Cisco UCS C-Series Integrated Management Controller GUI Configuration Guide - Cisco UCS M7 and Later Rack Servers, Release 6.0

First Published: 2025-09-02

Last Modified: 2026-03-16

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

© 2025 –2026 Cisco Systems, Inc. All rights reserved.

CONTENTS

PREFACE

Preface xv

Audience xv

Conventions xv

Related Cisco UCS Documentation xvii

CHAPTER 1

Overview 1

Overview of the Cisco UCS C-Series Rack-Mount Servers 1

Overview of the Server Software 2

Server Ports 2

Cisco Integrated Management Controller 3

Overview of the Cisco IMC User Interface 5

Navigation and Apps 6

Menubar 8

Cisco Integrated Management Controller Online Help Overview 9

Logging into Cisco IMC 9

Logging out of Cisco IMC 10

CHAPTER 2

Installing the Server OS 11

CHAPTER 3

Managing Chassis 13

Intersight Infrastructure Service License 13

Viewing Chassis Summary 14

Chassis Inventory 18

Viewing Power Supply Properties 18

Viewing Cisco VIC Adapter Properties 19

Viewing Storage Properties 20

Viewing GPU Inventory 20

CHAPTER 4 **Managing the Server 23**

Server Boot Order 23

Configuring the Precision Boot Order 24

Managing a Boot Device 28

Overview to UEFI Secure Boot 36

Enabling UEFI Secure Boot 37

Disabling UEFI Secure Boot 38

Viewing the Actual Server Boot Order 38

Configuring a Server to Boot With a One-Time Boot Device 39

Creating a Server Asset Tag 39

BIOS Tokens 40

Cisco UCS C220 M8 and C240 M8 40

I/O Tab 40

Server Management Tab 47

Memory Tab 50

Power/Performance Tab 56

Processor Tab 60

Security Tab 69

Cisco UCS C225 M8 and C245 M8 73

I/O Tab 73

Server Management Tab 85

Memory Tab 88

Power/Performance Tab 93

Processor Tab 96

Security Tab 101

Cisco UCS C220 and C240 M7 103

I/O Tab 103

Server Management Tab 109

Memory Tab 112

Power/Performance Tab 118

Processor Tab 122

Security Tab 133

Configuring Power Policies 137
Power Capping 137
Setting Power Redundancy Policy 138
Enabling Power Characterization 139
Enabling Power Capping 140
Power Profiles 140
Configuring Standard Power Profiles Settings 140
Configuring Advanced Power Profile Settings 142
Resetting Power Profiles to Default 145
Power Monitoring 145
Viewing Power Monitoring Summary 146
Viewing the Power Statistics in a Chart 148
Configuring the Power Restore Policy 150
Configuring Fan Policies 151
Fan Control Policies 151
Configuring the Fan Policy 152
Configuring DIMM Blocklisting 155
DIMM Block Listing 155
Enabling DIMM block Listing 156
Configuring BIOS Settings 156
Configuring BIOS Settings 156
Entering BIOS Setup 157
Clearing the BIOS CMOS 157
Restoring BIOS Manufacturing Custom Settings 158
Restoring BIOS Defaults 158
BIOS Profiles 158
Uploading a BIOS Profile 159
Activating a BIOS Profile 161
Deleting a BIOS Profile 161
Backing up a BIOS Profile 161
Viewing BIOS Profile Details 162
Secure Boot Certificate Management 162
Viewing Secure Boot Certificate Details 162
Uploading Secure Boot Certificate 164

Deleting a Secure Boot Certificate 165
Setting Dynamic Front Panel Temperature Threshold 166
Persistent Memory Modules 166

CHAPTER 5 **Viewing Server Properties** 167
Viewing Server Utilization 167
Viewing Server Components - Thermal Performance 168
Viewing CPU Properties 170
Viewing Memory Properties 171
Viewing PCI Adapter Properties 174
Viewing Storage Properties 176
Viewing TPM Properties 177
Viewing PID Catalog 178

CHAPTER 6 **Vewing Sensors** 181
Viewing Temperature Sensors 181
Viewing LED Sensors 182
Viewing Storage Sensors 182
Viewing Power Supply Sensors 183
Viewing Fan Sensors 184

CHAPTER 7 **Managing Remote Presence** 185
Configuring Serial Over LAN 185
Configuring Virtual Media 186
Creating a Cisco IMC Mapped vMedia Volume 187
Viewing Cisco IMC-Mapped vMedia Volume Properties 192
Removing a Cisco IMC-Mapped vMedia Volume 193
Remapping an Existing Cisco IMC vMedia Image 193
Deleting a Cisco IMC vMedia Image 193
Virtual KVM Console 194
Launching KVM Console 194
Virtual KVM Console - Cisco UCS C-Series M6 and Later Servers 195
Configuring the Virtual KVM 207
Enabling the Virtual KVM 208

Disabling the Virtual KVM 209

CHAPTER 8 **Managing User Accounts** 211

Adding Local Users for Cisco UCS C-Series M7 and Later Servers 211

Modifying Local Users for Cisco UCS C-Series M7 and Later Servers 214

Managing SSH Keys in User Accounts 218

Configuring SSH Keys 218

Adding SSH Keys 219

Modifying SSH Keys 221

Deleting SSH Keys 223

Password Expiry 223

Enabling and Configuring Password Expiry Duration 224

Changing Password as a Non-Admin User 225

Configuring Account Lockout Details 226

Configuring User Authentication Precedence 227

Resetting User Credentials to Factory Default Values 227

LDAP Servers 228

Configuring the LDAP Server 229

Configuring the LDAP Server on Cisco IMC 230

Configuring LDAP Settings and Group Authorization 232

LDAP Certificates Overview 235

Viewing LDAP CA Certificate Status 235

Exporting an LDAP CA Certificate 236

Uploading an LDAP CA Certificate 236

Testing LDAP Binding 238

TACACS+ Authentication 239

TACACS+ Server Configuration 239

Enabling TACACS+ Authentication 239

Configuring TACACS+ Remote Server Settings 240

Viewing and Terminating User Sessions 241

CHAPTER 9 **Configuring Chassis-Related Settings** 243

Managing Server Power 243

Pinging a Hostname/IP Address from the Web UI 244

Toggling the Locator LEDs 244
Selecting a Time Zone 245

CHAPTER 10 **Configuring Network-Related Settings** 247
Configuring Network-Related Settings 247
Server NICs 247
Configuring Server NICs 250
Cisco VIC mLOM and OCP Card Replacement Considerations 254
Single IP Configuration 255
Configuring Single IP Properties 256
Common Properties Configuration 257
Overview to Common Properties Configuration 257
Configuring Common Properties 258
Configuring IPv4 259
Configuring IPv6 259
Connecting to a VLAN 261
Network Security Configuration 261
Network Security 261
Configuring Network Security 261
Network Time Protocol Settings 263
Network Time Protocol Service Setting 263
Configuring Network Time Protocol Settings 263

CHAPTER 11 **Managing Network Adapters** 265
Overview of the Cisco UCS C-Series Network Adapters 265
Viewing Cisco UCS Network Adapter Properties 268
Managing vHBAs 276
Guidelines for Managing vHBAs 276
Viewing and Modifying vHBA Properties 276
Creating a vHBA 282
Cloning a vHBA 287
Deleting a vHBA 288
vHBA Boot Table 289
Creating a Boot Table Entry 289

Deleting a Boot Table Entry 289
vHBA Persistent Binding 290
Viewing and Enabling Persistent Bindings 290
Rebuilding Persistent Bindings 291
Managing vNICs 291
Guidelines for Managing vNICs 291
Viewing and Modifying vNIC Properties 291
Creating a vNIC 307
Cloning a vNIC 319
Deleting a vNIC 320
Configuring iSCSI Boot Capability 320
Configuring iSCSI Boot Capability for vNICs 320
Configuring iSCSI Boot Capability on a vNIC 321
Removing iSCSI Boot Configuration from a vNIC 324
Managing Cisco usNIC 325
Viewing and Configuring Cisco usNIC on a vNIC 325
Backing Up and Restoring the Adapter Configuration 327
Exporting the Adapter Configuration 327
Importing the Adapter Configuration 328
Restoring Adapter Defaults 329
Resetting the Adapter 330

CHAPTER 12 **Managing Storage Adapters** 331
Self Encrypting Drives (Full Disk Encryption) 332
Enabling Controller Security 333
Modifying Controller Security 334
Disabling Controller Security 335
Switching Controller Security Between Local and Remote Key Management 335
Create Virtual Drive from Unused Physical Drives 335
Create Virtual Drive from an Existing Drive Group 338
Setting a Virtual Drive as Transport Ready 341
Importing Foreign Configuration 341
Clearing Foreign Configuration 342
Clearing a Boot Drive 343

Enabling a JBOD 344
Disabling a JBOD 344
Retrieving TTY Logs for a Controller 344
Clearing Controller Configuration 345
Restoring Storage Controller to Factory Defaults 345
Preparing a Drive for Removal 346
Making a Dedicated Hot Spare 347
Making a Global Hot Spare 348
Removing a Drive from Hot Spare Pools 348
Toggling Physical Drive Status 349
Setting a Physical Drive as a Controller Boot Drive 349
Initializing a Virtual Drive 350
Set as Boot Drive 351
Editing a Virtual Drive 352
Deleting a Virtual Drive 354
Hiding a Virtual Drive 355
Starting Learn Cycles for a Battery Backup Unit 355
Viewing Storage Controller Logs 356
Viewing SSD Smart Information for MegaRAID Controllers 357
Viewing NVMe Controller Details 358
Viewing NVMe Physical Drive Details 359
Viewing PCI Switch Details 361
Starting Copyback Operation 365
Managing the Flexible Flash Controller 366
Cisco Flexible Flash 366
Upgrading from Single Card to Dual Card Mirroring with FlexFlash 368
Configuring the Flexible Flash Controller Properties 368
Configuring the Flexible Flash Controller Firmware Mode 370
Configuring the Flexible Flash Controller Cards 370
Booting from the Flexible Flash Card 371
Resetting the Flexible Flash Controller 372
Editing a Virtual Drive 372
Erasing Virtual Drives 374
Syncing Virtual Drives 374

Adding an ISO Image Configuration 375
Updating an ISO Image 377
Unmapping an ISO Image 377
Resetting the Cisco Flexible Flash Card Configuration 378
Retaining Configuration of the Cisco Flexible Flash Cards 379
Viewing FlexFlash Log Details 380
Managing the FlexUtil Controller 382
Configuring FlexUtil Controller Properties 382
Resetting FlexUtil Card Configuration 383
Viewing Cisco FlexUtil Controller Properties 384
Viewing Physical Drive Properties 385
Viewing Virtual Drive Properties 390
Mapping an Image to a Virtual Drive 392
Updating an Image on the Virtual Drive 393
Unmapping an Image From a Virtual Drive 394
Erasing a Virtual Drive 394
Cisco Boot Optimized M.2 Raid Controller 395
Viewing Cisco Boot Optimized M.2 Raid Controller Details 395
Viewing Physical Drive Info for Cisco Boot Optimized M.2 Raid Controller 398
Viewing the Virtual Drive Info for Cisco Boot Optimized M.2 Raid Controller 403
Cisco FlexMMC 407
Viewing Cisco FlexMMC Details 407
Uploading New Image File 408
Deleting an Image File 413
Mapping or Un-mapping an Image 413
Resetting FlexMMC to Default Settings 414

CHAPTER 13 **Configuring Communication Services** 415
Enabling or Disabling TLS v1.2 415
Configuring HTTP 417
Configuring SSH 419
Configuring XML API 419
XML API for Cisco IMC 419
Enabling the XML API 420

Enabling Redfish 420
Configuring IPMI 421
IPMI Over LAN 421
Configuring IPMI over LAN 421
Configuring SNMP 422
SNMP 422
Configuring SNMP Properties 423
Configuring SNMP Trap Settings 425
Sending a Test SNMP Trap Message 426
Managing SNMP Users for Cisco UCS C-Series M7 and Later Servers 427
Configuring a Server to Send Email Alerts Using SMTP 427
Configuring SMTP Server For Receiving Email Alerts 427
Adding SMTP Email Recipients 428

CHAPTER 14 **Managing Certificates and Server Security** 431
Managing the mTLS Certificate 431
Uploading an mTLS Certificate 431
Viewing mTLS Certificate 432
Managing the Server Certificate 433
Managing the Server Certificate 433
Generating a Certificate Signing Request 434
Certificate a Self Signing Request 437
Creating a Self-Signed Certificate using Linux 441
Creating a Self-Signed Certificate Using Windows 443
Uploading a Server Certificate 443
Managing the External Certificate 444
Uploading an External Certificate 445
Uploading an External Private Key 447
Activating the External Certificate 448
SPDM Security - MCTP SPDM 449
SPDM Security 449
Configuring and Viewing the MCTP SPDM Fault Alert Settings 450
Viewing SPDM Authentication Status 451
Adding Authorities Certificate 452

Viewing the List of Certificates and Certificate Details 453
Deleting Certificates 456
Key Management Interoperability Protocol 456
Viewing Secure Key Management Settings 457
Creating a Client Private Key and Client Certificate for KMIP Configuration 458
Root CA Certificate 459
Downloading a Root CA Certificate 459
Exporting a Root CA Certificate 461
Deleting a Root CA Certificate 462
Downloading a Client Certificate 462
Client Certificate 464
Exporting a Client Certificate 464
Deleting a Client Certificate 465
Downloading a Client Private Key 465
Client Private Key 467
Downloading a Client Private Key 467
Deleting a Client Private Key 468
Testing the KMIP Server Connection 468
Restoring the KMIP Server to Default Settings 469
Deleting KMIP Login Details 469
FIPS 140-2 Compliance in Cisco IMC 469
Enabling Security Configuration 469
Enabling Security Configuration (FIPS) 470

CHAPTER 15 **Managing Firmware** 471
Firmware Management Overview 471
Viewing Firmware Components 471
Updating the Firmware 472
Activating the Firmware 474
Canceling Firmware Activation 475

CHAPTER 16 **Viewing Faults and Logs** 477
Viewing the Fault Summary 477
Viewing Faults History 478

