.

Disabling Controller Security

This option is available only on some C-series servers.

Before you begin

- You must log in with admin privileges to perform this task.
- You must have first enabled controller security to disable it.

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

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

Step 3 In the **Controller Info** area, click **Disable Drive Security**.

Step 4 Click **OK** in the confirmation pop-up window.

This disables controller security.

Switching Controller Security Between Local and Remote Key Management

This task allows you to switch controller security from local management to remote management, and from remote to local management.

Before you begin

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

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

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

Step 3 In the **Controller Info** area, to switch the controller security from remote to local management, click **Switch to Local Key Management**.

Note When you switch from remote to local key management, ensure that you disable KMIP secure key management first.

Step 4 (Optional) Similarly, if you want to switch the controller security from local to remote management, click **Switch to Remote Key Management**.

Step 5 Click **OK** to confirm.

Creating Virtual Drive from Unused Physical Drives

Before you begin

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

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

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

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

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

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

This can be one of the following:

- **Raid 0**—Simple striping.
- **Raid 1**—Simple mirroring.
- **Raid 5**—Striping with parity.
- **Raid 6**—Striping with two parity drives.
- **Raid 10**—Spanned mirroring.
- **Raid 50**—Spanned striping with parity.
- **Raid 60**—Spanned striping with two parity drives.

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

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

Note

- The size of the smallest physical drive in the drive group defines the maximum size used for all the physical drives. To ensure maximum use of space for all physical drives, it is recommended that the size of all the drives in the drive group are similar.
- Cisco IMC manages only RAID controllers and not HBAs attached to the server.
- You must have multiple drive groups available to create virtual drives for certain RAID levels. While creating drives for these RAID levels, the create drive option is available only if the required number of drives are selected.

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

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

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

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

Step 8 Click **Close**.

Step 9 Click **Create Virtual Drive**.

Creating Virtual Drive from an Existing Drive Group

Before you begin

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

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

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

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

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

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

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

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

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

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

Step 7 Click **Close**.

Step 8 Click **Create Virtual Drive**.

Setting a Virtual Drive to Transport Ready State

You can move a virtual drive from one MegaRAID controller to another using the **Set Transport Ready** feature. This allows all the pending IOs of the virtual drive to complete their activities, hide the virtual drive from the operating system, flush cache, pause all the background operations, and save the current progress in disk data format, allowing you to move the drive. When you move a virtual drive, all other drives belonging to the same drive group inherit the same change as the moved drive.

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

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

Following restrictions apply to a transport ready virtual drive:

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

Setting a Virtual Drive as Transport Ready

Before you begin

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

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

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

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

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

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

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

Step 6 Update the following properties in the dialog box:

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

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

Clearing a Virtual Drive from Transport Ready State

Before you begin

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

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

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

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

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

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

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

Importing Foreign Configuration

When one or more physical drives that have previously been configured with a different controller are inserted into a server, they are identified as foreign configurations. You can import these foreign configurations to a controller.

Important You cannot import a foreign configuration in the following two scenarios:

1. When the secure virtual drive was created on server 1 (from which you want to import the configuration) using the remote key, and on server 2 (to which you want to import) using the local key.
2. When server 2 is configured with another KMIP server, which is not a part of the server 1 KMIP server cluster.

In order to import the foreign configuration in these scenarios, change the controller security on server 2 from local key management to remote key management, and use the same KMIP server from the same cluster where the server 1 KMIP is configured.

Before you begin

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

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

Step 2 In the **RAID controller** area, the **Controller Info** tab displays by default.

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

Note If KMIP is not enabled, a **Secure Key Verification** dialog box is displayed, prompting you to enter a security key to initiate the foreign configuration import process.

If KMIP is enabled, the **Secure Key Verification** dialog box is displayed with the following note: *"If drive security has been enabled via remote key management, specifying Security key is optional. Click on verify to start foreign configuration import."*

This allows you to click **Verify** without entering the Security Key, and initiate import.

Step 4 Click **OK** to confirm.

Clearing Foreign Configuration

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

Before you begin

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

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

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

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

Step 4 Click **OK** to confirm.

Clearing a Boot Drive

Important This task clears the boot drive configuration on the controller. This action cannot be reverted.

Before you begin

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

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

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

Step 3 In the **Actions** area, click **Clear Boot Drive**.

Step 4 Click **OK** to confirm.

Enabling JBOD Mode

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

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

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

Step 4 In the **Physical Drives** area, select an unconfigured good drive.

Step 5 In the **Actions** area, click **Enable JBOD**.

Step 6 Click **Ok** to confirm.

Disabling a JBOD

Note This option is available only on some UCS C-Series servers.

Before you begin

JBOD option must be enabled for the selected controller.

Step 1 In the **Navigation** pane, click the **Storage** menu.
Step 2 On the **Storage** menu, click the appropriate LSI MegaRAID or HBA controller.
Step 3 In the **RAID Controller** area, click the **Physical Drive Info** tab.
Step 4 In the **Physical Drives** area, select a JBOD drive.
Step 5 In the **Actions** area, click **Disable JBOD**.
Step 6 Click **Ok** to confirm.

Retrieving Storage Firmware Logs for a Controller

This task retrieves the storage firmware logs for the controller and places it in the `/var/log` location. This ensures that this log data is available when Technical Support Data is requested.

Before you begin

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

Step 1 In the **Navigation** pane, click the **Storage** menu.
Step 2 In the working area, the **Controller Info** tab displays by default.
Step 3 In the **Actions** area, click **Get Storage Firmware Log**.
Step 4 Click **OK** to confirm.

Important Retrieving storage firmware logs for a controller could take up to 2-4 minutes. Until this process is complete, do not initiate exporting technical support data.

Clearing Controller Configuration

Before you begin

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

Step 1 In the **Navigation** pane, click the **Storage** menu.
Step 2 In the **Storage** menu, click the appropriate LSI MegaRAID or HBA controller.
Step 3 In the **Controller Info** area, click **Clear All Configuration**.
Step 4 Click **OK** to confirm.

This clears the existing controller configuration.

Restoring Storage Controller to Factory Defaults

Before you begin

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

Step 1 In the **Navigation** pane, click the **Storage** menu.
Step 2 In the **Storage** menu, click the appropriate LSI MegaRAID or HBA controller.
Step 3 In the **Controller Info** area, click **Set Factory Defaults**.
Step 4 Click **OK** to confirm.

This restores the controller configuration to factory defaults.

Preparing a Drive for Removal

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

Before you begin

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

Step 1 In the **Navigation** pane, click the **Storage** menu.
Step 2 On the **Storage** menu, click the appropriate LSI MegaRAID or HBA controller.
Step 3 In the **RAID Controller** area, click the **Physical Drive Info** tab.
Step 4 In the **Physical Drives** area, select the drive you want to remove.
Step 5 In the **Actions** area, click **Prepare for Removal**.
Step 6 Click **OK** to confirm.

Undo Preparing a Drive for Removal

Before you begin

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

Step 1 In the **Navigation** pane, click the **Storage** menu.
Step 2 On the **Storage** menu, click the appropriate LSI MegaRAID or HBA controller.
Step 3 On the **RAID Controller** area, click the **Physical Drive Info** tab.
Step 4 In the **Physical Drives** area, select a drive with a status of **Ready to Remove**.

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

Step 6 Click **OK** to confirm.

Making a Dedicated Hot Spare

Before you begin

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

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

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

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

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

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

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

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

Name	Description
Virtual Drive Number drop-down list	Select the virtual drive to which you want to dedicate the physical drive as hot spare.
Virtual Drive Name field	The name of the selected virtual drive.
Make Dedicated Hot Spare button	Creates the dedicated hot spare.
Cancel button	Closes the dialog box without saving any changes made while the dialog box was open.

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

Making a Global Hot Spare

Before you begin

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

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

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

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

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

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

Removing a Drive from Hot Spare Pools

Before you begin

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

Step 1 In the **Navigation** pane, click the **Storage** menu.
Step 2 On the **Storage** tab, click the appropriate LSI MegaRAID controller.
Step 3 On the **Work** pane, click the **Physical Drive Info** tab.
Step 4 In the **Physical Drives** area, select the global or dedicated hot spare you want to remove from the hot spare pools.
Step 5 In the **Actions** area, click **Remove From Hot Spare Pools**.

Toggling Physical Drive Status

Before you begin

- You must log in with admin privileges to perform this task.
- The controller must support the JBOD mode and the JBOD mode must be enabled.

Step 1 In the **Navigation** pane, click the **Storage** tab.
Step 2 On the **Storage** menu, click the appropriate LSI MegaRAID or HBA controller.
Step 3 In the **RAID Controller** area, click the **Physical Drive Info** tab.
Step 4 In the **Physical Drives** area, select the drive you want to set as unconfigured good.
Step 5 In the **Actions** area, click **Set State as Unconfigured Good**.
Step 6 Click **OK** to confirm that the JBOD mode be disabled.

The **Set State as JBOD** option is enabled.

Step 7 To enable the JBOD mode for the physical drive, click **Set State as JBOD**.
Step 8 Click **OK** to confirm.

The **Set State as Unconfigured Good** option is enabled.

Setting a Physical Drive as a Controller Boot Drive

Before you begin

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

- The controller must support the JBOD mode and the JBOD mode must be enabled.

Step 1 In the **Navigation** pane, click the **Storage** menu.
Step 2 On the **Storage** menu, click the appropriate LSI MegaRAID or HBA controller.
Step 3 In the **RAID Controller** area, click the **Physical Drive Info** tab.
Step 4 In the **Physical Drives** area, select the drive you want to set as boot drive for the controller.
Step 5 In the **Actions** area, click **Set as Boot Drive**.
Step 6 Click **OK** to confirm.

Initializing a Virtual Drive

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

Before you begin

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

Step 1 In the **Navigation** pane, click the **Storage** menu.
Step 2 On the **Storage** menu, click the appropriate LSI MegaRAID or HBA controller.
Step 3 In the **RAID Controller** area, click the **Virtual Drive Info** tab.
Step 4 In the **Virtual Drives** area, choose the drive that you want to initialize.
Step 5 In the **Actions** area, click **Initialize**.

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

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

This can be one of the following:

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

Step 7 Click **Initialize VD** to initialize the drive, or **Cancel** to close the dialog box without making any changes.
Step 8 To view the status of the task running on the drive, in the **Operations** area, click **Refresh**.

The following details are displayed:

Name	Description
Operation	Name of the operation that is in progress on the drive.
Progress in %	Progress of the operation, in percentage complete.

Name	Description
Elapsed Time in secs	The number of seconds that have elapsed since the operation began.

Set as Boot Drive

Before you begin

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

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

Editing a Virtual Drive

Step 1 In the **Navigation** pane, click the **Storage** menu.
Step 2 On the **Storage** menu, click the appropriate LSI MegaRAID or HBA controller.
Step 3 In the **RAID Controller** area, click the **Virtual Drive Info** tab.
Step 4 In the **Virtual Drives** area, click **Edit Virtual Drive**.
Step 5 Review the instructions, and then click **OK**.
The **Edit Virtual Drive** dialog box displays before prompting you to take a backup of your data.
Step 6 From the **Select RAID Level to migrate** drop-down list, choose a RAID level.

See the following table for RAID migration criteria:

Name	Description
Select RAID Level to migrate drop-down list	Select the RAID level to which you want to migrate. Migrations are allowed for the following RAID levels: • **RAID 0** to **RAID 1** • **RAID 0** to **RAID 5** • **RAID 0** to **RAID 6** • **RAID 1** to **RAID 0** • **RAID 1** to **RAID 5** • **RAID 1** to **RAID 6** • **RAID 5** to **RAID 0** • **RAID 6** to **RAID 0** • **RAID 6** to **RAID 5** When you are migrating from one raid level to another, the data arms of the new RAID level should be equal to or greater than the existing one. In case of RAID 6, the data arms will be number of drives minus two, as RAID 6 has double distributed parity. For example, when you create RAID 6 with eight drives, the number of data arms will be 8 – 2 = 6. In this case, if you are migrating from RAID 6 to RAID 0, RAID 0 must have a minimum of six drives. If you select lesser number of drives then **Edit** or **Save** button will be disabled. If you are adding, you can migrate to RAID 0 as you will not be deleting any drives. **Note** RAID level migration is not supported in the following cases: • When there are multiple virtual drives in a RAID group. • With a combination of SSD/HDD RAID groups.

Step 7 From the **Write Policy** drop-down list in the **Virtual Drive Properties** area, choose one of the following:

- **Write Through**— Data is written through the cache and to the physical drives. Performance is improved, because subsequent reads of that data can be satisfied from the cache.
- **Write Back**— Data is stored in the cache, and is only written to the physical drives when space in the cache is needed. Virtual drives requesting this policy fall back to **Write Through** caching when the BBU cannot guarantee the safety of the cache in the event of a power failure.
- **Write Back Bad BBU**—With this policy, write caching remains **Write Back** even if the battery backup unit is defective or discharged.

Step 8 Click **Save Changes**.

Deleting a Virtual Drive

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

Before you begin

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

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

Hiding a Virtual Drive

Before you begin

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

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

Starting Learn Cycles for a Battery Backup Unit

Before you begin

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

Step 1 In the **Navigation** pane, click the **Storage** menu.
Step 2 On the **Storage** menu, click the appropriate LSI MegaRAID or HBA controller.
Step 3 In the **RAID Controller** area, click the **Battery Backup Unit** tab.

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

A dialog prompts you to confirm the task.

Step 5 Click **OK**.

Viewing Storage Controller Logs

Before you begin

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

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

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

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

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

Viewing SSD Smart Information for MegaRAID Controllers

You can view smart information for a solid state drive. Complete these steps:

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

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

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

Step 4 In the **Smart Information** area, review the following information:

Name	Description
Power Cycle Count field	Number of power cycles that the drive went through from the time it was manufactured.
Power on Hours field	Total number of hours that the drive is in the 'Power On' mode.
Percentage Life Left field	The number of write cycles remaining in a solid state drive (SSD). For instance, if an SSD is capable of 100 write cycles during its life time, and it has completed 15 writes, then the percentage of life left in the drive is 85%. Each percentage range is represented in a different color. For instance, green for 75% to 100% and red for 1 to 25%.
Wear Status in Days field	The number of days an SSD has gone through with the write cycles. SSD vendors provide a finite number of writes per day on the SSD, based on which, you can calculate the total number of years the SSD would continue to work.
Operating Temperature field	The current temperature of the drive at which the selected SSD operates at the time of selection.
Percentage Reserved Capacity Consumed field	The total capacity (out of the percentage reserved for it) consumed by the SSD.
Time of Last Refresh field	Time period since the drive was last refreshed.

Viewing NVMe Controller Details

Before you begin

- The server must be powered on.

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

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

Step 3 In the **Controller** area, the **Controller Info** tab displays by default.

Step 4 In the **Work** pane's **Health/Status** area, review the following information:

Name	Description
Composite Health field	The health of the controller. This can be one of the following: • **Good**- All the drives under the controller is in optimal state. • **Severe Fault**- When one or more drives under the controller is in faulty state. • **N/A**
Drive Count field	The number of drives configured on the controller.

Step 5 In the **Manufacturer Information** area, review the following information:

Name	Description
Vendor ID field	The vendor ID of the NVMe controller.
Product ID field	The controller product ID.
Component ID field	The component ID of the NVMe controller.
Product Revision field	The board revision number, if any.

Step 6 In the **Group PCI Info** area, review the following information:

Name	Description
Vendor ID field	The PCI vendor ID, in hexadecimal.
Device ID field	The PCI device ID, in hexadecimal.

Step 7 In the **Group Firmware Information** area, review the following information:

Name	Description
Running Firmware Images field	NVMe drive fimware version.

Step 8 In the **Group Switch Information** area, review the following information:

Name	Description
Temperature field	Temperature in degree centigrade of the switch.
Switch Status field	The current status of the switch. This can be one of the following: • **Optimal** — The controller is functioning properly. • **Failed** — The controller is not functioning. • **Unresponsive** — The controller is down.

Name	Description
Link Status field	The current status of the link. This field indicates if any of the upstream or downstream links in the switch are down. Individual drive also has a link status that can then be used to identify which drive causes the switch link status to be Link Degraded. This can be one of the following: • **Optimal** — The controller is functioning properly. • **Failed** — The controller is not functioning. • **Unresponsive** — The controller is down.
Shutdown Temperature field	This is the temperature beyond which the safe operation of switch is not guaranteed and recommends shutting down the system.

Viewing NVMe Physical Drive Details

Before you begin

- The server must be powered on.

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

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

Step 3 Click **Physical Drive** tab and review the following information:

Name	Description
Physical Drives column	The list of available physical drives.
PCI Slot column	The PCI slot number in which the physical drive resides.
Managed ID column	Internal ID referenced in debug.
Product Name column	The name of the drive as assigned by the vendor.
Firmware Version column	The firmware version running on the drive.
Vendor column	The drive vendor name.
Serial Number column	Drive serial number.

Step 4 **Physical Drives** Details

Note These details of a physical drive are displayed when you expand one of the listed physical drives.

Name	Description
PCI Slot field	The PCI slot number in which the physical drive resides.
Managed ID field	Internal ID referenced in debug.
Throttle State field	The state of the throttle.
Serial Number field	Controller serial number.
Chip Temperature field	Temperature of the drive in degree centigrade. This is the max temperature read from internal sensors in the drive.
Percentage Drive Life Used field	The percentage of the drive life that is used up.
Device ID field	The PCI device ID, in hexadecimal.
Sub Device ID field	The PCI subdevice ID, in hexadecimal.
Drive Status field	Status of the drive.
Performance Level field	Indicates the performance of the drive.
Shutdown Temperature field	Temperature at which the drive shuts down.
Percentage of Total Power On Hours field	The percentage of time the drive was powered on.
Vendor ID field	The PCI vendor ID, in hexadecimal.
SubVendor ID field	The PCI subvendor ID, in hexadecimal.
LED Fault Status field	The status of the LED fault.
Controller Temperature field	Temperature of the controller in degree centigrade. This is the overall composite temperature of the NVMe subsystem ID.
Running Firmware Images field	NVMe drive fimware version.
Throttle Start Temperature field	Temperature at which the drive starts to throttle.

Starting Copyback Operation

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

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

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

Step 4 In the **Physical Drives** area, select a drive, which is in online state.

Step 5 In the **Actions** area, click **Start Copyback**.

Step 6 A **Start Copyback Operation** dialog box appears.

Step 7 Select the **Destination Physical Drive** to which the copyback operation needs to be done.

Step 8 Click **Start Copyback**.

Step 9 You can also perform the following copyback operations:

- **Pause Copyback** - If the drive is in copyback state, you can pause the copyback operation.
- **Resume Copyback**- The paused copyback operation can be resumed.
- **Abort Copyback** - If the drive is in copyback state, you can abort the copyback operation.

Managing the Flexible Flash Controller

Cisco Flexible Flash

On the M5 servers, Flexible Flash Controller is inserted into the mini storage module socket. The mini storage socket is inserted into the M.2 slot on the motherboard. M.2 slot also supports SATA M.2 SSD slots.

Note M.2 slot does not support NVMe in this release.

Some C-Series Rack-Mount Servers support an internal Secure Digital (SD) memory card for storage of server software tools and utilities. The SD card is hosted by the Cisco Flexible Flash storage adapter.

The SD storage is available to Cisco IMC as a single hypervisor (HV) partition configuration. Prior versions had four virtual USB drives. Three were preloaded with Cisco UCS Server Configuration Utility, Cisco drivers and Cisco Host Upgrade Utility, and the fourth as user-installed hypervisor. A single HV partition configuration is also created when you upgrade to the latest version of Cisco IMC or downgrade to the prior version, and reset the configuration.

For more information about installing and configuring the M.2 drives, see the **Storage Controller Considerations (Embbeded SATA RAID Requirements)** and **Replacing an M.2 SSD in a Mini-Storage Carrier For M.2** sections in the Cisco UCS Server Installation and Service Guide for the C240 M5 servers at this URL:

https://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-c-series-rack-servers/products-installation-guides-list.html

For information about the Cisco software utilities and packages, see the *Cisco UCS C-Series Servers Documentation Roadmap* at this URL:

http://www.cisco.com/go/unifiedcomputing/c-series-doc

Card Management Feature in the Cisco Flexible Flash Controller

The Cisco Flexible Flash controller supports management of both single and two SD cards as a RAID-1 pair. With the introduction of card management, you can perform the following tasks:

Note

- If you want to upgrade from version 1.4(5e) to 1.5(4) or higher versions, you must first upgrade to version1.5(2) and then upgrade to a higher version of Cisco IMC.
- Reset the Cisco Flexible Flash controller to load the latest Flex Flash firmware after every Cisco IMC firmware upgrade.

Action	Description
Reset Cisco Flex Flash	Allows you to reset the controller.
Reset Partition Defaults	Allows you to reset the configuration in the selected slot to the default configuration.
Synchronize Card Configuration	Allows you to retain the configuration for an SD card that supports firmware version 253 and later.
Configure Operational Profile	Allows you to configure the SD cards on the selected Cisco Flexible Flash controller.

RAID Partition Enumeration

Non-RAID partitions are always enumerated from the primary card and the enumeration does not depend on the status of the primary card.

Following is the behavior of the RAID partition enumeration when there are two cards in the Cisco Flexible Flash controller:

Scenario	Behavior
Single card	RAID partitions are enumerated if the card is healthy, and if the mode is either **Primary** or **Secondary-active**.
Dual paired cards	RAID partitions are enumerated if one of the cards is healthy. When only one card is healthy, all read/write operations occur on this healthy card. You must use UCS SCU to synchronize the two RAID partitions.
Dual unpaired cards	If this scenario is detected when the server is restarting, then neither one of the RAID partitions is enumerated. If this scenario is detected when the server is running, when a user connects a new SD card, then the cards are not managed by the Cisco Flexible Flash controller. This does not affect the host enumeration. You must pair the cards to manage them. You can pair the cards using the **Reset Partition Defaults** or **Synchronize Card Configuration** options.

Upgrading from Single Card to Dual Card Mirroring with FlexFlash

You can upgrade from a single card mirroring to dual card mirroring with FlexFlash in one of the following methods:

- Add an empty FlexFlash card to the server, and then upgrade its firmware to the latest version.
- Upgrade the FlexFlash firmware to the latest version and then add an empty card to the server.

Prior to using either of these methods, you must keep in mind the following guidelines:

- To create RAID1 mirroring, the empty card that you want to add to the server must be of the exact size of the card that is already in the server. Identical card size is a must to set up RAID1 mirroring.
- Ensure that the card with valid data in the Hypervisor partition is marked as the primary healthy card. You can determine this state either in the Cisco IMC GUI or from the Cisco IMC CLI. To mark the state of the card as primary healthy, you can either use the **Reset Configuration** option in the Cisco IMC GUI or run the **reset-config** command in the Cisco IMC CLI. When you reset the configuration of a particular card, the secondary card is marked as secondary active unhealthy.
- In a Degraded RAID health state all read-write transactions are done on the healthy card. In this scenario, data mirroring does not occur. Data mirroring occurs only in the Healthy RAID state.
- Data mirroring is only applicable to RAID partitions. In the C-series servers, only Hypervisor partitions operate in the RAID mode.
- If you have not configured SD cards for use with prior versions, then upgrading to the latest version loads the latest 253 firmware and enumerates all four partitions to the host.

While upgrading versions of the FlexFlash, you may see the following error message:

```
Unable to communicate with Flexible Flash controller: operation ffCardsGet, status
CY_AS_ERROR_INVALID_RESPONSE"
```

In addition, the card status may be shown as **missing**. This error occurs because you accidently switched to an alternate release or a prior version, such as 1.4(x). In this scenario, you can either revert to the latest version, or you can switch back to the FlexFlash 1.4(x) configuration. If you choose to revert to the latest Cisco IMC version, then the Cisco FlexFlash configuration remains intact. If you choose to switch back to the prior version configuration, you must reset the Flexflash configuration. In this scenario, you must be aware of the following:

- If multiple cards are present, and you revert to a prior version, then the second card cannot be discovered or managed.
- If the card type is SD253, then you must run the **reset-config** command twice from the Cisco IMC CLI - once to reload the old firmware on the controller and to migrate SD253 to SD247 type, and the second time to start the enumeration.

Configuring the Flexible Flash Controller Properties

After you upgrade to the latest verison of Cisco IMC or downgrade to a prior version, and reset the configuration, the server will access HV partition only.

Before you begin

- You must log in with admin privileges to perform this task.
- Cisco Flexible Flash must be supported by your platform.

Note This task results in the host re-scanning all the virtual drives, and a loss of virtual drive connectivity. We recommend that you configure the Cisco Flexible Flash controller properties before using any virtual drives, or power down the host prior to starting this task

Configuring the Flexible Flash Controller Firmware Mode

Before you begin

- You must log in with admin privileges to perform this task.
- Cisco Flexible Flash must be supported by your platform.

Note This task results in the host re-scanning all the virtual drives, and a loss of virtual drive connectivity. We recommend that you configure the Cisco Flexible Flash controller properties before using any virtual drives, or power down the host prior to starting this task.

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

Step 2 On the **Storage** tab, click **Cisco FlexFlash**.

Step 3 In the **Actions** area, click **Configure Firmware Mode**.

Step 4 Click **OK** in the confirmation box.

Switches the controller firmware mode from the current firmware mode to the other.

Configuring the Flexible Flash Controller Cards

Before you begin

- You must log in with admin privileges to perform this task.
- Cisco Flexible Flash must be supported by your platform.

Note This task results in the host re-scanning all the virtual drives, and a loss of virtual drive connectivity. We recommend that you configure the Cisco Flexible Flash controller properties before using any virtual drives, or power down the host prior to starting this task.

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

Step 2 On the **Storage** tab, click **Cisco FlexFlash**.

Step 3 In the **Actions** area, click **Configure Cards**.
Configure Cards dialog box appears.

Step 4 In the **Configure Cards** dialog box, update the following fields:

Name	Description
Mirror radio button	Enter the following: • **Mirror Partition Name** field—The name that you want to assign to the partition. • **Auto Sync** checkbox—If selected, data from the selected primary card will sync automatically with the secondary card. **Note** • There must be two cards for you to choose this option. • If this option is selected, data on the secondary card is erased and overwritten by the data on the primary card. • The status of this is displayed under the **Physical Driver Info** tab. • **Select Primary Card** drop-down—Slot that you want to set as the primary card. This can be one of the following: • **Slot1** • **Slot2**

Name	Description
Util radio button	Select this option to configure the card in **Util** mode. When you configure the cards in the Util mode, the following situations occur: • The card in the selected slot creates four partitions that has a partition each for the utilities: SCU, HUU, Drivers and one partition that can be used by the user and the card is marked healthy. • The card in the other slot, if it exists, creates a single partition and the card is marked healthy. • The card read/write error counts and read/write threshold are set to 0. • Host connectivity could be disrupted. • The configured cards will be paired. Enter the following: • **User Partition Name** field—The name that you want to assign to the fourth partition of the Util card. • **Non Util Card Partition Name** field—The name that you want to assign to the single partition on the second card, if it exists. • **Select Util Card** drop-down—Slot that you want to set for Util. This can be one of the following: • **Slot1** • **Slot2** • **None**—Applicable only when the server has one SD card.

Step 5 Click **Save**.

The cards are configured in the chosen mode.

Booting from the Flexible Flash Card

You can specify a bootable virtual drive on the Cisco Flexible Flash card that overrides the default boot priority the next time that the server is restarted, regardless of the default boot order defined for the server. The specified boot device is used only once. After the server has rebooted, this setting is ignored. You can choose a bootable virtual drive only if a Cisco Flexible Flash card is available. Otherwise, the server uses a default boot order.

Note Before you reboot the server, ensure that the virtual drive that you select is enabled on the Cisco Flexible Flash card. Go to the **Storage** tab, choose the card, and then go to the **Virtual Drive Info** subtab.

Before you begin

- You must log in with admin privileges to perform this task.
- Cisco Flexible Flash must be supported by your platform.

Step 1 In the **Navigation** pane, click the **Server** tab.
Step 2 On the **Server** tab, click **BIOS**.
Step 3 In the **Actions** area, click **Configure Boot Override Priority**.

The **Boot Override Priority** dialog box appears.

Step 4 From the **Boot Override Priority** drop-down list, choose a virtual drive to boot from.
Step 5 Click **Apply**.

Resetting the Flexible Flash Controller

In normal operation, it should not be necessary to reset the Cisco Flexible Flash. We recommend that you perform this procedure only when explicitly directed to do so by a technical support representative.

Note This operation will disrupt traffic to the virtual drives on the Cisco Flexible Flash controller.

Before you begin

- You must log in with admin privileges to perform this task.
- Cisco Flexible Flash must be supported by your platform.

Step 1 On the **Storage Adapters** pane, click **Cisco FlexFlash**.
Step 2 In the **Cisco FlexFlash** pane, click the **Controller Info** tab.
Step 3 In the **Actions** area, click **Reset FlexFlash Controller**.
Step 4 Click **OK** to confirm.

Enabling Virtual Drives

Before you begin

- You must log in with admin privileges to perform this task.
- Cisco Flexible Flash must be supported by your platform.

Note This task results in the host re-scanning all the virtual drives, and a loss of virtual drive connectivity. We recommend that you configure the Cisco Flexible Flash controller properties before using any virtual drives.

Step 1 In the **Navigation** pane, click the **Storage** tab.
Step 2 On the **Storage** tab, click **Cisco FlexFlash**.
Step 3 Click the **Virtual Drive Info** tab.
Step 4 In the **Virtual Drive Info** tab, click **Enable/Disable Virtual Drive(s)**.
Step 5 In the **Enable/Disable VD(s)** dialog box, select the virtual drives that you want to enable.
Step 6 Click **Save**.
The selected virtual drives are enabled to the host.

Erasing Virtual Drives

Before you begin

- You must log in with admin privileges to perform this task.
- Cisco Flexible Flash must be supported by your platform.

Note This task results in the host re-scanning all the virtual drives, and a loss of virtual drive connectivity. We recommend that you configure the Cisco Flexible Flash controller properties before using any virtual drives.

Step 1 In the **Navigation** pane, click the **Storage** tab.
Step 2 On the **Storage** tab, click **Cisco FlexFlash**.
Step 3 Click the **Virtual Drive Info** tab.
Step 4 In the **Virtual Drive Info** tab, click **Erase Virtual Drive(s)**.
Step 5 In the **Erase Virtual Drive(s)** dialog box, select the virtual drives that you want to erase.
Step 6 Click **Save**.
Data on the selected virtual drives is erased.

Syncing Virtual Drives

Before you begin

- You must log in with admin privileges to perform this task.
- Cisco Flexible Flash must be supported by your platform.

- Cards must be in mirror mode.

Note This task results in the host re-scanning all the virtual drives, and a loss of virtual drive connectivity. We recommend that you configure the Cisco Flexible Flash controller properties before using any virtual drives.

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

Step 2 On the **Storage** tab, click **Cisco FlexFlash**.

Step 3 Click the **Virtual Drive Info** tab.

Step 4 In the **Virtual Drive Info** tab, click **Sync Virtual Drive**.

Step 5 Click **OK** in the confirmation dialog box.
Syncs the virtual drive hypervisor with the primary card.

Adding an ISO Image Configuration

Before you begin

- You must log in with admin privileges to perform this task.
- Cisco Flexible Flash must be supported by your platform.
- The cards must be configured in Util mode.