Viewing System Event Logs 479
Viewing the Cisco IMC Log 480
Logging Controls 481
Viewing Logging Controls 481
Sending the Cisco IMC Log to a Remote Server 483
Configuring the Cisco IMC Log Threshold 485
Sending a Test Cisco IMC Log to a Remote Server 486
Managing the Remote Syslog Certificate 487
Uploading a Remote Syslog Certificate 487
Deleting a Remote Syslog Certificate 489

CHAPTER 17 Server Utilities 491
Exporting Technical Support Data 491
Downloading Technical Support Data to a Local File 494
Resetting to Factory Default 495
Exporting and Importing the Cisco IMC Configuration 499
Exporting the Cisco IMC Configuration 499
Importing the Cisco IMC Configuration 501
Generating Non Maskable Interrupts to the Host 503
Adding or Updating the Cisco IMC Banner 504
Viewing Cisco IMC Last Reset Reason 504
Downloading Hardware Inventory to a Local File 505
Exporting Hardware Inventory Data to a Remote Server 506
PID Catalog 507
Uploading a PID Catalog 507
Activating a PID Catalog 509
Deleting a PID Catalog 509
Enabling Smart Access USB 510
Device Connector Configuration 511
Enabling or Disabling Cisco Intersight Management 511
Viewing Intersight Device Connector Properties 511
Configuring HTTPS Proxy Settings for Device Connector 517

Preface

This preface includes the following sections:

- Audience, on page xv
- Conventions, on page xv
- Related Cisco UCS Documentation, on page xvii

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

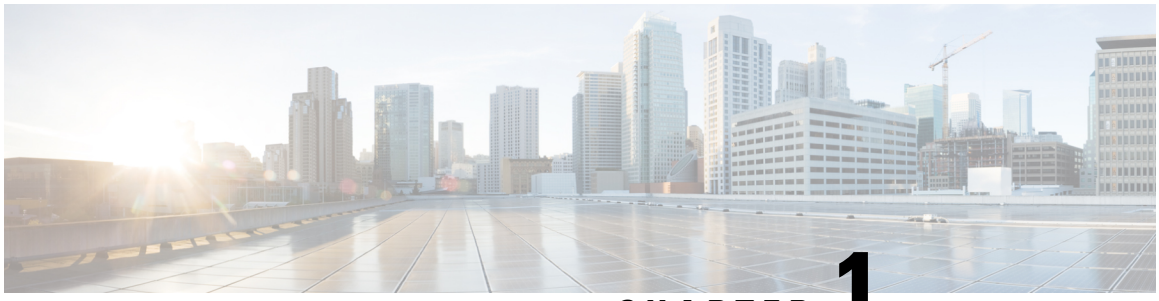
Related Cisco UCS Documentation

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 Roadmapdoc 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 C-Series Rack-Mount Servers, on page 1
- Overview of the Server Software, on page 2
- Server Ports, on page 2
- Cisco Integrated Management Controller, on page 3
- Overview of the Cisco IMC User Interface, on page 5

Overview of the Cisco UCS C-Series Rack-Mount Servers

The new web GUI of the Cisco Integrated Management Controller is compatible with these server models:

- Cisco UCS C220 M8 Rack-Mount Server
- Cisco UCS C240 M8 Rack-Mount Server
- Cisco UCS C225 M8 Rack-Mount Server
- Cisco UCS C245 M8 Rack-Mount Server
- Cisco UCS C220 M7 Rack-Mount Server
- Cisco UCS C240 M7 Rack-Mount Server

The Cisco UCS C-Series rack-mount servers include the following models:

- Cisco UCS C220 M8 Rack-Mount Server
- Cisco UCS C240 M8 Rack-Mount Server
- Cisco UCS C225 M8 Rack-Mount Server
- Cisco UCS C245 M8 Rack-Mount Server
- Cisco UCS C220 M7 Rack-Mount Server
- Cisco UCS C240 M7 Rack-Mount Server
- Cisco UCS C220 M6 Rack-Mount Server
- Cisco UCS C240 M6 Rack-Mount Server

- Cisco UCS C225 M6 Rack-Mount Server
- Cisco UCS C245 M6 Rack-Mount Server
- Cisco UCS C240 SD M5 Rack-Mount Server
- Cisco UCS C220 M5 Rack-Mount Server
- Cisco UCS C240 M5 Rack-Mount Server
- Cisco UCS C480 M5 Rack-Mount Server

Note To determine which Cisco UCS C-Series rack-mount servers are supported by this firmware release, see the associated *Release Notes*. The C-Series release notes are available at the following URL:

http://www.cisco.com/en/US/products/ps10739/prod_release_notes_list.html

Overview of the Server Software

The Cisco UCS C-Series Rack-Mount Server ships with the Cisco Integrated Management Controller (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 C-Series rack server supports operating systems such as Windows, Linux, Oracle and so on. For more information on supported operating systems, see the UCS Hardware and Software Compatibility. 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

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

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:

OS Version	Browser	Browser Version
MAC OS 14.2.1 (23C71)	Google Chrome	Version 122.0.6261.129 (Official Build) (x86_64)
MAC OS 14.2.1 (23C71)	Mozilla Firefox	123.0.1
MAC OS 14.2.1 (23C71)	Safari	Version 17.2.1 (19617.1.17.11.12)
Windows 11	Google Chrome	Version 122.0.6261.131 (Official Build) (64-bit)
Windows 11	Microsoft Edge	Version 122.0.2365.92 (Official build) (64-bit)
Windows 11	Google Chrome	Version 123.0.6312.59 (Official Build) (64-bit)
Windows 11	Firefox	124.0.1 (64-bit)
Windows 11	Firefox	24.0.1
Windows 11	Chrome	123.0.6312.58[(Official Build) (64-bit)]
Ubuntu 20.04.3 LTS	Mozilla Firefox	125.0.2(64-bit)

For the latest set of browser specifications, see Release Notes for Cisco UCS Rack Server Software.

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.

Navigation and Apps

The Cisco Integrated Management Controller GUI menu bar comprises of the following Apps drop-down list:

Dashboard App

The **Dashboard** App displays the following information:

- **Server Details**—Displays the server details like Product name, Serial Number, and so on. Also allows you to view BIOS summary, boot order, and actions.
- **CIMC Information**—Displays Cisco IMC information like IP address, MAC address, and so on. Also allows you to view and update time zone.
- **Chassis Status**—Displays the overall server component status. Also allows you to view the fault summary page.
- **Processor and Memory summary**—Displays the server CPUs and Memory summary and allows you to view the CPU and Memory details.
- **Storage summary**—Displays the controllers, physical drives, and virtual drives summary.
- **Networking summary**—Displays the adapters, host interfaces, external interfaces summary.
- **Interactive KVM Console**—Allows you to perform KVM server action.
- **Quick Actions**—Allows you to quickly access links to perform actions such as creating RAID volume, creating virtual NIC interface, creating new user, creating virtual HBA interface, Uploading firmware, Generating technical logs, Importing/Exporting Cisco IMC configuration, and Monitoring performance.
- **Server Actions**—Allows you to perform server power and system actions.

System App

The **System** App contains the following tabs:

- **General tab**—Server properties, Chassis status, Cisco Integrated Management Controller (Cisco IMC) information, and Server Utilization.
- **Inventory tab**—CPU, memory, PCI adapters, power supplies, cisco VIC adapters, network adapters, storage, SAS expander, and TPM.
- **Sensors tab**— Power Supply, Fan, Temperature, Voltage, Current, LEDs, and Storage
- **Backplane Management tab**—Involves monitoring and configuring the operational status and modes of various slots within a network device.

- **Power Management tab**—Power Cap Configuration and Power Monitoring.
- **Faults and Logs tab**—Fault summary, Fault history, System Event Log, Cisco IMC Log, and logging controls.

Compute App

The **Compute**App contains the following information about the server:

- **BIOS**—The installed BIOS firmware version and BIOS profile configuration, server boot order configuration, I/O, Server management, Security, Processor, Memory, Power or Performance.
  - Tokens
  - Boot Order
  - Profiles
  - Secure Boot Certificate Management
- **Remote Management**—Virtual KVM, Virtual Media, and Serial over LAN.

Networking App

The **Networking** App shows the following information under Cisco VIC Adapters:

- **General**—Adapter card properties, firmware, external ethernet interfaces, and actions to export or import configurations, and reset status.
- **DCE Interfaces**—External Ethernet interfaces information such as port, admin speed, MAC address, link state.
- **vNIC Interfaces**—Host Ethernet interfaces information such as name, CDN, MAC address, MTU and individual vNIC properties.
- **vHBA Interfaces**—Host fibre channel interfaces information such as name, WWPN, WWNN, boot, uplink, port profile, channel number, and individual vHBA properties.

Storage App

The **Storage** App contains the following menus:

- Controllers
  - **Controller Info**—General and settings information about the raid controller.
  - **Physical Drive Info**—General physical drive and corresponding RAID information.
  - **Virtual Drive Info**—General virtual drive and corresponding RAID information.
- Cisco FlexMMC—General information about storage for IMC images and user files. Allows you to upload files to IMC images partition and user files partition.

Administration App

The **Administration** App contains the following menus:

- **User Management**—Local User Management, LDAP, Session Management, and TACACS+.
- **Networking**—Network properties and network settings.
- **Communication Services**—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.
  - **Communication Services**—HTTP Properties, SSH Properties, XML API Properties, Redfish Properties, Serial over LAN, TLS Configuration, and IPMI over LAN Properties
  - **SNMP**—SNMP Properties, User Settings, and Trap Destinations
  - **Mail Alert**—SMTP Properties and SMTP Recipients
- **Security Management**—Certificate Management, Security Key Management, Security Configuration, and MCTP SPDM.
- **Event Management**—Enable/Disable Platform Event Filters and Reset Event Filters
- **Firmware Management**— Cisco IMC and BIOS firmware information and management.
- **Utilities**—Last Technical Support Data Export, Cisco IMC Last Reset, Cisco IMC Configuration Import/Export,Inventory Data, VIC Adapter Import/Export, Factory Default Status, Front Panel USB.
- **Device Connector**—Cisco Intersight management and network settings.

Menubar

Table 2: Toolbar

Name	Description
App drop-down list	Allows you to select the desired App from the list.
Information icon	Allows you to view Cisco IMC version information.
Help icon	Allows you to launch online help.
Secure Mode icon	Displays the security logs for various Cisco IMC features.
Alert icon	Displays details about various faults that happened over a period of time. For more information, see
Tasks Collection icon	Allows you to view the different task statuses.

Name	Description
Cisco IMC info	Shows the following information: • Login user role • Cisco IMC hostname • **Logout** button • **Dark/Light** theme toggle button—Allows you to change between light and dark theme for the UI.

Cisco Integrated Management Controller Online Help Overview

Beginning with the release 4.3(5), Cisco Integrated Management Controller (Cisco IMC) software GUI has the following Apps in the menu bar:

- Dashboard App
- System App
- Compute App
- Networking App
- Storage App
- Administration App

This help system describes the fields and dialog boxes on each Cisco IMC GUI page for each app.

To access the page help, click the **Help** icon in the menu bar.

Logging into Cisco IMC

Procedure

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**.

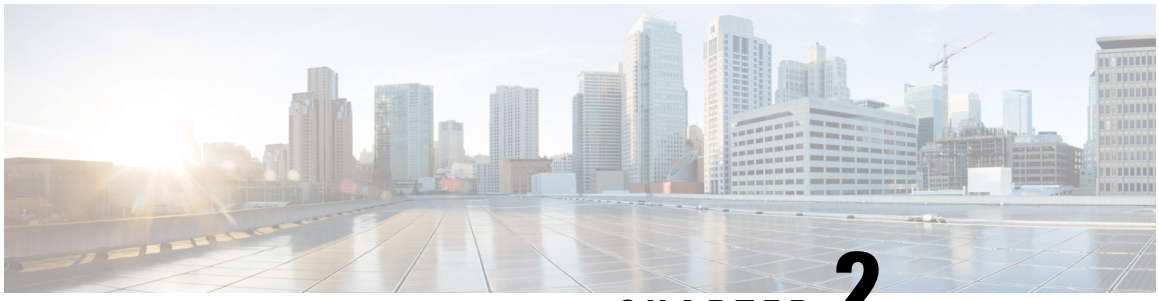
Logging out of Cisco IMC

Procedure

Step 1 In the upper right of Cisco IMC, click the server information area and click **Log Out** from the drop-down dialog box.

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

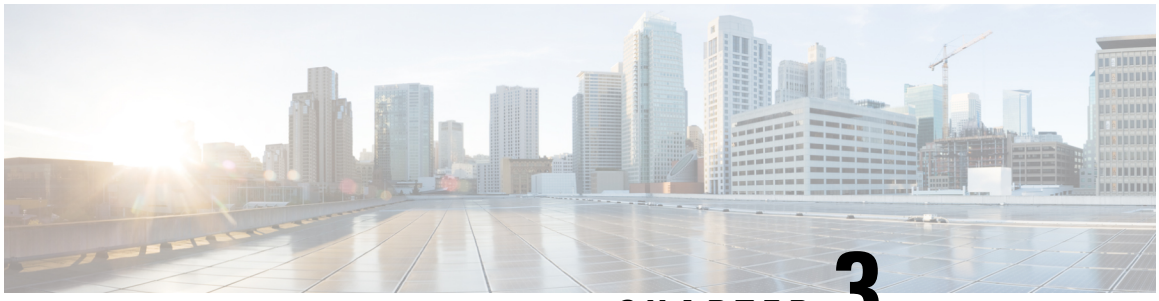
Step 2 (Optional) Log back in or close your web browser.



CHAPTER 2

Installing the Server OS

This chapter includes the following sections:



CHAPTER 3

Managing Chassis

- Intersight Infrastructure Service License, on page 13
- Viewing Chassis Summary, on page 14
- Chassis Inventory, on page 18

Intersight Infrastructure Service License

Intersight Infrastructure Service License

Beginning with release 4.3(2.230207), for Cisco UCS C-Series adservers, Cisco IMC displays the following warning if the Device Connector does not detect a connection to Cisco Intersight Services:

```
The Device Connector is unable to detect a connection to Cisco Intersight.
Please check your settings and ensure that the server is claimed in
Intersight with an Intersight Infrastructure Services license to be in
compliance.( 1/5 )
```

You may click **OK** to go to **Device Connector** and configure the settings or click **Cancel** to continue.

Note The warning counter (1/5) continues to increment till it reaches (5/5). The prompt stops after it reaches (5/5) or if the Device Connector is configured, whichever is first. If the Device Connector is configured once, and later disabled, the warning is displayed again and the counter continues from the last count. The counter is reset only in case restore factory default is performed.

Apart from the warning, Cisco IMC also shows the following static ribbon at the top of screen:

```
Please note: Intersight Infrastrucutre Services license is required with
this server. Learn More.
```

You may click **Learn More** to get more information from Intersight Help Center.

Note This message is not displayed if the Device Connector is configured. If the Device Connector is configured once, and later disabled, the message is displayed again.

Viewing Chassis Summary

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

Before you begin

You must log in as a user with admin privileges.

Procedure

Step 1 From the **Apps** drop-down list, select **Dashboard**.

Step 2 In the **Server Details** area of the **Dashboard** page, review the following information:

Table 3: Server Details Area

Name	Description
Product Name	The model name of the server.
UUID	The UUID assigned to the server.
PID	The product ID.
Serial Number	The serial number for the server.
BIOS Version	The version of the BIOS running on the server.

Step 3 In the **CIMC Information** area of the **Dashboard** page, review the following information:

Table 4: CIMC Information Area

Name	Description
IP Address	The IP address for the Cisco IMC. Click to see Management Network details.
MAC Address	The MAC address assigned to the active network interface to the Cisco IMC.
Firmware Version	The current Cisco IMC firmware version.
Host Name	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.
Current Time (UTC)	The local time of the region according to the chosen time zone.

Name	Description
Timezone	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.

Step 4 In the **Chassis Status** area of the **Dashboard** page, review the following information:

Table 5: Chassis Status Area

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

Name	Description
Temperature	The temperature status. This can be one of the following: • Good • Fault • Severe Fault
Fans	The overall status of the power supplies. This can be one of the following: • Good • Fault • Severe Fault
POST Completion Status	BIOS POST completion status.
Locator LED	Whether the locator LEDs are on or off.
Cooling	Displays the current cooling mode.

Step 5 In the **Processors & Memory** area of the **Dashboard** page, review the following information:

Table 6: Processors & Memory Area

Name	Description
CPUs	Number of CPUs in the server.
Cores	Number of cores in the CPU.
Threads	Maximum number of threads that the CPU can process concurrently.
Cores Enabled	Number of cores enabled out of the total cores.
CPUs Speed (Mhz)	The base operating frequency of the CPU, in megahertz.
Memory Capacity (MB)	The total amount of memory available on the server if all DIMMs are fully functional.
Clock Speed (Mhz)	The operating frequency of the memory (RAM), measured in megahertz (MHz), indicating how fast the memory can read from or write to its storage.

Name	Description
Effective Memory (MB)	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.
Memory Layout	Graphical representation of the memory DIMM locations. Click to view the graphical representation of DIMM location in the server.

Step 6 In the **Storage** area of the **Dashboard** page, review the following information:

Table 7: Storage Area

Name	Description
Controllers	Number of RAIDs available.
Capacity Available to OS	Storage space available to the installed OS in gigabytes.
Physical Drives	Total number of physical drives available in the server.
Virtual Drives	Total number of virtual drives available.

Step 7 In the **Networking** area of the **Dashboard** page, review the following information:

Table 8: Networking Area

Name	Description
Adapters	Number of Cisco UCS VIC adapters available.
DCE Interfaces	Number of DCE interfaces available.
vNIC Interfaces	Number of vNIC interfaces available.
vHBA Interfaces	Number of vHBA interfaces available.

Step 8 Using the **KVM Console** area of the **Dashboard** page, you can view the following information:

Table 9: KVM Console Area

Name	Description
Launch KVM icon	Opens a KVM session in a new tab or window depending on the browser settings.
Remote Management icon	Opens the Remote Management page.
KVM Console interactive window	You can use this interactive window to perform all the actions you can perform a new KVM session.

Step 9 In the **Quick Actions** area of the **Dashboard** page, you can perform the following actions:

Table 10: Quick Actions Area

Name	Description
Create a RAID Volume link	Opens **Create Virtual Drive** window.
Create a New User link	Opens **Local User Details** window.
Upload Firmware link	Allows you to upload BMC or BIOS firmware using remote or local.
Cisco IMC Configuration Import/Export link	Opens **Cisco IMC Configuration Import/Export** window.
Create a new Virtual NIC Interface link	Allows you to add vNIC.
Create a Virtual HBA Interface link	Allows you to add vHBA.
Generate Tech Support Logs link	Opens **Export Technical Support Data** window.
Performance Monitor link	Allows you to view the overall server and power utilization.

Chassis Inventory

Viewing Power Supply Properties

Procedure

Step 1 From the **Apps** drop-down list, select **System**.

Step 2

Step 3 Select the **Inventory** tab.

Step 4 In the **Inventory** work pane, click the **Power Supplies** tab and review the following information for each power supply:

Table 11: Power Supplies

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

Viewing Cisco VIC Adapter Properties

Procedure

Step 1 From the **Apps** drop-down list, select **Dashboard**.

Step 2 Under **Networking**, click **Adapters**.

Step 3 Review the following information under **Cisco VIC Adapters** window:

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.
Product Name column	The product name for the adapter.
Firmware Version column	Current firmware version of the adapter.

Step 4 You may click **Show More...** to view more information.

Viewing Storage Properties

Procedure

Step 1 From the **Apps** drop-down list, select **Dashboard**.

Step 2 Under **Storage**, click **Controllers**.

Step 3 Review the following information under **Storage Adapters** window:

Table 12: Storage Adapters

Name	Description
PCI Slot column	PCI slot in which the controller drive is located.
Name column	Name of the controller.
Firmware Version column	The active firmware package version number.
Serial Number column	The serial number of the storage controller.

Step 4 You may click **Show More...** to view more information.

Viewing GPU Inventory

The GPU Inventory option is available only on some C-Series servers.

Procedure

Step 1 From the **Apps** drop-down list, select **System**.

Step 2 Select the **Inventory** tab.

Step 3 From the navigation pane, select **PCIe Devices**.

Step 4 From the drop-down list, select **GPU**.

Step 5 You can view the following properties:

Name	Description
ID column	The PCIe Device ID.
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.
MAC Address	MAC Address of the Intel(R) Network Controller **Note** This field is displayed only for Intel(R) Network Controller.

Note
Cisco IMC displays the information for Third-Party adapters, depending on the adapter installed in your server.

You may not see all the fields listed below. For few adapters, Cisco IMC may not show the value of the displayed field.

Table 13: Third-Party Adapter Information

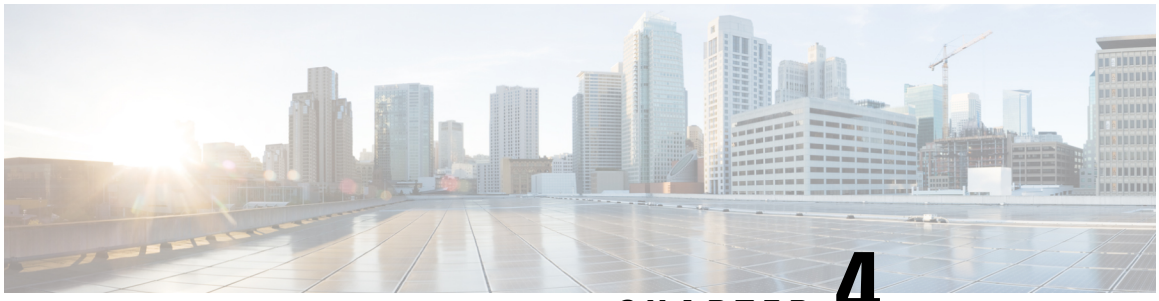
Name	Description
Name	Name of the PCIe adapter.
Vendor	The vendor for the PCIe adapter.
Serial Number	Serial number of the PCIe adapter.
Part Number	Part number of the PCIe adapter.
Manufacturer	PCIe adapter manufacturer.
Firmware Version	Current firmware version of the PCIe adapter.

Table 14: Port Details

Name	Description
Port column	Port used to make external connection to the adapter.
Status column	The status of the PCIe adapter. This can be up or down.
Link Speed column	Displays the speed of an adapter card installed in PCIs slot.
WWPN column	The World Wide Port Name for the adapter.
Factory WWPN column	Factory supplied World Wide Port Name for the adapter.
WWNN column	The World Wide Node Name for the adapter.
Factory WWNN column	The World Wide Node Name for the adapter from factory settings.

Table 15: Temperature Details

Name	Description
ID column	ID of the PCIe adapter.
Temperature (°C / °F)	The temperature of the PCIe adatper.



CHAPTER 4

Managing the Server

- Server Boot Order, on page 23
- BIOS Tokens, on page 40
- Configuring Power Policies, on page 137
- Configuring Fan Policies, on page 151
- Configuring DIMM Blocklisting, on page 155
- Configuring BIOS Settings, on page 156
- BIOS Profiles, on page 158
- Secure Boot Certificate Management, on page 162
- Setting Dynamic Front Panel Temperature Threshold, on page 166
- Persistent Memory Modules, on page 166

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.

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, click **Add Boot Device** > **Basic** optoin under **Boot Order Configuration** area. 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 Order** section displays the boot order actually used by BIOS when the server last booted. The actual boot order will differ from the configured boot order if either of the following conditions occur:

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

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

Configuring the Precision Boot Order

Before you begin

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

Procedure

Step 1 From the **Apps** drop-down list, select **Compute**.

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

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

Step 4 In the **Boot Order** area, review the following information.

Table 16: Properties Area

Name	Description
Running Version field	The version of BIOS running on the server.

Name	Description
UEFI Secure Boot toggle button	Allows you to enable or disable UEFI secure boot. **Note** If enabled, the configured boot is set to UEFI mode, by default and you cannot edit this option until UEFI secure boot is disabled. **Note** In case of RFD (Reset Factory Default), re-enable UEFI Secure Boot.
Actual Boot Mode	The boot mode that BIOS is booted to. This field is read-only parameters through BIOS and it gets updated only when the host is rebooted.
Configured Boot Mode	Sets the boot mode in which BIOS tries to boot the devices. This can be one of the following: • **Legacy** • **UEFI** **Note** If UEFI secure boot is enabled, the boot mode is set to UEFI by default. You cannot modify the configured boot mode until UEFI secure boot option is disabled.
Last Configured Boot Order Source	The last source used by the BIOS to configure the boot order. This can be one of the following: • **BIOS** • **CIMC** • **CIMCOneTimeBoot** • **Unknown**
Configured One time boot device drop-down list	Select a one time configured boot device from the drop-down list. You can configure a server to boot from an existing advanced device for just the next server boot. Once the server boots from this device, subsequently the server boots from the existing boot order which is already configured. **Note** The host boots to the one time boot device even when configured with a disabled advanced boot device.

Actual Boot Order Area

Table 17: Actual Boot Order Area

Name	Description
Name column	Name of the boot device.
Order column	Boot order of the device.
Type column	Type of the booting device.

Boot Order Configuration Area

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

Basic

- **Basic**

Advanced

- **Local HDD**
- **PXE Boot**
- **SAN Boot**
- **iSCSI Boot**
- **USB**
- **Virtual Media**
- **PCHStorage**
- **UEFISHELL**
- **NVME**
- **Local CDD**
- **HTTP Boot**

Table 18: Boot Order Configuration Area

Name	Description
Add Boot Device button	Following options are available: • Basic Boot Order Configuration • Add Local HDD Boot Device • Add PXE Boot Device • Add SAN Boot Device • Add iSCSI Boot Device • Add USB Boot Device • Add Virtual Media Boot Device • Add PCH Storage Boot Device • Add UEFI SHELL Boot Device • Add NVME Boot Device • Add Local CDD Boot Device • Add HTTP Boot Device • Add Embedded Storage Boot Device
Enable/Disable button	Allows you to enable or disable a boot device. Select the row with the boot device and then click **Enable/Disable**.
Delete button	Allows you to delete a boot device. Select the row with the boot device and then click **Delete**.
Name column	Name of the boot device.
Level column	This can be one of the following: • Basic • Advance
Type column	Type of the boot device.
Order column	Order of this book device.
State column	Displays whether the device is enabled or disabled.

Step 5 Click **Re-Apply**.

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.

Procedure

Step 1 From the **Apps** drop-down list, select **Compute**.

Step 2 In the left pane, click **BIOS** menu.

Step 3 In the **BIOS** menu, select **Boot Order**.

Step 4 In the **Boot Order** pane, click **Add Boot Device** from the **Boot Order Configuration** tab.

Step 5 From the **Add Boot Device** drop-down list, choose the device that you want add to the boot order.

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

Table 19: Add Local HDD Boot Device

Name	Description
Name field	The name of the device. **Note** Once created, you cannot rename the device.
Enabled toggle button	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.
UEFI Boot Loader Parameters (Optional)	
Bootloader Name field	The bootloader version associated with the boot-loader software of the component.

Name	Description
Bootloader Path field	Specifies the file path to the bootloader used for system startup.
Bootloader Description field	Brief description of the bootloader.

To add the PXE device, select **PXE Boot**, and update the following parameters:

Table 20: Add PXE Boot Device

Name	Description
Name field	The name of the device. This name cannot be changed after the device has been created.
Enabled toggle button	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.
MAC Address	MAC address of the network ethernet interface. **Note** This option is available only on some C-Series servers.
IP Type button	This can be one of the following: • None • IPv4 • IPv6
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.

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

Table 21: Add SAN Boot Device

Name	Description
Name field	The name of the device. This name cannot be changed after the device has been created.