Note This task results in the host re-scanning all the virtual drives, and a loss of virtual drive connectivity. We recommend that you configure the Cisco Flexible Flash controller properties before using any virtual drives, or power down the host prior to starting this task.

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

Step 2 On the **Storage** tab, click **Cisco FlexFlash**.

Step 3 Click the **Virtual Drive Info** tab.

Step 4 In the **Virtual Drive Info** tab, select the virtual drive for which you want to add an image, click **Add Image**.

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

Name	Description
Volume field	The identity of the image mounted for mapping. This can be one of the following: • **SCU** • **HUU** • **Drivers**

Name	Description
Mount Type drop-down list	The type of mapping. This can be one of the following: • **NFS**—Network File System. • **CIFS**—Common Internet File System.
Remote Share field	The URL of the image to be mapped. The format depends on the selected **Mount Type**: • **NFS**—Use **`serverip:/share path`**. • **CIFS**—Use **`//serverip/share path`**.
Remote File field	The name and location of the .iso file in the remote share. Following are the example of remote share files: • **NFS** — **`/softwares/ucs-cxx-scu-3.1.9.iso`** • **CIFS** — **`/softwares/ucs-cxx-scu-3.1.9.iso`**
Mount Options field	Industry-standard mount options entered in a comma separated list. The options vary depending on the selected **Mount Type**. If you are using **NFS**, leave the field blank or enter one or more of the following: • **`ro`** • **`rw`** • **`nolock`** • **`noexec`** • **`soft`** • **`port=VALUE`** • **`timeo=VALUE`** • **`retry=VALUE`** If you are using **CIFS**, leave the field blank or enter one or more of the following: • **`soft`** • **`nounix`** • **`noserverino`**
User Name field	The username for the specified **Mount Type**, if required.
Password field	The password for the selected username, if required.

Step 6 Click **Save**.

Updating an ISO Image

Before you begin

- You must log in with admin privileges to perform this task.
- Cisco Flexible Flash must be supported by your platform.
- This task is available only when the cards are configured in **Util** mode.

Note This task results in the host re-scanning all the virtual drives, and a loss of virtual drive connectivity. We recommend that you configure the Cisco Flexible Flash controller properties before using any virtual drives, or power down the host prior to starting this task.

Step 1 In the **Navigation** pane, click the **Storage** tab.
Step 2 On the **Storage** tab, click **Cisco FlexFlash**.
Step 3 Click the **Virtual Drive Info** tab.
Step 4 In the **Virtual Drive Info** tab, select the virtual drive on which you want to update the image, click **Update Image**.

Note SCU and HUU update may take up to an hour and the drivers update may take up to five hours.

Unmapping an ISO Image

Before you begin

- You must log in with admin privileges to perform this task.
- Cisco Flexible Flash must be supported by your platform.

Note This task results in the host re-scanning all the virtual drives, and a loss of virtual drive connectivity. We recommend that you configure the Cisco Flexible Flash controller properties before using any virtual drives, or power down the host prior to starting this task.

Step 1 In the **Navigation** pane, click the **Storage** tab.
Step 2 On the **Storage** tab, click **Cisco FlexFlash**.
Step 3 Click the **Virtual Drive Info** tab.

Step 4 In the **Virtual Drive Info** tab, select the virtual drive for which you want to un map the image, click **Unmap Image**.

Resetting the Cisco Flexible Flash Card Configuration

When you reset the configuration of the slots in the Cisco Flexible Flash card, the following situations occur:

- The card in the selected slot is marked as primary healthy.
- The card in the other slot is marked as secondary-active unhealthy.
- One RAID partition is created.
- The card read/write error counts and read/write threshold are set to 0.
- Host connectivity could be disrupted.

If you upgrade to the latest version and select reset configuration option, a single hypervisor (HV) partition is created, and the existing four partition configurations are erased. This may also result in data loss. You can retrieve the lost data only if you have not done any data writes into HV partition, and downgrade to prior version.

Before you begin

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

Step 1 On the **Storage Adapters** pane, click **Cisco FlexFlash**.

Step 2 In the **Cisco FlexFlash** pane, click the **Controller Info** tab.

Step 3 In the **Actions** area, click **Reset Partition Defaults**.

Step 4 In the **Reset Partition Defaults** dialog box, update the following fields:

Name	Description
Slot radio button	Select the slot for which you want to mark the card as primary healthy. The card in the other slot, if any, is marked as secondary-active unhealthy.
Reset Partition Defaults button	Resets the configuration of the selected slot.
Cancel button	Closes the dialog box without making any changes.

Step 5 Click **Yes**.

Retaining Configuration of the Cisco Flexible Flash Cards

You can retain the configuration for an FlexFlash that supports firmware version 253 and later card in the following situations:

- There are two unpaired FlexFlash
- The server is operating from a single FlexFlash, and an unpaired FlexFlash is in the other slot.

- One FlexFlash supports firmware version 253, and the other FlexFlash is unpartitioned.

When you retain the configuration, the following situations occur:

- The configuration for the FlexFlash in the selected slot is copied to the other card.
- The card in the selected slot is marked as primary healthy.
- The card in the secondary slot is marked as secondary-active unhealthy.

Before you begin

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

Step 1 On the **Storage Adapters** pane, click **Cisco FlexFlash**.

Step 2 In the **Cisco FlexFlash** pane, click the **Controller Info** tab.

Step 3 In the **Actions** area, click **Synchronize Card Configuration**.

Step 4 In the **Synchronize Card Configuration** dialog box, update the following fields:

Name	Description
Slot radio button	Select the slot for which you want the configuration retained. The configuration is copied from the selected slot to the card in the other slot, and the card in the selected slot is marked as primary healthy.
Synchronize Card Configuration button	Copies the configuration from the selected card only if the selected card is of type SD253 and has single HV configuration.
Cancel button	Closes the dialog box without making any changes.

Step 5 Click **Yes**.

Cisco Boot Optimized M.2 Raid Controller

Viewing Cisco Boot Optimized M.2 Raid Controller Details

Before you begin

The server must be powered on.

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

Step 2 In the **Storage** menu, click the appropriate M.2 Raid controller.

Step 3 In the **Controller** area, the **Controller Info** tab displays by default.

Step 4 In the Work pane's **Health/Status** area, review the following information:

Name	Description
Composite Health field	The combined health of the controller, the attached drives, and the battery backup unit. This can be one of the following: • **Good** • **Moderate Fault** • **Severe Fault** • **N/A**
Controller Status field	The current status of the controller. This can be one of the following: • **Optimal** — The controller is functioning properly. • **Failed** — The controller is not functioning.

Step 5 In the **Firmware Versions** area, review the following information:

Name	Description
Product Name field	The name of the Cisco Boot optimized M.2 Raid controller.
Product PID field	The product PID of the Cisco Boot optimized M.2 Raid controller.
Serial Number field	The serial number of the Cisco Boot optimized M.2 Raid controller.
Firmware Package Build field	The active firmware package version number. For the firmware component version numbers, see the **Running Firmware Images** area.

Step 6 In the **PCI Info** area, review the following information:

Name	Description
PCI Slot field	The name of the PCIe slot in which the controller is located.
Vendor ID field	The PCI vendor ID, in hexadecimal.
Device ID field	The PCI device ID, in hexadecimal.
SubVendor ID field	The PCI subvendor ID, in hexadecimal.
SubDevice ID field	The PCI subdevice ID, in hexadecimal.

Step 7 In the **Manufacturing Data** area, review the following information:

Name	Description
Manufactured Date field	The manufacturing date of the Cisco Boot optimized M.2 Raid controller, in the format yyyy-mm-dd.
Revision No field	The board revision number, if any.

Step 8 In the **Next Patrol Read Schedule** area, review the following information:

Name	Description
PR State field	The patrol read state of the M.2 Raid controllers. It can be one of the following: • **ready** • **stopped** • **active** Default state: **N/A**.
PR Schedule Mode field	The patrol read schedule mode of the M.2 Raid controllers. The **PR Schedule Mode** is **manual** by default.

Step 9 In the **Running Firmware Images** area, review the following information:

Name	Description
BIOS Version field	The BIOS option PROM version number.
Firmware Version field	The active firmware version number.
Boot Block Version field	The boot block version number.

Step 10 In the **Virtual Drive Count** area, review the following information:

Name	Description
Virtual Drive Count field	The number of virtual drives configured on the controller.
Degraded Drive Count field	The number of virtual drives in a degraded state on the controller.
Offline Drive Count field	The number of virtual drives that have failed on the controller.

Step 11 In the **Physical Drive Count** area, review the following information:

Name	Description
Disk Present Count field	The number of physical drives present on the controller.

Name	Description
Critical Disk Count field	The number of physical drives in a critical state on the controller.
Failed Disk Count field	The number of physical drives that have failed on the controller.

Step 12 In the **Capabilities** area, review the following information:

Name	Description
RAID Levels Supported field	The RAID levels supported by the controller. **Raid 1**—Simple mirroring.

Step 13 In the **HW Configuration** area, review the following information:

Name	Description
Number of Backend Ports field	The number of SATA ports on the controller.

Viewing Physical Drive Info for Cisco Boot Optimized M.2 Raid Controller

Before you begin

The server must be powered on.

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

Step 2 In the **Storage** menu, click the appropriate M.2 raid controller.

Step 3 Click **Physical Drive Info** tab and in the **Physical Drives** area, review the following information:

Name	Description
Controller column	The name of the PCIe slot in which the controller drive is located.
Physical Drive Number column	The physical drive number.

Name	Description
Status column	The physical drive status. This can be one of the following: • **JBOD**—The drive is in JBOD mode. • **Failed**—The drive was in use, but it has failed. • **Offline**—The drive is offline and cannot be accessed. • **Online**—The drive is in use as part of a drive group. • **Predicted Failure**—The drive is marked as due to fail soon by the controller. • **Rebuild**—The drive is currently being rebuilt. • **Unknown**—The drive status is unknown.
State column	The state of the physical drive. This can be one of the following: • **JBOD**— The physical drive is in JBOD state. • **Online**— The physical drive is in use as part of a drive group. • **Failed**— The physical drive is in failed state. • **Rebuild**— The physical drive is in rebuild state.
Health column	The health of the physical drive. This can be one of the following: • **Good** • **Moderate Fault** • **Severe Fault** The health field includes both text and a color-coded icon. If the color-coded icon is: • Green — It indicates normal operation. • Yellow — It is an informational message. • Red — It indicates warning, critical, and non-recoverable errors.
Drive Firmware column	The firmware version running on the drive.
Model column	The drive vendor name.
Type column	Whether the drive is a hard drive (HDD) or a solid state drive (SSD).

Step 4 In the **Health/Status** area, review the following information:

Name	Description
Health	The health of the physical drive. This can be one of the following: • **Good** • **Moderate Fault** • **Severe Fault**
State	The state of the physical drive. This can be one of the following: • **JBOD**— The physical drive is in JBOD state. • **Online**— The physical drive is in use as part of a drive group. • **Failed**— The physical drive is in failed state. • **Rebuild**— The physical drive is in rebuild state.
Status	The physical drive status. This can be one of the following: • **JBOD**—The drive is in JBOD mode. • **Failed**—The drive was in use, but it has failed. • **Offline**—The drive is offline and cannot be accessed. • **Online**—The drive is in use as part of a drive group. • **Predicted Failure**—The drive is marked as due to fail soon by the controller. • **Rebuild**—The drive is currently being rebuilt. • **Unknown**—The drive status is unknown.
Fault	If this field displays **true**, the drive is in the **failed** state.
Online	If this field displays **true**, the drive is in the **online** state.

Step 5 In the **Smart Information** area, review the following information:

Name	Description
Power Cycle Count	Number of power cycles that were performed on the drive from the time it was manufactured. Power Cycle Count this field.
Power On Hours	Total number of hours that the drive is in the 'Power On' mode.

Name	Description
Percentage Life Left	The number of write cycles remaining in a M.2 drive. For instance, if an M.2 drive is capable of 100 write cycles during its life time, and it has completed 15 writes, then the percentage of life left in the drive is 85%. Each percentage range is represented in a different color. For instance, green for 75% to 100% and red for 1 to 25%.
Wear Status in Days	The number of days an M.2 drive has gone through with the write cycles.
Operating Temperature (°C)	The current temperature of the drive at which the selected M.2 drive operates at the time of selection.
Percentage Reserved Capacity Consumed	The total capacity (out of the percentage reserved for it) consumed by the M.2 drive.
Time of Last Refresh	Time period since the drive was last refreshed.

Step 6 In the **Operation Status** area, review the following information:

Name	Description
Operation	The current operation that is in progress on the drive. This can be one of the following: • **Rebuild in progress** • **Patrol read in progress**
Progress in %	The progress of the operation, in percentage.

Step 7 In the **Inquiry Data** area, review the following information:

Name	Description
Product ID	The drive product ID. This field generally displays the drive model number.
Vendor	The vendor for the drive.
Drive Firmware	The active firmware version on the drive.
Drive Serial Number	The serial number for the drive.

Step 8 In the **General** area, review the following information:

Name	Description
Slot Number	The slot number in which the physical drive resides.
Raw Size	The capacity of drive in megabytes, including the space used for formatting.

Name	Description
Negotiated Link Speed	The speed of the link between the drive and the controller.
Media Type	The drive type is a solid state drive (SSD).
Interface Type	The drive interface type.
Enclosure Association	Indicates whether the drives are associated to the controller directly or not. This can be: **Direct attached**—drives are directly attached to the controller.

Viewing the Virtual Drive Info for Cisco Boot Optimized M.2 Raid Controller

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

Step 2 In the **Storage** menu, click the M.2 Raid Controller.

Step 3 Select the **Virtual Drive Info** tab and in the **Virtual Drives** area, review the following information:

Name	Description
Virtual Drive Number column	The number of the virtual drive.
Name column	The name of the virtual drive.
Status column	The virtual drive state. This can be one of the following: • **Partially Degraded**—Virtual drive or physical drive rebuild is in progress. • **Degraded**—One or more spans of the drive has no redundancy. • **Off Line**—The drive is not visible to the host. • **Unknown**—The virtual drive state is unknown. • **Optimal**—The drive has full redundancy.

Name	Description
Health column	The health of the virtual drive. This can be one of the following: • **Good** • **Moderate Fault** • **Severe Fault** The health field includes both text and a color-coded icon. If the color-coded icon is: • Green — It indicates normal operation. • Yellow — It is an informational message. • Red — It indicates warning, critical, and non-recoverable errors.
Size column	The capacity of the drive in megabytes.
RAID Level column	The RAID level on the virtual drive. **Raid 1**—Simple mirroring.

Step 4 In the **General** area, review the following information:

Name	Description
Name	The name of the virtual drive.
Strip Size	The size of each strip, in KB.

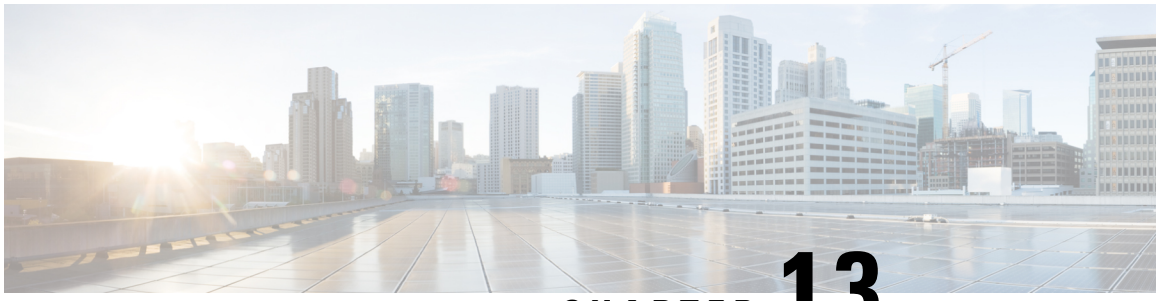
Step 5 In the **Physical Drives** area, review the following information:

Name	Description
Physical Drive Number	The physical drive number.
State	The state of the physical drive. This can be one of the following: • **JBOD**— The physical drive is in JBOD state. • **Online**— The physical drive is in use as part of a drive group. • **Failed**— The physical drive is in failed state. • **Rebuild**— The physical drive is in rebuild state.

Name	Description
Status	The physical drive status. This can be one of the following: • **JBOD**—The drive is in JBOD mode. • **Failed**—The drive was in use, but it has failed. • **Offline**—The drive is offline and cannot be accessed. • **Online**—The drive is in use as part of a drive group. • **Predicted Failure**—The drive is marked as due to fail soon by the controller. • **Rebuild**—The drive is currently being rebuilt. • **Unknown**—The drive status is unknown.

Step 6 In the **Operation Status** area, review the following information:

Name	Description
Operation	The current operation that is in progress on the drive. This can be: **Rebuild in progress**
Progress in %	The progress of the operation, in percentage.



CHAPTER 13

Configuring Communication Services

This chapter includes the following sections:

Enabling or Disabling TLS v1.2

Beginning with release 4.2(2a), Cisco IMC supports disabling TLS v1.2 and also customize the cipher values for both v1.2 and v1.3.

Before you begin

If **CC** (Common Criteria) under **Security Configuration** is enabled, you cannot disable TLS v1.2. Ensure that **CC** is disabled before you disable TLS v1.2.

Enabling or disabling TLS v1.2, restarts vKVM, Webserver, XML API, and Redfish API sessions.

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

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

Step 3 In the **TLS Configuration** area, update the following properties:

Name	Description
Enable TLS v1.2 check box	Whether TLS v1.2 is enabled on Cisco IMC. **Note** Enabling or disabling TLS v1.2, restarts vKVM, Webserver, XML API, and Redfish API sessions. **Note** If **CC** (Common Criteria) under **Security Configuration** is enabled, you cannot disable TLS v1.2.

Name	Description
Configured TLS Version field	TLS versions supported by Cisco IMC. This field is not user configurable. The value shown here depends on the value selected for **Enable TLS v1.2** check box.
TLS v1.2 Cipher Mode drop-down list	Allows you to select the desired cipher mode when TLS v1.2 is enabled. This can be one of the following: • **High** • **Medium** • **Low** **Note** If **FIPS** under **Security Configuration** is enabled, you cannot select **Low** mode. • **Custom**—You can enter custom cipher values. **Note** When FIPS is enabled, you are not allowed to set **Custom** ciphers. Refer https://www.openssl.org/docs/man1.0.2/man1/ciphers.html for OpenSSL equivalent cipher name for a specific cipher to be provided in custom cipher field. For example: To set **TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384**, provide **ECDHE-RSA-AES256-GCM-SHA384** input in the cipher list as input.

Name	Description
TLS v1.2 Cipher List field	Displays the list of ciphers based on the value selected in **TLS v1.2 Cipher Mode** drop-down list. You can edit the cipher values if you choose **TLS v1.2 Cipher Mode** as **Custom**. **Note** When FIPS is enabled, you are not allowed to set FIPS unsupported ciphers. When FIPS is enabled, you are not allowed to set **Custom** ciphers. **Note** If the cipher value entered is invalid or unsupported, then while saving the configuration, Cisco IMC automatically changes the **TLS v1.2 Cipher Mode** value to **High** and saves the configuration. For example: If **DH-RSA-AES256-GCM-SHA384** is set, **TLS v1.2 Cipher Mode** sets to **High** automatically After saving the configuration, Cisco IMC disables the **TLS v1.2 Cipher List** field and when you hover the mouse over **TLS v1.2 Custom Cipher Status** icon, it displays an error message similar to the following: `TLS v1.2 Custom Cipher Status: Error: Configuring an invalid or unsupported TLS v1.2 Cipher List-'Cipher_Name'. Setting TLS v1.2 Cipher Mode to High.`
TLS v1.3 Cipher Suite field	Allows you to edit the cipher values for TLS v1.3 **Note** When FIPS is enabled, you are not allowed to set FIPS unsupported ciphers.

Configuring HTTP

Beginning with release 4.1(2b), Cisco IMC supports separate HTTPS and HTTP communication services. You can disable only HTTP services using this functionality.

This functionality is supported only on the following servers:

- Cisco UCS S3260 M4/M5

Note If **Redirect HTTP to HTTPS Enabled** was disabled in any release earlier than 4.1(2b), then after upgrading to release 4.1(2b) or later, **HTTP Enabled** value is set to **Disabled** by the system.

Before you begin

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

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

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

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

Name	Description
HTTPS Enabled check box	**Warning** Disabling this option terminates the exiting Cisco IMC Web GUI session. Disabling this option, disables both HTTP and HTTPS services to access Cisco IMC. This option enables only HTTPS services to access Cisco IMC.
HTTP Enabled check box	**Warning** To successfully save any changes for this option, Cisco IMC Web GUI is restarted automatically. Communication with the management controller is lost momentarily and you must log in again after the restart. This option enables only HTTP services to access Cisco IMC. **Note** If HTTPS is disabled, HTTP services to access Cisco IMC are also disabled.
Redirect HTTP to HTTPS Enabled check box	**Note** This option is applicable only when HTTP Enabled is checked. If enabled, all attempts to communicate via HTTP are redirected to the equivalent HTTPS address. We strongly recommend that you enable this option if you enable HTTP.
HTTP Port field	The port to use for HTTP communication. The default is 80.
HTTPS Port field	The port to use for HTTPS communication. The default is 443
Session Timeout field	The number of seconds to wait between HTTP requests before the Cisco IMC times out and terminates the session. Enter an integer between 60 and 10,800. The default is 1,800 seconds.
Max Sessions field	The maximum number of concurrent HTTP and HTTPS sessions allowed on the Cisco IMC. This value may not be changed.
Active Sessions field	The number of HTTP and HTTPS sessions currently running on the Cisco IMC.

Step 4 Click **Save Changes**.

Configuring SSH

Before you begin

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

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

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

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

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

Step 4 Click **Save Changes**.

Configuring XML API

XML API for Cisco IMC

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

For detailed information about the XML API, see *Cisco UCS Rack-Mount Servers Cisco IMC XML API Programmer's Guide*.

Enabling the XML API

Before you begin

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

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

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

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

Name	Description
XML API Enabled check box	Whether API access is allowed on this server.
Max Sessions field	The maximum number of concurrent API sessions allowed on the Cisco IMC. This value may not be changed.
Active Sessions field	The number of API sessions currently running on the Cisco IMC.

Step 4 Click **Save Changes**.

Enabling Redfish

Before you begin

You must be logged in as admin to perform this action.

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

Step 2 On the **Admin** tab, click **Communications Services**.

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

Name	Description
XML API Enabled check box	Whether API access is allowed on this server.
Max Sessions field	The maximum number of concurrent API sessions allowed on the Cisco IMC. This value may not be changed.
Active Sessions field	The number of API sessions currently running on the Cisco IMC.

Step 4 Click **Save Changes**.

Configuring IPMI

IPMI Over LAN

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

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

Configuring IPMI over LAN

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

Note

- If you would want to run IPMI commands without issuing an encryption key, set the **Encryption Key** field in Cisco IMC to any even number of zeroes and save. This allows you to issue IPMI commands without including an encryption key.
- You are only allowed a maximum of four concurrent IPMI sessions.

Before you begin

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

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

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

Step 3 In the **IPMI over LAN Properties** area, update the following properties for BMC 1, BMC 2, CMC 1, or CMC 2:

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

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

Step 4 Click **Save Changes**.

Configuring SNMP

SNMP

The Cisco UCS C-Series Rack-Mount 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 Cisco IMC, see the *MIB Quick Reference for Cisco UCS* at this URL: http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/mib/b-series/b_UCS_MIBRef.html.

Beginning with release 4.1(3b), Cisco IMC introduces enhanced authentication protocol for SNMP v3 version. SNMP v3 users cannot be added with **DES** security protocol.

Cisco IMC GUI displays a warning when you select an existing v3 version with unsupported security level, authentication type, or privacy type. You may select and modify the user details.

Configuring SNMP Properties

Before you begin

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

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

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

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

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

Name	Description
SNMP Enabled check box	Whether this server sends SNMP traps to the designated host. **Note** After you check this check box, you need to click **Save Changes** before you can configure SNMP users or traps.
SNMP Port field	The port on which Cisco IMC SNMP agent runs. Enter an SNMP port number within the range 1 to 65535. The default port number is 161. **Note** The port numbers that are reserved for system calls, such as 22,23,80,123,443,623,389,636,3268,3269 and 2068, cannot be used as an SNMP port.
Access Community String field	The default SNMP v1 or v2c community name Cisco IMC includes on any SNMP get operations. Enter a string up to 18 characters.
SNMP Community Access drop-down list	This can be one of the following: • **Disabled** — This option blocks access to the information in the inventory tables. • **Limited** — This option provides partial access to read the information in the inventory tables. • **Full** — This option provides full access to read the information in the inventory tables. **Note** SNMP Community Access is applicable only for SNMP v1 and v2c users.
Trap Community String field	The name of the SNMP community group used for sending SNMP trap to other devices. Enter a string up to 18 characters. **Note** This field is visible only for SNMP v1 and v2c users. SNMP v3 version need to use SNMP v3 credentials.
System Contact field	The system contact person responsible for the SNMP implementation. Enter a string up to 254 characters, such as an email address or a name and telephone number.
System Location field	The location of the host on which the SNMP agent (server) runs. Enter a string up to 254 characters.

Name	Description
SNMP Input Engine ID field	User-defined unique identification of the static engine.
SNMP Engine ID field	Unique string to identify the device for administration purpose. This is generated from the SNMP Input Engine ID if it is already defined, else it is derived from the BMC serial number.

Step 5 Click **Save Changes**.

What to do next

Configure SNMP trap settings.

Configuring SNMP Trap Settings

Before you begin

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

Step 1 In the **Navigation** pane, click the **Admin** menu.
Step 2 In the **Admin** menu, click **Communication Services**.
Step 3 In the **Communications Services** pane, click the **SNMP** tab.
Step 4 Click on **Trap Destinations** tab.
Step 5 In the **Trap Destinations** area, you can perform one of the following:

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

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

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

Name	Description
ID field	The trap destination ID. This value cannot be modified.
Enabled drop-down list	If checked, then this trap is active on the server.
Version drop-down list	The SNMP version and model used for the trap. This can be one of the following: • **V2** • **V3**

Name	Description
Trap Type drop-down list	The type of trap to send. This can be one of the following: • **Trap**: If this option is chosen, the trap will be sent to the destination but you do not receive any notifications. • **Inform**: You can choose this option only for V2 users. If chosen, you will receive a notification when a trap is received at the destination.
User drop-down list	The drop-down list displays all available users, select a user from the list. **Note** While Configuring SNMP v3 version, SNMP users with Encryption Method set as **DES** are not displayed in the drop-down list.
Trap Destination Address field	Address to which the SNMP trap information is sent. You can set an IPv4 or IPv6 address or a domain name as the trap destination.
Port	The port the server uses to communicate with the trap destination. Enter a trap destination port number within the range 1 to 65535.

Step 7 Click **Save Changes**.

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

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

Sending a Test SNMP Trap Message

Before you begin

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

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

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

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

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

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

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

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

Managing SNMP Users for Cisco UCS C-Series M7 and Later Servers

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

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

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

Step 4 In the **v3 User Settings** area, click **CLICK HERE to change the Users configurations**

Refer Adding Local Users for Cisco UCS C-Series M7 and Later Servers, on page 106 to change user settings.

Configuring a Server to Send Email Alerts Using SMTP

The Cisco IMC supports email-based notification of server faults to recipients without relying on the SNMP. The system uses the Simple Mail Transfer Protocol (SMTP) to send server faults as email alerts to the configured SMTP server.

A maximum of four recipients is supported.

Configuring SMTP Server For Receiving Email Alerts

Configure the SMTP properties and add email recipients on the **Mail Alert** tab to receive email notifications for server faults.

Before you begin

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

Step 1

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

Step 3 In the **Communications Services** pane, click the **Mail Alert** tab.

Step 4 In the **SMTP Properties** area, update the following properties.

Name	Description
SMTP Enabled check box	If checked, it enables the SMTP service.
SMTP Server Address field	Allows you to enter the SMTP server address.
SMTP Port field	Allows you to enter the SMTP port number. The default port number is 25.
SMTP From Address	Allows you to set the From address of the SMTP mail alerts that are sent. The email address that you enter in this field will be displayed as the from address (mail received from address) of all the SMTP mail alerts that you receive. **Note** This is an optional field. If you do not enter an email address in this field, by default the server hostname ID is displayed as the from address (mail received from address).

Step 5 In the **SMTP Recipients** area, do the following:

a) Click the **Add (+)** button to add the email recipients to whom notifications should be sent. Enter the email ID and click **Save**.

To delete an email recipient, select the email recipient and click the **Delete (X)** button.

b) **Minimum Severity to Report** drop-down list allows you to choose the minimum severity level for receiving the email alert. This can be one of the following:

- Condition
- Warning
- Minor
- Major
- Critical

If you choose a minimum severity level, the mail alerts are sent for that level and the other higher severity levels. For example, if you choose 'Minor' as the minimum severity level, you will receive email alerts for the minor, major, and critical fault events.

c) Click **Send Test Mail** to check whether the email recipient you added is reachable.
If the email address and the SMTP settings are valid, a confirmation pop-up window appears with the message that an email has been sent. If the settings are not valid, a confirmation pop-up window appears with the message that no email has been sent. The **Reachability** column indicates whether test mails have been sent successfully to the email recipient. The **Reachability** column has one of the following values:

- **Yes** (if the test mail has been sent successfully)
- **No** (if the test mail has not been sent successfully)
- **na** (if no test mail has been sent)

Step 6 Click **Save Changes**.

Troubleshooting

The following table describes troubleshooting suggestions for SMTP mail alert configuration issues (when the reachability status is **No**) that may appear in the Cisco IMC logs:

Issue	Suggested Solution
Timeout was reached	This could occur when you are not able to reach the configured SMTP IP address. Enter a valid IP address.
Couldn't resolve host name	This could occur when you are not able to reach the configured SMTP domain name. Enter a valid domain name.
Couldn't connect to server	This could occur when the SMTP IP or domain name or port number is/are incorrectly configured. Enter valid configuration details.
Failed sending data to the peer	This could occur when the an invalid recipient email ID is configured. Enter a valid email ID.

Adding SMTP Email Recipients

Add email recipients on the **Mail Alert** tab to receive email notifications for server faults.

Before you begin

- You must log in as a user with admin privileges to perform this task.
- Configure the SMTP server properties in the SMTP Properties area. See Configuring SMTP Server For Receiving Email Alerts, on page 306

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

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

Step 3 In the **Communications Services** pane, click the **Mail Alert** tab.

Step 4 In the **SMTP Recipients** area, do the following:

a) Click the **Add (+)** button to add the email recipients to whom notifications should be sent. Enter the email ID and click **Save**.