Name	Description
Enabled toggle button	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.
UEFI Boot Loader Parameters (Optional)	
Bootloader Name field	The bootloader version associated with the boot-loader software of the component.
Bootloader Path field	Specifies the file path to the bootloader used for system startup.
Bootloader Description field	Brief description of the bootloader.

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

Table 22: Add iSCSI Boot Device

Name	Description
Name field	The name of the device. This name cannot be changed after the device has been created.
Enabled toggle button	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.

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

Table 23: Add USB Boot Device

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

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

Table 24: Add Virtual Media Boot Device

Name	Description
Name field	The name of the device. This name cannot be changed after the device has been created.
State toggle button	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.

Name	Description
Sub Type drop-down list	The subdevice type under a certain device type. This could be any one of the following: • **KVM Mapped DVD** • **KVM Mapped HDD** • **KVM Mapped FDD** • **CIMC Mapped DVD** • **CIMC Mapped HDD**

To add the PCH storage device, select **PCHStorage**, and update the following parameters:

Table 25: Add PCH Storage Boot Device

Name	Description
Name field	The name of the device. This name cannot be changed after the device has been created.
Enabled toggle button	The visibility of the device by BIOS. This can be one of the following: • **Enabled**—The device is visible to BIOS in a boot order configuration. • **Disabled**—The device is not visible to BIOS in a boot order configuration.
Order field	The order of the device in the available list of devices. Enter between 1 and n, where n is the number of devices.
LUN field	Logical unit in a slot where the device is present. • Enter a number between 0 and 255 • SATA in AHCI mode—Enter a value between 1 and 10 • SATA in SWRAID mode—Enter 0 for SATA , and enter 1 for SATA **Note** SATA mode is available only on some UCS C-Series servers.

To add the UEFI shell device, select **UEFIShell**, and update the following parameters:

Table 26: Add UEFI SHELL Boot Device

Name	Description
Name field	The name of the device. This name cannot be changed after the device has been created.

Name	Description
Enabled toggle button	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.

To add the NVME boot device, select **NVME**, and update the following parameters:

Table 27: Add NVME Boot Device

Name	Description
Name field	The name of the device. **Note** Once created, you cannot rename the device.
Enabled toggle button	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.

To add the Local CDD boot device, select **Local CDD**, and update the following parameters:

Table 28: Add Local CDD Boot Device

Name	Description
Name field	The name of the device. **Note** Once created, you cannot rename the device.
Enabled toggle button	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.

To add the HTTP boot device, select **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

Table 29: Add HTTP Boot Device

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.
Enabled toggle button	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.
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: • OCP • MLOM • L • 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 button	The type of IP configuration. The following options are displayed in the drop-down list: • **None** • **DHCP** • **Static**
URI field	The Uniform Resource Identifier HTTP server path location. You can enter between 1 and 255 characters.
IP Type button	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.

To add the Embedded Storage boot device, select **Embedded Storage**, and update the following parameters:

Table 30: Add Embedded Storage Boot Device

Name	Description
Name field	The name of the device. **Note** Once created, you cannot rename the device.
Enabled toggle button	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.

Name	Description
Sub Type drop-down list	The subdevice type under a certain device type. This could be any one of the following: • FlexMMC Mapped DVD • FlexMMC Mapped HDD

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 2025 • Windows Server 2022 • ESX 6.7 • ESX 6.5 • ESXi 7.0 • ESXi 8.0 • Linux 9.4 • Linux 9.5 • Ubuntu 24.04

Components	Types
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

Enabling UEFI Secure Boot

Procedure

Step 1 In the **Properties** area of the **Boot Order** tab, select the **UEFI Secure Boot** toggle button.

Note
If selected, the boot mode is set to UEFI secure boot. You cannot modify the **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 2 Click **Save**.

What to do next

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

Disabling UEFI Secure Boot

Procedure

Step 1 In the **Properties** area, deselect the **UEFI Secure Boot** toggle button.

Step 2 Click **Save**.

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.

Procedure

Step 1 From the **Apps** drop-down list, select **Compute**.

Step 2 In the left pane, click **BIOS** menu.

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

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

The **Boot Order Configuration** section displays the boot order (**Basic** or **Advanced**) configured through Cisco IMC. If this configuration changes, then 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 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 Order** 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.

Procedure

Step 1 From the **Apps** drop-down list, select **Compute**.

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

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

Step 4 In the **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.

Procedure

Step 1 From the **Apps** drop-down list, select **System**.

Step 2 In the **System** menu, click the **General** tab.

Step 3 In the **Server Details** area, update the **Asset Tag** field.

Step 4 Click **Save**.

BIOS Tokens

Cisco UCS C220 M8 and C240 M8

I/O Tab

Note BIOS parameters listed in this tab may vary depending on the configuration of the server.

Table 31: I/O

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. • **GEN4**—Link speed can reach up to fourth generation. • **GEN5**—Link speed can reach up to fifth generation.
MLOM OptionROM toggle button	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.

Name	Description
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. • **GEN4**—Link speed can reach up to fourth generation. • **GEN5**—Link speed can reach up to fifth generation.
PCIe Slot Option ROM	
PCIe Slot*n* OptionROM toggle button	Allows you to enable or disable the feature whether the server can use the 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.
PCIe Slot MSTOR RAID OptionROM toggle button	Allows you to enable or disable the feature 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.
MRAID Link Speed	

Name	Description
MRAID*n* Link Speed drop-down list	This option allows you to restrict the maximum speed of an MRAID adapter card installed. 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. • **GEN4**—16GT/s is the maximum speed allowed. • **GEN5**—Link speed can reach up to fifth generation.
MRAID OptionROM	
MRAID OptionROM toggle button	This options allows you to control the Option ROM execution of the MRAID PCIe adapter connected. This can be one of the following: • **Disabled**—Does not execute Option ROM of the MRAID PCIe adapter. • **Enabled**—Executes Option ROM of the MRAID PCIe adapter.
NVME Link Speed	

Name	Description
Front NVME-*n* Link Speed drop-down list	Link speed for NVMe front slot designated by slot *n*. 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. • **GEN4**—Link speed can reach up to fourth generation. • **GEN5**—Link speed can reach up to fifth generation.
Rear NVME-*n* Link Speed drop-down list	Link speed for NVMe rear slot designated by slot *n*. 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. • **GEN4**—Link speed can reach up to fourth generation. • **GEN5**—Link speed can reach up to fifth generation.
NVME OptionROM	

Name	Description
Front NVME-*n* OptionROM toggle button	This option allows you to control the Option ROM execution of the PCIe adapter connected to the SSD:NVMe slot *n*. 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
Rear NVME-*n* OptionROM toggle button	This option allows you to control the Option ROM execution of the PCIe adapter connected to the rear SSD:NVMe slot *n*. 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
VMD Enable toggle button	Intel Volume Management Device (VMD) is for PCIe NVMe SSDs that provides hardware logic to manage and aggregate NVMe SSDs. This can be one the following: • **Enabled**— Enables benefits like robust surprise hot-plug, status LED management. • **Disabled**— Disables the feature. Default value: **Disabled**. Refer Intel® Virtual RAID on CPU User Guide to configure VMD. **Note** VROC is not supported with Cisco UCS C-Series M7 servers.
PCIe RAS Support toggle button	Allows you to enable or disable the feature where PCIe RAS Support is available on the PCIe slot. This can be one of the following: • **Disabled**—PCIe RAS is not available on the slot. • **Enabled**—PCIe RAS is available on port.

Name	Description
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: • **On Board**—Priority is given to the onboard VGA device. BIOS post screen and OS boot are driven through the onboard VGA port. • **Off Board**—Priority is given to the PCIE Graphics adapter. BIOS post screen and OS boot are driven through the external graphics adapter port. • **On Board 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.
USB Port Rear toggle button	Allows you to enable or disable the rear panel USB devices. 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.
IPv6 PXE Support toggle button	Allows you to enable or disable 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.
Network Stack toggle button	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.

Name	Description
External SSC enable drop-down list	This option controls the use of an external Secure Socket Controller (SSC) for cryptographic operations, typically in relation to Trusted Platform Module (TPM) functionalities. This can be one of the following: • **Off** • **OP*n*_Percent** • **Hardware**
IPV4 PXE Support toggle button	Allows you to enable or disable 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.
IIO eDPC Support drop-down list	eDPC allows a downstream link to be disabled after an uncorrectable error, making recovery possible in a controlled and robust manner. This can be one of the following: • **Disabled**—eDPC support is disabled. • **On Fatal Error**—eDPC is enabled only for fatal errors. • **On Fatal and Non-Fatal Errors**—eDPC is enabled for both fatal and non-fatal errors.
IPv4 HTTP Support toggle button	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 toggle button	Enables or disables IPv6 support for HTTP. This can be one of the following: • **Disabled**—IPv6 HTTP support is not available. • **Enabled**—IPv6 HTTP support is always available.

Name	Description
Re-Size BAR Support toggle button	This feature allows the system to dynamically resize the BAR, providing more flexible and efficient use of memory resources. • **Disabled**—Re-Size BAR Support is disabled. • **Enabled**—Re-Size BAR Support is enabled.
PreBoot DMA Protection toggle button	Using this, the server can restrict or control DMA operations during the preboot phase, ensuring that only trusted devices can access system memory. • **Disabled**—Re-Size BAR Support is disabled. • **Enabled**—Re-Size BAR Support is enabled.

Server Management Tab

Note BIOS parameters listed in this tab may vary depending on the configuration of the server.

Table 32: BIOS Parameters in Server Management Tab

Name	Description
FRB 2 Timer toggle button	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 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.

Name	Description
OS Watchdog Timer toggle button	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 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.

Name	Description
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.
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: • **COM 0**—Enables console redirection on serial port A during POST. • **COM 1**—Enables console redirection on serial port B during POST. • **Disabled**—No console redirection occurs during POST.
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	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.

Name	Description
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.

Memory Tab

Note BIOS parameters listed in this tab may vary depending on the configuration of the server.

Table 33: BIOS Parameters in Memory Tab

Name	Description
NUMA toggle button	Whether the BIOS supports Non-Uniform Memory Access (NUMA). This can be one of the following: • **Disabled**—Support is disabled. • **Enabled**—Support is enabled.
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. • **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.

Name	Description
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.
BME DMA Mitigation toggle button	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.
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.
Partial Memory Mirror Mode toggle button	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. • **Disabled**—Partial memory mirror is disabled.
Partial Mirror percentage field	Percentage of memory to mirror above 4GB. Enter an integer between 0 and 50.

Name	Description
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.
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.
UMA drop-down list	Allows you to set UMA settings. This can be one of the following: • Disable(All2All) • Hemisphere(2-clusters)
Enhanced 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. • **Auto**—Automatically determines whether to perform the Enhanced Memory Test based on system conditions and requirements.

Name	Description
Adaptive Refresh Management Level drop-down list	Refresh management settings are read-only. Adaptive RFM allows the controller flexibility to choose additional RFM threshold settings called RFM levels. The RFM levels permit alignment of the controller-issued RFM commands with the in-DRAM management of these commands. This can be one of the following: • **Default** • **Level A** • **Level B** • **Level C**
Error Check Scrub drop-down list	You can enable memory check with or without result collection. This can be one of the following: • **Disabled** • **Enabled without Result Collection** • **Enabled with Result Collection**
Rank Margin Tool toggle button	Indicates whether the rank margin tool is used and whether a margin test (which tests the memory sequence and voltage signals) is performed. This can be one of the following: • **Disabled** • **Enabled**

Name	Description
MMIO High Base drop-down list	MMIO High Base configures the base address for the high memory-mapped I/O (MMIO) region, which is used to map device memory and I/O resources above the 4GB address space, optimizing system memory allocation and performance. This can be one of the following: • **512G**—Sets the MMIO High Base to 512 gigabytes. • **1T**—Sets the MMIO High Base to 1 terabyte. • **2T**—Sets the MMIO High Base to 2 terabytes. • **4T**—Sets the MMIO High Base to 4 terabytes. • **16T**—Sets the MMIO High Base to 16 terabytes. • **24T**—Sets the MMIO High Base to 24 terabytes. • **32T**—Sets the MMIO High Base to 32 terabytes. • **40T**—Sets the MMIO High Base to 40 terabytes. • **56T**—Sets the MMIO High Base to 56 terabytes. • **Auto**—The server dynamically sets the High Base value.

Name	Description
MMIO High Granularity Size drop-down list	MMIO High Granularity Size configures the granularity of the high memory-mapped I/O (MMIO) region, determining the size increments for allocating MMIO space above the 4GB address range, which helps optimize memory allocation and system performance. This can be one of the following: • **1G**—Sets the MMIO High Granularity Size to 1 gigabyte. • **4G**—Sets the MMIO High Granularity Size to 4 gigabytes. • **16G**—Sets the MMIO High Granularity Size to 16 gigabytes. • **32G**—Sets the MMIO High Granularity Size to 32 gigabytes. • **64G**—Sets the MMIO High Granularity Size to 64 gigabytes. • **256G**—Sets the MMIO High Granularity Size to 256 gigabytes. • **1024G**—Sets the MMIO High Granularity Size to 1024 gigabytes. • **Auto**—The server dynamically sets the High Granularity Size.
UEFI Memory Map Special Purpose Memory Flag	This setting determines the behavior of the UEFI memory map special knob, which impacts CXL cards under certain operating systems. This can be one of the following: • **Disabled** • **Enabled**
ACPI SRAT Special Purpose Memory Flag	This setting allows or disallows the ACPI SRAT special purpose memory flag to be set when the UEFI Memory Map special purpose flag is enabled. This can be one of the following: • **Disabled** • **Enabled**

Name	Description
Runtime Post Package Repair	Enables the soft post-package repairs of the corrected memory errors during OS runtime. This can be one of the following: • **Disabled** • **Enabled**

Power/Performance Tab

Note BIOS parameters listed in this tab may vary depending on the configuration of the server.

Table 34: BIOS Parameters in Power/Performance Tab

Name	Description
Adjacent Cache Line Prefetcher toggle button	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.
Hardware Prefetcher toggle button	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.
DCU IP Prefetcher toggle button	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
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.
Virtual Numa toggle button	Virtual NUMA (virtual non-uniform memory access) is a memory-access optimization method for VMware virtual machines (VMs), which helps prevent memory-bandwidth bottlenecks. This can be one of the following: • **Disabled**—Functionality is disabled. • **Enabled**—Functionality is enabled.
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.

Name	Description
LLC Dead Line drop-down list	In CPU non-inclusive cache scheme, MLC evictions are filled into the LLC. When lines are evicted from the MLC, the core can flag them as **dead** (not likely to be read again). The LLC has the option to drop dead lines and not fill them in the LLC. If this feature is disabled, dead lines are always dropped and are never filled into the LLC. If this feature is enabled, the LLC can fill dead lines into the LLC if there is free space available. This can be one of the following: • **Disabled**—Feature is disabled. • **Enabled**—Feature is enabled. • **Auto**—CPU determines the LLC dead line allocation.
XPT Remote Prefetch drop-down list	This feature allows an LLC request to be duplicated and sent to an appropriate memory controller in a remote machine based on the recent LLC history to reduce latency. This can be one of the following: • **Disabled**—Feature is disabled. • **Enabled**—Feature is enabled. • **Auto**—CPU determines the functionality.
UPI Link Enablement drop-down list	Enables the minimum number of UPI links required by the processor. This can be one of the following: • **1** • **2** • **4** • **Auto**

Name	Description
Enhanced CPU Performance drop-down list	**Note** Once you enable this functionality, you cannot enable **Enable Power Characterization** and **Power Capping**. **Note** This option is not availabe on Cisco UCS C220 M8 servers. Enhances CPU performance by adjusting server settings automatically. **Note** Enabling this functionality may increase power consumption. The server should meet the following requirements in order to use this functionality: • Server should not contain Barlow Pass DIMMs • DIMM module size present in the Cisco UCS C220 M6 server should be less than 64GB and in Cisco UCS C240 M6 server should be less than 256GB • No GPU cards are present in the server. This can be one of the following: • **Disabled**—The processor does not run with this functionality. • **Auto**—Allows Cisco IMC to adjust server settings to increase performance.
UPI Power Management toggle button	UPI power management is used to conserve power on the server. This can be one of the following: • **Disabled**—The processor does not run with this functionality. • **Auto**—Functionality is enabled.
LatencyOptimizedMode_M5 toggle button	This option indicates a mode within the server's BIOS settings that prioritizes reducing latency. • **Disabled**—The processor does not run with this functionality. • **Enabled**—Functionality is enabled.

Processor Tab

Note BIOS parameters listed in this tab may vary depending on the configuration of the server.

Table 35: BIOS Parameters in Processor Tab

Name	Description
Intel Virtualization Technology toggle button	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.
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: • **Auto** • **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.

Name	Description
Processor C1E toggle button	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.
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.
Turbo Mode toggle button	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.

Name	Description
Boot Performance Mode drop-down list	Allows you 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
SpeedStep (Pstates) toggle button	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.
Processor CMCI toggle button	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.

Name	Description
HyperThreading [ALL] toggle button	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.
Workload Configuration drop-down list	This feature allows for workload optimization. The options are Balanced and I/O Sensitive: • **Balanced** • **IO Sensitive**
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 48**—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.
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. • **Auto** —CPU determines the UPI Prefetch mode.

Name	Description
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: • **Auto** — The BIOS determines what Sub NUMA clustering is done. • **Disabled**— Sub NUMA clustering does not occur. • **Enabled**— Sub NUMA clustering is enabled.
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. • **PECI**—Chooses Platform Environmental Control Interface for energy performance tuning.
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.

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 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.
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.

Name	Description
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)
LLC Prefetch toggle button	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.
Energy Efficient Turbo toggle button	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.
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. • **Enable at End of POST**—The system checks for memory ECC errors after BIOS POST.

Name	Description
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
Intel Dynamic Speed Select toggle button	**Intel Dynamic Speed Select** modes allow you to run the CPU with different speed and cores in auto mode. This can be one of the following: • **Disabled**—**Intel Dynamic Speed Select** is disabled. • **Enabled**—**Intel Dynamic Speed Select** is enabled.
IOAT Configuration toggle button	IOAT Configuration enables or disables Intel I/O Acceleration Technology (IOAT), which improves data transfer efficiency and reduces CPU overhead by offloading memory copy operations. This can be one of the following: • **Disabled**—Disables the feature. • **Enabled**—Enables the feature.

Name	Description
PRMRR Size drop-down list	PRMRR Size configures the size of the Protected Range Memory Region Register (PRMRR), which is used to define protected memory regions for enhanced security and isolation in the system. This can be one of the following: • **128MB**—Defines a 128 megabyte protected memory region. • **256MB**—Defines a 256 megabyte protected memory region. • **512MB**—Defines a 512 megabyte protected memory region. • **1GB**—Defines a 1 gigabyte protected memory region. • **2GB**—Defines a 2 gigabyte protected memory region. • **4GB**—Defines a 4 gigabyte protected memory region. • **8GB**—Defines an 8 gigabyte protected memory region. • **16GB**—Defines a 16 gigabyte protected memory region. • **32GB**—Defines a 32 gigabyte protected memory region. • **64GB**—Defines a 64 gigabyte protected memory region. • **128GB**—Defines a 128 gigabyte protected memory region. • **256GB**—Defines a 256 gigabyte protected memory region. • **512GB**—Defines a 512 gigabyte protected memory region. • **Invalid Config.**—Indicates an invalid configuration for the protected memory region. • **Auto**—Automatically configures the protected memory region size based on system requirements.

Security Tab

Note BIOS parameters listed in this tab may vary depending on the configuration of the server.

Table 36: BIOS Parameters in Security Management Tab

Name	Description
Trusted Platform Module State toggle button	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. This 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.
Security Device Support toggle button	You should enable TPM support to enable security device support. This can be one of the following: • **Disabled**—Feature is disabled. • **Enabled**—Feature is enabled if TPM is enabled.
SHA256 PCR Bank drop-down list	PCR bank available for OS when BIOS is performing measurements. • **Disabled**—SHA256 PCR Bank is not available for BIOS. • **Enabled**—SHA256 PCR Bank is available for BIOS.
SHA-1 PCR Bank drop-down list	PCR bank available for OS when BIOS is performing measurements. • **Disabled**—SHA-1 PCR Bank is not available for BIOS. • **Enabled**—SHA-1 PCR Bank is available for BIOS.

Name	Description
TPM Pending Operation drop-down list	Trusted Platform Module (TPM) Pending Operation option allows you to control the status of the pending operation. This can be one of the following: • None—No action. • TpmClear—Clears the pending operations.
SHA384 PCR Bank drop-down list	The Platform Configuration Register (PCR) is a memory location in the TPM. Multiple PCRs are collectively referred to as a PCR bank. A Secure Hash Algorithm 384-bit or SHA-384PCR Bank allows to enable or disable TPM security. This can be one of the following: • **Disabled**—The server does not use this feature. • **Enabled**—The server uses this feature.
Intel Trusted Execution Technology Support toggle button	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.
TPM Minimal Physical Presence toggle button	This token allows you to apply recommended Microsoft default settings for TPM. • **Disabled**—Support is disabled. • **Enabled**—Support is enabled.
Total Memory Encryption (TME) toggle button	Allows you to provide the capability to encrypt the entirety of the physical memory of a system. This can be one of the following: • **Disabled**—Support is disabled. • **Enabled**—Support is enabled.
Power on Password toggle button	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. This can be one of the following: • **Disabled**—Support is disabled. • **Enabled**—Support is enabled.

Name	Description
SW Guard Extensions (SGX) toggle button	Allows you to enable Software Guard Extensions (SGX) feature. This can be one of the following: • **Disabled**—Support is disabled. • **Enabled**—Support is enabled.
Multikey Total Memory Encryption (MK-TME) toggle button	MK-TME allows you to have multiple encryption domains with one with own key. Different memory pages can be encrypted with different keys. This can be one of the following: • **Disabled**—Support is disabled. • **Enabled**—Support is enabled.
SGX Pkg info In-Band Access toggle button	Allows you to enable SGX Package Info In-Band Access. This can be one of the following: • **Disabled**—Support is disabled. • **Enabled**—Support is enabled.
SGX Factory Reset toggle button	Allows the system to perform SGX factory reset on subsequent boot. This deletes all registration data. This can be one of the following: • **Disabled**—Support is disabled. • **Enabled**—Support is enabled.
Select Owner EPOCH input type drop-down list	Allows you to change the seed for the security key used for the locked memory region that is created. This can be one of the following: • **SGX Owner EPOCH activated**—Does not change the current input type. • **SGX Owner EPOCH deactivated**—Changes the current input type. • **Change to New Random Owner EPOCHs**—Changes EPOCH to a system generated random number. • **Manual User Defined Owner EPOCHs**—Changes the EPOCH seed to a hexadecimal value that you enter.

Name	Description
SGX QoS toggle button	Allows you to enable SGX QoS. This can be one of the following: • **Disabled**—Support is disabled. • **Enabled**—Support is enabled.
SGX Auto MP Registration Agent toggle button	Allows you to enable the registration authority service to store the platform keys. This can be one of the following: • **Disabled**—Support is disabled. • **Enabled**—Support is enabled.
SGX Write Enable toggle button	Allows you to enable SGX Write feature. This can be one of the following: • **Disabled**—Support is disabled. • **Enabled**—Support is enabled.
SProcessor Epoch *n* field	Allows you to define the SGX EPOCH owner value for the EPOCH number designated by *n*.
SGX PUBKEY HASH*n* field	Allows you to set the Software Guard Extensions (SGX) value. This value can be set between: • SGX PUBKEY HASH0—Between 7-0 • SGX PUBKEY HASH1—Between 15-8 • SGX PUBKEY HASH2—Between 23-16 • SGX PUBKEY HASH3—Between 31-24
DMA Control Opt-In Flag toggle button	DMA Control Opt-In Flag - Enabling this token allows the operating system to enable Input Output Memory Management Unit (IOMMU) to prevent the DMA attacks from possible malicious devices. • **Disabled**—Support is disabled. • **Enabled**—Support is enabled.
LIMIT CPU PA to 46 Bits toggle button	Enable this option for Intel® VT-d enabling boot to boot with 2019 OS. This can be one of the following: • **Disabled**—Support is disabled. • **Enabled**—Support is enabled.

Name	Description
TDX Secure Arbitration Mode (SEAM) Loader: toggle button	Enable this for a security feature that enables the initialization and management of Intel® Trusted Domain Extensions (TDX) for secure virtualized environments. This can be one of the following: • **Disabled**—Support is disabled. • **Enabled**—Support is enabled.
Trust Domain Extension (TDX) toggle button	Allows you to enhance the security of virtualized environments by creating isolated execution environments, known as Trust Domains, that protect sensitive data and code from other software, including the hypervisor. This can be one of the following: • **Disabled**—Support is disabled. • **Enabled**—Support is enabled.

Cisco UCS C225 M8 and C245 M8

I/O Tab

Note BIOS parameters listed in this tab may vary depending on the configuration of the server.

Table 37: BIOS Parameters in I/O Tab

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. • **GEN3**—16GT/s is the maximum speed allowed. • **GEN4**—Link speed can reach up to fourth generation. • **GEN5**—Link speed can reach up to fifth generation.
MLOM OptionROM 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.

Name	Description
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. • **GEN4**—Link speed can reach up to fourth generation. • **GEN5**—Link speed can reach up to fifth generation.
PCIe Slot MSTOR Link Speed drop-down list	Link speed for PCIe front slot designated by slot *n*. 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. • **GEN4**—Link speed can reach up to fourth generation. • **GEN5**—Link speed can reach up to fifth generation.

Name	Description
PCI Slot*n* OptionROM drop-down list	Whether the server can use the 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.
MRAID Link Speed drop-down list	RAID 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. • **GEN4**—Link speed can reach up to fourth generation. • **GEN5**—Link speed can reach up to fifth generation.
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
Front NVME-*n* Link Speed drop-down list	Link speed for NVMe front slot designated by slot *n*. 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. • **GEN4**—Link speed can reach up to fourth generation. • **GEN5**—Link speed can reach up to fifth generation.
Front NVME-*n* OptionROM drop-down list	This options allows you to control the Option ROM execution of the PCIe adapter connected to the SSD:NVMe slot *n*. 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
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.

Name	Description
IPv4 PXE Support toggle button	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.
IPv6 PXE Support toggle button	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.
SR-IOV Support toggle button	SR-IOV feature allows a PCIe device to appear to be multiple separate physical PCIe devices. This can be one of the following: • **Disabled**—SR-IOV feature is disabled. • **Enabled**—SR-IOV feature is enabled.
PCIe ARI Support drop-down list	Whether PCI Alternative Routing ID Interpretation (ARI) support in Windows is enabled. This can be one of the following: • **Auto**—ARI support is set to auto controlled by the system. • **Disabled**—ARI support is not available. • **Enabled**—ARI support is always available.
Re-Size BAR Support toggle button	This feature allows the system to dynamically resize the BAR, providing more flexible and efficient use of memory resources. • **Disabled**—Re-Size BAR Support is disabled. • **Enabled**—Re-Size BAR Support is enabled.
IPv4 HTTP Support toggle button	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.

Name	Description
IPv6 HTTP Support toggle button	Enables or disables IPv6 support for HTTP. This can be one of the following: • **Disabled**—IPv6 HTTP support is not available. • **Enabled**—IPv6 HTTP support is always available.
IIO eDPC Support drop-down list	eDPC allows a downstream link to be disabled after an uncorrectable error, making recovery possible in a controlled and robust manner. This can be one of the following: • Disabled—eDPC support is disabled. • On Fatal and Non-Fatal Errors—eDPC is enabled for both fatal and non-fatal errors.
PCIe Ten Bit Tag Support field	Enables PCIe ten bit tags for supported devices. This can be one of the following: • **Disabled**—PCIe ten bit tags support is disabled in the BIOS. • **Enabled**—PCIe ten bit tags support is enabled in the BIOS.
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.

Table 38: BIOS Parameters in I/O Tab

Name	Description
Reboot Host Immediately check 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.