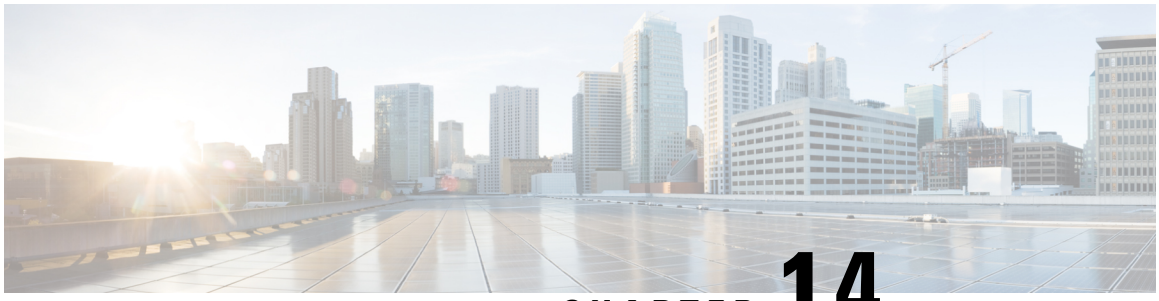
b) **Minimum Severity to Report** drop-down list allows you to choose the minimum severity level for receiving the email alert. This can be one of the following:

- Condition
- Warning
- Minor
- Major
- Critical

If you choose a minimum severity level, the mail alerts are sent for that level and the other higher severity levels. For example, if you choose 'Minor' as the minimum severity level, you will receive email alerts for the minor, major, and critical fault events.

c) Click **Send Test Mail** to check whether the email recipient you added is reachable.
If the email address and the SMTP settings are valid, a confirmation pop-up window appears with the message that an email has been sent. If the settings are not valid, a confirmation pop-up window appears with the message that no email has been sent. The **Reachability** column indicates whether test mails have been sent successfully to the email recipient. The **Reachability** column has one of the following values:

- **Yes** (if the test mail has been sent successfully)
- **No** (if the test mail has not been sent successfully)
- **na** (if no test mail has been sent)



CHAPTER 14

Managing Certificates and Server Security

This chapter includes the following sections:

Managing the Server Certificate

You can generate a certificate signing request (CSR) to obtain a new certificate, and you can upload the new certificate to the Cisco IMC to replace the current server certificate. The server certificate may be signed either by a public Certificate Authority (CA), such as Verisign, or by your own certificate authority. The generated certificate key length is 2048 bits.

Note Before performing any of the following tasks in this chapter, ensure that the Cisco IMC time is set to the current time.

Step 1 Generate the CSR from the Cisco IMC.

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 Cisco IMC.

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

Generating a Certificate Signing Request

Note Do not use special characters (For example ampersand (**&**)) in the **Common Name** and **Organization Unit** fields.

Before you begin

- You must log in as a user with admin privileges to configure certificates.
- Ensure that the Cisco IMC time is set to the current time.

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

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

Step 3 In the **Actions** area, click the **Generate New Certificate Signing Request** link.

The **Generate New Certificate Signing Request** dialog box appears.

Step 4 In the **Generate New Certificate Signing Request** dialog box, update the following properties:

Name	Description
Common Name field	The fully qualified name of the Cisco IMC. By default the CN of the servers appears in CXXX-YYYYYY format, where XXX is the model number and YYYYYY is the serial number of the server. When you upgrade to latest version, CN is retained as is.
Subject Alternate Name (SAN)	You can now provide additional input parameter for Subject Alternate Name. This allows various values to be associated using the subject field of the certificate. The various options of SAN includes: • Email • DNS name • IP address • Uniform Resource Identifier (URI) **Note** This field is optional. You can configure any number of SAN instances of each type, but all together the instances count must not exceed 10.
Organization Name field	The organization requesting the certificate.
Organization Unit field	The organizational unit.

Name	Description
Locality field	The city or town in which the company requesting the certificate is headquartered.
State Name field	The state or province in which the company requesting the certificate is headquartered.
Country Code drop-down list	The country in which the company resides.
Email field	The email contact at the company.
Signature Algorithm	Allows you to select the signature algorithm for generating certificate signing request. This can be one of the following: • SHA1 • SHA256 • SHA384 • SHA512 • ECDSA • RSA The default signature algorithm selected for generating certificate signing request is SHA384. **Note** The signature algorithms ECDSA and RSA are available in Cisco UCS C-series M7 servers only.
Key Length drop-down list	**Note** • This option is available in Cisco UCS C-series M7 servers only. This option is available for all the **Signature Algorithm** except **ECDSA**. You may select from one of the following: • 1024 • 2048 • 4096

Name	Description
Key Curve drop-down list	**Note** • This option is available in Cisco UCS C-series M7 servers only. • This option is available only for **ECDSA Signature Algorithm**. You may select from one of the following: • P256 • P384 • P512
Challenge Password check box	A **Challenge Password** is to be embedded in the Certificate Signing Request (CSR) dialog box, which the issuer Certificate Authority (CA) uses to authenticate the certificate. If **Challenge Password** option is selected, then **Challenge Password String** will be populated for the user to enter the valid password string. **Note** The user has an option not to select the **Challenge Password** in which case the **Challenge Password String** is not populated. However, the user can proceed with generating the CSR successfully.
Challenge Password String field	This option is displayed only when **Challenge Password String** is selected. Enter a string.
String Mask drop-down list	This sets a mask for permitted string types in Certificate Signing Request (CSR) dialog box. This option masks out the use of certain string types in certain fields. The string types are as follows: • **Default**: Uses PrintableString, T61String, BMPString. • **pkix**: Uses PrintableString, BMPString. • **utf8only**: Uses only UTF8Strings. • **nombstr**: Uses PrintableString, T61String (no BMPStrings or UTF8Strings).
Self Signed Certificate check box	Generates a Self Signed Certificate. **Warning** After successful certificate generation, the Cisco IMC Web GUI restarts. Communication with the management controller may be lost momentarily and you will need to re-login. **Note** If enabled, CSR is generated, signed and uploaded automatically.
Generate CSR button	Click to generate the certificate.
Reset Values button	Reset all values in the dialog box.

Note If Self-signed certificate is enabled, ignore steps 5 and 6.

Step 5 Click **Generate CSR**.

The **Opening csr.txt** dialog box appears.

Step 6 Perform any one of the following steps to manage the CSR file, csr.txt:

a) Click **Open With** to view csr.txt.

b) Click **Save File** and then click **OK** to save csr.txt to your local machine.

What to do next

- Submit the CSR file to a certificate authority that will issue and sign your certificate. If your organization generates its own self-signed certificates, you can use the CSR file to generate a self-signed certificate.
- Ensure that the certificate is of type **Server**.

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 Cisco IMC.

Before you begin

- Obtain and install a certificate server software package on a server within your organization.
- Ensure that the Cisco IMC time is set to the current time.

Procedure

	Command or Action	Purpose
Step 1	**openssl genrsa -out** *CA_keyfilename keysize* **Example:** `# openssl genrsa -out ca.key 2048`	This command generates an RSA private key that will be 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.
Step 2	**openssl req -new -x509 -days** *numdays* **-key** *CA_keyfilename* **-out** *CA_certfilename*	This command generates a new self-signed certificate for the CA using the specified key. The certificate is valid for

	Command or Action	Purpose
	Example: `# openssl req -new -x509 -days 365 -key ca.key -out ca.crt`	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 file to designate the certificate as a server-only certificate. This designation is a defense against a man-in-the-middle attack, in which an authorized client attempts to impersonate the server. The OpenSSL configuration file openssl.conf contains the statement "nsCertType = server".
Step 4	**openssl x509 -req -days** *numdays* **-in** *CSR_filename* **-CA** *CA_certfilename* **-set_serial 04 -CAkey** *CA_keyfilename* **-out** *server_certfilename* **-extfile openssl.conf** **Example:** `# openssl x509 -req -days 365 -in csr.txt -CA ca.crt -set_serial 04 -CAkey ca.key -out myserver05.crt -extfile openssl.conf`	This command directs the CA to use your CSR file to generate a server certificate. Your server certificate is contained in the output file.
Step 5	**openssl x509 -noout -text -purpose -in <cert file>** **Example:** `openssl x509 -noout -text -purpose -in <cert file>`	Verifies if the generated certificate is of type **Server**. **Note** If the values of the fields **Server SSL** and **Netscape SSL** server are not yes, ensure that openssl.conf is configured to generate certificates of type server.
Step 6	(Optional) If the generated certificate does not have the correct validity dates, ensure the Cisco IMC time is set to the current time, and regenerate the certificate by repeating steps 1 through 5.	Certificate with the correct validity dates is created.

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.

```
# /usr/bin/openssl genrsa -out ca.key 2048
Generating RSA private key, 2048 bit long modulus
.............++++++
.....++++++
e is 65537 (0x10001)
# /usr/bin/openssl req -new -x509 -days 365 -key ca.key -out ca.crt
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
```

```
-----
Country Name (2 letter code) [GB]:US
State or Province Name (full name) [Berkshire]:California
Locality Name (eg, city) [Newbury]:San Jose
Organization Name (eg, company) [My Company Ltd]:Example Incorporated
Organizational Unit Name (eg, section) []:Unit A
Common Name (eg, your name or your server's hostname) []:example.com
Email Address []:admin@example.com
# echo "nsCertType = server" > openssl.conf
# /usr/bin/openssl x509 -req -days 365 -in csr.txt -CA ca.crt -set_serial 01
-CAkey ca.key -out server.crt -extfile openssl.conf
Signature ok
subject=/C=US/ST=California/L=San Jose/O=Example Inc./OU=Unit
A/CN=example.com/emailAddress=john@example.com
Getting CA Private Key
#
```

What to do next

Upload the new certificate to the Cisco IMC.

Creating a Self-Signed Certificate Using Windows

Before you begin

- You must log in as a user with admin privileges to configure certificates.
- Ensure that the Cisco IMC time is set to the current time.

Step 1 Open **IIS Manager** and navigate to the level you want to manage.

Step 2 In the **Features** area, double-click **Server Certificate**.

Step 3 In the **Action** pane, click **Create Self-Signed Certificate**.

Step 4 On the **Create Self-Signed Certificate** window, enter name for the certificate in the **Specify a friendly name for the certificate** field.

Step 5 Click **Ok**.

Step 6 (Optional) If the generated certificate does not have the correct validity dates, ensure the Cisco IMC time is set to the current time, and regenerate the certificate by repeating steps 1 through 5.
Certificate with the correct validity dates is created.

Uploading a Server Certificate

You can either browse and select the certificate to be uploaded to the server or copy the entire content of the signed certificate and paste it in the **Paste certificate content** text field and upload it.

Before you begin

- You must log in as a user with admin privileges to upload a certificate.
- The certificate file to be uploaded must reside on a locally accessible file system.
- Ensure that the generated certificate is of type server.
- The following certificate formats are supported:
  - .crt
  - .cer
  - .pem

Note You must first generate a CSR using the Cisco IMC Certificate Management menu, and you must use that CSR to obtain the certificate for uploading. Do not upload a certificate that was not obtained by this method.

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

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

Step 3 In the **Actions** area, click **Upload Server Certificate**.

The **Upload Certificate** dialog box appears.

Step 4 In the **Upload Certificate** dialog box, update the following properties:

Name	Description
Upload Certificate through browser client button	Allows you to upload the certificate.
File	The certificate file you want to upload.
Browse button	Opens a dialog box that allows you to navigate to the appropriate certificate file.
Paste Certificate content radio button	Opens a text box that allows you to copy the entire content of the signed certificate and paste it in the **Paste certificate content** text field. **Note** Ensure the certificate is signed before uploading.
Upload button	Click **Upload** to upload the certificate.

Step 5 Click **Upload Certificate**.

Managing the External Certificate

Prior to the 4.1.2 release, you can generate a certificate signing request (CSR) and upload a new server certificate to Cisco IMC. Release 4.1.2 onwards, you can also upload a wildcard or an external certificate and an external private key, in addition to a server certificate. Unlike a server certificate, you could upload and use the same external certificate and key pair for ***multiple*** Cisco IMC servers.

1. Upload the external certificate and external private key to Cisco IMC.
2. Activate the uploaded certificate.

   On activation, the new certificate and private key pair replaces the existing certificate and key pair in Cisco IMC.

Uploading an External Certificate

Before you begin

- You must log in as a user with admin privileges.
- The certificate file to be uploaded must reside on a locally accessible file system.
- The following certificate formats are supported:
  - .crt
  - .cer
  - .pem

Note
- Cisco IMC supports external private key size of 2048 bits, 4096 bits and 8192 bits in Cisco UCS S-Series servers.

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

Step 2 On the **Admin** tab, click **Certificate Management**.

Step 3 In the **Actions** area, click **Upload External Certificate**.

The **Upload External Certificate** dialog box appears.

Step 4 In the **Upload External Certificate** dialog box, select the appropriate options and enter the relevant details:

- **Upload from remote location**: Select this radio button to upload an external certificate from a remote location.

Name	Description
Upload from remote location field	Select from one of the following protocols: • TFTP • FTP • SCP • SFTP • HTTP **Note** If you select FTP, SCP or SFTP, you will be prompted to enter your username and password.
Server IP/ Hostname button	Enter the remote server IP address or hostname.
Path and Filename	Enter the filepath on the remote server from where you want to upload the external certificate along with the filename. **Note** The maximum file size supported for upload using this option is: • Up to 8 KB in Cisco UCS S-Series servers
Username	Enter the user name for your remote server.
Password	Password for your remote server.

- **Upload through browser Client**: Select this radio button to upload an external certificate using a browser client.

  Click **Browse** and navigate to the location from where you want to upload the external certificate.

  Note The maximum file size supported for upload using this option is up to 5 KB in:
  - Cisco UCS S-Series servers

- **Paste External Certificate Content**: Select this radio button to paste the external certificate details directly in the dialog box.

  Note The maximum file size supported for upload using this option is:
  - Up to 8 KB in Cisco UCS S-Series servers

Step 5 Click **Upload** to upload the external certificate.

What to do next

Upload the external private key and then activate the uploaded external certificate.

Important After you upload the external certificate and the external private key, the **Activate External Certificate** tab is enabled. Select **Activate External Certificate** to activate the uploaded external certificate.

Activating the uploaded certificate replaces the existing certificate and key pair, and disconnects any existing HTTPS and SSH sessions.

Uploading an External Private Key

Before you begin

- You must log in as a user with admin privileges to upload an external private key.
- Ensure that you have uploaded an external certificate.

Note
- Cisco IMC supports external private key size of 2048 bits, 4096 bits and 8192 bits in Cisco UCS S-Series servers.

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

Step 2 On the **Admin** tab, click **Certificate Management**.

Step 3 In the **Actions** area, click **Upload External Private Key**.

The **Upload External Private Key** dialog box appears.

Step 4 In the **Upload External Private Key** dialog box, select the appropriate options and enter the relevant details:

- **Upload from remote location**: Select this radio button to upload an external certificate from a remote location.

Name	Description
Upload from remote location field	Select from one of the following protocols: • SFTP • SCP
Server IP/ Hostname button	Enter the remote server IP address or hostname.
Path and Filename	Enter the filepath on the remote server from where you want to upload the external private key along with the filename. **Note** The maximum file size supported for upload using this option is: • Up to 8 KB in Cisco UCS S-Series servers
Username	Enter the user name for your remote server.

Name	Description
Password	Password for your remote server.

- **Upload through browser Client**: Select this radio button to upload an external private key using a browser client.

  Click **Browse** and navigate to the location from where you want to upload the external private key.

  Note The maximum file size supported for upload using this option is up to 5 KB in:

  - Cisco UCS S-Series servers

- **Paste External Private Key Content**: Select this radio button to paste the external private key details directly in the dialog box.

  Note The maximum file size supported for upload using this option is:

  - Up to 8 KB in Cisco UCS S-Series servers

Step 5 Click **Upload** to upload the external private key.

What to do next

After uploading the external certificate and external private key, activate the uploaded external certificate.

Important After you upload the external certificate and the external private key, the **Activate External Certificate** tab is enabled. Select **Activate External Certificate** to activate the uploaded external certificate.

Activating the uploaded certificate replaces the existing certificate and key pair, and disconnects any existing HTTPS and SSH sessions.

Activating the External Certificate

Before you begin

- You must log in as a user with admin privileges to activate an external certificate.
- Ensure that you have uploaded the external certificate and external private key.

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

Step 2 On the **Admin** tab, click **Certificate Management**.

After uploading the external certificate and the private key, the **Activate External Certificate** tab is enabled in the **Actions** area.

Step 3 Click **Activate External Certificate**.

Note Activating the external certificate overwrites any existing certificate and key pair, and disconnects any existing HTTPS and SSH sessions.

Key Management Interoperability Protocol

Key Management Interoperability Protocol (KMIP) is a communication protocol that defines message formats to handle keys or classified data on a key management server. KMIP is an open standard and is supported by several vendors. Key management involves multiple interoperable implementations, so a KMIP client works effectively with any KMIP server.

Self-Encrypting Drives(SEDs) contain hardware that encrypts incoming data and decrypts outgoing data in realtime. A drive or media encryption key controls this function. However, the drives need to be locked in order to maintain security. A security key identifier and a security key (key encryption key) help achieve this goal. The key identifier provides a unique ID to the drive.

Different keys have different usage requirements. Currently, the responsibility of managing and tracking local keys lies primarily with the user, which could result in human error. The user needs to remember the different keys and their functions, which could prove to be a challenge. KMIP addresses this area of concern to manage the keys effectively without human involvement.

Downloading a Client Certificate

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

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

Step 3 On the **Server** tab, click **Secure Key Management**.

Step 4 In the **Actions** area of the **Secure Key Management** tab, click **Download Client Certificate**.

Step 5 In the **Download Client Certificate** dialog box, complete these fields:

Name	Description
Download From Remote Location radio button	Selecting this option allows you to choose the certificate from a remote location and download it. Enter the following details: • • **TFTP Server** • **FTP Server** • **SFTP Server** • **SCP Server** • **HTTP Server** **Note** If you chose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message *Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*. Click Yes or No depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to. • **Server IP/Hostname** field — The IP address or hostname of the server on which the client certificate file should be stored. Depending on the setting in the **Download Certificate from** drop-down list, the name of the field may vary. • **Path and Filename** field — The path and filename Cisco IMC should use when downloading the file to the remote server. • **Username** field — The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP. • **Password** field — The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP.
Download Through Browser Client radio button	Selecting this option allows you to navigate to the certificate stored on a drive that is local to the computer running the Cisco IMC GUI. When you select this option, Cisco IMC GUI displays a **Browse** button that lets you navigate to the file you want to import.
Paste Content radio button	Selecting this option allows you to copy the entire content of the signed certificate and paste it in the **Paste Certificate Content** text field. **Note** Ensure the certificate is signed before uploading.

Exporting a Client Certificate

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

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

Step 3 On the **Server** tab, click **Secure Key Management**.

Step 4 In the **Actions** area of the **Secure Key Management** tab, click **Export Client Certificate**.

Step 5 In the **Export Client Certificate** dialog box, complete these fields:

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

Deleting a Client Certificate

Step 1 In the **Navigation** pane, click the **Compute** menu.
Step 2 In the **Compute** menu, select a server.
Step 3 On the **Server** tab, click **Secure Key Management**.
Step 4 In the **Actions** area of the **Secure Key Management** tab, click **Delete Client Certificate**.
Step 5 At the prompt, click **OK** to delete the client certificate, or **Cancel** to cancel the action.

Downloading a Client Private Key

Step 1 In the **Navigation** pane, click the **Compute** menu.
Step 2 In the **Compute** menu, select a server.
Step 3 On the **Server** tab, click **Secure Key Management**.
Step 4 In the **Actions** area of the **Secure Key Management** tab, click **Download Client Private Key**.
Step 5 In the **Download Client Private Key** dialog box, complete these fields:

Name	Description
Download From Remote Location radio button	Selecting this option allows you to choose the private key from a remote location and download it. Enter the following details: • • **TFTP Server** • **FTP Server** • **SFTP Server** • **SCP Server** • **HTTP Server** **Note** If you chose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message *Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*. Click Yes or No depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to. • **Server IP/Hostname** field — The IP address or hostname of the server on which the client private key should be stored. Depending on the setting in the **Download Certificate From** drop-down list, the name of the field may vary. • **Path and Filename** field — The path and filename Cisco IMC should use when downloading the file to the remote server. • **Username** field — The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP. • **Password** field — The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP.
Download Through Browser Client radio button	Selecting this option allows you to navigate to the private key stored on a drive that is local to the computer running the Cisco IMC GUI. When you select this option, Cisco IMC GUI displays a **Browse** button that lets you navigate to the file you want to import.
Paste Content radio button	Selecting this option allows you to copy the entire content of the signed private key and paste it in the **Paste Private Key Content** text field.

What to do next

Exporting a Client Private Key

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

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

Step 3 On the **Server** tab, click **Secure Key Management**.

Step 4 In the **Actions** area of the **Secure Key Management** tab, click **Export Client Private Key**.

Step 5 In the **Export Client Private Key** dialog box, complete these fields:

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

Deleting a Client Private Key

Step 1 In the **Navigation** pane, click the **Compute** menu.
Step 2 In the **Compute** menu, select a server.
Step 3 On the **Server** tab, click **Secure Key Management**.
Step 4 In the **Actions** area of the **Secure Key Management** pane, click **Delete Client Private Key**.
Step 5 At the prompt, click **OK** or **Cancel** to delete the client private key, or cancel the action.

Downloading a Root CA Certificate

Step 1 In the **Navigation** pane, click the **Compute** menu.
Step 2 In the **Compute** menu, select a server.
Step 3 On the **Server** tab, click **Secure Key Management**.
Step 4 In the **Actions** area of the **Secure Key Management** tab, click **Download Root CA Certificate**.
Step 5 In the **Download Root CA Certificate** dialog box, complete these fields:

Name	Description
Download From Remote Location radio button	Selecting this option allows you to choose the certificate from a remote location and download it. Enter the following details: • • **TFTP Server** • **FTP Server** • **SFTP Server** • **SCP Server** • **HTTP Server** **Note** If you chose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message *Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*. Click Yes or No depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to. • **Server IP/Hostname** field — The IP address or hostname of the server on which the root CA certificate file should be stored. Depending on the setting in the **Download Certificate from** drop-down list, the name of the field may vary. • **Path and Filename** field — The path and filename Cisco IMC should use when downloading the file to the remote server. • **Username** field — The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP. • **Password** field — The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP.
Download Through Browser Client radio button	Selecting this option allows you to navigate to the certificate stored on a drive that is local to the computer running the Cisco IMC GUI. When you select this option, Cisco IMC GUI displays a **Browse** button that lets you navigate to the file you want to import.
Paste Content radio button	Selecting this option allows you to copy the entire content of the signed certificate and paste it in the **Paste Certificate Content** text field. **Note** Ensure the certificate is signed before uploading.

Exporting a Root CA Certificate

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

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

Step 3 On the **Server** tab, click **Secure Key Management**.

Step 4 In the **Actions** area of the **Secure Key Management** tab, click **Export Root CA Certificate**.

Step 5 In the **Export Root CA Certificate** dialog box, complete these fields:

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

Deleting a Root CA Certificate

Step 1 In the **Navigation** pane, click the **Compute** menu.
Step 2 In the **Compute** menu, select a server.
Step 3 On the **Server** tab, click **Secure Key Management**.
Step 4 In the **Actions** area of the **Secure Key Management** tab, click **Delete Root CA Certificate**.
Step 5 At the prompt, click **OK** or **Cancel** to delete the root CA certificate, or cancel the action.

Deleting KMIP Login Details

Step 1 In the **Navigation** pane, click the **Compute** menu.
Step 2 In the **Compute** menu, select a server.
Step 3 On the **Server** tab, click **Secure Key Management**.
Step 4 In the **Actions** area of the **Secure Key Management** pane, click **Delete KMIP Login**.
Step 5 At the prompt, click **OK** to delete the KMIP login details, or **Cancel** to cancel the action.

Restoring the KMIP Server to Default Settings

Step 1 In the **Navigation** pane, click the **Compute** menu.
Step 2 In the **Compute** menu, select a server.
Step 3 On the **Server** tab, click **Secure Key Management**.
Step 4 In the **KMIP Servers** area of the **Secure Key Management** tab, select a row by checking the check box and click **Delete**.
Step 5 At the prompt, click **OK**

This restores the KMIP server to its default settings.

Testing the KMIP Server Connection

Step 1 In the **Navigation** pane, click the **Compute** menu.
Step 2 In the **Compute** menu, select a server.
Step 3 On the **Server** tab, click **Secure Key Management**.
Step 4 In the **KMIP Servers** area of the **Secure Key Management** tab, select a row by checking the check box and click **Test Connection**.

Step 5 If the connection is successful, a success message is displayed.

Viewing Secure Key Management Settings

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

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

Step 3 On the **Server** tab, click **Secure Key Management**.

Step 4 In the **Work** pane, review the following field:

Name	Description
Enable Secure Key Management check box	If checked, allows you to enable the secure key management feature.

Step 5 In the **Actions** Area, review the following fields:

Name	Description
Download Root CA Certificate link	This allows you to download the root CA certificate to Cisco IMC.
Export Root CA Certificate link	This allows you to export the downloaded root CA certificate to a local file or remote server.
Delete Root CA Certificate link	This allows you to delete the root CA certificate.
Download Client Certificate link	This allows you to download the client certificate to Cisco IMC.
Export Client Certificate link	This allows you to export the downloaded client certificate to a local file or remote server.
Delete Client Certificate link	This allows you to delete the client certificate.
Download Client Private Key link	This allows you to download the client private key to Cisco IMC.
Export Client Private Key link	This allows you to export the downloaded root CA certificate to local file or remote server.
Delete Client Private Key link	This allows you to delete the root CA certificate.
Delete KMIP Login link	This allows you to delete the KMIP login details.

Step 6 In the **KMIP Servers** Area, review the following fields:

Name	Description
ID field	ID for the KMIP server configuration.

Name	Description
IP Address field	IP address of the KMIP server.
Port field	Communication port to the KMIP server.
Timeout field	Time period that Cisco IMC waits for a response from the KMIP server.
Delete button	Deletes the KMIP server configuration.
Test Connection button	Tests whether or not the KMIP connection was successful.

Step 7 In the **KMIP Root CA Certificate** Area, review the following fields:

Name	Description
Server Root CA Certificate field	Indicates the availability of the root CA certificate.
Download Status field	This field displays the status of the root CA certificate download.
Download Progress field	This field displays the progress of the root CA certificate download.
Export Status field	This field displays the status of the root CA certificate export.
Export Progress field	This field displays the progress of the root CA certificate export.

Step 8 In the **KMIP Client Certificate** Area, review the following fields:

Name	Description
Client Certificate field	Indicates the availability of the client certificate.
Download Status field	This field displays the status of the client certificate download.
Download Progress field	This field displays the progress of the client certificate download.
Export Status field	This field displays the status of the client certificate export.
Export Progress field	This field displays the progress of the client certificate export.

Step 9 In the **KMIP Login Details** Area, review the following fields:

Name	Description
Use KMIP Login check box	Allows you to choose whether or not to use KMIP login details.

Name	Description
Login name to KMIP Server field	User name of the KMIP server.
Password to KMIP Server field	Password of the KMIP server.
Change Password check box	Allows you to change the KMIP password.
New Password field	Allows you to enter the new password that you want to assign to the KMIP server. **Note** This option is only visible when you enable the **Change Password** check box.
Confirm Password field	Enter the new password again in this field. **Note** This option is only visible when you enable the **Change Password** check box.

Step 10 In the **KMIP Client Private Key** Area, review the following fields:

Name	Description
Client Private Key field	Indicates the availability of the client private key.
Download Status field	This field displays the status of the client private key download.
Download Progress field	This field displays the progress of the client private key download.
Export Status field	This field displays the status of the client private key export.
Export Progress field	This field displays the progress of the client private key export.

FIPS 140-2 Compliance in Cisco IMC

The Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2), is a U.S. government computer security standard used to approve cryptographic modules. Prior to the 3.1(3) release, the Rack Cisco IMC is not FIPS compliant as per NIST guideline. It does not follow FIPS 140-2 approved cryptographic algorithms and modules. With this release, all CIMC services will use the Cisco FIPS Object Module (FOM), which provides the FIPS 140-2 compliant cryptographic module.

The Cisco FIPS Object Module is a software library that provides cryptographic services to a vast array of Cisco's networking and collaboration products. The module provides FIPS 140 validated cryptographic algorithms and KDF functionality for services such as IPSec (IKE), SRTP, SSH, TLS, and SNMP.

Enabling Security Configuration

Before you begin

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

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

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

Step 3 In the **Security Management** pane, click **Security Configuration**.

Step 4 In the **Federal Information Processing Standard Configuration (FIPS) and Common Criteria (CC) Configuration** pane, check the **Enable FIPS** check-box.

Table 18: Federal Information Processing Standard Configuration (FIPS) and Common Criteria (CC) Configuration

Name	Description
Enable FIPS check box	If checked, allows you to enable the FIPS feature. By default, this option is disabled. When you enable FIPS, the following is an impact on the SNMP configuration: • The community string configuration for the SNMPv2 protocols, and the SNMPv3 users configured with **noAuthNoPriv** or **authNoPriv** security-level option are disabled. • The traps configured for SNMPv2 or SNMPv3 users with the **noAuthNoPriv** security-level option are disabled. • The **MD5** and **DES** Authentication type and Privacy type are disabled. **Note** DES privacy type is not applicable for release 4.1(3b) or later. However, if DES was configured in an earlier release before you upgraded to release 4.1(3b) or later, then you may see DES privacy type, which is disabled if FIPS is enabled. • It also ensures only FIPS-compliant ciphers in SSH, webserver, and vKVM connections. • Allows the Common Criteria (CC) to be enabled. • Disables TACACS+ Authentication.

Name	Description
Enable CC check box	**Note** Enabling CC requires FIPS to be enabled. If checked, allows you to enable the CC feature. By default, this option is disabled. **Note** If **Enable TLS v1.2** check under **Communication Services** is disabled, you cannot enable **CC**.

Note When you switch the FIPS or CC mode, it restarts the SSH, KVM, SNMP, webserver, XMLAPI, and redfish services. You will be prompted to continue. If you wish to continue, click **OK** else click on **Cancel**.

Enabling Security Configuration (FIPS)

Before you begin

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

Note If **Configured TLS Version** is set to **Custom**, then you cannot enable FIPS.

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

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

Step 3 In the **Security Management** pane, click **Security Configuration**.

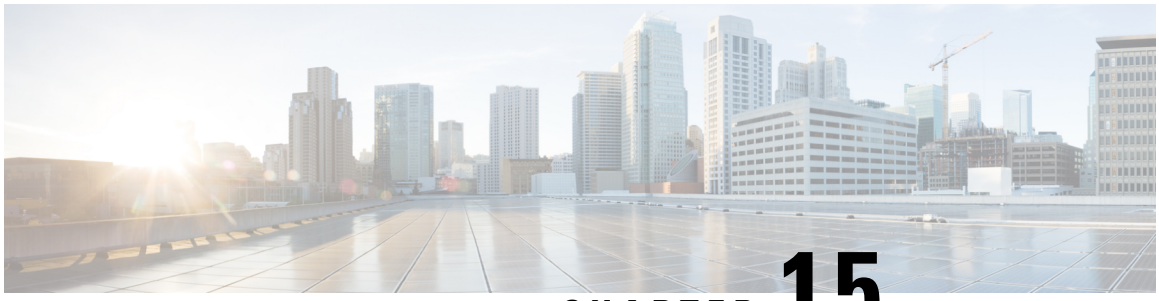
Step 4 In the **Work** pane, check the **Enable FIPS** check-box.

Note When you switch the FIPS mode, it restarts the SSH, KVM, SNMP, webserver, XMLAPI, and redfish services.

Step 5 You will be prompted to continue. If you wish to continue, click **OK** else click on **Cancel**.

Note When you enable FIPS, the following is an impact on the SNMP configuration:

- The community string configuration for the SNMPv2 protocols, and the SNMPv3 users configured with **noAuthNoPriv** or **authNoPriv** security-level option are disabled.
- The traps configured for SNMPv2 or SNMPv3 users with the **noAuthNoPriv** security-level option are disabled.
- The **MD5** and **DES** Authentication type and Privacy type are disabled.
- It also ensures only FIPS-compliant ciphers in SSH, webserver, and KVM connections.



CHAPTER 15

Managing Firmware

This chapter includes the following sections:

Firmware Management Overview

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

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

  You can upload a firmware image from either a local file system or a TFTP server.
- Bootloader firmware—The bootloader firmware cannot be installed from the Cisco IMC. You can install this firmware using the Host Upgrade Utility.

Firmware for the following individual components can be updated:

- BMC
- BIOS
- CMC
- SAS Expander

- Adapter

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

Note If you choose to update the firmware of individual components, **you must first update and activate the CMC firmware** to the version that you want to update the individual component.

Viewing Firmware Components

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

Step 2 In the **General** tab's **Firmware Management** area, review the following information:

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

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

Viewing the HDD Firmware

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

Step 2 In the **Firmware Management** pane, click **HDD**.

Step 3 In the **HDD** tab's **HDD Firmware Management** area, review the following information:

Name	Description
Update button	Opens a dialog box that allows you to install a firmware image file that is available to your local machine or on a remote server.
Slot Number column	The slot in which the physical drive is present.
Vendor column	The vendor of the physical drive.
Product ID column	The product ID of the physical drive.
Product Rev Label column	The product revision number of the physical drive, if any.
Health column	The health of the physical drive.
Update Stage column	The status of the firmware activation of the physical drive.
Progress (%) column	The progress of the operation, in percentage.

What to do next

Update or activate HDD firmware.

Updating the Firmware

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

Note If you choose to update the firmware of individual components, **you must first update and activate the CMC firmware** to the version that you want to update the individual component.

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

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

The **Update Firmware** dialog box appears.

Step 3 Review the following information in the dialog box:

Name	Description
Install Firmware through Browser Client radio button	If the firmware package resides on a local machine, click this radio button.
Install Firmware through Remote Server radio button	If the firmware package resides on a remote server, click this radio button.

Step 4 To install the firmware through the browser client, click **Browse** and navigate to the firmware file that you want to install.

Step 5 After you select the file, click **Install Firmware**.

Step 6 To update the firmware using remote server, select the remote server type from the **Install Firmware from** drop-down list. This could be one of the following:

- **TFTP**
- **FTP**
- **SFTP**
- **SCP**
- **HTTP**

Step 7 Depending on the remote server type you choose, enter details in the server's **IP/Hostname** and **Image Path and Filename** fields.

Once you install the firmware, the new image replaces the non-active image. You can activate the image after it is installed.

Important For FTP, SFTP, and SCP server types, you need to provide user credentials.

Step 8 Click **Install Firmware** to begin download and installation.

Activating the Firmware

Step 1 In the **Admin** menu, click **Firmware Management**.

Step 2 In the **Firmware Management** area, select a component from the **Component** column and click **Activate**.

The **Activate Firmware** dialog box appears.

Step 3 In the **Activate Firmware** dialog box, select the desired firmware image (radio button) to activate. This image becomes the running version.

Step 4 Click **Activate Firmware**.

Depending on the firmware image you chose, the activation process begins.

Important While the activation is in progress, do not:

- Reset, power off, or shut down the server
- Reboot or reset BMC
- Activate any other firmware
- Export technical support or configuration data

Cancelling Firmware Activation

Before you begin

BIOS firmware must be in **Activation Pending** state for you to cancel the activation.

Step 1 In the **Admin** menu, click **Firmware Management**.

Step 2 In the **Firmware Management** area, select the BIOS firmware for which you want to cancel the activation.

Step 3 Click **Cancel Activation**.

Cancel Activation button is displayed only when you choose a BIOS firmware that is in **Activation Pending**

Updating the HDD Firmware

Step 1 In the **Admin** menu, click **Firmware Management**.

Step 2 In the **Firmware Management** pane, click **HDD**.

Step 3 In the **HDD** tab's **HDD Firmware Management** area, review the following information:

Name	Description
Update button	Opens a dialog box that allows you to install a firmware image file that is available to your local machine or on a remote server.
Slot Number column	The slot in which the physical drive is present.

Name	Description
Vendor column	The vendor of the physical drive.
Product ID column	The product ID of the physical drive.
Product Rev Label column	The product revision number of the physical drive, if any.
Health column	The health of the physical drive.
Update Stage column	The status of the firmware activation of the physical drive.
Progress (%) column	The progress of the operation, in percentage.

Step 4 Select a slot number from the **Slot Number** column and click **Update**.

The **Update Firmware** dialog box appears.

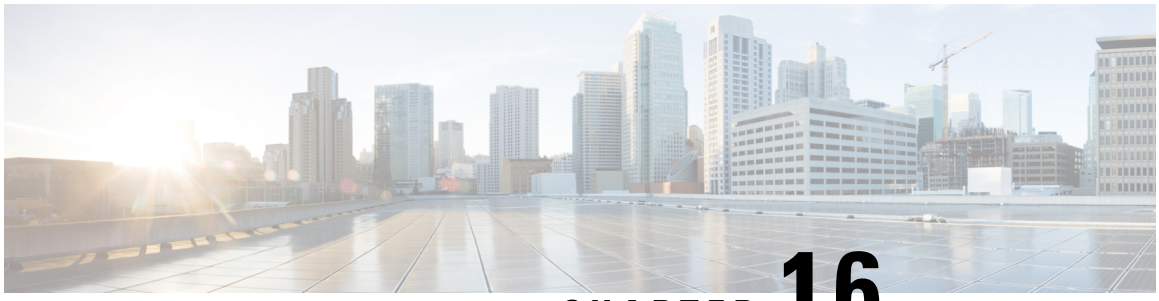
Step 5 Review the following information in the dialog box:

Name	Description
Install HDD Firmware through Browser Client checkbox	If the firmware package resides on a local machine, click this radio button.
Install HDD Firmware through Remote Server checkbox	If the firmware package resides on a remote server, click this radio button and complete the required fields.

Step 6 Click **Install Firmware** to begin download and installation.

What to do next

Activate HDD firmware.



CHAPTER 16

Viewing Faults and Logs

This chapter includes the following sections:

Faults Summary

Viewing the Fault Summary

Step 1 In the **Navigation** pane, click the **Chassis** menu.

Step 2 In the **Chassis** menu, click **Faults and Logs**.

Step 3 In the **Faults Summary** tab, review the following information:

Table 19: Actions Area

Name	Description
Total	Displays the total number of rows in the Fault Entries table.
Column drop-down list	Allows you to choose the columns you wish to be displayed.

Name	Description
Show drop-down list	Customize the way you want to view fault entries using filters. These can be: • **Quick Filter** - Default view. • **Advanced Filter** - Filter options to display the fault entries based on one or more criteria. Using the matching rule, you can view entries matching all the rules or any one combination of rules you specified in the **Filter** fields. Click **Go** to view the entries matching the filter criteria that you set. Click the **Save** icon to save the filter criteria that you set. This becomes a user-defined filter which you can use later. **Note** The user-defined filter appears in the **Manage Preset Filters** dialog box. • **All** - Displays all entries • **Manage Preset Filters** - Displays user-defined filters. You can edit or remove the user-defined filter from this dialog box. • **List of pre-defined filters** - Displays the system-defined filters. **Note** You can use the **Filter** icon to hide or unhide the filter fields.

Table 20: Fault Entries Area

Name	Description
Time	The time when the fault occurred.
Severity	This can be one of the following: • **Cleared** - A fault or condition was cleared. • **Critical** • **Info** • **Major** • **Minor** • **Warning**
Code	The unique identifier assigned to the fault.

Name	Description
DN	The distinguished name (DN) is a hierarchical representation of the device endpoint and its instance on the server.
Probable Cause	The unique identifier associated with the event that caused the fault.
Description	More information about the fault. It also includes a proposed solution.

Fault History

Viewing Faults History

Step 1 In the **Navigation** pane, click the **Chassis** menu.

Step 2 In the **Chassis** menu, click **Faults and Logs**.

Step 3 In the **Faults History** tab, review the following information

Table 21: Actions Area

Name	Description
Total	Displays the total number of rows in the Fault History table.
Column drop-down list	Allows you to choose the columns you wish to be displayed.

Name	Description
Show drop-down list	Customize the way you want to view fault history entries using filters. These can be: • **Quick Filter** - Default view. • **Advanced Filter** - Filter options to display the entries based on one or more criteria. Using the matching rule, you can view entries matching all the rules or any one combination of rules you specified in the **Filter** fields. Click **Go** to view the entries matching the filter criteria that you set. Click the **Save** icon to save the filter criteria that you set. This becomes a user-defined filter which you can use later. **Note** The user-defined filter appears in the **Manage Preset Filters** dialog box. • **All** - Displays all entries • **Manage Preset Filters** - Displays user-defined filters. You can edit or remove the user-defined filter from this dialog box. • **List of pre-defined filters** - Displays the system-defined filters. **Note** You can use the **Filter** icon to hide or unhide the filter fields.

Table 22: Faults History Area

Name	Description
Time	The time when the fault occurred.
Severity	This can be one of the following: • **Emergency** • **Alert** • **Critical** • **Error** • **Warning** • **Notice** • **Informational** • **Debug**

Name	Description
Source	The software module that logged the event.
Probable Cause	The unique identifier associated with the event that caused the fault.
Description	More information about the fault. It also includes a proposed solution.

What to do next

Cisco IMC Log

Viewing the Cisco IMC Log

Step 1 In the **Navigation** pane, click the **Chassis** menu.

Step 2 In the **Chassis** menu, click **Faults and Logs**.

Step 3 In the **Cisco IMC Log** tab, review the following information:

Table 23: Actions Area

Name	Description
Clear Log button	Clears all log files. **Note** This option is only available if your user ID is assigned the **admin** or **user** user role.
Total	Displays the total number of rows in the Cisco IMC Log table.
Column drop-down list	Allows you to choose the columns you wish to be displayed.

Name	Description
Show drop-down list	Customize the way you want to view Cisco IMC log entries using filters. These can be: • **Quick Filter** - Default view. • **Advanced Filter** - Filter options to display the log entries based on one or more criteria. Using the matching rule, you can view entries matching all the rules or any one combination of rules you specified in the **Filter** fields. Click **Go** to view the entries matching the filter criteria that you set. Click the **Save** icon to save the filter criteria that you set. This becomes a user-defined filter which you can use later. **Note** The user-defined filter appears in the **Manage Preset Filters** dialog box. • **All** - Displays all entries • **Manage Preset Filters** - Displays user-defined filters. You can edit or remove the user-defined filter from this dialog box. • **List of pre-defined filters** - Displays the system-defined filters. **Note** You can use the **Filter** icon to hide or unhide the filter fields.

Table 24: Cisco IMC Log Table

Name	Description
Time column	The date and time the event occurred.

Name	Description
Severity column	The event severity. This can be one of the following: • **Emergency** • **Alert** • **Critical** • **Error** • **Warning** • **Notice** • **Informational** • **Debug**
Source column	The software module that logged the event.
Description column	A description of the event.

System Event Log

Viewing System Event Logs

Step 1 In the **Navigation** pane, click the **Chassis** menu.

Step 2 In the **Chassis** menu, click **Faults and Logs**.

Step 3 On the **System Event Log** tab, review the following information:

Table 25: Actions Area

Name	Description
Clear Log button	Clears all events from the log file. **Note** This option is only available if your user ID is assigned the **admin** or **user** user role.
Chassis drop-down list	Select a chassis or a server to view its logs.
Total	Displays the total number of rows in the System Event Log table.
Column drop-down list	Allows you to choose the columns you wish to be displayed.

Name	Description
Show drop-down list	Customize the way you want to view events using filters. These can be: • **Quick Filter** - Default view. • **Advanced Filter** - Filter options to display the events based on one or more criteria. Using the matching rule, you can view entries matching all the rules or any one combination of rules you specified in the **Filter** fields. Click **Go** to view the entries matching the filter criteria that you set. Click the **Save** icon to save the filter criteria that you set. This becomes a user-defined filter which you can use later. **Note** The user-defined filter appears in the **Manage Preset Filters** dialog box. • **All** - Displays all entries • **Manage Preset Filters** - Displays user-defined filters. You can edit or remove the user-defined filter from this dialog box. • **List of pre-defined filters** - Displays the system-defined filters. **Note** You can use the **Filter** icon to hide or unhide the filter fields.

Table 26: System Event Log Table

Name	Description
Time column	The date and time the event occurred.
Severity column	The severity field includes both text and a color-coded icon. For the icon, green indicates normal operation, yellow is informational, and warning, critical, and non-recoverable errors are shown in shades of red.
Description column	A description of the event.

Logging Controls

Viewing Logging Controls

Step 1 In the **Navigation** pane, click the **Chassis** menu.

Step 2 In the **Chassis** menu, click **Faults and Logs**.

Step 3 In the **Logging Controls** tab, review the following information:

Remote Logging

Name	Description
Enabled check box	If checked, the Cisco IMC sends log messages to the Syslog server named in the **IP Address** field.
Enable Secure Remote Syslog	If checked, Cisco IMC makes a secure, encrypted outbound connection to remote syslog servers supporting secure connectivity for logging. **Note** If this check box is selected, then the **Protocol** field is disabled, by default.
Host Name/IP Address field	The address of the Syslog server on which the Cisco IMC log should be stored. You can set an IPv4 or IPv6 address or a domain name as the remote system address.
Port field	Enter a destination port number of the Syslog server within the range 1 to 65535. The default port number is 514.
Protocol field	The transport layer protocol for transmission of syslog messages. You can select one of the following: • TCP • UDP
Handshake Status	If secured remote syslog is enabled, then Cisco IMC performs SSL handshake to verify if the certificate is for the given IP address.

Name	Description
Minimum Severity to Report field	Specify the lowest level of messages that will be included in the remote logs. You can select one of the following: • **Emergency** • **Alert** • **Critical** • **Error** • **Warning** • **Notice** • **Informational** • **Debug**

Note The Cisco IMC does not remotely log any messages with a severity below the selected severity. For example, if you select **Error**, then the Cisco IMC remote log contains all messages with the severity **Emergency**, **Alert**, **Critical**, or **Error**. It does not show **Warning**, **Notice**, **Informational**, or **Debug** messages.

Local Logging

This area displays only the **Minimum Severity to Report** drop-down list as shown in the table above. You can specify the lowest level of messages to be included in the local log

Sending the Cisco IMC Log to a Remote Server

You can configure profiles for one or two remote syslog servers to receive Cisco IMC log entries.

Before you begin

- The remote syslog server must be configured to receive logs from a remote host.
- The remote syslog server must be configured to receive all types of logs, including authentication-related logs.
- The remote syslog server's firewall must be configured to allow syslog messages to reach the syslog server.

Step 1 In the **Navigation** pane, click the **Chassis** menu.

Step 2 In the **Chassis** menu, click **Faults and Logs**.

Step 3 In either of the **Remote Syslog Server** areas, complete the following fields:

Name	Description
Enabled check box	If checked, the Cisco IMC sends log messages to the Syslog server named in the **IP Address** field.

Name	Description
Host Name/IP Address field	The address of the Syslog server on which the Cisco IMC log should be stored. You can set an IPv4 or IPv6 address or a domain name as the remote system address.
Port field	Enter a destination port number of the Syslog server within the range 1 to 65535. The default port number is 514.

Step 4 (Optional) In the **Minimum Severity to Report** drop-down list, specify the lowest level of messages that will be included in the remote logs.

You can select one of the following, in decreasing order of severity:

- **Emergency**
- **Alert**
- **Critical**
- **Error**
- **Warning**
- **Notice**
- **Informational**
- **Debug**

Note Cisco IMC does not remotely log any messages with a severity below the selected severity. For example, if you select **Error**, then the Cisco IMC remote log will contain all messages with the severity Emergency, Alert, Critical, or Error. It will not show Warning, Notice, Informational, or Debug messages.

Step 5 Click **Save Changes**.

Configuring the Cisco IMC Log Threshold

Before you begin

Step 1 In the **Navigation** pane, click the **Chassis** menu.

Step 2 In the **Chassis** menu, click **Faults and Logs**.

Step 3 Required: In the **Local Logging** area, use the **Minimum Severity to Report** drop-down list to specify the lowest level of messages that will be included in the Cisco IMC log.

You can select one of the following, in decreasing order of severity:

- **Emergency**
- **Alert**
- **Critical**

- **Error**
- **Warning**
- **Notice**
- **Informational**
- **Debug**

Note Cisco IMC does not log any messages with a severity below the selected severity. For example, if you select **Error**, then the Cisco IMC log will contain all messages with the severity Emergency, Alert, Critical, or Error. It will not show Warning, Notice, Informational, or Debug messages.

Sending a Test Cisco IMC Log to a Remote Server

Before you begin

- The remote syslog server must be configured to receive logs from a remote host.
- The remote syslog server must be configured to receive all types of logs, including authentication-related logs.
- The remote syslog server's firewall must be configured to allow syslog messages to reach the syslog server.

Step 1 In the **Navigation** pane, click the **Chassis** menu.

Step 2 In the **Chassis** menu, click **Faults and Logs**.

Step 3 In the **Faults and Logs** pane, click the **Logging Controls** tab.

Step 4 In the **Action** area, click **Send Test Syslog**.

A test Cisco IMC log is sent to the configured remote servers.

Managing the Remote Syslog Certificate

Beginning with release 4.2(2a), you can upload a remote syslog certificate to Cisco UCS C-series servers. You can upload the certificate to one or two Cisco UCS C-series servers.

Uploading a Remote Syslog Certificate

You can upload a remote syslog certificate either from a remote server location or from a local location.

Before you begin

- You must log in as a user with admin privileges.
- The certificate file to be uploaded must reside on a locally accessible file system.

- The following certificate formats are supported:
  - .crt
  - .cer
  - .pem

Step 1 In the **Navigation** pane, click the **Chassis** menu.

Step 2 In the **Chassis** menu, select **Faults and Logs**.

Step 3 In the **Faults and Logs** pane, select **Logging Controls**.

Step 4 To upload the remote syslog certificate, click the **Upload Remote Syslog Certificate** button.

The **Upload Remote Syslog Certificate** dialog box appears.

Step 5 Select a server to which you want to upload the remote syslog certificate from the **Select Server:** drop-down list

Step 6 You can upload the certificate using one of the following methods.

- Upload from remote location
- Upload through browser Client
- Paste the certificate content directly in the **Paste Remote Syslog Certificate** text box.

- **Upload from remote location**: Select this radio button to upload a remote syslog certificate from a remote location.

Name	Description
Upload from remote location field	Select from one of the following protocols: • TFTP • FTP • SCP • SFTP • HTTP **Note** If you select FTP, SCP or SFTP, you will be prompted to enter your username and password.
Server IP/ Hostname button	Enter the remote server IP address or hostname.
Path and Filename	Enter the filepath on the remote server from where you want to upload the remote syslog certificate along with the filename.
Username	Enter the user name for your remote server.
Password	Password for your remote server.

- **Upload through browser Client**: Select this radio button to upload a remote syslog certificate using a browser client.

Click **Browse** and navigate to the location from where you want to upload the remote syslog certificate.

- **Paste Remote Syslog Certificate Content**: Select this radio button to paste the remote syslog certificate details directly in the text box.

Deleting a Remote Syslog Certificate

You can delete a remote syslog certificate from the server.

Before you begin

You must log in as a user with admin privileges.

Step 1 In the **Navigation** pane, click the **Chassis** menu.

Step 2 In the **Chassis** menu, select **Faults and Logs**.

Step 3 In the **Faults and Logs** pane, select **Logging Controls**.

Step 4 To delete the remote syslog certificate, click the **Delete Remote Syslog Certificate** button.

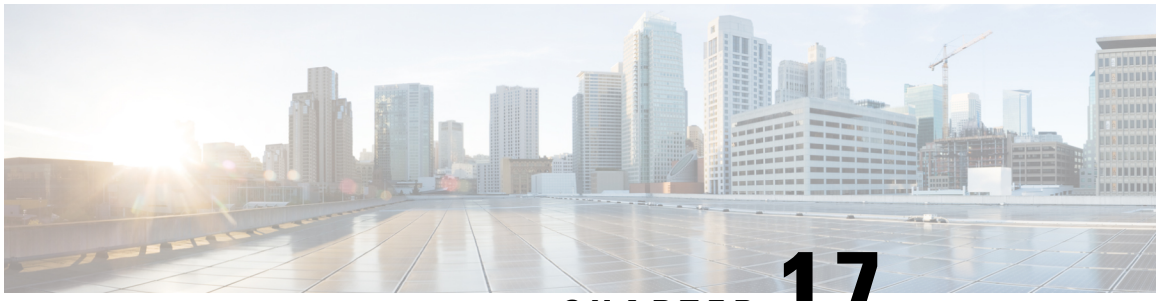
The **Delete Remote Syslog Certificate** dialog box appears.

Step 5 Select the respective check box of the server from which you want to delete the remote syslog certificate.

Step 6 Click **Delete**.

The confirmation message of the deletion is displayed in a pop-up window.

Step 7 Click **OK**.



CHAPTER 17

Server Utilities

This chapter includes the following sections:

Exporting Technical Support Data

Exporting Technical Support Data

Perform this task when requested by the Cisco Technical Assistance Center (TAC). This utility creates a summary report containing configuration information, logs and diagnostic data that will help TAC in troubleshooting and resolving a technical issue.

Step 1 In the **Navigation** pane, click the **Admin** menu.

Step 2 In the **Admin** menu, click **Utilities**.

Step 3 In the **Actions** area of the **Utilities** pane, click **Export Technical Support Data**.

Step 4 In the **Export Technical Support Data** dialog box, complete the following fields:

Name	Description
Select Component checkbox	Check to select a component. This can be one of the following: • **All** • **CMC** • **PEERCMC** • **BMC 1** • **BMC 2** Depending on the component you choose, technical support data for that component is exported. **Note** If you choose **All**, the technical data for all components is exported.
Export Technical Support Data to drop-down list	The remote server type. This can be one of the following: • **TFTP Server** • **FTP Server** • **SFTP Server** • **SCP Server** • **HTTP Server** **Note** If you chose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message *Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*. Click Yes or No depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.
Server IP/Hostname field	The IP address or hostname of the server on which the support data file should be stored. Depending on the setting in the **Export Technical Support Data to** drop-down list, the name of the field may vary.
Path and Filename field	The path and filename Cisco IMC should use when exporting the file to the remote server. **Note** If the server includes any of the supported network adapter cards, the data file also includes technical support data from the adapter card.
Username	The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP.
Password	The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP.

Step 5 Click **Export**.

What to do next

Provide the generated report file to Cisco TAC.

Downloading Technical Support Data to a Local File

Perform this task when requested by the Cisco Technical Assistance Center (TAC). This utility creates a summary report containing configuration information, logs and diagnostic data that will help TAC in troubleshooting and resolving a technical issue.

Step 1 In the **Navigation** pane, click the **Admin** menu.

Step 2 In the **Admin** menu, click **Utilities**.

Step 3 In the **Actions** area of the **Utilities** pane, click **Generate Technical Support Data for Local Download**.

Step 4 In the **Download Technical Support Data to Local File** dialog box, complete the following fields:

Name	Description
Generate Technical Support Data radio button	Cisco IMC disables this radio button when there is no technical support data file to download. Click **Generate** to create the data file. When data collection is complete, click **Download Technical Support Data to Local File** in the **Actions** area to download the file.
Select Component checkbox	Check to select a component. This can be one of the following: • **All** • **CMC** • **PEERCMC** • **BMC 1** • **BMC 2** Depending on the component you choose, technical support data for that component is downloaded. **Note** If you choose **All**, the technical data for all components is downloaded.
Download to local file radio button	Cisco IMC enables this radio button when a technical support data file is available to download. To download the existing file, select this option and click **Download**. **Note** If the server includes any of the supported network adapter cards, the data file also includes technical support data from the adapter card.

Name	Description
Generate and Download button	Allows you to generate and download the technical support data file.
Generate button	Allows you to generate the technical support data file.
Download button	Allows you to download the technical support data file after it is generated.

Step 5 Click **Generate** to create the data file. When data collection is complete, click **Download Technical Support Data to Local File** in the **Actions** area to download the file..

What to do next

Provide the generated report file to Cisco TAC.

Resetting to Factory Default

On rare occasions, such as an issue with the current running firmware or troubleshooting a server, you might require to reset the server components to the factory default. When this happens, all user-configurable settings are reset.

This procedure is not part of the normal server maintenance. After you reset the server components, you are logged off and must log in again. You might also lose connectivity and might need to reconfigure the network settings. Some of the inventory information might not be available during this transition.

When you reset the BMC to factory settings, the serial number is displayed in the Cisco IMCXXXXXX format, where XXXXXX is the serial number of the server.

Before you begin

You must log in as a user with admin privileges to reset the server components to factory defaults.

Step 1 In the **Navigation** pane, click the **Admin** menu.

Step 2 In the **Admin** menu, click **Utilities**.

Step 3 In the **Actions** area of the **Utilities** pane, click **Reset to Factory Default**.

Step 4 In the **Reset to Factory Default** dialog box, review the following information:

Name	Description
All checkbox	If checked, it resets all the components of the server to factory settings. Expand to select the specific component that you want to reset to factory settings.
Chassis checkbox	If checked, it resets the chassis to factory settings.
BMC 1 checkbox	If checked, it resets BMC 1 to factory settings.
BMC 2 checkbox	If checked, it resets BMC 2 to factory settings.

Name	Description
Storage checkbox	If checked, it resets all the available storage adapters to factory settings. Expand to select the specific storage adapters that you want to reset to factory settings. **Note** The host must be powered on to reset storage adapters to factory defaults.
VIC checkbox	If checked, it resets all the available VICs to factory settings. Expand to select the specific VICs that you want to reset to factory settings. **Note** The host must be powered on to reset VIC adapters to factory defaults.
Reset button	Resets the selected component to the factory settings. **Note** When you reset to factory default settings, the network configuration mode is set to **Cisco Card** mode by default for S3260 M5 servers.

Step 5 Click **Reset** to reset the selected components to the factory-default settings.

A reboot of Cisco IMC, while the host is performing BIOS POST (Power on Self Test) or is in EFI shell, powers down the host for a short amount of time. Cisco IMC powers on when it is ready. Upon restart, the network configuration mode is set to **Cisco Card** mode by default.

Exporting and Importing the Cisco IMC Configuration

Exporting and Importing the Cisco IMC Configuration

To perform a backup of the Cisco IMC configuration, you take a snapshot of the system configuration and export the resulting Cisco IMC 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 Cisco IMC configuration file to the same system or you can import it to another Cisco IMC 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 Cisco IMC configuration file is an XML text file or JSON file whose structure and elements correspond to the Cisco IMC command modes.

Note The configuration file is supported in XML format in Cisco UCS M5 and M6 servers in GUI, CLI, XML API and Redfish API interfaces.

The configuration file is supported in JSON format in Cisco UCS M7 servers in GUI, CLI, XML API and Redfish API interfaces.

When performing an export or import operation, consider these guidelines:

- You can perform an export or an import while the system is up and running. While an export operation has no impact on the server or network traffic, some modifications caused by an import operation, such as IP address changes, can disrupt traffic or cause a server reboot.
- You cannot execute an export and an import simultaneously.

You can perform an import or an export operation on the following features:

- Cisco IMC version

Note You can only export this information.

- Network settings
- Technical support
- Logging control for local and remote logs
- Power policies
- BIOS - BIOS Parameters

Note Precision boot is not supported.

- Communication services
- Remote presence
- User management - LDAP
- SNMP
- Dynamic Storage Configuration
- Chassis Description

Exporting the Cisco IMC Configuration

Note For security reasons, this operation does not export user accounts or the server certificate.

Before you begin

Obtain the backup remote server IP address.

Step 1 In the **Navigation** pane, click the **Admin** menu.

Step 2 In the **Admin** menu, click **Utilities**.

Step 3 In the **Actions** area of the **Utilities** pane, click **Export Configuration**.

Step 4 In the **Export Configuration** dialog box, complete the following fields:

Name	Description
Select Component for Export drop-down list	The component type. This can be one of the following: • **Chassis** • **BMC 1** • **BMC 2** • **VIC Adapter(s)** Depending on the component you choose, the configuration of that component is exported.
Export To drop-down list	The location where you want to save the configuration file. This can be one of the following: • **Local**: Select this option and click **Export** to save the configuration file to a drive that is local to the computer running the Cisco IMC GUI.. When you select this option, Cisco IMC GUI displays a **File Download** dialog box that lets you navigate to the location to which the configuration file should be saved. • **Remote Server**: Select this option to import the configuration file from a remote server. When you select this option, Cisco IMC GUI displays the remote server fields.

Name	Description
Export To drop-down list	The remote server type. This can be one of the following: • **TFTP Server** • **FTP Server** • **SFTP Server** • **SCP Server** • **HTTP Server** **Note** If you chose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message *Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*. Click Yes or No depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.
Server IP/Hostname field	The IPv4 or IPv6 address, or hostname of the server to which the configuration file will be exported. Depending on the remote server type selected in the **Export to** drop-down list, the name of the field may vary.
Path and Filename field	The path and filename Cisco IMC should use when exporting the file to the remote server.
Username	The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP.
Password	The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP.
Passphrase	The passphrase that uses the AES256 algorithm to encrypt the LDAP and SNMP v3 user passwords in the exported configuration files. Enter a string of 6 to 127 characters. Do not enter the following characters: ! # $ & < > ? ; ' | ` ~ \ % ^ ( )" This option is available only with CMC export.

Step 5 Click **Export**.

Importing the Cisco IMC Configuration

Before you begin

If you want to restore the SNMP configuration information when you import the configuration file, make sure that SNMP is disabled on this server before you do the import. If SNMP is enabled when you perform the import, Cisco IMC does not overwrite the current values with those saved in the configuration file.

Step 1 In the **Navigation** pane, click the **Admin** menu.

Step 2 In the **Admin** menu, click **Utilities**.

Step 3 In the **Actions** area of the **Utilities** pane, click **Import Configuration**.

Step 4 In the **Import Configuration** dialog box, complete the following fields:

Name	Description
Select Component for Import drop-down list	The component type. This can be one of the following: • **Chassis** • **BMC 1** • **BMC 2** • **VIC Adapter(s)** Depending on the component you choose, the configuration of that component is imported.
Import From drop-down list	The location of the configuration file. This can be one of the following: • **Local**: Select this option to import the configuration file to a drive that is local to the computer running Cisco IMC GUI. When you select this option, Cisco IMC GUI displays a **Browse** button that lets you navigate to the file you want to import. • **Remote Server**: Select this option to import the configuration file from a remote server. When you select this option, Cisco IMC GUI displays the remote server fields.
Import From drop-down list	**Note** These options are available only when you choose **Remote**. The remote server type. This can be one of the following: • **TFTP Server** • **FTP Server** • **SFTP Server** • **SCP Server** • **HTTP Server** **Note** If you chose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message *Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*. Click Yes or No depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.