Name	Description
MLOM OptionROM 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.
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. • **GEN3**—16GT/s is the maximum speed allowed.
PCIe Slot*n* OptionROM drop-down list	Whether the server can use the 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
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. • **GEN4**—Link speed can reach up to fourth generation.
MRAID1 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.
MRAID1 Link Speed drop-down list	RAID 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. • **GEN4**—Link speed can reach up to fourth generation.

Name	Description
MRAID2 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.
MRAID2 Link Speed drop-down list	RAID 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. • **GEN4**—Link speed can reach up to fourth generation.
Front NVME-*n* OptionROM drop-down list	This options allows you to control the Option ROM execution of the PCIe adapter connected to the SSD:NVMe slot *n*. 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

Name	Description
Front NVME-*n* Link Speed drop-down list	Link speed for NVMe front slot designated by slot *n*. 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. • **GEN4**—Link speed can reach up to fourth generation.
PCIe Slot MSTOR Link Speed drop-down list	Link speed for PCIe front slot designated by slot *n*. 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. • **GEN4**—Link speed can reach up to fourth generation.
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 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.

Name	Description
PCIe ARI Support drop-down list	Whether PCI Alternative Routing ID Interpretation (ARI) support in Windows is enabled. This can be one of the following: • **Auto**—ARI support is set to auto controlled by the system. • **Disabled**—ARI support is not available. • **Enabled**—ARI support is always available.
SR-IOV Support drop-down list	SR-IOV feature allows a PCIe device to appear to be multiple separate physical PCIe devices. This can be one of the following: • **Disabled**—SR-IOV feature is disabled. • **Enabled**—SR-IOV feature is enabled.
IPv6 HTTP Support drop-down list	Enables or disables IPv6 support for HTTP. This can be one of the following: • **Disabled**—IPv6 HTTP support is not available. • **Enabled**—IPv6 HTTP support is always available.
IPv4 HTTP Support drop-down list	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.
IIO eDPC Support drop-down list	eDPC allows a downstream link to be disabled after an uncorrectable error, making recovery possible in a controlled and robust manner. This can be one of the following: • Disabled—eDPC support is disabled. • On Fatal and Non-Fatal Errors—eDPC is enabled for both fatal and non-fatal errors.
PCIe Ten Bit Tag Support field	Enables PCIe ten bit tags for supported devices. This can be one of the following: • **Disabled**—PCIe ten bit tags support is disabled in the BIOS. • **Enabled**—PCIe ten bit tags support is enabled in the BIOS.

Name	Description
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.

Server Management Tab

Note BIOS parameters listed in this tab may vary depending on the configuration of the server.

Table 39: BIOS Parameters in Server Management

Name	Description
Reboot Host Immediately check 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.
FRB 2 Timer toggle button	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 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.

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.
OS Watchdog Timer toggle button	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.
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
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.
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.
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: • **COM 0**—Enables console redirection on COM 1 during POST. • **COM 1**—Enables console redirection on COM 1 during POST. • **Disabled**—No console redirection occurs during POST.
CDN Control toggle button	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.

Name	Description
PCIe Slots CDN Control toggle button	**Note** This option is available on Cisco UCS C225 and C245 M8 servers. This option is available on Cisco UCS C245 M6 servers equipped with Mellanox 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.
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.

Memory Tab

Note BIOS parameters listed in this tab may vary depending on the configuration of the server.

Table 40: BIOS Parameters in Memory Tab

Name	Description
Reboot Host Immediately check 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.
Above 4G Decoding toggle button	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.
NUMA Nodes per Socket drop-down list	Allows you to configure the memory NUMA domains per socket. This can be one of the following: • **Auto**—Number of channels is set to auto. • **NPS0**—One NUMA node per system. • **NPS1**—One NUMA node per socket. • **NPS2**—Two NUMA nodes per socket, one per Left/Right Half of the SoC. • **NPS4**—Four NUMA nodes per socket, one per Quadrant.
Chipselect Interleaving drop-down list	Whether memory blocks across the DRAM chip selects for node 0 are interleaved. This can be one of the following: • **Disabled**—Chip selects are not interleaved within the memory controller. • **Auto**—The CPU automatically determines how to interleave chip selects.

Name	Description
Bank Group Swap	Determines how physical addresses are assigned to applications. This can be one of the following: • **Auto**—The CPU automatically determines how to assign physical addresses to applications. • **Disabled**—Bank group swap is not used. • **Enabled**—Bank group swap is used to improve the performance of applications.
IOMMU drop-down list	Input Output Memory Management Unit (IOMMU) allows AMD processors to map virtual addresses to physical addresses. This can be one of the following: • **Auto**—The CPU determines how map these addresses. • **Disabled**—IOMMU is not used. • **Enabled**—Address mapping takes place through the IOMMU.
SMEE drop-down list	Whether the processor uses the Secure Memory Encryption Enable (SMEE) function, which provides memory encryption support. This can be one of the following: • **Auto**—The CPU determines how map these addresses. • **Disabled**—The processor does not use the SMEE function. • **Enabled**—The processor uses the SMEE function.
TSME drop-down list	Allows you to enable Transparent Secure Memory Encryption (TSME). This can be one of the following: • **Auto**—Feature usage is set to auto. • **Disabled**—The processor does not use the TSME function. • **Enabled**—The processor uses the TSME function.

Name	Description
SEV-SNP Support drop-down list	Allows you to enable Secure Nested Paging feature. This can be one of the following: • **Disabled**—The processor does not use the SEV-SNP function. • **Enabled**—The processor uses the SEV-SNP function.
SNP Memory Coverage drop-down list	Allows you to configure SNP memory coverage. This can be one of the following: • **Auto**—System decides the memory coverage. • **Disabled**—The processor does not use this function. • **Enabled**—This feature is enabled. • **Custom**—Custom size can be defined in **SNP Memory Size to Cover**.
SNP Memory Size to Cover in MB (0 - 1048576 MB) field	Allows you to configure SNP memory size. Enter the value in the range (0 - 1048576 MB).
BME DMA Mitigation toggle button	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.
Post Package Repair field	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. • **Disabled**—Support is disabled.
Runtime Post Package Repairtoggle button	This is a specific configuration setting related to the system's ability to perform repairs on the processor's package during runtime. • **Disabled**—The processor does not use the function. • **Enabled**—The processor uses the function.

Name	Description
Burst and Postponed Refresh toggle button	This option relates to memory refresh operations and affect the way the system handles memory refresh cycles, which are necessary to maintain data integrity in DRAM (Dynamic Random Access Memory). • **Disabled**—The processor does not use the function. • **Enabled**—The processor uses the function.
DRAM Scrub Time field	Select a value to indicate the number of hours to scrub the entire memory. This can be one of the following: • **Auto** — Feature is set to auto mode. • **Disabled** — Support is disabled. • **1 hour** • **4 hours** • **8 hours** • **16 hours** • **24 hours** • **48 hours**
SEV-ES ASID Space Limit	The SEV-ES ASID Space Limit BIOS setting determines the number of ASIDs for AMD® SEV-ES, affecting VM memory encryption and isolation. Adjusting it balances security needs with system resources. Enter an integer between 1 and 1007.
Memory Interleaving field	Allows for disabling memory interleaving. Note that NUMA nodes per socket will be honored regardless of this setting. This can be one of the following: • **Auto**—Feature is set to auto mode. • **Disabled**—Support is disabled.
Memory Refresh Rate field	Controls the refresh rate of the memory controller and might affect the memory performance and power depending on memory configuration and workload. This can be one of the following: • **1x Refresh** • **2x Refresh**

Name	Description
Enhanced Memory Test drop-down list	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: • **Auto**—Feature is set to auto mode. • **Disabled**—Support is disabled. • **Enabled**—Support is disabled.

Power/Performance Tab

Note BIOS parameters listed in this tab may vary depending on the configuration of the server.

Table 41: BIOS Parameters in Power/Performance Tab

Name	Description
Reboot Host Immediately check 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.
Core Performance Boost drop-down list	Whether the AMD processor increases its frequency on some cores when it is idle or not being used much. This can be one of the following: • **Auto**—The CPU automatically determines how to boost performance. • **Disabled**—Core performance boost is disabled.
Global C-state Control drop-down list	Whether the AMD processors control IO-based C-state generation and DF C-states This can be one of the following: • **Auto**—The CPU automatically determines how to control IO-based C-state generation. • **Disabled**—Global C-state control is disabled. • **Enabled**—Global C-state control is enabled.

Name	Description
L1 Stream HW Prefetcher drop-down list	Whether the processor allows the AMD hardware prefetcher to speculatively fetch streams of data and instruction from memory into the L1 cache when necessary. This can be one of the following: • **Auto**—The CPU determines how to place data from I/O devices into the processor cache. • **Disabled**—The hardware prefetcher is not used. • **Enabled**—The processor uses the hardware prefetcher when cache issues are detected.
L2 Stream HW Prefetcher drop-down list	Whether the processor allows the AMD hardware prefetcher to speculatively fetch streams of data and instruction from memory into the L2 cache when necessary. This can be one of the following: • **Auto**—The CPU determines how to place data from I/O devices into the processor cache. • **Disabled**—The hardware prefetcher is not used. • **Enabled**—The processor uses the hardware prefetcher when cache issues are detected.
Determinism Slider drop-down list	Allows AMD processors to determine how to operate. This can be one of the following: • **Auto**—The CPU automatically uses default power determinism settings. • **Performance**—Processor operates at the best performance in a consistent manner. • **Power**—Processor operates at the maximum allowable performance on a per die basis.
CPPC drop-down list	Allows you to configure Collaborative Processor Performance Control. This can be one of the following: • **Auto**—The CPU automatically uses default CPPC settings. • **Disabled**—Feature is disabled. • **Enabled**—Collaborative Processor Performance is enabled.

Name	Description
Power Profile Selection F19h drop-down list	The Power Profile Selection F19h BIOS setting allows you to choose a predefined power management profile tailored for specific performance or energy efficiency goals on AMD® Family 19h processors. This setting optimizes the CPU power consumption and performance characteristics based on the selected profile. This can be one of the following: • **High Performance Mode**—High Performance mode is enabled. • **Efficiency Mode**—Efficiency mode is enabled. • **Maximum IO Performance Mode**—Maximum IO Performance mode is enabled. • **Balanced Memory Performance Mode**—Balanced Memory Performance mode is enabled.
Enhanced CPU Performance drop-down list	**Note** Once you enable this functionality, you cannot enable **Enable Power Characterization** and **Power Capping**. Enhances CPU performance by adjusting server settings automatically. **Note** Enabling this functionality may increase power consumption. The server should meet the following requirements in order to use this functionality: • Server should not contain Barlow Pass DIMMs • DIMM module size present in the server should be less than 64GB • No GPU cards are present in the server. This can be one of the following: • **Disabled**—The processor does not run with this functionality. • **Auto**—Allows Cisco IMC to adjust server settings to increase performance.

Processor Tab

Note BIOS parameters listed in this tab may vary depending on the configuration of the server.

Table 42: BIOS Parameters in Processor Tab

Name	Description
Reboot Host Immediately check 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.
SVM Mode toggle button	Whether the processor uses AMD Secure Virtual Machine Technology. This can be one of the following: This can be one of the following: • **Disabled**—The processor does not use SVM Technology. • **Enabled**—The processor uses SVM Technology.
SMT Mode drop-down list	Whether the processor uses AMD Simultaneous MultiThreading Technology, which allows multithreaded software applications to execute threads in parallel within each processor. This can be one of the following: • **Auto**—The processor allows for the parallel execution of multiple threads. • **Disabled**—The processor does not use SMT Mode. • **Enabled**—The processor uses SMT Mode.

Name	Description
CPU Downcore control F19 M10h-1Fh drop-down list	The ability to remove one or more cores from operation is supported in the silicon. It may be desirable to reduce the number of cores due to OS restrictions, or power reduction requirements of the system. This item allows the control of how many cores are running. This setting can only reduce the number of cores from those available in the processor. This can be one of the following: • **Auto**—The CPU determines how many cores need to be enabled. • One (1+0)—One cores enabled on one CPU complex. • TWO (2+0)—Two cores enabled on one CPU complex. • THREE (3+0)—Three cores enabled on one CPU complex. • FOUR (4+0)—Four cores enabled on one CPU complex. • Five (5+0)—Five cores enabled on one CPU complex. • SIX (6+0)—Six cores enabled on one CPU complex. • SEVEN (7+0)—Seven cores enabled on one CPU complex.

Name	Description
Downcore control F19 MA0h-AFh drop-down list	Allows the AMD processors to disable cores and, thus, select how many cores to enable. This can be one of the following: • **Auto**—The CPU determines how many cores need to be enabled. • TWO (1+1)—Two cores enabled on one CPU complex. • FOUR (2+2)—Four cores enabled on one CPU complex. • SIX (3+3)—Six cores enabled on one CPU complex. • EIGHT (4+4)—Eight cores enabled on one CPU complex. • TEN (5+5)—Ten cores enabled on one CPU complex. • TWELVE (6+6)—Twelve cores enabled on one CPU complex. • FOURTEEN (7+7)—Fourteen cores enabled on one CPU complex.
Fixed SOC P-State SP5 F19h (0 - 2 P State) drop-down list	This option defines the target PState when APBDIS is set. **P*x*** – Specify a valid PState for the processor installed. This can be one of the following: • P0 • P1 • P2 • P3 • Auto
APBDIS drop-down list	Allows you to select the APB Disable value for the SMU. This can be one of the following: • **0**—Clear ApbDis to SMU • **1**—Set ApbDis to SMU. • **Auto**—The CPU determines the value.

Name	Description
CCD Control drop-down list	Allows you to specify the number of CCDs that are desired to be enable in the system. This can be one of the following: • **Auto**—The maximum CCDs provided by the processor is enabled. • 2 CCDs • 3 CCDs • 4 CCDs • 6 CCDs
Streaming Stores Control drop-down list	Enables the streaming stores functionality. This can be one of the following: • **Auto**—Set to auto mode. • **Disabled**—Feature is disabled. • **Enabled**—Feature is enabled.
ACPI SRAT L3 Cache As NUMA Domain drop-down list	Creates a layer of virtual domains on top of the physical domains in which each CCX is declared to be in its on domain. This can be one of the following: • **Auto**—Set to auto mode. • **Disabled**—Use NPS settings for domain configuration. • **Enabled**— Each CCX is declared to be in its own domain.
DF C-States drop-down list	When long duration idleness is expected in a system, this control allows the system to transition into a DF Cstate which can set the system into an even lower power state. This can be one of the following: • **Auto**—Set to auto mode. • **Disabled**—Long periods of idleness are not expected so no power savings would be achieved. • **Enabled**— This option is active, saving power when the system is very idle.

Name	Description
Local APIC Mode drop-down list	This control selects the APIC mode to be used. • **Auto**—Set to auto mode. • **Compatibility**—Set to Compatibility mode. • **XAPIC**—Set to XAPIC mode. • **X2APIC**—Set to X2APIC mode.
4-link xGMI max speed	This setting allows you to manually specify the number of lanes used for the xGMI (Inter-chip Global Memory Interconnect) link, which can impact the bandwidth and performance of the data transfer between CPUs. Adjusting this setting can be used for troubleshooting, performance tuning, or to ensure compatibility with certain workloads or system configurations. This can be one of the following: • **Auto**—Set to auto mode. • **20Gbps**—Set to 20Gbps. • **25Gbps**—Set to 25Gbps. • **32Gbps**—Set to 32Gbps.
DF PState Frequency Optimizer	Enable or disable DF PState Frequency Optimizer. This can be one of the following: • **Auto**—Set to auto mode. • **Disabled**—Feature is disabled. • **Enabled**—Feature is enabled.
AVX512	The AVX512 BIOS setting enables or disables the use of AVX512 instruction set extensions, which are advanced vector extensions used by certain Intel® processors to improve performance for heavy computational tasks Adjusting this setting can affect compatibility and stability with some software, as well as influence CPU power consumption and heat output. This can be one of the following: • **Auto**—Set to auto mode. • **Disabled**—Feature is disabled. • **Enabled**—Feature is enabled.

Name	Description
Power Down Enable	This setting controls whether the memory (RAM) can enter a low power state when the system is idle or during periods of low usage. Enabling this setting typically allows the RAM to consume less power, potentially saving energy and reducing heat output, while disabling it keeps the RAM fully powered for possibly quicker wake-up times at the expense of higher power consumption. This can be one of the following: • **Auto**—Set to auto mode. • **Disabled**—Feature is disabled. • **Enabled**—Feature is enabled.
xGMI Force Link Width	This setting allows users to manually specify the number of lanes used for the xGMI (Inter-chip Global Memory Interconnect) link, which can impact the bandwidth and performance of the data transfer between CPUs. Adjusting this setting can be used for troubleshooting, performance tuning, or to ensure compatibility with certain workloads or system configurations. This can be one of the following: • **Auto**—Set to auto mode. • **0**—Set to 0. • **1**—Set to 1. • **2**—Set to 2.

Security Tab

Note BIOS parameters listed in this tab may vary depending on the configuration of the server.

Table 43: BIOS Parameters in Security Tab

Name	Description
Reboot Host Immediately check 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.

Name	Description
Security Device Support toggle button	This option allows you to control the Security Device support for the system. This can be one of the following: • **Disabled**—The option is disabled. • **Enabled**—The server is disabled.
Trusted Platform Module State toggle button	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. This 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 toggle button	Enable or Disable SHA-1 PCR Bank. This can be one of the following: • **Disabled**—The server does not use this feature. • **Enabled**—The server uses this feature.
SHA256 PCR Bank toggle button	Enable or Disable SHA256 PCR Bank. This can be one of the following: • **Disabled**—The server does not use this feature. • **Enabled**—The server uses this feature.
SHA384 PCR Bank toggle button	Enable or Disable SHA384 PCR Bank. This can be one of the following: • **Disabled**—The server does not use this feature. • **Enabled**—The server uses this feature.
TPM Pending Operation drop-down list	Trusted Platform Module (TPM) Pending Operation option allows you to control the status of the pending operation. This can be one of the following: • None—No action. • TpmClear—Clears the pending operations.

Name	Description
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. This can be one of the following: • **Disabled**—Support is disabled. • **Enabled**—Support is enabled.

Cisco UCS C220 and C240 M7

I/O Tab

Note BIOS parameters listed in this tab may vary depending on the configuration of the server.

Table 44: BIOS Parameters in I/O Tab

Name	Description
MLOM OptionROM toggle button	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.

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. • **GEN4**—16GT/s is the maximum speed allowed. • **GEN5**—32GT/s is the maximum speed allowed.
PCIe Slot*n* OptionROM toggle button	Whether the server can use the 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.
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. • **GEN4**—Link speed can reach up to fourth generation. • **GEN5**—Link speed can reach up to fifth generation.

Name	Description
MRAID OptionROM drop-down list	This options allows you to control the Option ROM execution of the MRAID PCIe adapter connected. This can be one of the following: • **Disabled**—Does not execute Option ROM of the MRAID PCIe adapter. • **Enabled**—Executes Option ROM of the MRAID PCIe adapter.
MRAID Link Speed drop-down list	This option allows you to restrict the maximum speed of an MRAID adapter card installed. 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. • **GEN4**—16GT/s is the maximum speed allowed. • **GEN5**—32GT/s is the maximum speed allowed.
Front NVME-*n* OptionROM toggle button	This options allows you to control the Option ROM execution of the PCIe adapter connected to the SSD:NVMe slot *n*. 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

Name	Description
Front NVME-*n* Link Speed drop-down list	Link speed for NVMe front slot designated by slot *n*. 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. • **GEN4**—Link speed can reach up to fourth generation. • **GEN5**—Link speed can reach up to fifth generation.
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 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
PCIe RAS Support drop-down list	Whether PCIe RAS Support is available on the PCIe slot. This can be one of the following: • **Disabled**—PCIe RAS is not available on the slot. • **Enabled**—PCIe RAS is available on port.
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.
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. • **OnBoardDisabled**—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.
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.

Name	Description
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.
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.
IPV4 HTTP Support drop-down list	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.
IIO eDPC Support drop-down list	eDPC allows a downstream link to be disabled after an uncorrectable error, making recovery possible in a controlled and robust manner. This can be one of the following: • Disabled—eDPC support is disabled. • On Fatal Error—eDPC is enabled only for fatal errors. • On Fatal and Non-Fatal Errors—eDPC is enabled for both fatal and non-fatal errors.
Re-Size BAR Support drop-down list	Re-Size BAR Support allows the system to dynamically adjust the size of the Base Address Registers (BAR) for PCIe devices to optimize memory allocation and performance. This can be one of the following: • **Disabled**—IPv6 HTTP support is not available. • **Enabled**—IPv6 HTTP support is always available.

Name	Description
IPV6 HTTP Support drop-down list	Enables or disables IPv6 support for HTTP. This can be one of the following: • **Disabled**—IPv6 HTTP support is not available. • **Enabled**—IPv6 HTTP support is always available.

Server Management Tab

Note BIOS parameters listed in this tab may vary depending on the configuration of the server.

Table 45: BIOS Parameters in Server Management Tab

Name	Description
Reboot Host Immediately check 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.
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.
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.

Name	Description
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: • **Power Off**—The watchdog timer is not used to track how long the server takes to boot. • **Reset**—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 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.

Name	Description
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.
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: • **COM 0**—Enables console redirection on serial port A during POST. • **COM 1**—Enables console redirection on serial port B during POST. • **Disabled**—No console redirection occurs during POST.
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	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.

Name	Description
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.
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.

Memory Tab

Note BIOS parameters listed in this tab may vary depending on the configuration of the server.

Table 46: BIOS Parameters in Memory Tab

Name	Description
Reboot Host Immediately check 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.

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. • **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.
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.
Partial Cache Line Sparing drop-down list	Partial cache line sparing (PCLS) is an error-prevention mechanism in memory controllers. PCLS statically encodes the locations of the faulty nibbles of bits into a sparing directory along with the corresponding data content for replacement during memory accesses. This can be one of the following: • **Disabled**—Support is disabled. • **Enabled**—Support is enabled.
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.

Name	Description
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.
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.
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*n* Size in GB field	Size of the first partial *nth* memory mirror in GB. n = 1, 2, or 3 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 Mirror percentage field	Percentage of memory to mirror above 4GB. Enter an integer between 0 and 50.
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
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.
UMA drop-down list	Allows you to set UMA settings. This can be one of the following: • Disable(All2All) • Hemisphere(2-clusters) • Quadrant(4-clusters)
Enhanced 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. • **Auto**—Automatically determines whether to perform the Enhanced Memory Test based on system conditions and requirements.

Name	Description
Adaptive Refresh Management Level drop-down list	Refresh management settings are read-only. Adaptive RFM allows the controller flexibility to choose additional RFM threshold settings called RFM levels. The RFM levels permit alignment of the controller-issued RFM commands with the in-DRAM management of these commands. This can be one of the following: • **Default** • **Level A** • **Level B** • **Level C**
Memory Bandwidth Boost drop-down list	Intel® Memory Bandwidth Boost is a feature of the Intel® Optane™ persistent memory that provides a dynamic range of power and bandwidth when thermal headroom is available. This can be one of the following: • **Disabled**—Support is disabled. • **Enabled**—Support is enabled.
Error Check Scrub drop-down list	You can enable memory check with or without result collection. This can be one of the following: • **Disabled** • **Enabled without Result Collection** • **Enabled with Result Collection**
Rank Margin Tool drop-down list	Indicates whether the rank margin tool is used and whether a margin test (which tests the memory sequence and voltage signals) is performed. This can be one of the following: • **Disabled** • **Enabled**

Name	Description
MMIO High Base drop-down list	MMIO High Base configures the base address for the high memory-mapped I/O (MMIO) region, which is used to map device memory and I/O resources above the 4GB address space, optimizing system memory allocation and performance. This can be one of the following: • **512G**—Sets the MMIO High Base to 512 gigabytes. • **1T**—Sets the MMIO High Base to 1 terabyte. • **2T**—Sets the MMIO High Base to 2 terabytes. • **4T**—Sets the MMIO High Base to 4 terabytes. • **16T**—Sets the MMIO High Base to 16 terabytes. • **24T**—Sets the MMIO High Base to 24 terabytes. • **32T**—Sets the MMIO High Base to 32 terabytes. • **40T**—Sets the MMIO High Base to 40 terabytes. • **56T**—Sets the MMIO High Base to 56 terabytes.
MMIO High Granularity Size drop-down list	MMIO High Granularity Size configures the granularity of the high memory-mapped I/O (MMIO) region, determining the size increments for allocating MMIO space above the 4GB address range, which helps optimize memory allocation and system performance. This can be one of the following: • **1G**—Sets the MMIO High Granularity Size to 1 gigabyte. • **4G**—Sets the MMIO High Granularity Size to 4 gigabytes. • **16G**—Sets the MMIO High Granularity Size to 16 gigabytes. • **64G**—Sets the MMIO High Granularity Size to 64 gigabytes. • **256G**—Sets the MMIO High Granularity Size to 256 gigabytes. • **1024G**—Sets the MMIO High Granularity Size to 1024 gigabytes.

Power/Performance Tab

Note BIOS parameters listed in this tab may vary depending on the configuration of the server.

Table 47: BIOS Parameters in Power/Performance Tab

Name	Description
Reboot Host Immediately check 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.
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.
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.
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
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.
Virtual Numa drop-down list	Virtual NUMA (virtual non-uniform memory access) is a memory-access optimization method for VMware virtual machines (VMs), which helps prevent memory-bandwidth bottlenecks. This can be one of the following: • **Disabled**—Functionality is disabled. • **Enabled**—Functionality is enabled.
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.

Name	Description
LLC Dead Line drop-down list	In CPU non-inclusive cache scheme, MLC evictions are filled into the LLC. When lines are evicted from the MLC, the core can flag them as **dead** (not likely to be read again). The LLC has the option to drop dead lines and not fill them in the LLC. If this feature is disabled, dead lines are always dropped and are never filled into the LLC. If this feature is enabled, the LLC can fill dead lines into the LLC if there is free space available. This can be one of the following: • **Disabled**—Feature is disabled. • **Enabled**—Feature is enabled. • **Auto**—CPU determines the LLC dead line allocation.
XPT Remote Prefetch drop-down list	This feature allows an LLC request to be duplicated and sent to an appropriate memory controller in a remote machine based on the recent LLC history to reduce latency. This can be one of the following: • **Disabled**—Feature is disabled. • **Enabled**—Feature is enabled. • **Auto**—CPU determines the functionality.
UPI Link Enablement drop-down list	Enables the minimum number of UPI links required by the processor. This can be one of the following: • **1** • **2** • **Auto**

Name	Description
Enhanced CPU Performance drop-down list	**Note** Once you enable this functionality, you cannot enable **Enable Power Characterization** and **Power Capping**. Enhances CPU performance by adjusting server settings automatically. **Note** Enabling this functionality may increase power consumption. The server should meet the following requirements in order to use this functionality: • Server should not contain Barlow Pass DIMMs • DIMM module size present in the Cisco UCS C220 M6 server should be less than 64GB and in Cisco UCS C240 M6 server should be less than 256GB • No GPU cards are present in the server. This can be one of the following: • **Disabled**—The processor does not run with this functionality. • **Auto**—Allows Cisco IMC to adjust server settings to increase performance.
C1 Auto Demotion drop-down list	If enabled, CPU automatically demotes to C1 based on un-core auto-demote information. • **Disabled**—The processor does not run with this functionality. • **Enabled**—Functionality is enabled. • **Auto**—The server dynamically determines the value for this field.
UPI Power Management toggle button	UPI power management is used to conserve power on the server. This can be one of the following: • **Disabled**—The processor does not run with this functionality. • **Auto**—Functionality is enabled.

Name	Description
Optimized Power Mode drop-down list	Optimized Power Mode is used to save power while having minimal impact on performance for certain workloads that run at 30-40% CPU utilization. This can be one of the following: • **Disabled**—The processor does not run with this functionality. • **Auto**—Functionality is enabled.
C1 Auto UnDemotion drop-down list	Select whether to enable processors to automatically undemote from C1. • **Disabled**—The processor does not run with this functionality. • **Enabled**—Functionality is enabled. • **Auto**—The server dynamically determines the value for this field.