Name	Description
Server IP/Hostname field	The IPv4 or IPv6 address, or hostname of the server on which the configuration file resides. Depending on the remote server type selected in the **Import From** drop-down list, the name of the field might vary.
Path and Filename field	The path and filename of the configuration file on the remote server.
Username	The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP.
Password	The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP.
Passphrase	The passphrase that uses the AES256 algorithm to encrypt the LDAP and SNMP v3 user passwords in the imported configuration files. Enter a string of 6 to 127 characters. Do not enter the following characters: ! # $ & < > ? ; ' | ` ~ \ % ^ ( )" **Note** If you edit the encrypted sections in the configuration file and try to import it, the edits will be ignored and the import operation displays a partially successful message.

Step 5 Click **Import**.

Generating Non Maskable Interrupts to the Host

In some situations, the server might hang and not respond to traditional debug mechanisms. By generating a non maskable interrupt (NMI) to the host, you can create and send a crash dump file of the server and use it to debug the server.

Depending on the type of operating system associated with the server, this task might restart the OS.

Before you begin

- You must log in as a user with admin privileges.
- The server must be powered on.

Step 1 In the **Navigation** pane, click the **Admin** menu.

Step 2 In the **Admin** menu, click **Utilities**.

Step 3 In the **Actions** area of the **Utilities** pane, click **Generate NMI to Host**.

Step 4 In the **Generate NMI to Host** dialog box, review the following information:

Actions	Description
Generate NMI to drop-down list	Allows you to select the server for which you want to generate the non maskable interrupt (NMI). This can be one of the following: • **Server 1** • **Server 2**

Step 5 Click **Send**.

This action sends an NMI signal to the host, which might restart the OS.

Adding or Updating the Cisco IMC Banner

You can add or update the Cisco IMC banner by entering important information such as copyright or customized messages. Complete the following steps:

Before you begin

Step 1 In the **Navigation** pane, click the **Admin** menu.

Step 2 In the **Admin** menu, click **Utilities**.

Step 3 In the **Actions** area of the **Utilities** pane, click **Add/Update Cisco IMC Banner**.

Step 4 In the **Add/Update Cisco IMC Banner** dialog box, complete the following fields:

Name	Description
Banner (80 Chars per line. Max 2K Chars.) field	Enter copyright information or messages that you want to display on the login screen, before logging on to the Web UI or the command line interface.
Restart SSH checkbox	When checked, the active SSH sessions are terminated after you click the **Save Banner** button.

Step 5 Click **Save Banner**.

What to do next

Viewing Cisco IMC Last Reset Reason

Step 1 In the **Navigation** pane, click the **Admin** menu.

Step 2 In the **Admin** menu, click **Utilities**.

Step 3 In the **Actions** area of the **Utilities** pane, view the following information under the **Last Reset Reason** area.

Name	Description
Component field	The component that was last reset.
Status field	The reason why the component was last reset. This can be one of the following: • **watchdog-reset**—The watchdog timer expired due to kernel panic or hung task. • **ac-cycle**— PSU power cables are removed (no power input). • **graceful-reboot**— Cisco IMC reboot occurs.

Downloading Hardware Inventory to a Local File

Step 1 In the **Navigation** pane, click the **Admin** menu.

Step 2 In the **Admin** menu, click **Utilities**.

Step 3 In the **Actions** area of the **Utilities** pane, click **Generate Inventory Data**.

Step 4 In the **Generate Inventory Data** dialog box, complete the following fields:

Name	Description
Generate Inventory Data radio button	Cisco IMC displays this radio button when there is no hardware inventory data file to download.
Download to local file radio button	Cisco IMC enables this radio button when a inventory data file is available to download. To download the existing file, select this option and click **Download**.

Step 5 Click **Generate** to create the data file. When data collection is complete, select the **Download Inventory Data to Local File** radio button and click **Download** to download the file locally.

Exporting Hardware Inventory Data to a Remote Server

Step 1 In the **Navigation** pane, click the **Admin** menu.

Step 2 In the **Admin** menu, click **Utilities**.

Step 3 In the **Actions** area of the **Utilities** pane, click **Export Hardware Inventory Data to Remote**.

Step 4 In the **Export Hardware Inventory Data** dialog box, complete the following fields:

Name	Description
Export Hardware Inventory Data to drop-down list	The remote server type. This can be one of the following: • **TFTP Server** • **FTP Server** • **SFTP Server** • **SCP Server** • **HTTP Server** **Note** If you chose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message *Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*. Click Yes or No depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.
Server IP/Hostname field	The IP address or hostname of the server on which the data file should be stored. Depending on the setting in the **Export Hardware Inventory Data to** drop-down list, the name of the field may vary.
Path and Filename field	The path and filename Cisco IMC should use when exporting the file to the remote server.
Username	The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP.
Password	The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP.

Step 5 Click **Export**.

Uploading a PID Catalog

Before you begin

You must log in as a user with admin privileges to upload a PID catalog.

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Utilities**.

Step 3 In the **Work** pane, click the **Upload PID Catalog** link.

The **Upload PID Catalog** dialog box appears.

Depending on the location of the catalog file, choose one of the options.

Step 4 In the **Upload PID Catalog from Local File** dialog box, click **Browse** and use the **Choose File to Upload** dialog box to select the catalog file that you want to upload.

Name	Description
File field	The PID catalog file that you want to upload.
Browse button	Opens a dialog box that allows you to navigate to the appropriate file.

Step 5 In the **Upload PID Catalog from Remote Server** dialog box, complete the following fields:

Name	Description
Upload PID Catalog from Remote Server drop-down list	The remote server type. This can be one of the following: • **TFTP** • **FTP** • **SFTP** • **SCP** • **HTTP**
Server IP/Hostname field	The IP address or hostname of the server on which the PID catalog information is available. Depending on the setting in the Upload PID Catalog from drop-down list, the name of the field may vary.
Path and Filename field	The path and filename of the catalog file on the remote server.
Username field	Username of the remote server.
Password field	Password of the remote server.
Upload button	Uploads the selected PID catalog. **Note** If you chose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message *Server (RSA) key fingerprint is <server_finger_print_ID> Do you wish to continue?*. Click Yes or No depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.

Name	Description
Cancel button	Closes the wizard without making any changes to the firmware versions stored on the server.

Activating a PID Catalog

Caution BMC reboots automatically once a PID catalog is activated.

You must reboot the server after activating a PID catalog.

Before you begin

You must log in as a user with admin privileges to activate a PID catalog.

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Utilities**.

Step 3 In the **Work** pane, click the **Activate PID Catalog** link.

The **Activate PID Catalog** dialog box appears. Complete the following fields:

Name	Description
Server check box	Allows you to select the server or servers for which you want to activate the PID Catalog.
Activate button	Allows you to activate the PID catalog.

Note The **Activate PID Catalog** link is greyed out when you log on to the system for the first time. It gets activated once you upload a PID catalog to the server. After you upload a PID file, the link remains active and you can activate the PID multiple times.

Deleting a PID Catalog

Caution BMC reboots automatically once a PID catalog is deleted.

You must reboot the server after deleting a PID catalog.

Before you begin

You must log in as a user with admin privileges to perform this task.

SUMMARY STEPS

1. In the **Navigation** pane, click the **Admin** tab.
2. In the **Admin** tab, click **Utilities**.
3. In the **Actions** area of the Utilities pane, click **Delete PID Catalog** and click **OK** to confirm.

DETAILED STEPS

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, click **Utilities**.

Step 3 In the **Actions** area of the Utilities pane, click **Delete PID Catalog** and click **OK** to confirm.

Note You can delete a PID catalog only if it has been previously updated and activated.

Viewing Intersight Device Connector Properties

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, click **Device Connector**.

Step 3 In the **Intersight Management** area, review the following information:

Action Name	Description
Enabled radio button	Allows you to enable or disable the Intersight management. This can be one of the following: • **On**—Enables the Intersight management. You can claim this system and leverage the capabilities of Cisco Intersight. • **Off**—Disables the Intersight management. No communication will be allowed to Cisco Intersight.

Step 4 In the **Connection** area, review the following information:

Name	Description
Status field	Displays the status of the connection to Intersight. This can be one of the following: • **Administratively Disabled**—Indicates that the Intersight management has been disabled. • **DNS Misconfigured**— Indicates that the DNS details have not been configured in BMC. • **UCS Connect Network Error**—Indicates the invalid network configurations. • **Certification Validation Error**—Indicates invalid certificate. • **Claimed**—Indicates that the device is claimed in Intersight. • **Not Claimed**—Indicates that the device is registered, but not claimed in Intersight.
Access Mode	The mode will be **Allow Control** by default.
Details & Recommendations drop-down list	Lists the details and recommendations to fix the connection issues based on the status.
Device ID	This indicates the ID of the device.
Claim Code	This is the security code required to claim the device from Intersight. **Note** This code is available only when **Connection** status is **Not Claimed**.

Step 5 In the **Settings** area, review the following information:

Name	Description
General tab	**Access Mode** • **Read-only** — When the **Read-only** access mode is selected, you cannot configure the device through Intersight. • **Allow Control** — When the **Allow Control** mode is selected, you will have full control to configure the device through Intersight. **Configuration from Intersight only** This option is configurable only when **Allow Control** mode is enabled. The Configure Lockout options are as follows: **OFF**— To manage the device both locally and from Intersight you can turn OFF the option **Configuration from Intersight only** . The setting will terminate all the existing sessions (webUI, XML and CLI). **ON** — To lock out Cisco IMC configuration for Intersight you can turn ON the option **Configuration from Intersight only** . The setting will terminate all the existing sessions (webUI, XML and CLI). **Note** When you are logged in as admin in the Configuration Lock Out mode, the admin role will be mapped to the User role, so the interfaces behave as user logged in with the User role.
Proxy Configuration tab	Allows you to manually configure HTTPS proxy settings required for the Intersight connection.
HTTPS Proxy field radio button	OFF - Disables the HTTPS proxy settings. ON - Enables the HTTPS proxy settings.
Proxy Hostname/IP field	The IP address or the host name of the proxy server.
Proxy Port field	The port number of the proxy server.
Authentication toggle button	Enabling this option allows you to provide the credentials for the proxy server. **Note** The Device Connector does not mandate the format of the login credentials. They are passed as-is to the configured HTTP proxy server. Whether or not the username must be qualified with a domain name will depend on the configuration of the HTTP proxy server.
Username field **Password** field	The credentials for the proxy server.

Name	Description
Certificate Manager tab	Allows you to view a list of trusted certificates and import a valid trusted certificate. • **Import**—Allows you to select and Import a CA signed certificate. **Note** The imported certificates must be in the *.pem (base64 encoded) format. • You can view the list of certificates with the following information: • **Name**—Common name of the CA certificate. • **In Use**—Whether the certificate in the trust store was used to successfully verify the remote server. • **Issued By**—The issuing authority for the certificate. • **Expires**—The expiry date of the certificate. **Note** You cannot delete bundled certificates (certificates with the lock icon).

Recovering PCIe Switch

Before you begin

- You must log in as a user with admin privileges.
- The server must be powered on.

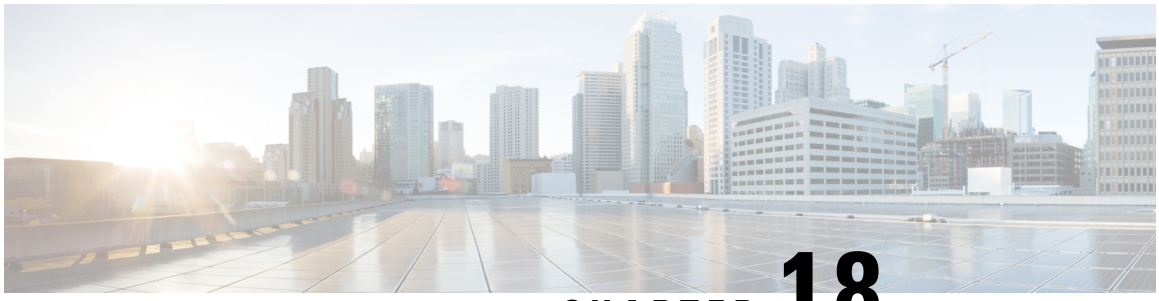
Step 1 In the **Navigation** pane, click the **Admin** menu.

Step 2 In the **Admin** menu, click **Utilities**.

Step 3 In the **Actions** area of the **Utilities** pane, click **Recover PCIe Switch**.

Step 4 In the **Recover PCIe Switch** dialog box, review the following information:

Name	Description
Controller drop-down	Lists the PCIe switches available on the server. You can select the switch on which you want to perform the recover controller action from this list.
Recover Controller button	Clicking on the recover controller button initiates the recovery of the chosen controller.
Cancel button	Cancels the action and closes the dialog box.



CHAPTER 18

Troubleshooting

This chapter includes the following sections:

Recording the Last Boot Process

Step 1 In the **Navigation** pane, click the **Compute** menu.

Step 2 In the work pane, click the **TroubleShooting** tab.

Step 3 In the **Bootstrap Process Recording** area of the **Troubleshooting** tab, check **Enable Recording** check-box.

By default, this option is enabled.

Caution This task is for troubleshooting purpose, and might impact Cisco IMC performance if it is enabled all the time.

Step 4 (Optional) If you want to record the boot process until BIOS POST, then check **Stop On BIOS POST** check-box.

Step 5 Click **Save Changes**

Step 6 On the tool bar above the **Work** pane, click **Power On Server**.

Step 7 In the **Actions** area, of the **Bootstrap Process Recording** pane, click **Play Recording**.

A confirmation dialog box with instructions on supported Java version appears.

Step 8 Review the instructions and click **Ok**.

The **DVR Player Controls** dialog box opens. This dialog box plays the recording of the last boot process. If you have enabled **Stop On BIOS POST** option then the system plays the recording process only till BIOS POST.

This recording can be reviewed to analyze the factors that caused the system to reboot.

Step 9 In the **Actions** area of the **Bootstrap Process Recording** area, click **Download Recording**.

Follow the instructions to download.

Note The file is saved in a `.dvc` format to a local drive. You can view this recording using KVM player or an offline player. Every time you choose **Download Recording** option, the last boot process is recorded, it autogenerate the file name, and save it in the path specified earlier.

Step 10 Once the download is complete, you can select the file that you want play the video of the recording, and click **Open**. A **DVR Player Controls** window opens and plays the video of the selected file.

Recording the Last Crash

Step 1 In the **Navigation** pane, click the **Compute** menu.

Step 2 In the work pane, click the **TroubleShooting** tab.

Step 3 In the **Crash Recording** area of the **Troubleshooting** tab, check the **Enable Recording** check-box.

Caution This task is for troubleshooting purpose, and might impact Cisco IMC performance if it is enabled all the time.

Step 4 Click **Save Changes**.
Capture Recording button in the **Actions** area is enabled.

Step 5 (Optional) In the **Actions** area, click **Capture Recording**, to capture the recording of the system that crashed automatically.

Note If you choose this option, it overwrites the existing crash records file. Click **OK** to continue.

Step 6 Click **Play Recording** in the **Actions** area to view the recording of the operations that ran on the server.

A confirmation dialog box with instructions on supported Java version appears.

Step 7 Review the instructions and click **Ok**.

The **DVR Player Controls** dialog box appears. This dialog box plays the recording of the operations that ran on the server in the last few minutes. This recording can be reviewed to analyze the factors that caused system to crash.

Step 8 In the **Actions** area of the **Crash Recording** area, click **Download Recording**.

Follow the instructions to download.

Note The file is saved in a `.dvc` format to a local drive. You can view this recording using KVM player or an offline player. Every time you choose **Download Recording** option, the last crash process is recorded, it autogenerate the file name, and save it in the path specified earlier.

Step 9 Once the download is complete, you can select the file that you want play the video of the recording, and click **Open**. A **DVR Player Controls** window opens and plays the video of the selected file.

Downloading a DVR Player

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Troubleshooting**.

Step 3 In the **Player** area of the **Troubleshooting** tab, click **Download Player**.

Step 4 Follow the instructions to download. These files are saved to your local drive as a zipped file in a .tgz file format.

The offline player is stored for Windows, Linux, and MAC.

Step 5 Extract the zip file. The zip file generally gets saved below the bootstrap file, and its name follows the format `offline.tgz`

Step 6 Open the script file that you want to review the video recording.

Note If you want to play the recording for Windows, then ensure that the Java version running on your system and in the script file are the same. If the Windows script file fails to play the recording, then follow these steps:

a) Extract the Windows script file to your desktop.
b) Open the file using notepad.
c) Search for jre, and replace the Java version to match the version running on your system. By default, the Java version is set to jre7.
d) Save the file.

After you update the Java version, you can delete the extracted files from your desktop.

Note Verification of Java version is required only for Windows OS. For Linux and MAC, the Java version is picked automatically.

Step 7 Navigate to the folder in which these files are downloaded and open the script file that you want to play the video recording. The DVR player is launched, playing the video of the operations that ran on the server.

Playing a Recorded Video Using the DVR Player on the KVM Console

Step 1 In the **Navigation** pane, click the **Server** tab.

Step 2 On the **Server** tab, click **Sensors**.

Step 3 In the **Remote Presence** pane, click the **Virtual KVM** tab.

Step 4 In the **Actions** area of the **Virtual KVM** tab, click **Launch KVM Console**.

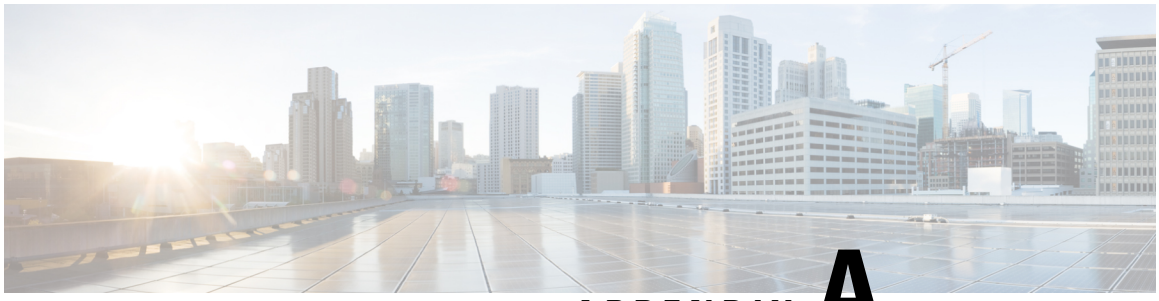
Note You can also launch KVM console by clicking **Launch KVM Console** button on the toolbar displayed above the **Work** pane.

The **KVM Console** opens in a separate window.

Step 5 On the **KVM Console** window, choose **Tools** > **Recorder /Playback Controls**.
A DVR Player Controls window opens.

Step 6 On the **DVR Player Controls** window, click **Open** button.

Step 7 Choose the file that you want to play the recording, and click **Open**.
The DVR player is launched, playing the video of the operations that ran on the server.



APPENDIX A

BIOS Parameters by Server Model

This appendix contains the following sections:

S3260 M3 Servers

Main Tab

Name	Description
Reboot Host Immediately checkbox	Upon checking, reboots the host server immediately. You must check the checkbox after saving changes.
TPM Support	TPM (Trusted Platform Module) is a microchip designed to provide basic security-related functions primarily involving encryption keys. This option allows you to control the TPM Security Device support for the system. It can be one of the following: • **Disabled**—The server does not use the TPM. • **Enabled**—The server uses the TPM. **Note** We recommend that you contact your operating system vendor to make sure the operating system supports this feature.

Name	Description
Power ON Password Support drop-down	This token requires that you set a BIOS password before using the F2 BIOS configuration. If enabled, password needs to be validated before you access BIOS functions such as IO configuration, BIOS set up, and booting to an operating system using BIOS. It can be one of the following: • **Disabled**—Support is disabled. • **Enabled**—Support is enabled. **Note** This field is available only on some C-series servers.

Actions Area

Name	Description
Save button	Saves the settings for the BIOS parameters on all three tabs and closes the dialog box. If the **Reboot Host Immediately** check box is checked, the server is rebooted immediately and the new BIOS settings go into effect. Otherwise the changes are saved until the server is manually rebooted.
Reset button	Resets the values for the BIOS parameters on all three tabs to the settings that were in effect when this dialog box was first opened.
Restore Defaults button	Sets the BIOS parameters on all three tabs to their default settings.

Advanced Tab

Reboot Server Option

If you want to apply your changes at a later time, clear the **Reboot Host Immediately** check box. Cisco IMC stores the changes and applies them the next time the server reboots.

Note If there are existing BIOS parameter changes pending, Cisco IMC automatically overwrites the stored values with the current settings when you click **Save Changes**.

Processor Configuration Parameters

Name	Description
Intel Hyper-Threading Technology	Whether the processor uses Intel Hyper-Threading Technology, which allows multithreaded software applications to execute threads in parallel within each processor. This can be one of the following: • **Disabled**—The processor does not permit hyperthreading. • **Enabled**—The processor allows for the parallel execution of multiple threads. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.
Number of Enabled Cores	Allows you to disable one or more of the physical cores on the server. This can be one of the following: • **All**—Enables all physical cores. This also enables Hyper Threading on the associated logical processor cores. • **1** through ***n***—Specifies the number of physical processor cores that can run on the server. Each physical core has an associated logical core. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.
Execute Disable	Classifies memory areas on the server to specify where application code can execute. As a result of this classification, the processor disables code execution if a malicious worm attempts to insert code in the buffer. This setting helps to prevent damage, worm propagation, and certain classes of malicious buffer overflow attacks. This can be one of the following: • **Disabled**—The processor does not classify memory areas. • **Enabled**—The processor classifies memory areas. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.
Intel VT	Whether the processor uses Intel Virtualization Technology (VT), which allows a platform to run multiple operating systems and applications in independent partitions. This can be one of the following: • **Disabled**—The processor does not permit virtualization. • **Enabled**—The processor allows multiple operating systems in independent partitions. **Note** If you change this option, you must power cycle the server before the setting takes effect.

Name	Description
Intel VT-d	Whether the processor uses Intel Virtualization Technology for Directed I/O (VT-d). This can be one of the following: • **Disabled**—The processor does not use virtualization technology. • **Enabled**—The processor uses virtualization technology.
Intel VT-d Coherency Support	Whether the processor supports Intel VT-d Coherency. This can be one of the following: • **Disabled**—The processor does not support coherency. • **Enabled**—The processor uses VT-d Coherency as required.
Intel VT-d ATS Support	Whether the processor supports Intel VT-d Address Translation Services (ATS). This can be one of the following: • **Disabled**—The processor does not support ATS. • **Enabled**—The processor uses VT-d ATS as required.
CPU Performance	Sets the CPU performance profile for the server. The performance profile consists of the following options: • DCU Streamer Prefetcher • DCU IP Prefetcher • Hardware Prefetcher • Adjacent Cache-Line Prefetch This can be one of the following: • **Enterprise**—All options are enabled. • **High Throughput**—Only the DCU IP Prefetcher is enabled. The rest of the options are disabled. • **HPC**—All options are enabled. This setting is also known as high performance computing. • **Custom**—All performance profile options can be configured from the BIOS setup on the server. In addition, the Hardware Prefetcher and Adjacent Cache-Line Prefetch options can be configured in the fields below.

Name	Description
Hardware Prefetcher	Whether the processor allows the Intel hardware prefetcher to fetch streams of data and instruction from memory into the unified second-level cache when necessary. This can be one of the following: • **Disabled**—The hardware prefetcher is not used. • **Enabled**—The processor uses the hardware prefetcher when cache issues are detected.
Adjacent Cache Line Prefetcher	Whether the processor fetches cache lines in even/odd pairs instead of fetching just the required line. This can be one of the following: • **Disabled**—The processor only fetches the required line. • **Enabled**— The processor fetches both the required line and its paired line.
DCU Streamer Prefetch	Whether the processor uses the DCU IP Prefetch mechanism to analyze historical cache access patterns and preload the most relevant lines in the L1 cache. This can be one of the following: • **Disabled**—The processor does not try to anticipate cache read requirements and only fetches explicitly requested lines. • **Enabled**—The DCU prefetcher analyzes the cache read pattern and prefetches the next line in the cache if it determines that it may be needed.
DCU IP Prefetcher	Whether the processor uses the DCU IP Prefetch mechanism to analyze historical cache access patterns and preload the most relevant lines in the L1 cache. This can be one of the following: • **Disabled**—The processor does not preload any cache data. • **Enabled**—The DCU IP prefetcher preloads the L1 cache with the data it determines to be the most relevant.
Direct Cache Access Support	Allows processors to increase I/O performance by placing data from I/O devices directly into the processor cache. This setting helps to reduce cache misses. This can be one of the following: • **Disabled**—Data from I/O devices is not placed directly into the processor cache. • **Enabled**—Data from I/O devices is placed directly into the processor cache.

Name	Description
Power Technology	Enables you to configure the CPU power management settings for the following options: • Enhanced Intel Speedstep Technology • Intel Turbo Boost Technology • Processor Power State C6 Power Technology can be one of the following: • **Custom**—The server uses the individual settings for the BIOS parameters mentioned above. You must select this option if you want to change any of these BIOS parameters. • **Disabled**—The server does not perform any CPU power management and any settings for the BIOS parameters mentioned above are ignored. • **Energy Efficient**—The server determines the best settings for the BIOS parameters mentioned above and ignores the individual settings for these parameters.
Enhanced Intel Speedstep Technology	Whether the processor uses Enhanced Intel SpeedStep Technology, which allows the system to dynamically adjust processor voltage and core frequency. This technology can result in decreased average power consumption and decreased average heat production. This can be one of the following: • **Disabled**—The processor never dynamically adjusts its voltage or frequency. • **Enabled**—The processor utilizes Enhanced Intel SpeedStep Technology and enables all supported processor sleep states to further conserve power. We recommend that you contact your operating system vendor to make sure the operating system supports this feature. **Note** **Power Technology** must be set to **Custom** or the server ignores the setting for this parameter.

Name	Description
Intel Turbo Boost Technology	Whether the processor uses Intel Turbo Boost Technology, which allows the processor to automatically increase its frequency if it is running below power, temperature, or voltage specifications. This can be one of the following: • **Disabled**—The processor does not increase its frequency automatically. • **Enabled**—The processor utilizes Turbo Boost Technology if required. **Note** **Power Technology** must be set to **Custom** or the server ignores the setting for this parameter.
Processor Power State C6	Whether the BIOS sends the C6 report to the operating system. When the OS receives the report, it can transition the processor into the lower C6 power state to decrease energy usage while maintaining optimal processor performance. This can be one of the following: • **Disabled**—The BIOS does not send the C6 report. • **Enabled**—The BIOS sends the C6 report, allowing the OS to transition the processor to the C6 low power state. **Note** **Power Technology** must be set to **Custom** or the server ignores the setting for this parameter.
Processor Power State C1 Enhanced	Whether the CPU transitions to its minimum frequency when entering the C1 state. This can be one of the following: • **Disabled**—The CPU continues to run at its maximum frequency in C1 state. • **Enabled**—The CPU transitions to its minimum frequency. This option saves the maximum amount of power in C1 state.
Frequency Floor Override	Whether the CPU is allowed to drop below the maximum non-turbo frequency when idle. This can be one of the following: • **Disabled**— The CPU can drop below the maximum non-turbo frequency when idle. This option decreases power consumption but may reduce system performance. • **Enabled**— The CPU cannot drop below the maximum non-turbo frequency when idle. This option improves system performance but may increase power consumption.

Name	Description
P-STATE Coordination	Allows you to define how BIOS communicates the P-state support model to the operating system. There are 3 models as defined by the Advanced Configuration and Power Interface (ACPI) specification. • **HW_ALL**—The processor hardware is responsible for coordinating the P-state among logical processors with dependencies (all logical processors in a package). • **SW_ALL**—The OS Power Manager (OSPM) is responsible for coordinating the P-state among logical processors with dependencies (all logical processors in a physical package), and must initiate the transition on all of the logical processors. • **SW_ANY**—The OS Power Manager (OSPM) is responsible for coordinating the P-state among logical processors with dependencies (all logical processors in a package), and may initiate the transition on any of the logical processors in the domain. **Note** **Power Technology** must be set to **Custom** or the server ignores the setting for this parameter.
Energy Performance	Allows you to determine whether system performance or energy efficiency is more important on this server. This can be one of the following: • **Balanced Energy** • **Balanced Performance** • **Energy Efficient** • **Performance**

Memory Configuration Parameters

Name	Description
Select Memory RAS	How the memory reliability, availability, and serviceability (RAS) is configured for the server. This can be one of the following: • **Maximum Performance**—System performance is optimized. • **Mirroring**—System reliability is optimized by using half the system memory as backup. • **Lockstep**—If the DIMM pairs in the server have an identical type, size, and organization and are populated across the SMI channels, you can enable lockstep mode to minimize memory access latency and provide better performance. This option offers better system performance than Mirroring and better reliability than Maximum Performance but lower reliability than Mirroring and lower system performance than Maximum Performance.
DRAM Clock Throttling	Allows you to tune the system settings between the memory bandwidth and power consumption. This can be one of the following: • **Balanced**— DRAM clock throttling is reduced, providing a balance between performance and power. • **Performance**—DRAM clock throttling is disabled, providing increased memory bandwidth at the cost of additional power. • **Energy Efficient**—DRAM clock throttling is increased to improve energy efficiency.
NUMA	Whether the BIOS supports Non-Uniform Memory Access (NUMA). This can be one of the following: • **Disabled**—The BIOS does not support NUMA. • **Enabled**—The BIOS includes the ACPI tables that are required for NUMA-aware operating systems. If you enable this option, the system must disable Inter-Socket Memory interleaving on some platforms.

Name	Description
Low Voltage DDR Mode	Whether the system prioritizes low voltage or high frequency memory operations. This can be one of the following: • **Power Saving Mode**—The system prioritizes low voltage memory operations over high frequency memory operations. This mode may lower memory frequency in order to keep the voltage low. • **Performance Mode**—The system prioritizes high frequency operations over low voltage operations.
DRAM Refresh rate	Allows you to set the rate at which the DRAM cells are refreshed. This can be one of the following: • **1x**—DRAM cells are refreshed every 64ms. • **2x**—DRAM cells are refreshed every 32ms. • **3x**—DRAM cells are refreshed every 21ms. • **4x**—DRAM cells are refreshed every 16ms. • **Auto**—DRAM cells refresh rate is automatically chosen by the BIOS based on the system configuration. This is the recommended setting for this parameter.
Channel Interleaving	Whether the CPU divides memory blocks and spreads contiguous portions of data across interleaved channels to enable simultaneous read operations. This can be one of the following: • **Auto**—The CPU determines what interleaving is done. • **1 Way**—Some channel interleaving is used. • **2 Way** • **3 Way** • **4 Way**—The maximum amount of channel interleaving is used.
Rank Interleaving	Whether the CPU interleaves physical ranks of memory so that one rank can be accessed while another is being refreshed. This can be one of the following: • **Auto**—The CPU determines what interleaving is done. • **1 Way**—Some rank interleaving is used. • **2 Way** • **4 Way** • **8 Way**—The maximum amount of rank interleaving is used.

Name	Description
Patrol Scrub	Whether the system actively searches for, and corrects, single bit memory errors even in unused portions of the memory on the server. This can be one of the following: • **Disabled**—The system checks for memory ECC errors only when the CPU reads or writes a memory address. • **Enabled**—The system periodically reads and writes memory searching for ECC errors. If any errors are found, the system attempts to fix them. This option may correct single bit errors before they become multi-bit errors, but it may adversely affect performance when the patrol scrub is running.
Demand Scrub	Whether the system corrects single bit memory errors encountered when the CPU or I/O makes a demand read. This can be one of the following: • **Disabled**— Single bit memory errors are not corrected. • **Enabled**— Single bit memory errors are corrected in memory and the corrected data is set in response to the demand read.
Altitude	The approximate number of meters above sea level at which the physical server is installed. This can be one of the following: • **Auto**—The CPU determines the physical elevation. • **300 M**—The server is approximately 300 meters above sea level. • **900 M**—The server is approximately 900 meters above sea level. • **1500 M**—The server is approximately 1500 meters above sea level. • **3000 M**—The server is approximately 3000 meters above sea level.

QPI Configuration Parameters

Name	Description
QPI Link Frequency Select	The Intel QuickPath Interconnect (QPI) link frequency, in gigatransfers per second (GT/s). This can be one of the following: • **Auto**—The CPU determines the QPI link frequency. • **6.4 GT/s** • **7.2 GT/s** • **8.0 GT/s**
QPI Snoop Mode Drop-down list	The Intel QuickPath Interconnect (QPI) snoop mode. This can be one of the following: • **Auto**—The CPU automatically recognizes this as Early Snoop mode. • **Early Snoop**—The distributed cache ring stops can send a snoop probe or a request to another caching agent directly. This mode has lower latency and it is best for workloads that have shared data sets across threads and can benefit from a cache-to-cache transfer, or for workloads that are not NUMA optimized. • **Home Snoop**—The snoop is always spawned by the home agent (centralized ring stop) for the memory controller. This mode has a higher local latency than early snoop, but it provides extra resources for a larger number of outstanding transactions. • **Home Directory Snoop**— The home directory is an optional enabled feature that is implemented at both the HA and iMC logic in the processor. The goal of the directory is to filter snoops to the remote sockets and a node controller in scalable platforms and 2S and 4S configurations. • **Home Directory Snoop with OSB**— In the Opportunistic Snoop Broadcast (OSB) directory mode, the HA could choose to do speculative home snoop broadcast under very lightly loaded conditions even before the directory information has been collected and checked. • **Cluster on Die**—Enables Cluster On Die. When enabled LLC is split into two parts with an independent caching agent for each. This helps increase the performance in some workloads. This mode is available only for processors that have 10 or more cores. It is the best mode for highly NUMA optimized workloads.

SATA Configuration Parameters

Name	Description
SATA Mode	Mode of operation of Serial Advanced Technology Attachment (SATA) Solid State Drives (SSD). • **Disabled**— All SATA ports is disabled, and drivers are not enumerated. • **AHCI Mode**—The default mode. Drives operate according to newer standard of Advance Host Controller Interface(AHCI).

USB Configuration Parameters

Name	Description
Legacy USB Support	Whether the system supports legacy USB devices. This can be one of the following: • **Disabled**—USB devices are only available to EFI applications. • **Enabled**—Legacy USB support is always available. • **Auto**—Disables legacy USB support if no USB devices are connected.
Port 60/64 Emulation	Whether the system supports 60h/64h emulation for complete USB keyboard legacy support. This can be one of the following: • **Disabled**—60h/64 emulation is not supported. • **Enabled**—60h/64 emulation is supported. You should select this option if you are using a non-USB aware operating system on the server.
All USB Devices	Whether all physical and virtual USB devices are enabled or disabled. This can be one of the following: • **Disabled**—All USB devices are disabled. • **Enabled**—All USB devices are enabled.
USB Port: Rear	Whether the rear panel USB devices are enabled or disabled. This can be one of the following: • **Disabled**—Disables the rear panel USB ports. Devices connected to these ports are not detected by the BIOS and operating system. • **Enabled**—Enables the rear panel USB ports. Devices connected to these ports are detected by the BIOS and operating system.

Name	Description
USB Port: Internal	Whether the internal USB devices are enabled or disabled. This can be one of the following: • **Disabled**—Disables the internal USB ports. Devices connected to these ports are not detected by the BIOS and operating system. • **Enabled**—Enables the internal USB ports. Devices connected to these ports are detected by the BIOS and operating system.
USB Port: KVM	Whether the vKVM ports are enabled or disabled. This can be one of the following: • **Disabled**—Disables the vKVM keyboard and/or mouse devices. Keyboard and/or mouse will not work in the vKVM window. • **Enabled**—Enables the vKVM keyboard and/or mouse devices.
USB Port: vMedia	Whether the virtual media devices are enabled or disabled. This can be one of the following: • **Disabled**—Disables the vMedia devices. • **Enabled**—Enables the vMedia devices.

PCI Configuration Parameters

Name	Description
PCI ROM CLP	PCI ROM Command Line Protocol (CLP) controls the execution of different Option ROMs such as PxE and iSCSI that are present in the card. By default, it is disabled. • **Enabled**— Enables you to configure execution of different option ROMs such as PxE and iSCSI for an individual ports separately. • **Disabled**—The default option. You cannot choose different option ROMs. A default option ROM is executed during PCI enumeration.
ASPM Support	Allows you to set the level of ASPM (Active Power State Management) support in the BIOS. This can be one of the following: • **Disabled**—ASPM support is disabled in the BIOS. • **Force L0s**—Force all links to L0 standby (L0s) state. • **Auto**—The CPU determines the power state.

Serial Configuration Parameters

Name	Description
Out-of-Band Mgmt Port	Allows you to configure the COM port 0 that can be used for Windows Emergency Management services. ACPI SPCR table is reported based on this setup option. This can be one of the following: • **Disabled**—Configures the COM port 0 as a general purpose port for use with the Windows Operating System. • **Enabled**—Configures the COM port 0 as a remote management port for Windows Emergency Management services.
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. • **COM 0**—Enables console redirection on COM port 0 during POST. • **COM 1**—Enables console redirection on COM port 1 during POST.
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+**—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.
Bits per second	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: • **9600**—A 9,600 BAUD rate is used. • **19200**—A 19,200 BAUD rate is used. • **38400**—A 38,400 BAUD rate is used. • **57600**—A 57,600 BAUD rate is used. • **115200**—A 115,200 BAUD rate is used. **Note** This setting must match the setting on the remote terminal application.

Name	Description
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. • **Hardware RTS/CTS**—RTS/CTS is used for flow control. **Note** This setting must match the setting on the remote terminal application.
Putty KeyPad	Allows you to change the action of the PuTTY function keys and the top row of the numeric keypad. This can be one of the following: • **VT100**—The function keys generate **`ESC OP`** through **`ESC O[.`** • **LINUX**—Mimics the Linux virtual console. Function keys F6 to F12 behave like the default mode, but F1 to F5 generate **`ESC [[A`** through **`ESC [[E`**. • **XTERMR6**—Function keys F5 to F12 behave like the default mode. Function keys F1 to F4 generate **ESC OP** through ESC OS, which are the sequences produced by the top row of the keypad on Digital terminals. • **SCO**—The function keys F1 to F12 generate **`ESC [M`** through **`ESC [X`**. The function and shift keys generate **`ESC [Y`** through **`ESC [j`**. The control and function keys generate **`ESC [k`** through **`ESC [v`**. The shift, control and function keys generate **`ESC [w`** through **`ESC [{`**. • **ESCN**—The default mode. The function keys match the general behavior of Digital terminals. The function keys generate sequences such as **`ESC [11~`** and **`ESC [12~`**. • **VT400**—The function keys behave like the default mode. The top row of the numeric keypad generates **`ESC OP`** through **`ESC OS`**.
Redirection After BIOS POST	Whether BIOS console redirection should be active after BIOS POST is complete and control given to the OS bootloader. This can be one of the following: • **Always Enable**—BIOS Legacy console redirection is active during the OS boot and run time. • **Bootloader**—BIOS Legacy console redirection is disabled before giving control to the OS boot loader.

LOM and PCIe Slots Configuration Parameters

Name	Description
CDN Support for VIC	Whether the Ethernet Network naming convention is according to Consistent Device Naming (CDN) or the traditional way of naming conventions. This can be one of the following: • **Disabled**— CDN support for VIC cards is disabled. • **Enabled**— CDN support is enabled for VIC cards. **Note** CDN support for VIC cards work with Windows 2012 or the latest OS only.
All PCIe Slots OptionROM	Whether the server can use Option ROM present in the PCIe Cards. This can be one of the following: • **Disabled**—The Option ROM for all PCIe slots are not available. • **Enabled**—The Option ROMs for all the PCIe slots are available. • **UEFI Only**—The Opiton ROMs for slot ***n*** are available for UEFI only. • **Legacy Only**—The Option ROM for slot ***n*** are available for legacy only.
PCIe Slot:*n* OptionROM	Whether the server can use the Option ROMs present in the PCIe Cards. This can be one of the following: • **Disabled**—The Option ROM for slot ***n*** is not available. • **Enabled**—The Option ROM for slot ***n*** is available. • **UEFI Only**—The Option ROM for slot ***n*** is available for UEFI only. • **Legacy Only**—The Option ROM for slot ***n*** is available for legacy only.
PCIe Mezzanine OptionROM	Whether the PCIe mezzanine slot expansion ROM is available to the server. This can be one of the following: • **Disabled**— The Option ROM for slot ***M*** is not available. • **Enabled**— The Option ROM for slot ***M*** is available. • **UEFI Only**—The Option ROM for slot ***M*** is available for UEFI only. • **Legacy Only**—The expansion slot for slot ***M*** is available for legacy only.

Name	Description
SIOC1 Link Speed	System IO Controller 1 (SIOC1) add-on slot 1 link speed. • **GEN1** — Link speed can reach up to first generation. • **GEN2** — Link speed can reach up to second generation. • **GEN3**— The default link speed. Link speed can reach up to third generation. • **Disabled** — Slot is disabled, and the card is not enumerated.
SIOC2 Link Speed	System IO Controller 2 (SIOC2) add-on slot 2 link speed. • **GEN1** — Link speed can reach up to first generation. • **GEN2** — Link speed can reach up to second generation. • **GEN3**— The default link speed. Link speed can reach up to third generation. • **Disabled** — Slot is disabled, and the card is not enumerated.
Mezz Link Speed	Mezz link speed. This can be one of the following: • **GEN 1**— Link speed can reach up to first generation. • **GEN 2**— Link speed can reach up to second generation. • **GEN 3**—The default link speed. Link speed can reach up to third generation. • **Disabled**—Slot is disabled, and the card is not enumerated.

BIOS Configuration Dialog Box Button Bar

Important The buttons in this dialog box affect all BIOS parameters on all available tabs, not just the parameters on the tab that you are viewing.

Name	Description
Save Changes button	Saves the settings for the BIOS parameters on all three tabs and closes the dialog box. If the **Reboot Host Immediately** check box is checked, the server is rebooted immediately and the new BIOS settings go into effect. Otherwise the changes are saved until the server is manually rebooted.
Reset button	Restores the values for the BIOS parameters on all three tabs to the settings that were in effect when this dialog box was first opened.
Restore Defaults button	Sets the BIOS parameters on all three tabs to their default settings.

Server Management Tab

Server Management BIOS Parameters

Name	Description
FRB-2 Timer	Whether the FRB2 timer is used by Cisco IMC 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.
OS Watchdog Timer	Whether the BIOS programs the watchdog timer with a specified timeout value. 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 in the **OS Boot Watchdog Timer Timeout** field, the Cisco IMC logs an error and takes the action specified in the **OS Boot Watchdog Policy** field.
OS Watchdog Timer Timeout	If OS does not boot within the specified time, OS watchdog timer expires and system takes action according to timer policy. This can be one of the following: • **5 Minutes**—The OS watchdog timer expires 5 minutes after it begins to boot. • **10 Minutes**—The OS watchdog timer expires 10 minutes after it begins to boot. • **15 Minutes**—The OS watchdog timer expires 15 minutes after it begins to boot. • **20 Minutes**—The OS watchdog timer expires 20 minutes after it begins to boot. **Note** This option is only applicable if you enable the OS Boot Watchdog Timer.

Name	Description
OS Watchdog Timer Policy	What action the system takes if the watchdog timer expires. This can be one of the following: • **Do Nothing**—The server takes no action if 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.

S3260 M4 Servers

Main Tab

Name	Description
Reboot Host Immediately checkbox	Upon checking, reboots the host server immediately. You must check the checkbox after saving changes.
TPM Support	TPM (Trusted Platform Module) is a microchip designed to provide basic security-related functions primarily involving encryption keys. This option allows you to control the TPM Security Device support for the system. It can be one of the following: • **Disabled**—The server does not use the TPM. • **Enabled**—The server uses the TPM. **Note** We recommend that you contact your operating system vendor to make sure the operating system supports this feature.
Power ON Password Support drop-down	This token requires that you set a BIOS password before using the F2 BIOS configuration. If enabled, password needs to be validated before you access BIOS functions such as IO configuration, BIOS set up, and booting to an operating system using BIOS. It can be one of the following: • **Disabled**—Support is disabled. • **Enabled**—Support is enabled.

Actions Area

Name	Description
Save button	Saves the settings for the BIOS parameters on all three tabs and closes the dialog box. If the **Reboot Host Immediately** check box is checked, the server is rebooted immediately and the new BIOS settings go into effect. Otherwise the changes are saved until the server is manually rebooted.
Reset button	Resets the values for the BIOS parameters on all three tabs to the settings that were in effect when this dialog box was first opened.
Restore Defaults button	Sets the BIOS parameters on all three tabs to their default settings.

Advanced Tab

Reboot Server Option

If you want your changes applied automatically after you click **Save Changes**, check the **Reboot Host Immediately** check box. Cisco IMC immediately reboots the server and applies your changes.

If you want to apply your changes at a later time, clear the **Reboot Host Immediately** check box. Cisco IMC stores the changes and applies them the next time the server reboots.

Note If there are existing BIOS parameter changes pending, Cisco IMC automatically overwrites the stored values with the current settings when you click **Save Changes**.

Processor Configuration Parameters

Name	Description
Intel Hyper-Threading Technology	Whether the processor uses Intel Hyper-Threading Technology, which allows multithreaded software applications to execute threads in parallel within each processor. This can be one of the following: • **Disabled**—The processor does not permit hyperthreading. • **Enabled**—The processor allows for the parallel execution of multiple threads. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.

Name	Description
Number of Enabled Cores	Allows you to disable one or more of the physical cores on the server. This can be one of the following: • **All**—Enables all physical cores. This also enables Hyper Threading on the associated logical processor cores. • **1** through ***n***—Specifies the number of physical processor cores that can run on the server. Each physical core has an associated logical core. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.
Execute Disable	Classifies memory areas on the server to specify where application code can execute. As a result of this classification, the processor disables code execution if a malicious worm attempts to insert code in the buffer. This setting helps to prevent damage, worm propagation, and certain classes of malicious buffer overflow attacks. This can be one of the following: • **Disabled**—The processor does not classify memory areas. • **Enabled**—The processor classifies memory areas. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.
Intel VT	Whether the processor uses Intel Virtualization Technology (VT), which allows a platform to run multiple operating systems and applications in independent partitions. This can be one of the following: • **Disabled**—The processor does not permit virtualization. • **Enabled**—The processor allows multiple operating systems in independent partitions. **Note** If you change this option, you must power cycle the server before the setting takes effect.
Intel VT-d	Whether the processor uses Intel Virtualization Technology for Directed I/O (VT-d). This can be one of the following: • **Disabled**—The processor does not use virtualization technology. • **Enabled**—The processor uses virtualization technology.

Name	Description
Intel VT-d Interrupt Remapping	Whether the processor supports Intel VT-d Interrupt Remapping. This can be one of the following: • **Disabled**—The processor does not support remapping. • **Enabled**—The processor uses VT-d Interrupt Remapping as required.
Intel VT-d PassThrough DMA	Whether the processor supports Intel VT-d Pass-through DMA. This can be one of the following: • **Disabled**—The processor does not support pass-through DMA. • **Enabled**—The processor uses VT-d Pass-through DMA as required.
Intel VT-d Coherency Support	Whether the processor supports Intel VT-d Coherency. This can be one of the following: • **Disabled**—The processor does not support coherency. • **Enabled**—The processor uses VT-d Coherency as required.
Intel VT-d ATS Support	Whether the processor supports Intel VT-d Address Translation Services (ATS). This can be one of the following: • **Disabled**—The processor does not support ATS. • **Enabled**—The processor uses VT-d ATS as required.

Name	Description
CPU Performance	Sets the CPU performance profile for the server. The performance profile consists of the following options: • DCU Streamer Prefetcher • DCU IP Prefetcher • Hardware Prefetcher • Adjacent Cache-Line Prefetch This can be one of the following: • **Enterprise**—All options are enabled. • **High Throughput**—Only the DCU IP Prefetcher is enabled. The rest of the options are disabled. • **HPC**—All options are enabled. This setting is also known as high performance computing. • **Custom**—All performance profile options can be configured from the BIOS setup on the server. In addition, the Hardware Prefetcher and Adjacent Cache-Line Prefetch options can be configured in the fields below.
Hardware Prefetcher	Whether the processor allows the Intel hardware prefetcher to fetch streams of data and instruction from memory into the unified second-level cache when necessary. This can be one of the following: • **Disabled**—The hardware prefetcher is not used. • **Enabled**—The processor uses the hardware prefetcher when cache issues are detected.
Adjacent Cache Line Prefetcher	Whether the processor fetches cache lines in even/odd pairs instead of fetching just the required line. This can be one of the following: • **Disabled**—The processor only fetches the required line. • **Enabled**— The processor fetches both the required line and its paired line.

Name	Description
DCU Streamer Prefetch	Whether the processor uses the DCU IP Prefetch mechanism to analyze historical cache access patterns and preload the most relevant lines in the L1 cache. This can be one of the following: • **Disabled**—The processor does not try to anticipate cache read requirements and only fetches explicitly requested lines. • **Enabled**—The DCU prefetcher analyzes the cache read pattern and prefetches the next line in the cache if it determines that it may be needed.
DCU IP Prefetcher	Whether the processor uses the DCU IP Prefetch mechanism to analyze historical cache access patterns and preload the most relevant lines in the L1 cache. This can be one of the following: • **Disabled**—The processor does not preload any cache data. • **Enabled**—The DCU IP prefetcher preloads the L1 cache with the data it determines to be the most relevant.
Direct Cache Access Support	Allows processors to increase I/O performance by placing data from I/O devices directly into the processor cache. This setting helps to reduce cache misses. This can be one of the following: • **Disabled**—Data from I/O devices is not placed directly into the processor cache. • **Enabled**—Data from I/O devices is placed directly into the processor cache.
Power Technology	Enables you to configure the CPU power management settings for the following options: • Enhanced Intel Speedstep Technology • Intel Turbo Boost Technology • Processor Power State C6 Power Technology can be one of the following: • **Custom**—The server uses the individual settings for the BIOS parameters mentioned above. You must select this option if you want to change any of these BIOS parameters. • **Disabled**—The server does not perform any CPU power management and any settings for the BIOS parameters mentioned above are ignored. • **Energy Efficient**—The server determines the best settings for the BIOS parameters mentioned above and ignores the individual settings for these parameters.

Name	Description
Enhanced Intel Speedstep Technology	Whether the processor uses Enhanced Intel SpeedStep Technology, which allows the system to dynamically adjust processor voltage and core frequency. This technology can result in decreased average power consumption and decreased average heat production. This can be one of the following: • **Disabled**—The processor never dynamically adjusts its voltage or frequency. • **Enabled**—The processor utilizes Enhanced Intel SpeedStep Technology and enables all supported processor sleep states to further conserve power. We recommend that you contact your operating system vendor to make sure the operating system supports this feature. **Note** **Power Technology** must be set to **Custom** or the server ignores the setting for this parameter.
Intel Turbo Boost Technology	Whether the processor uses Intel Turbo Boost Technology, which allows the processor to automatically increase its frequency if it is running below power, temperature, or voltage specifications. This can be one of the following: • **Disabled**—The processor does not increase its frequency automatically. • **Enabled**—The processor utilizes Turbo Boost Technology if required. **Note** **Power Technology** must be set to **Custom** or the server ignores the setting for this parameter.
Processor C3 Report	Whether the BIOS sends the C3 report to the operating system. When the OS receives the report, it can transition the processor into the lower C3 power state to decrease energy usage while maintaining optimal processor performance. This can be one of the following: • **Disabled**—BIOS does not send C3 report. • **Enabled**—BIOS sends the C3 report, allowing the OS to transition the processor to the C3 low power state. **Note** **Power Technology** must be set to **Custom** or the server ignores the setting for this parameter.

Name	Description
Processor C6 Report	Whether the BIOS sends the C6 report to the operating system. When the OS receives the report, it can transition the processor into the lower C6 power state to decrease energy usage while maintaining optimal processor performance. This can be one of the following: • **Disabled**—The BIOS does not send the C6 report. • **Enabled**—The BIOS sends the C6 report, allowing the OS to transition the processor to the C6 low power state. **Note** **Power Technology** must be set to **Custom** or the server ignores the setting for this parameter.
Processor Power State C1 Enhanced	Whether the CPU transitions to its minimum frequency when entering the C1 state. This can be one of the following: • **Disabled**—The CPU continues to run at its maximum frequency in C1 state. • **Enabled**—The CPU transitions to its minimum frequency. This option saves the maximum amount of power in C1 state.
P-STATE Coordination	Allows you to define how BIOS communicates the P-state support model to the operating system. There are 3 models as defined by the Advanced Configuration and Power Interface (ACPI) specification. • **HW_ALL**—The processor hardware is responsible for coordinating the P-state among logical processors with dependencies (all logical processors in a package). • **SW_ALL**—The OS Power Manager (OSPM) is responsible for coordinating the P-state among logical processors with dependencies (all logical processors in a physical package), and must initiate the transition on all of the logical processors. • **SW_ANY**—The OS Power Manager (OSPM) is responsible for coordinating the P-state among logical processors with dependencies (all logical processors in a package), and may initiate the transition on any of the logical processors in the domain. **Note** **Power Technology** must be set to **Custom** or the server ignores the setting for this parameter.

Name	Description
Boot Performance Mode drop-down list	Allows the user to select the BIOS performance state that is set before the operating system handoff. This can be one of the following: • **Max Performance**—Processor P-state ratio is maximum • **Max Efficient**— Processor P-state ratio is minimum
Energy Performance Tuning	Allows you to choose BIOS or Operating System for energy performance bias tuning. This can be one of the following: • **OS**— Chooses OS for energy performance tuning. • **BIOS**— Chooses BIOS for energy performance tuning.
Energy Performance	Allows you to determine whether system performance or energy efficiency is more important on this server. This can be one of the following: • **Balanced Energy** • **Balanced Performance** • **Energy Efficient** • **Performance**

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: • **C0 state**—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. • **C1 state**—When the CPU is idle, the system slightly reduces the power consumption. This option requires less power than C0 and allows the server to return quickly to high performance mode. • **C3 state**—When the CPU is idle, the system reduces the power consumption further than with the C1 option. This requires less power than C1 or C0, but it takes the server slightly longer to return to high performance mode. • **C6 state**—When the CPU is idle, the system reduces the power consumption further than with the C3 option. This option saves more power than C0, C1, or C3, but there may be performance issues until the server returns to full power. • **C7 state**—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. • **No Limit**—The server may enter any available C state.
Extended APIC	Allows you to enable or disable extended APIC support. This can be one of the following: • **XAPIC**—Enables APIC support. • **X2APIC**—Enables APIC and also enables Intel VT-d and Interrupt Remapping .
Workload Configuration	Allows you to set a parameter to optimize workload characterization. This can be one of the following: • **Balanced**— Chooses balanced option for optimization. • **I/O Sensitive**— Chooses I/O sensitive option for optimization. **Note** We recommend you to set the workload configuration to **Balanced**.

Name	Description
CPU HWPM drop-down list	Enables the Hardware Power Management (HWPM) interface for better CPU performance and energy efficiency. This can be one of the following: • **Disabled**—The P-States are controlled the same way as on predecessor processor generations. • **Native Mode**—HWPM works with the operating system through a software interface. • **OOB Mode**—The CPU autonomously controls its frequency based on the operating system energy efficiency.
CPU Autonomous Cstate drop-down list	Enables CPU Autonomous C-State, which converts the HALT instructions to the MWAIT instructions. This can be one of the following: • **Disabled**—CPU Autonomous C-state is disabled. This is the default value. • **Enabled**—CPU Autonomous C-state is enabled.
Processor CMCI drop-down list	Allows the CPU to trigger interrupts on corrected machine check events. The corrected machine check interrupt (CMCI) allows faster reaction than the traditional polling timer. This can be one of the following: • **Disabled**—Disables CMCI. • **Enabled**—Enables CMCI. This is the default value.

Memory Configuration Parameters

Name	Description
Select Memory RAS	How the memory reliability, availability, and serviceability (RAS) is configured for the server. This can be one of the following: • **Maximum Performance**—System performance is optimized. • **Mirroring**—System reliability is optimized by using half the system memory as backup. • **Lockstep**—If the DIMM pairs in the server have an identical type, size, and organization and are populated across the SMI channels, you can enable lockstep mode to minimize memory access latency and provide better performance. This option offers better system performance than Mirroring and better reliability than Maximum Performance but lower reliability than Mirroring and lower system performance than Maximum Performance.

Name	Description
NUMA	Whether the BIOS supports Non-Uniform Memory Access (NUMA). This can be one of the following: • **Disabled**—The BIOS does not support NUMA. • **Enabled**—The BIOS includes the ACPI tables that are required for NUMA-aware operating systems. If you enable this option, the system must disable Inter-Socket Memory interleaving on some platforms.
Channel Interleaving	Whether the CPU divides memory blocks and spreads contiguous portions of data across interleaved channels to enable simultaneous read operations. This can be one of the following: • **Auto**—The CPU determines what interleaving is done. • **1 Way**—Some channel interleaving is used. • **2 Way** • **3 Way** • **4 Way**—The maximum amount of channel interleaving is used.
Rank Interleaving	Whether the CPU interleaves physical ranks of memory so that one rank can be accessed while another is being refreshed. This can be one of the following: • **Auto**—The CPU determines what interleaving is done. • **1 Way**—Some rank interleaving is used. • **2 Way** • **4 Way** • **8 Way**—The maximum amount of rank interleaving is used.
Patrol Scrub	Whether the system actively searches for, and corrects, single bit memory errors even in unused portions of the memory on the server. This can be one of the following: • **Disabled**—The system checks for memory ECC errors only when the CPU reads or writes a memory address. • **Enabled**—The system periodically reads and writes memory searching for ECC errors. If any errors are found, the system attempts to fix them. This option may correct single bit errors before they become multi-bit errors, but it may adversely affect performance when the patrol scrub is running.

Name	Description
Demand Scrub	Whether the system corrects single bit memory errors encountered when the CPU or I/O makes a demand read. This can be one of the following: • **Disabled**— Single bit memory errors are not corrected. • **Enabled**— Single bit memory errors are corrected in memory and the corrected data is set in response to the demand read.
Altitude	The approximate number of meters above sea level at which the physical server is installed. This can be one of the following: • **Auto**—The CPU determines the physical elevation. • **300 M**—The server is approximately 300 meters above sea level. • **900 M**—The server is approximately 900 meters above sea level. • **1500 M**—The server is approximately 1500 meters above sea level. • **3000 M**—The server is approximately 3000 meters above sea level.
Panic and High Watermark drop-down list	When set to low, the memory controller does not postpone refreshes while **Memory Refresh Rate** is set to **1X Refresh**. This can be one of the following: • **Low**—Refresh rate is set to low. • **High** —Refresh rate is set to high.

QPI Configuration Parameters

Name	Description
QPI Link Frequency Select	The Intel QuickPath Interconnect (QPI) link frequency, in gigatransfers per second (GT/s). This can be one of the following: • **Auto**—The CPU determines the QPI link frequency. • **6.4 GT/s** • **7.2 GT/s** • **8.0 GT/s**

Name	Description
QPI Snoop Mode	The Intel QuickPath Interconnect (QPI) snoop mode. This can be one of the following: • **Home Snoop**—The snoop is always spawned by the home agent (centralized ring stop) for the memory controller. This mode has a higher local latency than early snoop, but it provides extra resources for a larger number of outstanding transactions. • **Cluster on Die**—Enables Cluster On Die. When enabled LLC is split into two parts with an independent caching agent for each. This helps increase the performance in some workloads. This mode is available only for processors that have 10 or more cores. It is the best mode for highly NUMA optimized workloads. • **Early Snoop**—The distributed cache ring stops can send a snoop probe or a request to another caching agent directly. This mode has lower latency and it is best for workloads that have shared data sets across threads and can benefit from a cache-to-cache transfer, or for workloads that are not NUMA optimized.

USB Configuration Parameters

Name	Description
Legacy USB Support	Whether the system supports legacy USB devices. This can be one of the following: • **Disabled**—USB devices are only available to EFI applications. • **Enabled**—Legacy USB support is always available. • **Auto**—Disables legacy USB support if no USB devices are connected.
Port 60/64 Emulation	Whether the system supports 60h/64h emulation for complete USB keyboard legacy support. This can be one of the following: • **Disabled**—60h/64 emulation is not supported. • **Enabled**—60h/64 emulation is supported. You should select this option if you are using a non-USB aware operating system on the server.
xHCI Mode	Whether the xHCI controller legacy support is enabled or disabled. This can be one of the following: • **Disabled**—Disables the xHCI controller legacy support. • **Enabled**—Enables the xHCI controller legacy support.

Name	Description
xHCI Legacy Support drop-down list	Whether the system supports legacy xHCI controller. This can be one of the following: • **Disabled**—Disables xHCI legacy support. • **Enabled**—Enables xHCI legacy support. This is the default value.
All USB Devices	Whether all physical and virtual USB devices are enabled or disabled. This can be one of the following: • **Disabled**—All USB devices are disabled. • **Enabled**—All USB devices are enabled.
USB Port: Rear	Whether the rear panel USB devices are enabled or disabled. This can be one of the following: • **Disabled**—Disables the rear panel USB ports. Devices connected to these ports are not detected by the BIOS and operating system. • **Enabled**—Enables the rear panel USB ports. Devices connected to these ports are detected by the BIOS and operating system.
USB Port: KVM	Whether the vKVM ports are enabled or disabled. This can be one of the following: • **Disabled**—Disables the vKVM keyboard and/or mouse devices. Keyboard and/or mouse will not work in the vKVM window. • **Enabled**—Enables the vKVM keyboard and/or mouse devices.
USB Port: vMedia	Whether the virtual media devices are enabled or disabled. This can be one of the following: • **Disabled**—Disables the vMedia devices. • **Enabled**—Enables the vMedia devices.

PCI Configuration Parameters

Name	Description
Memory Mapped I/O Above 4GB	Whether to enable or disable MMIO above 4GB or not. This can be one of the following: • **Disabled**—The server does not map I/O of 64-bit PCI devices to 4GB or greater address space. • **Enabled**—The server maps I/O of 64-bit PCI devices to 4GB or greater address space. **Note** PCI devices that are 64-bit compliant but use a legacy option ROM may not function correctly with this setting enabled.
Sriov	Whether SR-IOV (Single Root I/O Virtualization) is enabled or disabled on the server. This can be one of the following: • **Disabled**—SR-IOV is disabled. • **Enabled**—SR-IOV is enabled.

Serial Configuration Parameters

Name	Description
Out-of-Band Mgmt Port	Allows you to configure the COM port 0 that can be used for Windows Emergency Management services. ACPI SPCR table is reported based on this setup option. This can be one of the following: • **Disabled**—Configures the COM port 0 as a general purpose port for use with the Windows Operating System. • **Enabled**—Configures the COM port 0 as a remote management port for Windows Emergency Management services.
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. • **COM 0**—Enables console redirection on COM port 0 during POST. • **COM 1**—Enables console redirection on COM port 1 during POST.

Name	Description
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+**—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.
Bits per second	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: • **9600**—A 9,600 BAUD rate is used. • **19200**—A 19,200 BAUD rate is used. • **38400**—A 38,400 BAUD rate is used. • **57600**—A 57,600 BAUD rate is used. • **115200**—A 115,200 BAUD rate is used. **Note** This setting must match the setting on the remote terminal application.
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. • **Hardware RTS/CTS**—RTS/CTS is used for flow control. **Note** This setting must match the setting on the remote terminal application.

Name	Description
Putty KeyPad	Allows you to change the action of the PuTTY function keys and the top row of the numeric keypad. This can be one of the following: • **VT100**—The function keys generate **ESC OP** through **ESC O[.** • **LINUX**—Mimics the Linux virtual console. Function keys F6 to F12 behave like the default mode, but F1 to F5 generate **ESC [[A** through **ESC [[E**. • **XTERMR6**—Function keys F5 to F12 behave like the default mode. Function keys F1 to F4 generate **ESC OP** through ESC OS, which are the sequences produced by the top row of the keypad on Digital terminals. • **SCO**—The function keys F1 to F12 generate **ESC [M** through **ESC [X**. The function and shift keys generate **ESC [Y** through **ESC [j**. The control and function keys generate **ESC [k** through **ESC [v**. The shift, control and function keys generate **ESC [w** through **ESC [{**. • **ESCN**—The default mode. The function keys match the general behavior of Digital terminals. The function keys generate sequences such as **ESC [11~** and **ESC [12~**. • **VT400**—The function keys behave like the default mode. The top row of the numeric keypad generates **ESC OP** through **ESC OS**.
Redirection After BIOS POST	Whether BIOS console redirection should be active after BIOS POST is complete and control given to the OS bootloader. This can be one of the following: • **Always Enable**—BIOS Legacy console redirection is active during the OS boot and run time. • **Bootloader**—BIOS Legacy console redirection is disabled before giving control to the OS boot loader.

LOM and PCIe Slots Configuration Parameters

Name	Description
CDN Support for VIC	Whether the Ethernet Network naming convention is according to Consistent Device Naming (CDN) or the traditional way of naming conventions. This can be one of the following: • **Disabled**— CDN support for VIC cards is disabled. • **Enabled**— CDN support is enabled for VIC cards. **Note** CDN support for VIC cards work with Windows 2012 or the latest OS only.

Name	Description
PCI ROM CLP	PCI ROM Command Line Protocol (CLP) controls the execution of different Option ROMs such as PxE and iSCSI that are present in the card. By default, it is disabled. • **Enabled**— Enables you to configure execution of different option ROMs such as PxE and iSCSI for an individual ports separately. • **Disabled**—The default option. You cannot choose different option ROMs. A default option ROM is executed during PCI enumeration.
All PCIe Slots OptionROM	Whether the server can use Option ROM present in the PCIe Cards. This can be one of the following: • **Disabled**—The Option ROM for slot ***n*** is not available. • **Enabled**—The Option ROM for slot ***n*** is available. • **UEFI Only**—The Option ROM for slot ***n*** is available for UEFI only. • **Legacy Only**—The Option ROM for slot ***n*** is available for legacy only.
PCH SATA Mode	This options allows you to select the PCH SATA mode. This can be one of the following: • **AHCI**—Sets both SATA and sSATA controllers to AHCI mode. • **Disabled**—Disables both SATA and sSATA controllers. • **LSI SW Raid**— Sets both SATA and sSATA controllers to raid mode for LSI SW Raid
SBNVMe1 OptionROM	Whether the server can use Option ROM present in SBNVMe1 controller. This can be one of the following: • **Disabled**—The Option ROM for SBNVMe1 controllers is not available. • **Enabled**—The Option ROMs for SBNVMe1 controller is available. • **UEFI Only**—The Option ROMs for slot are available for UEFI only. • **Legacy Only**—The Option ROM for slot are available for legacy only.

Name	Description
SIOC1 OptionROM **set SIOC1OptionROM**	Whether the server can use Option ROM present in System IO Controller 1 (SIOC1). This can be one of the following: • **Disabled**—The Option ROM for System IO Controller 1 (SIOC1) is not available. • **Enabled**—The Option ROMs for System IO Controller 1 (SIOC1) is available. • **UEFI Only**—The Option ROMs for slot are available for UEFI only. • **Legacy Only**—The Option ROM for slot are available for legacy only.
SIOC2 OptionROM **set SIOC2OptionROM**	Whether the server can use Option ROM present in System IO Controller 2 (SIOC2). This can be one of the following: • **Disabled**—The Option ROM for System IO Controller 2 (SIOC2) is not available. • **Enabled**—The Option ROMs for System IO Controller 2 (SIOC2) is available. • **UEFI Only**—The Option ROMs for slot are available for UEFI only. • **Legacy Only**—The Option ROM for slot are available for legacy only.
SBMezz1 OptionROM	Whether the server can use Option ROM present in SBMezz1 controller. This can be one of the following: • **Disabled**—The Option ROM for SBMezz1 controllers is not available. • **Enabled**—The Option ROMs for SBMezz1 controller is available. • **UEFI Only**—The Option ROMs for slot are available for UEFI only. • **Legacy Only**—The Option ROM for slot are available for legacy only.

Name	Description
SBMezz2 OptionROM drop-down list	Whether the server can use Option ROM that is available in the SBMezz2 controller. This can be one of the following: • **Disabled**—The Option ROM for SBMezz 2 controllers is not available. • **Enabled**—The Option ROM for SBMezz 2 controllers is available. • **UEFI Only**—The Option ROMs for slot are available for UEFI only. • **Legacy Only**—The Option ROMs for slot are available for legacy only.
IOESlot1 OptionROM	Whether option ROM is enabled on the IOE slot 1. This can be one of the following: • **Disabled**— Option ROM is disabled. • **Enabled**— Default value. Option ROM is enabled. • **UEFI Only**— slot 1 option ROM is available for UEFI only. • **Legacy Only**— slot 1 option ROM is available for legacy only.
IOEMezz1 OptionROM	Whether option ROM is enabled on the IOE Mezz1. This can be one of the following: • **Disabled**— Option ROM is disabled. • **Enabled**— Default value. Option ROM is enabled. • **UEFI Only**— Mezz1 option ROM is available for UEFI only. • **Legacy Only**— Mezz1 option ROM is available for legacy only.
IOESlot2 OptionROM	Whether option ROM is enabled on the IOE slot 2. This can be one of the following: • **Disabled**— Option ROM is disabled. • **Enabled**— Default value. Option ROM is enabled. • **UEFI Only**— slot 2 option ROM is available for UEFI only. • **Legacy Only**— slot 2 option ROM is available for legacy only.

Name	Description
IOENVMe1 OptionROM	Whether option ROM is enabled on the IOE NVMe1. This can be one of the following: • **Disabled**— Option ROM is disabled. • **Enabled**— Default value. Option ROM is enabled. • **UEFI Only**— Mezz1 option ROM is available for UEFI only. • **Legacy Only**— Mezz1 option ROM is available for legacy only.
IOENVMe2 OptionROM	Whether option ROM is enabled on the IOE NVMe2. This can be one of the following: • **Disabled**— Option ROM is disabled. • **Enabled**— Default value. Option ROM is enabled. • **UEFI Only**— Mezz1 option ROM is available for UEFI only. • **Legacy Only**— Mezz1 option ROM is available for legacy only.
SBNVMe1 Link Speed	SBNVMe1 add-on slot 1 link speed. • **Auto**—Link speed is automatically assigned. • **GEN1**— Link speed can reach up to first generation. • **GEN2**—The default link speed. Link speed can reach up to second generation. • **GEN3**— Link speed can reach up to third generation. • **Disabled**—Slot is disabled, and the card is not enumerated.
SIOC1 Link Speed	System IO Controller 1 (SIOC1) add-on slot 1 link speed. • **GEN1** — Link speed can reach up to first generation. • **GEN2** — Link speed can reach up to second generation. • **GEN3**— The default link speed. Link speed can reach up to third generation. • **Disabled** — Slot is disabled, and the card is not enumerated.
SIOC2 Link Speed	System IO Controller 2 (SIOC2) add-on slot 2 link speed. • **GEN1** — Link speed can reach up to first generation. • **GEN2** — Link speed can reach up to second generation. • **GEN3**— The default link speed. Link speed can reach up to third generation. • **Disabled** — Slot is disabled, and the card is not enumerated.

Name	Description
SBMezz1 Link Speed	SBMezz1 add-on slot 1 link speed. • **Auto**—Link speed is automatically assigned. • **GEN1**— Link speed can reach up to first generation. • **GEN2**—The default link speed. Link speed can reach up to second generation. • **GEN3**— Link speed can reach up to third generation. • **Disabled**—Slot is disabled, and the card is not enumerated.
SBMezz2 Link Speed drop-down list	Assigns SBMezz2 add-on slot 2 link speed. This can be one of the following: • **Auto**— Default value. Slot is enabled. • **GEN 1**— Link speed can reach up to first generation. • **GEN 2**— Link speed can reach up to second generation. • **GEN 3**— Link speed can reach up to third generation. • **Disabled**—Slot is disabled, and the card is not enumerated.
IOESlot1 Link Speed	Slot 1 link speed. This can be one of the following: • **Auto**— Default value. Slot is enabled. • **GEN 1**— Link speed can reach up to first generation. • **GEN 2**— Link speed can reach up to second generation. • **GEN 3**— Link speed can reach up to third generation. • **Disabled**—Slot is disabled, and the card is not enumerated.
IOEMezz1 Link Speed **set IOEMezz1LinkSpeed**	Mezz1 link speed. This can be one of the following: • **Auto**— Default value. Slot is enabled. • **GEN 1**— Link speed can reach up to first generation. • **GEN 2**— Link speed can reach up to second generation. • **GEN 3**— Link speed can reach up to third generation. • **Disabled**—Slot is disabled, and the card is not enumerated.

Name	Description
IOESlot2 Link Speed	Slot 2 link speed. This can be one of the following: • **Auto**— Default value. Slot is enabled. • **GEN 1**— Link speed can reach up to first generation. • **GEN 2**— Link speed can reach up to second generation. • **GEN 3**— Link speed can reach up to third generation. • **Disabled**—Slot is disabled, and the card is not enumerated.
IOENVMe1 Link Speed	NVMe1 link speed. This can be one of the following: • **Auto**— Default value. Slot is enabled. • **GEN 1**— Link speed can reach up to first generation. • **GEN 2**— Link speed can reach up to second generation. • **GEN 3**— Link speed can reach up to third generation. • **Disabled**—Slot is disabled, and the card is not enumerated.
IOENVMe2 Link Speed	NVMe2 link speed. This can be one of the following: • **Auto**— Default value. Slot is enabled. • **GEN 1**— Link speed can reach up to first generation. • **GEN 2**— Link speed can reach up to second generation. • **GEN 3**— Link speed can reach up to third generation. • **Disabled**—Slot is disabled, and the card is not enumerated.

BIOS Configuration Dialog Box Button Bar

Important The buttons in this dialog box affect all BIOS parameters on all available tabs, not just the parameters on the tab that you are viewing.

Name	Description
Save Changes button	Saves the settings for the BIOS parameters on all three tabs and closes the dialog box. If the **Reboot Host Immediately** check box is checked, the server is rebooted immediately and the new BIOS settings go into effect. Otherwise the changes are saved until the server is manually rebooted.
Reset Values button	Restores the values for the BIOS parameters on all three tabs to the settings that were in effect when this dialog box was first opened.

Name	Description
Restore Defaults button	Sets the BIOS parameters on all three tabs to their default settings.
Cancel button	Closes the dialog box without making any changes.

Server Management Tab

Server Management BIOS Parameters

Name	Description
FRB-2 Timer	Whether the FRB2 timer is used by Cisco IMC 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.
OS Watchdog Timer	Whether the BIOS programs the watchdog timer with a specified timeout value. 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 in the **OS Boot Watchdog Timer Timeout** field, the Cisco IMC logs an error and takes the action specified in the **OS Boot Watchdog Policy** field.
OS Watchdog Timer Timeout	If OS does not boot within the specified time, OS watchdog timer expires and system takes action according to timer policy. This can be one of the following: • **5 Minutes**—The OS watchdog timer expires 5 minutes after it begins to boot. • **10 Minutes**—The OS watchdog timer expires 10 minutes after it begins to boot. • **15 Minutes**—The OS watchdog timer expires 15 minutes after it begins to boot. • **20 Minutes**—The OS watchdog timer expires 20 minutes after it begins to boot. **Note** This option is only applicable if you enable the OS Boot Watchdog Timer.

Name	Description
OS Watchdog Timer Policy	What action the system takes if the watchdog timer expires. This can be one of the following: • **Do Nothing**—The server takes no action if 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.

S3260 M5 Servers

I/O Tab

Note BIOS parameters listed in this tab may vary depending on the server.

Table 27: BIOS Parameters in I/O Tab

Name	Description
Reboot Host Immediately checkbox	Upon checking, reboots the host server immediately. You must check the checkbox after saving changes.
Legacy USB Support drop-down list	Whether the system supports legacy USB devices. This can be one of the following: • **Disabled**—USB devices are only available to EFI applications. • **Enabled**—Legacy USB support is always available.
Intel VT for directed IO drop-down list	Whether the processor uses Intel Virtualization Technology (VT), which allows a platform to run multiple operating systems and applications in independent partitions. This can be one of the following: • **Disabled**—The processor does not permit virtualization. • **Enabled**—The processor allows multiple operating systems in independent partitions. **Note** If you change this option, you must power cycle the server before the setting takes effect.

Name	Description
Intel VTD coherency support drop-down list	Whether the processor supports Intel VT-d Coherency. This can be one of the following: • **Disabled**—The processor does not support coherency. • **Enabled**—The processor uses VT-d Coherency as required.
Intel VTD ATS support drop-down list	Whether the processor supports Intel VT-d Address Translation Services (ATS). This can be one of the following: • **Disabled**—The processor does not support ATS. • **Enabled**—The processor uses VT-d ATS as required.
PCIe RAS Support drop-down list	Whether PCIe RAS Support is available on the PCIe slot. This can be one of the following: • **Enabled**— PCIe RAS is available on the slot. • **Disabled**— PCIe RAS is not available on port.
All Onboard LOM Ports drop-down list	Whether all LOM ports are enabled or disabled. This can be one of the following: • **Enabled**— All LOM ports are enabled. • **Disabled**— All LOM ports are disabled.
LOM Port 0 OptionROM drop-down list	Whether Option ROM is available on the LOM port 0. This can be one of the following: • **Disabled**—Option ROM is not available on LOM port 0. • **Enabled**—Option ROM is available on LOM port 0.
LOM Port 1 OptionROM	Whether Option ROM is available on the LOM port 1. This can be one of the following: • **Disabled**—Option ROM is not available on LOM port 1. • **Enabled**—Option ROM is available on LOM port 1.
PCIe Slot *n***OptionROM**drop-down list	Whether the server can use the Option ROMs present in the PCIe Cards. This can be one of the following: • **Disabled**—Option ROM is not available on slot *n*. • **Enabled**—Option ROM is available on slot *n*.
MRAID OptionROM	Whether the server can use the RAID Option ROMs present in the PCIe card slot designated by *n*. This can be one of the following: • **Disabled**—Option ROM for slot *n* is not available. • **Enabled**—Option ROM for slot *n* is available.

Name	Description
MLOM Oprom drop-down list	This options allows you to control the Option ROM execution of the PCIe adapter connected to the MLOM slot. This can be one of the following: • **Disabled**—Does not execute Option ROM of the PCIe adapter connected to the MLOM slot. • **Enabled**—Executes Option ROM of the PCIe adapter connected to the MLOM slot.
HBA Oprom drop-down list	This options allows you to control the Option ROM execution of the PCIe adapter connected to the HBA slot. This can be one of the following: • **Disabled**—Does not execute Option ROM of the PCIe adapter connected to the HBA slot. • **Enabled**—Executes Option ROM of the PCIe adapter connected to the HBA slot.
Front NVME1 Oprom drop-down list	This options allows you to control the Option ROM execution of the PCIe adapter connected to the SSD:NVMe1 slot. This can be one of the following: • **Disabled**—Does not execute Option ROM of the PCIe adapter connected to the SSD:NVMe1 slot. • **Enabled**—Executes Option ROM of the PCIe adapter connected to the SSD:NVMe1 slot
Front NVME2 Oprom drop-down list	This options allows you to control the Option ROM execution of the PCIe adapter connected to the SSD:NVMe2 slot. This can be one of the following: • **Disabled**—Does not execute Option ROM of the PCIe adapter connected to the SSD:NVMe2 slot. • **Enabled**—Executes Option ROM of the PCIe adapter connected to the SSD:NVMe2 slot
HBA Link Speed drop-down list	This option allows you to restrict the maximum speed of an adapter card installed in PCIe HBA slot. This can be one of the following: • **Disabled**—The maximum speed is not restricted. • **Auto**—System selects the maximum speed allowed. • **GEN1**—2.5GT/s (gigatransfers per second) is the maximum speed allowed. • **GEN2**—5GT/s is the maximum speed allowed. • **GEN3**—8GT/s is the maximum speed allowed.

Name	Description
MLOM Link Speed drop-down list	This option allows you to restrict the maximum speed of an adapter card installed in PCIe MLOM slot. This can be one of the following: • **Disabled**—The maximum speed is not restricted. • **Auto**—System selects the maximum speed allowed. • **GEN1**—2.5GT/s (gigatransfers per second) is the maximum speed allowed. • **GEN2**—5GT/s is the maximum speed allowed. • **GEN3**—8GT/s is the maximum speed allowed.
MRAID Link Speed drop-down list	This option allows you to restrict the maximum speed of an adapter card installed in MRAID slot. This can be one of the following: • **Disabled**—The maximum speed is not restricted. • **Auto**—System selects the maximum speed allowed. • **GEN1**—2.5GT/s (gigatransfers per second) is the maximum speed allowed. • **GEN2**—5GT/s is the maximum speed allowed. • **GEN3**—8GT/s is the maximum speed allowed.
PCIe Slot*n* Link Speed drop-down list	System IO Controller *n* (SIOCn) add-on slot (designated by *n*) link speed. This can be one of the following: • **Disabled**—Slot is disabled, and the card is not enumerated. • **Auto**— The default link speed. Link speed is automatically assigned. • **GEN1**—Link speed can reach up to first generation. • **GEN2**—Link speed can reach up to second generation. • **GEN3**—Link speed can reach up to third generation.
Front NVME1 Link Speed drop-down list	Link speed for NVMe front slot 1. This can be one of the following: • **Disabled**—Slot is disabled, and the card is not enumerated. • **Auto**—The default link speed. Link speed is automatically assigned. • **GEN1**—Link speed can reach up to first generation. • **GEN2**—Link speed can reach up to second generation. • **GEN3**—Link speed can reach up to third generation.

Name	Description
Front NVME2 Link Speed drop-down list	Link speed for NVMe front slot 2. This can be one of the following: • **Disabled**—Slot is disabled, and the card is not enumerated. • **Auto**—The default link speed. Link speed is automatically assigned. • **GEN1**—Link speed can reach up to first generation. • **GEN2**—Link speed can reach up to second generation. • **GEN3**—Link speed can reach up to third generation.
Rear NVME1 Link Speed drop-down list	Link speed for NVMe rear slot 1. This can be one of the following: • **Disabled**—Slot is disabled, and the card is not enumerated. • **Auto**—The default link speed. Link speed is automatically assigned. • **GEN1**—Link speed can reach up to first generation. • **GEN2**—Link speed can reach up to second generation. • **GEN3**—Link speed can reach up to third generation.
Rear NVME2 Link Speed drop-down list	Link speed for NVMe rear slot 2. This can be one of the following: • **Disabled**—Slot is disabled, and the card is not enumerated. • **Auto**—The default link speed. Link speed is automatically assigned. • **GEN1**—Link speed can reach up to first generation. • **GEN2**—Link speed can reach up to second generation. • **GEN3**—Link speed can reach up to third generation.
VGA Priority drop-down list	Allows you to set the priority for VGA graphics devices if multiple VGA devices are found in the system. This can be one of the following: • **OnBoard**—Priority is given to the onboard VGA device. BIOS post screen and OS boot are driven through the onboard VGA port. • **OffBoard**—Priority is given to the PCIE Graphics adapter. BIOS post screen and OS boot are driven through the external graphics adapter port. • **OnBoard VGA Disabled**—Priority is given to the PCIe Graphics adapter, and the onboard VGA device is disabled. The vKVM does not function when the onboard VGA is disabled.
P-SATA OptionROM drop-down list	Allows you to select the PCH SATA optionROM mode. This can be one of the following: • **LSI SW Raid**— Sets both SATA and sSATA controllers to raid mode for LSI SW Raid. • **Disabled**— Disables both SATA and sSATA controllers.

Name	Description
M2.SATA OptionROM drop-down list	Mode of operation of Serial Advanced Technology Attachment (SATA) Solid State Drives (SSD). This can be one of the following: • **AHCI**— Sets both SATA and sSATA controllers to AHCI mode. • **LSI SW Raid**— Sets both SATA and sSATA controllers to raid mode for LSI SW Raid. • **Disabled**— Disables both SATA and sSATA controllers.
USB Port Rear drop-down list	Whether the rear panel USB devices are enabled or disabled. This can be one of the following • **Disabled**— Disables the rear panel USB ports. Devices connected to these ports are not detected by the BIOS and operating system. • **Enabled**— Enables the rear panel USB ports. Devices connected to these ports are detected by the BIOS and operating system.
USB Port Front drop-down list	Whether the front panel USB devices are enabled or disabled. This can be one of the following • **Disabled**— Disables the front panel USB ports. Devices connected to these ports are not detected by the BIOS and operating system. • **Enabled**— Enables the front panel USB ports. Devices connected to these ports are detected by the BIOS and operating system.
USB Port Internal drop-down list	Whether the internal USB devices are enabled or disabled. This can be one of the following • **Disabled**— Disables the internal USB ports. Devices connected to these ports are not detected by the BIOS and operating system. • **Enabled**— Enables the internal USB ports. Devices connected to these ports are detected by the BIOS and operating system.
USB Port KVM drop-down list	Whether the vKVM ports are enabled or disabled. This can be one of the following • **Disabled**— Disables the vKVM keyboard and/or mouse devices. Keyboard and/or mouse will not work in the KVM window. • **Enabled**— Enables the vKVM keyboard and/or mouse devices.
USB Port Internal drop-down list	Whether the USB Port Internal is enabled or disabled. This can be one of the following • **Disabled**— Disables the USB Port Internal. Devices connected to these ports are not detected by the BIOS and operating system. • **Enabled**— Enables the USB Port Internal. Devices connected to these ports are detected by the BIOS and operating system.

Name	Description
IPV6 PXE Support drop-down list	Enables or disables IPv6 support for PXE. This can be one of the following • **Disabled**—IPv6 PXE support is not available. • **Enabled**—IPv6 PXE support is always available.
IPv4 HTTP Support	Enables or disables IPv4 support for HTTP. This can be one of the following • **Disabled**—IPv4 HTTP support is not available. • **Enabled**—IPv4 HTTP support is always available.
IPv6 HTTP Support	Enables or disables IPv6 support for HTTP. This can be one of the following • **Disabled**—IPv6 PXE support is not available. • **Enabled**—IPv6 PXE support is always available.
PCIe PLL SSC drop-down list	Enable this feature to reduce EMI interference by down spreading clock 0.5%. Disable this feature to centralize the clock without spreading. This can be one of the following: • **Auto**—EMI interference is auto adjusted. **Disabled**—EMI interference is auto adjusted. • **ZeroPointFive**—EMI interference is reduced by down spreading the clock 0.5%.
IPV4 PXE Support drop-down list	Enables or disables IPv4 support for PXE. This can be one of the following • **Disabled**—IPv4 PXE support is not available. • **Enabled**—IPv4 PXE support is always available.
Network Stack drop-down list	This option allows you to monitor IPv6 and IPv4. This can be one of the following • **Disabled**—Network Stack support is not available. **Note** When disabled, the value set for **IPV4 PXE Support** does not impact the system. • **Enabled**—Network Stack support is always available.
External SSC enable drop-down list	This option allows you to reduce the EMI of your motherboard by modulating the signals it generates so that the spikes are reduced to flatter curves. This can be one of the following: • **Disabled**—Clock Spread Spectrum support is not available. • **Enabled**—Clock Spread Spectrum support is always available.

Name	Description
PCIe Slot MSTOR RAID OptionROM drop-down list	Whether the server can use the Option ROMs present in the PCIe MSTOR RAID. This can be one of the following: • **Disabled**—Option ROM is not available. • **Enabled**—Option ROM is available.

Server Management Tab

Note BIOS parameters listed in this tab may vary depending on the server.

Table 28: BIOS Parameters in Server Management Tab

Name	Description
Reboot Host Immediately checkbox	If the Reboot Host Immediately check box is checked, the server is rebooted immediately and the new BIOS settings go into effect. Otherwise the changes are saved until the server is manually rebooted.
OS Boot Watchdog Timer Policy drop-down list	What action the system takes if the watchdog timer expires. This can be one of the following: • **Power Off**—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.
OS Watchdog Timer drop-down list	Whether the BIOS programs the watchdog timer with a specified timeout value. 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 in the **OS Boot Watchdog Timer Timeout** field, the Cisco IMC logs an error and takes the action specified in the **OS Boot Watchdog Policy** field.

Name	Description
OS Watchdog Timer Timeout drop-down list	If OS does not boot within the specified time, OS watchdog timer expires and system takes action according to timer policy. This can be one of the following: • **5 Minutes**—The OS watchdog timer expires 5 minutes after it begins to boot. • **10 Minutes**—The OS watchdog timer expires 10 minutes after it begins to boot. • **15 Minutes**—The OS watchdog timer expires 15 minutes after it begins to boot. • **20 Minutes**—The OS watchdog timer expires 20 minutes after it begins to boot. **Note** This option is only applicable if you enable the OS Boot Watchdog Timer.
Baud Rate drop-down list	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 9,600 Baud rate is used. • **19.2k**—A 19,200 Baud rate is used. • **38.4k**—A 38,400 Baud rate is used. • **57.6k**—A 57,600 Baud rate is used. • **115.2k**—A 115,200 Baud rate is used. This setting must match the setting on the remote terminal application.
Console Redirection drop-down list	Allows a serial port to be used for console redirection during POST and BIOS booting. After the OS has booted, console redirection is irrelevant. This can be one of the following: • **Serial Port A**—Enables console redirection on serial port A during POST. • **Serial Port B**—Enables console redirection on serial port B during POST. • **Disabled**—No console redirection occurs during POST.

Name	Description
Adaptive Memory Training	When this option is **Enabled**: The Memory training will not happen in every boot but the BIOS will use the saved memory training result in every re-boot. Some exceptions when memory training happens in every boot are: BIOS update, CMOS reset, CPU or Memory configuration change, SPD or run-time uncorrectable error or the last boot has occurred more than 24 hours before. When this option is **Disabled**, the Memory training happens in every boot. Default value: **Enabled**. **Note** To disable the Fast Boot option, the end user must set the following tokens as mentioned below: Adaptive Memory Training to **Disabled** BIOS Techlog level to **Normal** OptionROM Launch Optimization to **Disabled**.
BIOS Techlog Level	This option denotes the type of messages in **BIOS tech log** file. The log file can be one of the following types: • **Minimum** - Critical messages will be displayed in the log file. • **Normal** - Warning and loading messages will be displayed in the log file. • **Maximum** - Normal and information related messages will be displayed in the log file. Default value: **Minimum**. **Note** This option is mainly for internal debugging purposes.

Name	Description
OptionROM Launch Optimization	When this option is **Enabled**, the OptionROMs only for the controllers present in the boot order policy will be launched. **Note** Some controllers such as Onboard storage controllers, Emulex FC adapters, and GPU controllers though not listed in the boot order policy will have the OptionROM launched. When this option is **Disabled**, all the OptionROMs will be launched. Default value: **Enabled**
CDN Control drop-down list	Whether the Ethernet Network naming convention is according to Consistent Device Naming (CDN) or the traditional way of naming conventions. This can be one of the following: • **Disabled**— CDN support for VIC cards is disabled • **Enabled**— CDN support is enabled for VIC cards.
FRB 2 Timer drop-down list	Whether the FRB2 timer is used by Cisco IMC 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.
Flow Control drop-down list	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
Terminal type drop-down list	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.
PCIe Slots CDN Control drop-down list	**Note** This option is available only on Cisco UCS C240 M5 servers equipped with Qlogic cards in slots 2 or 5. Whether the Ethernet Network naming convention is according to Consistent Device Naming (CDN) or the traditional way of naming conventions. This can be one of the following: • **Disabled**— CDN support for VIC cards is disabled • **Enabled**— CDN support is enabled for VIC cards.

Security Tab

Note BIOS parameters listed in this tab may vary depending on the server.

Table 29: BIOS Parameters in Security Tab

Name	Description
Reboot Host Immediately checkbox	**If the Reboot Host Immediately check box is checked, the server is rebooted immediately and the new BIOS settings go into effect. Otherwise the changes are saved until the server is manually rebooted.**
Trusted Platform Module State drop-down list	Trusted Platform Module (TPM) is a microchip designed to provide basic security-related functions primarily involving encryption keys. This option allows you to control the TPM Security Device support for the system. It can be one of the following: • **Disabled**—The server does not use the TPM. • **Enabled**—The server uses the TPM. **Note** Contact your operating system vendor to make sure the operating system supports this feature.
SHA-1 PCR Bank	Enable or Disable SHA-1 PCR Bank. This can be one of the following: • **Disabled**—Support is disabled. • **Enabled**—Support is enabled.
SHA256 PCR Bank	Enable or Disable SHA256 PCR Bank. This can be one of the following: • **Disabled**—Support is disabled. • **Enabled**—Support is enabled.
Intel Trusted Execution Technology Support	Can be Enabled only when Trusted Platform Module (TPM) is Enabled. This can be one of the following: • **Disabled**—Support is disabled. • **Enabled**—Support is enabled.
Power ON Password drop-down list	This token requires that you set a BIOS password before using the F2 BIOS configuration. If enabled, password needs to be validated before you access BIOS functions such as IO configuration, BIOS set up, and booting to an operating system using BIOS. It can be one of the following: • **Disabled**—Support is disabled. • **Enabled**—Support is enabled.

Processor Tab

Note BIOS parameters listed in this tab may vary depending on the server.

Table 30: BIOS Parameters in Processor Tab

Name	Description
Intel Virtualization Technology drop-down list	Whether the processor uses Intel Virtualization Technology (VT), which allows a platform to run multiple operating systems and applications in independent partitions. This can be one of the following: • **Disabled**—The processor does not permit virtualization. • **Enabled**—The processor allows multiple operating systems in independent partitions.
Extended APIC drop-down list	Allows you to enable or disable extended APIC support. This can be one of the following: • **Enabled**—Enables APIC support • **Disabled**—Disables APIC support.
Processor C1E drop-down list	Whether the CPU transitions to its minimum frequency when entering the C1 state. This can be one of the following: • **Disabled**—The CPU continues to run at its maximum frequency in C1 state. • **Enabled**—The CPU transitions to its minimum frequency. This option saves the maximum amount of power in C1 state. **Note** This option is available only on some C-Series servers.

Name	Description
Processor C6 Report drop-down list	Whether the BIOS sends the C6 report to the operating system. When the OS receives the report, it can transition the processor into the lower C6 power state to decrease energy usage while maintaining optimal processor performance. This can be one of the following: • **Disabled**—The BIOS does not send the C6 report. • **Enabled**—The BIOS sends the C6 report, allowing the OS to transition the processor to the C6 low power state. **Note** **CPUPowerManagement** must be set to **Custom** or the server ignores the setting for this parameter. **Note** This option is available only on some C-Series servers.
Execute Disable Bit drop-down list	Classifies memory areas on the server to specify where application code can execute. As a result of this classification, the processor disables code execution if a malicious worm attempts to insert code in the buffer. This setting helps to prevent damage, worm propagation, and certain classes of malicious buffer overflow attacks. This can be one of the following: • **Disabled**—The processor does not classify memory areas. • **Enabled**—The processor classifies memory areas. **Note** Contact your operating system vendor to make sure the operating system supports this feature.

Name	Description
Turbo Mode drop-down list	Whether the processor uses Intel Turbo Boost Technology, which allows the processor to automatically increase its frequency if it is running below power, temperature, or voltage specifications. This can be one of the following: • **Disabled**—The processor does not increase its frequency automatically. • **Enabled**—The processor utilizes Turbo Boost Technology if required. **Note** **CPUPowerManagement** must be set to **Custom** or the server ignores the setting for this parameter.
EIST PSD Function drop-down list	EIST reduces the latency inherent with changing the voltage-frequency pair (P-state), thus allowing those transitions to occur more frequently. This allows for more granular, demand-based switching and can optimize the power-to-performance balance, based on the demands of the applications. This can be one of the following: • HW ALL: The processor is coordinates the P-state among logical processors dependencies. The OS keeps the P-state request up to date on all logical processors. • SW ALL: The OS Power Manager coordinates the P-state among logical processors with dependencies and initiates the transition on all of those Logical Processors.

Name	Description
SpeedStep (Pstates) drop-down list	Whether the processor uses Enhanced Intel SpeedStep Technology, which allows the system to dynamically adjust processor voltage and core frequency. This technology can result in decreased average power consumption and decreased average heat production. This can be one of the following: • **Disabled**—The processor never dynamically adjusts its voltage or frequency. • **Enabled**—The processor utilizes Enhanced Intel SpeedStep Technology and enables all supported processor sleep states to further conserve power. We recommend that you contact your operating system vendor to make sure the operating system supports this feature. **Note** **CPUPowerManagement** must be set to **Custom** or the server ignores the setting for this parameter.
HyperThreading [ALL] drop-down list	Whether the processor uses Intel Hyper-Threading Technology, which allows multithreaded software applications to execute threads in parallel within each processor. This can be one of the following: • **Disabled**—The processor does not permit hyperthreading. • **Enabled**—The processor allows for the parallel execution of multiple threads.
Cores Enabled drop-down list	Allows you to disable one or more of the physical cores on the server. This can be one of the following: • **All**—Enables all physical cores. This also enables Hyper Threading on the associated logical processor cores. • **1 through 27**—Specifies the number of physical processor cores that can run on the server. Each physical core has an associated logical core. **Note** Contact your operating system vendor to make sure the operating system supports this feature.

Name	Description
Processor CMCI drop-down list	Allows the CPU to trigger interrupts on corrected machine check events. The corrected machine check interrupt (CMCI) allows faster reaction than the traditional polling timer. This can be one of the following: • **Disabled**—Disables CMCI. • **Enabled**—Enables CMCI. This is the default value.
Enhanced Intel SpeedStep Tech drop-down list	Whether the processor uses Enhanced Intel SpeedStep Technology, which allows the system to dynamically adjust processor voltage and core frequency. This technology can result in decreased average power consumption and decreased average heat production. This can be one of the following: • **Disabled**—The processor never dynamically adjusts its voltage or frequency. • **Enabled**—The processor utilizes Enhanced Intel SpeedStep Technology and enables all supported processor sleep states to further conserve power. We recommend that you contact your operating system vendor to make sure the operating system supports this feature. **Note** **CPUPowerManagement** must be set to **Custom** or the server ignores the setting for this parameter.
Workload Configuration drop-down list	This feature allows for workload optimization. The options are Balanced and I/O Sensitive: • **NUMA** • **UMA**
Sub NUMA Clustering drop-down list	Whether the CPU supports sub NUMA clustering, in which the tag directory and the memory channel are always in the same region. This can be one of the following: • **Disabled**— Sub NUMA clustering does not occur. • **Enabled**— Sub NUMA clustering occurs. • **Auto** — The BIOS determines what Sub NUMA clustering is done.

Name	Description
Energy/Performance Bias Config	Displays the energy or performance bias configuration. This can be one of the following: • Balanced Performance • Performance • Balanced Power • Power
IMC Interleaving drop-down list	This BIOS option controls the interleaving between the Integrated Memory Controllers (IMCs). • **1-way Interleave**—There is no interleaving. • **2-way Interleave**—Addresses are interleaved between the two IMCs. • **Auto** —CPU determines the IMC Interleaving mode.
XPT Prefetch drop-down list	Whether XPT prefetch is used to enable a read request sent to the last level cache to issue a copy of that request to the memory controller prefetcher. This can be one of the following: • **Disabled**—The CPU does not use the XPT Prefetch option. • **Enabled**—The CPU enables the XPT prefetch option.
UPI Prefetch drop-down list	UPI prefetch is a mechanism to get the memory read started early on a DDR bus. This can be one of the following: • **Disabled**—The processor does not preload any cache data. • **Enabled**—The UPI prefetcher preloads the L1 cache with the data it determines to be the most relevant.

Name	Description
Energy Performance Bias Config drop-down list	Allows you to determine whether system performance or energy efficiency is more important on this server. This can be one of the following: • **Performance** — 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. • **Balanced Performance** — The server provides all server components with enough power to keep a balance between performance and power. • **Balanced Power** — The server provides all server components with enough power to keep a balance between performance and power. • **Power** — The server provides all server components with maximum power to keep reduce power consumption.
Power Performance Tuning drop-down list	Determines if the BIOS or Operating System can turn on the energy performance bias tuning. The options are BIOS and OS. • **BIOS**— Chooses BIOS for energy performance tuning. • **OS**— Chooses OS for energy performance tuning.
LLC Prefetch drop-down list	Whether the processor uses the LLC Prefetch mechanism to fetch the date into the LLC. This can be one of the following: • **Disabled**—The processor does not preload any cache data. • **Enabled**—The LLC prefetcher preloads the L1 cache with the data it determines to be the most relevant.

Name	Description
Package C State	The amount of power available to the server components when they are idle. This can be one of the following: • **No Limit**—The server may enter any available C state. • **Auto** —The CPU determines the physical elevation. • **C0 C1 State**—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. • **C2**—When the CPU is idle, the system reduces the power consumption further than with the C1 option. This requires less power than C1 or C0, but it takes the server slightly longer to return to high performance mode. • **C6 Non Retention**—When the CPU is idle, the system reduces the power consumption further than with the C3 option. This option saves more power than C0, C1, or C3, but there may be performance issues until the server returns to full power. • **C6 Retention**—When the CPU is idle, the system reduces the power consumption further than with the C3 option. This option saves more power than C0, C1, or C3, but there may be performance issues until the server returns to full power.
Hardware P-States drop-down list	Enables processor Hardware P-State. This can be one of the following: • **Disabled**—HWPM is disabled. • **HWPM Native Mode**—HWPM native mode is enabled. • **HWPM OOB Mode**—HWPM Out-Of-Box mode is enabled. • **Native Mode with no Legacy** (only GUI)

Name	Description
Intel Speed Select drop-down list	**Intel Speed Select** modes will allow users to run the CPU with different speed and cores. This can be one of the following: • **Base**— It will allow users to access maximum core and Thermal Design Power (TDP) ratio. • **Config 1**— It will allow users to access core and TDP ratio lesser than **Base**. • **Config 2**— It will allow users to access core and TDP ratio lesser than **Config 1**. Default value: **Base**.
Uncore Frequency Scaling drop-down list	This feature allows you configure the scaling of uncore frequency of the processor. This can be one of the following: • **Enabled**—Uncore frequency of the processor scales up or down based on the load. • **Disabled**—Uncore frequency of the processor remains fixed. Refer Intel® Dear Customer Letter (DCL) to know the fixed higher and lower values for **Uncore Frequency Scaling**.
Configurable TDP Level drop-down list	**Configurable TDP Level** feature allows adjustments in processor thermal design power values. By modifying the processor behavior and the performance levels, power consumption of a processor can be configured and TDP can be adjusted as the same time. Hence, a processor operates at higher or lower performance levels, depending on the available cooling capacities and desired power consumption. This can be one of the following: • **Normal** • **Level_1** • **Level_2** Refer Intel® Dear Customer Letter (DCL) to know the values for **TDP level**.

Name	Description
UPI Link Speed drop-down list	**Note** **UPI Link Frequency Select** token is not applicable for single socket configuration. This feature allows you to configure the Intel Ultra Path Interconnect (UPI) link speed between multiple sockets. This can be one of the following: • **Auto**—This option configures the optimal link speed automatically. • **9.6 GT/s**—This option configures the optimal link speed at 9.6GT/s. • **10.4 GT/s**—This option configures the optimal link speed at 10.4GT/s
Energy Efficient Turbo drop-down list	When energy efficient turbo is enabled, the optimal turbo frequency of the CPU turns dynamic based on CPU utilization. The power/performance bias setting also influences energy efficient turbo. This can be one of the following: • **Disabled**—Energy Efficient Turbo is disabled. • **Enabled**—Energy Efficient Turbo is enabled.
Processor EPP Enable	Displays the selected value for Processor EPP Enable. • **Disabled**—Processor EPP Enable is disabled. • **Enabled**—Processor EPP Enable is enabled.
Autonomous Core C-state drop-down list	Enables CPU Autonomous C-State, which converts the HALT instructions to the MWAIT instructions. This can be one of the following: • **Disabled**—CPU Autonomous C-state is disabled. • **Enabled**—CPU Autonomous C-state is enabled.

Name	Description
Patrol Scrub drop-down list	Allows the system to actively search for, and correct, single bit memory errors even in unused portions of the memory on the server. This can be one of the following: • **Disabled**—The system checks for memory ECC errors only when the CPU reads or writes a memory address. • **Enabled**—The system periodically reads and writes memory searching for ECC errors. If any errors are found, the system attempts to fix them. This option may correct single bit errors before they become multi-bit errors, but it may adversely affect performance when the patrol scrub is running. • **Enable at End of POST**—The system checks for memory ECC errors after BIOS POST.
Processor EPP Profile drop-down list	Allows you to determine whether system performance or energy efficiency is more important on this server. This can be one of the following: • Performance • Balanced Performance • Balanced Power • Power

Memory Tab

Note BIOS parameters listed in this tab may vary depending on the server.

Table 31: BIOS Parameters in Memory Tab

Name	Description
Reboot Host Immediately checkbox	Upon checking, reboots the host server immediately. You must check the checkbox after saving changes.

Name	Description
Select Memory RAS configuration drop-down list	Determines how the memory reliability, availability, and serviceability (RAS) is configured for the server. This can be one of the following: • **Maximum Performance**—System performance is optimized. • **ADDDC Sparing**—Adaptive virtual lockstep is an algorithm implemented in the hardware and firmware to support the ADDDC mode. When selected, the system performance is optimized till the algorithm is activated. The algorithm is activated in case of DRAM device failure. Once the algorithm is activated, the virtual lockstep regions are activated to map out the failed region during run-time dynamically, and the performance impact is restricted at a region level. • **Mirror Mode 1LM**—System reliability is optimized by using half the system memory as backup. • **Partial Mirror Mode 1LM**—Partial DIMM Mirroring creates a mirrored copy of a specific region of memory cells, rather than keeping the complete mirror copy. Partial Mirroring creates a mirrored region in memory map with the attributes of a partial mirror copy. Up to 50% of the total memory capacity can be mirrored, using up to 4 partial mirrors.
Above 4G Decoding drop-down list	Enables or disables MMIO above 4GB or not. This can be one of the following: • **Disabled**—The server does not map I/O of 64-bit PCI devices to 4GB or greater address space. • **Enabled**—The server maps I/O of 64-bit PCI devices to 4GB or greater address space. **Note** PCI devices that are 64-bit compliant but use a legacy option ROM may not function correctly with this setting enabled.
DCPMM Firmware Downgrade drop-down list	Whether the BIOS supports downgrading the DCPMM firmware. This can be one of the following: • **Disabled**—Support is disabled. • **Enabled**—Support is enabled.

Name	Description
Partial Memory Mirror Mode drop-down list	The partial memory size is either in percentage or in GB. This can be one of the following: • **Percentage**—The partial memory mirror is defined in percentage. • **Value in GB**—The partial memory mirror is defined in GB. • **Disabled**—Partial memory mirror is disabled.
Partial Mirror percentage field	Percentage of memory to mirror above 4GB. Enter an integer between 0 and 50.
Partial Mirror1 Size in GB field	Size of the first partial memory mirror in GB. Enter an integer between 0 and 65535. **Note** The combined memory size of all the partial mirror should not exceed 50% of the physical memory size.
Partial Mirror2 Size in GB field	Size of the second partial memory mirror in GB. Enter an integer between 0 and 65535. **Note** The combined memory size of all the partial mirror should not exceed 50% of the physical memory size.
Partial Mirror3 Size in GB field	Size of the third partial memory mirror in GB. Enter an integer between 0 and 65535. **Note** The combined memory size of all the partial mirror should not exceed 50% of the physical memory size.
Partial Mirror4 Size in GB field	Size of the fourth partial memory mirror in GB. Enter an integer between 0 and 65535. **Note** The combined memory size of all the partial mirror should not exceed 50% of the physical memory size.
Memory Size Limit in GB field	Use this option to reduce the size of the physical memory limit in GB. Enter an integer between 0 and 65535.

Name	Description
NUMA drop-down list	Whether the BIOS supports Non-Uniform Memory Access (NUMA). This can be one of the following: • **Disabled**—Support is disabled. • **Enabled**—Support is enabled.
BME DMA Mitigation drop-down list	Allows you to disable the PCI BME bit to mitigate the threat from an unauthorized external DMA. This can be one of the following: • **Disabled**—PCI BME bit is disabled in the BIOS. • **Enabled**—PCI BME bit is enabled in the BIOS.
Select PPR Type drop-down list	Cisco IMC supports **Hard-PPR**, which permanently remaps accesses from a designated faulty row to a designated spare row. This can be one of the following: • **Hard PPR**—Support is enabled. **Note** Hard PPR can be used only when **Memory RAS Configuration** is set to **ADDDC Sparing**. For other RAS selections, this setting should be set to **Disabled**. • **Disabled**—Support is disabled.
CR QoS drop-down list	Enables you to select the CR QoS tuning. This can be one of the following: • **Recipe 1**—For QoS knobs and is recommended for 2-2-2 memory configuration in active directory. • **Recipe 2**—For QoS knobs and is recommended for other memory configuration in active directory. • **Recipe 3**—For QoS knobs and is recommended for 1 DIMM per channel configuration. • **Disabled**—**CR QoS** feature is disabled.

Name	Description
Snoopy mode for AD drop-down list	Enables new AD specific feature to avoid directory updates to DDRT memory from non-NUMA optimized workloads. This can be one of the following: • **Disabled**—Support is disabled. • **Enabled**—Support is enabled.
CR FastGo Config drop-down list	Enables you to select CR QoS configuration profiles. This can be one of the following: • **Default** • **Option 1** • **Option 2** • **Option 3** • **Option 4** • **Option 5** • **Auto**
NVM Performance Setting drop-down list	Enables you to configure NVM baseline performance settings depending on the workload behavior. • **BW Optimized** • **Latency Optimized** • **Balanced Profile**
Snoopy mode for 2LM drop-down list	Enables you to avoid directory updates to far-memory from non-NUMA optimized workloads. This can be one of the following: • **Disabled**—Support is disabled. • **Enabled**—Support is enabled.

Name	Description
Memory Thermal Throttling Mode drop-down list	This function is used for adjusting memory temperature. If memory temperature is excessively high after the function is enabled, the memory access rate is reduced and Baseboard Management Controller (BMC) adjusts the fan to cool down the memory to avoid any DIMM damage. This can be one of the following: • **Disabled**—Support is disabled. • **CLTT with PECI**—Enables Closed Loop Thermal Throttling with Platform Environment Control Interface.
Memory Refresh Rate drop-down list	Enables you to increase or decrease memory refresh rate. Increasing the DRAM refresh rate reduces the maximum number of activates (hammers) that can occur before the next refresh. This can be one of the following: • **1X Refresh**—Refresh rate is at minimum. • **2X Refresh** —Refresh is 2X faster.
Panic and High Watermark drop-down list	When set to low, the memory controller does not postpone refreshes while **Memory Refresh Rate** is set to **1X Refresh**. This can be one of the following: • **Low**—Refresh rate is set to low. • **High** —Refresh rate is set to high.
Advanced Memory Test drop-down list	**Note** This feature is applicable only to Samsung, Hynix and Micron DIMMs. You can enable advance DIMM testing during BIOS POST using this feature. This can be one of the following: • **Disabled**—Support is disabled. • **Enabled**—Support is enabled.
Enhanced Memory Test drop-down list	This can be one of the following: • **Auto**—Support is set to Auto. • **Disabled**—Support is disabled. • **Enabled**—Support is enabled.

Power/Performance Tab

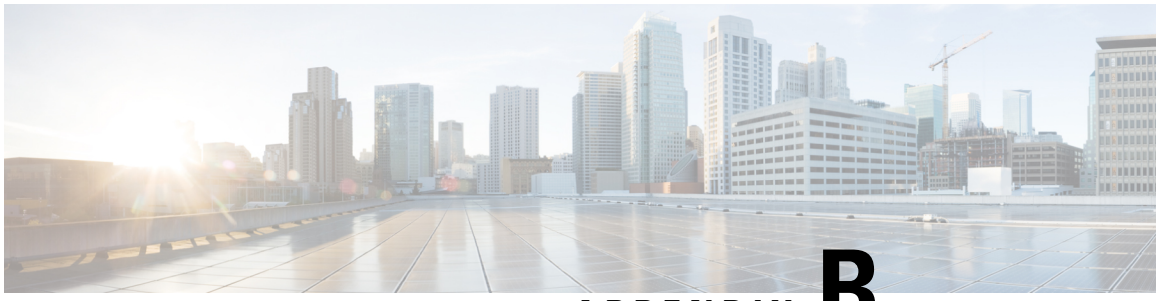
Note BIOS parameters listed in this tab may vary depending on the server.

Table 32: BIOS Parameters in Power/Performance Tab

Name	Description
Reboot Host Immediately checkbox	Upon checking, reboots the host server immediately. You must check the checkbox after saving changes.
Hardware Prefetcher drop-down list	Whether the processor allows the Intel hardware prefetcher to fetch streams of data and instruction from memory into the unified second-level cache when necessary. This can be one of the following: • **Disabled**—The hardware prefetcher is not used. • **Enabled**—The processor uses the hardware prefetcher when cache issues are detected.
Adjacent Cache Line Prefetcher drop-down list	Whether the processor fetches cache lines in even or odd pairs instead of fetching just the required line. This can be one of the following: • **Disabled**—The processor only fetches the required line. • **Enabled**—The processor fetches both the required line and its paired line.
DCU Streamer Prefetch drop-down list	Whether the processor uses the DCU IP Prefetch mechanism to analyze historical cache access patterns and preload the most relevant lines in the L1 cache. This can be one of the following: • **Disabled**—The processor does not try to anticipate cache read requirements and only fetches explicitly requested lines. • **Enabled**—The DCU prefetcher analyzes the cache read pattern and prefetches the next line in the cache if it determines that it may be needed.
DCU IP Prefetcher drop-down list	Whether the processor uses the DCU IP Prefetch mechanism to analyze historical cache access patterns and preload the most relevant lines in the L1 cache. This can be one of the following: • **Disabled**—The processor does not preload any cache data. • **Enabled**—The DCU IP prefetcher preloads the L1 cache with the data it determines to be the most relevant.

Name	Description
CPU Performance drop-down list	Sets the CPU performance profile for the options listed above. This can be one of the following: • **Enterprise**—All options are enabled. • **HPC**—All options are enabled. This setting is also known as high performance computing. • **Hight Throughput**—Only the DCU IP Prefetcher is enabled. The rest of the options are disabled. • **Custom**—All performance profile options can be configured from the BIOS setup on the server. In addition, the Hardware Prefetcher and Adjacent Cache-Line Prefetch options can be configured as well.

BIOS Parameters by Server Model



APPENDIX B

BIOS Token Name Comparison for Multiple Interfaces

This appendix contains the following section:

BIOS Token Name Comparison for Multiple Interfaces

The following table lists the BIOS token names used in the XML, CLI and Web GUI interfaces. You can use this list to map the names across these interfaces.

Note The parameters that are available depend on the type of Cisco UCS server you are using.

BIOS Token Group	BIOS Token Name	XML Object	CLI and Web GUI Object
Main	TPM Support	biosVfTPMSupport/ vpTPMSupport	TPMAdminCtrl
Process Configuration	Intel(R) Hyper-Threading Technology	biosVfIntelHyperThreadingTech/ vpIntelHyperThreadingTech	IntelHyperThread
	Number of Enable Cores	biosVfCoreMultiProcessing/ vpCoreMultiProcessing	CoreMultiProcessing
	Execute Disable	biosVfExecuteDisableBit/ vpExecuteDisableBit	ExecuteDisable
	Intel(R) VT	biosVfIntelVirtualizationTechnology/ vpIntelVirtualizationTechnology	IntelVT

BIOS Token Group	BIOS Token Name	XML Object	CLI and Web GUI Object
	Intel(R) VT-d	biosVfIntelVTForDirectedIO/ vpIntelVTForDirectedIO	IntelVTD
	Intel(R) VT-d Coherency Support	biosVfIntelVTForDirectedIO/ vpIntelVTDCoherencySupport	CoherencySupport
	Intel(R) VT-d ATS Support	biosVfIntelVTForDirectedIO/ vpIntelVTDATSSupport	ATS
	CPU Performance	biosVfCPUPerformance/ vpCPUPerformance	CpuPerformanceProfile
	Hardware Prefetcher	biosVfHardwarePrefetch/ vpHardwarePrefetch	HardwarePrefetch
	Adjacent Cache Line Prefetcher	biosVfAdjacentCacheLinePrefetch/ vpAdjacentCacheLinePrefetch	AdjacentCacheLinePrefetch
	DCU Streamer Prefetch	biosVfDCUPrefetch/ vvpStreamerPrefetch	DcuStreamerPrefetch
	DCU IP Prefetcher	biosVfDCUPrefetch/ vpIPPrefetch	DcuIpPrefetch
	Direct Cache Access Support	biosVfDirectCacheAccess/ vpDirectCacheAccess	DirectCacheAccess
	Power Technology	biosVfCPUPowerManagement/ vpCPUPowerManagement	CPUPowerManagement
	Enhanced Intel Speedstep(R) Technology	biosVfEnhancedIntelSpeedStepTech/ vpEnhancedIntelSpeedStepTech	EnhancedIntelSpeedStep
	Intel(R) Turbo Boost Technology	biosVfIntelTurboBoostTech/ vpIntelTurboBoostTech	IntelTurboBoostTech
	Processor Power state C6	biosVfProcessorCState/ vpProcessorCState	ProcessorC6Report
	Processor Power state C1 Enhanced	biosVfProcessorC1E/ vpProcessorC1E	ProcessorC1E

BIOS Token Group	BIOS Token Name	XML Object	CLI and Web GUI Object
	Frequency Floor Override	biosVfCPUFrequencyFloor/ vpCPUFrequencyFloor	CpuFreqFloor
	P-STATE Coordination	biosVfPStateCoordType/ vpPStateCoordType	PsdCoordType
	Energy Performance	biosVfCPUEnergyPerformance/ vpCPUEnergyPerformance	CpuEngPerfBias
Memory Configuration	Select Memory RAS	biosVfSelectMemoryRASConfiguration/ vpSelectMemoryRASConfiguration	SelectMemoryRAS
	DRAM Clock Throttling	biosVfDRAMClockThrottling/ vpDRAMClockThrottling	DRAMClockThrottling
	NUMA	biosVfNUMAOptimized/ vpNUMAOptimized	NUMAOptimize
	Low Voltage DDR Mode	biosVfLvDIMMSupport/ vpNUMAOptimized	LvDDRMode
	DRAM Refresh rate	biosVfDramRefreshRate/ vpDramRefreshRate	DramRefreshRate
	Channel Interleaving	biosVfMemoryInterleave/ vpChannelInterLeave	ChannelInterLeave
	Rank Interleaving	biosVfMemoryInterleave/ vpRankInterLeave	RankInterLeave
	Patrol Scrub	biosVfPatrolScrub/ vpPatrolScrub	PatrolScrub
	Demand Scrub	biosVfDemandScrub/ vpDemandScrub	DemandScrub
	Altitude	biosVfAltitude/ vpAltitude	Altitude
QPI Configuration	QPI Link Frequency Select	biosVfQPIConfig/ vpQPILinkFrequency	QPILinkFrequency
	Cluster on Die	biosVfCODEnable/ vpCODEnable	CODEnable

BIOS Token Name Comparison for Multiple Interfaces

BIOS Token Group	BIOS Token Name	XML Object	CLI and Web GUI Object
	Snoop Mode	biosVfEarlySnoop/ vpEarlySnoop	EarlySnoop
SATA Configuration	SATA Mode	Not supported	SATAMode
Onboard Storage	Onboard SCU Storage Support	biosVfOnboardStorage/ vpOnboardSCUStorageSupport	DisableSCU
	Onboard SCU Storage SW Stack	biosVfOnboardStorageSWStack vpOnboardSCUStorageSWStack	PchScuOromSelect
USB Configuration	Legacy USB Support	biosVfLegacyUSBSupport/ vpLegacyUSBSupport	LegacyUSBSupport
	Port 60/64 Emulation	biosVfUSBEmulation/ vpUSBEmul6064	UsbEmul6064
	All USB Devices	biosVfUSBPortsConfig/ vpAllUsbDevices	AllUsbDevices
	USB Port:Rear	biosVfUSBPortsConfig/ vpUsbPortRear	UsbPortRear
	USB Port:Front	biosVfUSBPortsConfig/ vpUsbPortFront	UsbPortFront
	USB Port:Internal	biosVfUSBPortsConfig/ vpUsbPortInternal	UsbPortInt
	USB Port:KVM	biosVfUSBPortsConfig/ vpUsbPortKVM	UsbPortKVM
	USB Port:Vmedia	biosVfUSBPortsConfig/ vpUsbPortVMedia	UsbPortVMedia
	USB Port:SD Card	biosVfUSBPortsConfig/ vpUsbPortSDCard	UsbPortSdCard
	xHCI Mode	biosVfPchUsb30Mode/ vpPchUsb30Mode	PchUsb30Mode
PCI Configuration	PCI ROM CLP	Not Supported	PciRomClp

BIOS Token Group	BIOS Token Name	XML Object	CLI and Web GUI Object
	MMIO above 4GB	biosVfMemoryMappedIOAbove4GB/ vpMemoryMappedIOAbove4GB	MemoryMappedIOAbove4GB
	ASPM Support	biosVfASPMSupport/ vpASPMSupport	ASPMSupport
	VGA Priority	biosVfVgaPriority/ vpVgaPriority	VgaPriority
Serial Configuration	Console Redirection	biosVfConsoleRedirection/ vpConsoleRedirection	ConsoleRedir
	Terminal Type	biosVfConsoleRedirection/ vpTerminalType	TerminalType
	Bits per second	biosVfConsoleRedirection/ vpBaudRate	BaudRate
	Flow Control	biosVfConsoleRedirection/ vpFlowControl	FlowCtrl
	Putty KeyPad	biosVfConsoleRedirection/ vpPuttyKeyPad	PuttyFunctionKeyPad
	Redirection After BIOS POST	biosVfConsoleRedirection/ vpLegacyOSRedirection	RedirectionAfterPOST
LOM and PCIe Slots Configuration	PCH SATA Mode	biosVfSataModeSelect/ vpSataModeSelect	SataModeSelect
	All Onboard LOM Ports	biosVfSataModeSelect/ vpSataModeSelect	AllLomPortControl
	LOM Port 0 OptionROM	biosVfLOMPortOptionROM/ vpLOMPort0State	LomOpromControlPort0
	LOM Port 1 OptionROM	biosVfLOMPortOptionROM/ vpLOMPort1State	LomOpromControlPort1
	All PCIe Slots OptionROM	biosVfPCIOptionROMs/ vpPCIOptionROMs	PcieOptionROMs

BIOS Token Name Comparison for Multiple Interfaces

BIOS Token Group	BIOS Token Name	XML Object	CLI and Web GUI Object
	PCIe Slot:*n* OptionROM	biosVfPCISlotOptionROMEnable/ vpSlot*n*State	PcieSlot*n*OptionROM
	PCIe Mezzanine OptionROM	biosVfPCISlotOptionROMEnable/ vpSlotMezzState	PcieMezzOptionROM
	PCIe Slot:1 Link Speed or SIOC1 Link Speed	biosVfPCISlotOptionROMEnable/ vpSlot1LinkSpeed	PcieSlot1LinkSpeed
	PCIe Slot:2 Link Speed or SIOC2 Link Speed	biosVfPCISlotOptionROMEnable/ vpSlot2LinkSpeed	PcieSlot2LinkSpeed
	PCIe Slot:MLOM OptionROM	biosVfPCISlotOptionROMEnable/ vpSlotMLOMState	PcieSlotMLOMOptionROM
	PCIe Slot:HBA OptionROM	biosVfPCISlotOptionROMEnable/ vpSlotHBAState	PcieSlotHBAOptionROM
	PCIe Slot:N1 OptionROM	biosVfPCISlotOptionROMEnable/ vpSlotN1State	PcieSlotN1OptionROM
	PCIe Slot:N2 OptionROM	biosVfPCISlotOptionROMEnable/ vpSlotN2State	PcieSlotN2OptionROM
Server Management	FRB-2 Timer	biosVfFRB2Enable/ vpFRB2Enable	FRB-2
	OS Watchdog Timer	biosVfOSBootWatchdogTimer/ vpOSBootWatchdogTimer	OSBootWatchdogTimer
	OS Watchdog Timer Timeout	biosVfOSBootWatchdogTimerPolicy/ vpOSBootWatchdogTimerPolicy	OSBootWatchdogTimerTimeout
	OS Watchdog Timer Policy	biosVfOSBootWatchdogTimerTimeOut/ vpOSBootWatchdogTimerPolicy	OSBootWatchdogTimerPolicy

BIOS Token Group	BIOS Token Name	XML Object	CLI and Web GUI Object
	Boot Order Rules	biosVfUCSMBootOrderRuleControl/ vpUCSMBootOrderRule	UCSMBootOrderRule

BIOS Token Name Comparison for Multiple Interfaces