Processor Tab

Note BIOS parameters listed in this tab may vary depending on the configuration of the server.

Table 48: BIOS Parameters in Processor Tab

Name	Description
Reboot Host Immediately check 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.
Extended APIC toggle button	Allows you to enable or disable extended APIC support. This can be one of the following: • Enabled—Enables APIC support. • Disabled—Disables APIC support.

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.
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.
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
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.
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.
Boot Performance Mode drop-down list	Allows you 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 • **Set by Intel NM**—Value is set automatically.

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.
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.
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.
Workload Configuration drop-down list	This feature allows for workload optimization. The options are Balanced and I/O Sensitive: • **Balanced** • **IO Sensitive**

Name	Description
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 48**—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.
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. • **Auto** —CPU determines the UPI Prefetch mode.
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. • **SNC2**—The processor is divided into two NUMA nodes, each with its own memory access paths. This can improve memory access times for workloads that benefit from lower memory latency and higher memory bandwidth. • **SNC4**—The processor is divided into four NUMA nodes. This can enhance memory access performance for workloads that benefit from extremely low memory latency and high memory bandwidth. • **Auto** — The BIOS determines what Sub NUMA clustering is done.

Name	Description
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. • **PECI**—Chooses Platform Environmental Control Interface for energy performance tuning.
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. • **Auto** — The BIOS determines what Sub NUMA clustering is done.

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.

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.
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)
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.
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
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.
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. • **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
Intel Dynamic Speed Select drop-down list	**Intel Dynamic Speed Select** modes allow you to run the CPU with different speed and cores in auto mode. This can be one of the following: • **Disabled**—**Intel Dynamic Speed Select** is disabled. • **Enabled**—**Intel Dynamic Speed Select** is enabled.
X2APIC Opt-Out Flag drop-down list	Allows the system to disable the extended x2APIC mode, reverting to the legacy APIC mode for interrupt management. This can be one of the following: • **Disabled**—Disables the feature. • **Enabled**—Enables the feature.

Name	Description
IOAT Configuration drop-down list	IOAT Configuration enables or disables Intel I/O Acceleration Technology (IOAT), which improves data transfer efficiency and reduces CPU overhead by offloading memory copy operations. This can be one of the following: • **Disabled**—Disables the feature. • **Enabled**—Enables the feature.

Name	Description
PRMRR Size drop-down list	PRMRR Size configures the size of the Protected Range Memory Region Register (PRMRR), which is used to define protected memory regions for enhanced security and isolation in the system. This can be one of the following: • **128MB**—Defines a 128 megabyte protected memory region. • **256MB**—Defines a 256 megabyte protected memory region. • **512MB**—Defines a 512 megabyte protected memory region. • **1GB**—Defines a 1 gigabyte protected memory region. • **2GB**—Defines a 2 gigabyte protected memory region. • **4GB**—Defines a 4 gigabyte protected memory region. • **8GB**—Defines an 8 gigabyte protected memory region. • **16GB**—Defines a 16 gigabyte protected memory region. • **32GB**—Defines a 32 gigabyte protected memory region. • **64GB**—Defines a 64 gigabyte protected memory region. • **128GB**—Defines a 128 gigabyte protected memory region. • **256GB**—Defines a 256 gigabyte protected memory region. • **512GB**—Defines a 512 gigabyte protected memory region. • **Invalid Config.**—Indicates an invalid configuration for the protected memory region. • **Auto**—Automatically configures the protected memory region size based on system requirements.

Security Tab

Note BIOS parameters listed in this tab may vary depending on the configuration of the server.

Table 49: BIOS Parameters in Security Management Tab

Name	Description
Reboot Host Immediately check 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.
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. This 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.
Security Device Support drop-down list	You should enable TPM support to enable security device support. This can be one of the following: • **Disabled**—Feature is disabled. • **Enabled**—Feature is enabled if TPM is enabled.
SHA256 PCR Bank drop-down list	PCR bank available for OS when BIOS is performing measurements. • **Disabled**—SHA256 PCR Bank is not available for BIOS. • **Enabled**—SHA256 PCR Bank is available for BIOS.
SHA-1 PCR Bank drop-down list	PCR bank available for OS when BIOS is performing measurements. • **Disabled**—SHA-1 PCR Bank is not available for BIOS. • **Enabled**—SHA-1 PCR Bank is available for BIOS.

Name	Description
TPM Pending Operation drop-down list	Trusted Platform Module (TPM) Pending Operation option allows you to control the status of the pending operation. This can be one of the following: • None—No action. • TpmClear—Clears the pending operations.
SHA384 PCR Bank drop-down list	The Platform Configuration Register (PCR) is a memory location in the TPM. Multiple PCRs are collectively referred to as a PCR bank. A Secure Hash Algorithm 384-bit or SHA-384PCR Bank allows to enable or disable TPM security. This can be one of the following: • **Disabled**—The server does not use this feature. • **Enabled**—The server uses this feature.
Intel Trusted Execution Technology Support drop-down list	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.
TPM Minimal Physical Presence drop-down list	This token allows you to apply recommended Microsoft default settings for TPM. • **Disabled**—Support is disabled. • **Enabled**—Support is enabled.
Total Memory Encryption (TME) drop-down list	Allows you to provide the capability to encrypt the entirety of the physical memory of a system. 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. This can be one of the following: • **Disabled**—Support is disabled. • **Enabled**—Support is enabled.

Name	Description
SW Guard Extensions (SGX) drop-down list	Allows you to enable Software Guard Extensions (SGX) feature. This can be one of the following: • **Disabled**—Support is disabled. • **Enabled**—Support is enabled.
Multikey Total Memory Encryption (MK-TME) drop-down list	MK-TME allows you to have multiple encryption domains with one with own key. Different memory pages can be encrypted with different keys. This can be one of the following: • **Disabled**—Support is disabled. • **Enabled**—Support is enabled.
SGX Pkg info In-Band Access drop-down list	Allows you to enable SGX Package Info In-Band Access. This can be one of the following: • **Disabled**—Support is disabled. • **Enabled**—Support is enabled.
SGX Factory Reset drop-down list	Allows the system to perform SGX factory reset on subsequent boot. This deletes all registration data. This can be one of the following: • **Disabled**—Support is disabled. • **Enabled**—Support is enabled.
Select Owner EPOCH input type drop-down list	Allows you to change the seed for the security key used for the locked memory region that is created. This can be one of the following: • **SGX Owner EPOCH activated**—Does not change the current input type. • **Change to New Random Owner EPOCHs**—Changes EPOCH to a system generated random number. • **Manual User Defined Owner EPOCHs**—Changes the EPOCH seed to a hexadecimal value that you enter.
SGX QoS drop-down list	Allows you to enable SGX QoS. This can be one of the following: • **Disabled**—Support is disabled. • **Enabled**—Support is enabled.

Name	Description
SGX Auto MP Registration Agent drop-down list	Allows you to enable the registration authority service to store the platform keys. This can be one of the following: • **Disabled**—Support is disabled. • **Enabled**—Support is enabled.
SGX Write Enable drop-down list	Allows you to enable SGX Write feature. This can be one of the following: • **Disabled**—Support is disabled. • **Enabled**—Support is enabled.
SProcessor Epoch *n* field	Allows you to define the SGX EPOCH owner value for the EPOCH number designated by *n*.
SGX PUBKEY HASH*n* field	Allows you to set the Software Guard Extensions (SGX) value. This value can be set between: • SGX PUBKEY HASH0—Between 7-0 • SGX PUBKEY HASH1—Between 15-8 • SGX PUBKEY HASH2—Between 23-16 • SGX PUBKEY HASH3—Between 31-24
DMA Control Opt-In Flag drop-down list	DMA Control Opt-In Flag - Enabling this token allows the operating system to enable Input Output Memory Management Unit (IOMMU) to prevent the DMA attacks from possible malicious devices. • **Disabled**—Support is disabled. • **Enabled**—Support is enabled.
LIMIT CPU PA to 46 Bits drop-down list	Enable this option for Intel® VT-d enabling boot to boot with 2019 OS. This can be one of the following: • **Disabled**—Support is disabled. • **Enabled**—Support is enabled.

Name	Description
TDX Secure Arbitration Mode (SEAM) Loader: drop-down list	Enable this for a security feature that enables the initialization and management of Intel® Trusted Domain Extensions (TDX) for secure virtualized environments. This can be one of the following: • **Disabled**—Support is disabled. • **Enabled**—Support is enabled.
Trust Domain Extension (TDX) drop-down list	Allows you to enhance the security of virtualized environments by creating isolated execution environments, known as Trust Domains, that protect sensitive data and code from other software, including the hypervisor. This can be one of the following: • **Disabled**—Support is disabled. • **Enabled**—Support is enabled.

Configuring Power Policies

Power Capping

Important

- This section is valid only for some UCS C-Series servers.

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.

Once power capping is enabled, you can configure multiple power profiles to either have standard or advanced power profiles with defined attributes. If you choose a standard power profile, you can set the power limit, correction time, corrective-action, suspend period, hard capping, and policy state (if enabled). If you choose an advanced power profile, in addition to the attributes of the standard power profile, you can also set the domain specific power limits, safe throttle level, and ambient temperature based power capping attributes.

Note The following changes are applicable for Cisco UCS C-Series release 2.0(13) and later:

- After upgrading to the 2.0(13) release, power characterization automatically runs during the first host power on. Subsequent characterization runs only if initiated as described in section **Run Power Characterization** section.
- Also, when a server is power cycled and there is a change to the CPU or DIMM configurations, power characterization automatically runs on first host boot. For any other hardware change like PCIe adapters, GPU or HDDs, power characterization does not run. The characterized power range is modified depending on the components present after the host power cycle.

The **Run Power Characterization** option power cycles the host and starts power characterization. You can enable the option in the following path:

Dashboard > **System** > **Power Management** > **Actions** drop-down list > **Run Power Characterization**.

Note The **Power Characterization Status** option is not available on Cisco UCS C220 M8 and C240 M8 servers.

Setting Power Redundancy Policy

Procedure

Step 1 From the **Apps** drop-down list, select **System**.

Step 2 From the **System** menu, select **Power Management** tab.

Step 3 In the **Power Management** page, click the **Power Policies** tab.

Step 4 Review the following sensor properties for power supply:

Properties Area

Name	Description
Power Supply Redundancy Policy drop-down list	The power supply redundancy policy. This can be one of the following: • **Grid** - N, the available PSU output capacity, equals half the number of PSUs installed (N/2), where N PSU failure or grid failure is supported. This policy implies that the you have connected N number of PSUs to one feed and the other N number of PSUs to another feed. • **N+1** - N, the available PSU output capacity, equals the number of PSUs installed minus 1 (N-1), where the single PSU failure is supported, but grid failure is not supported. • **Non-Redundant** - N, the available PSU output capacity, equals the number of PSUs installed, where PSU failure or grid failure is not supported.

Name	Description
Power Supply Redundancy Status field	The power supply redundancy status.

Step 5 Click **Save**.

Enabling Power Characterization

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.

Procedure

Step 1 From the **Apps** drop-down list, select **System**.

Step 2 In the **System** page, click the **Power Management** tab.

Step 3 In the **Power Management** tab, click the **Actions** drop-down list.

Step 4 In the **Actions** drop-down list, select **Power Characterization**.

Note
The **Power Characterization Status** option is not available on Cisco UCS C220 M8 and C240 M8 servers.

Step 5 Under **Power Characterization**, select **Run Power Characterization**.

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 **Power Characterization Status** field. The status can be one of the following:

- **Not Run**—When power characterization has not been run at all since the factory reset.
- **Running**—When a power characterization process is in progress.
- **Completed Successfully**—When a power characterization has run successfully.
- **Using Defaults**—After running the power characterization, if the system fails to obtain the valid values, it uses default value as the recommended maximum and minimum power for power capping.

  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.

  Three values for power capping limits are displayed: **Minimum (Allow Throttling)**, **Minimum (Efficient)** and **Maximum**:

  - **Minimum (Allow Throttling)** - This is the lower power limit for the chassis, when the CPU throttling is enabled.

    Note

You can use this minimum power limit value only when the **Allow Throttle** checkbox is enabled.

- **Minimum (Efficient)** - This is the lower power limit for the chassis, when the CPU throttling is disabled.
- **Maximum** - This is the upper power limit for the chassis.

Enabling Power Capping

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.
- Run power characterization.

Procedure

Step 1 From the **Apps** drop-down list, select **System**.

Step 2 From the **System** menu, select **Power Management** tab.

Step 3 In the **Power Management** page, click the **Power Cap Configuration** tab.

Step 4 Select the **Power Capping** toggle button.

Note
This is the global option to enable or disable power capping. You must enable this option if you want to configure power profile settings.

Power Profiles

You can configure multiple profiles and set the attributes. These profiles are configured by using either the web UI or CLI. 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:

- **Standard**—Enables you to set a power limit for the platform domain.
- **Advanced**—Enables you to set various attributes such as the power limiting policy, fail-safe power limiting policy, and the ambient temperature-based power limiting policy.

Configuring Standard Power Profiles Settings

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

Note The **Standard** Profile is not available on Cisco UCS C220 M8 and C240 M8 servers.

Before you begin

- You must enable power capping.
- You must log in with admin privileges to perform this task.

Procedure

Step 1 From the **Apps** drop-down list, select **System**.

Step 2 From the **System** menu, select **Power Management** tab.

Step 3 In the **Power Management** page, click the **Power Cap Configuration** tab.

Step 4 In the **Power Cap Configuration** page > **Power Capping** area, select the appropriate option in the following fields:

Name	Description
Power Capping toggle button	If enabled, then 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, then you cannot configure or modify individual power capping profiles in the **Power Profiles** area. **Note** You cannot enable Power Capping if **Enhanced CPU Performance** bios token is enabled.
Recommended Power Cap area	Recommended values to setup power cap for the server. The range is set by default for the server obtained after running power characterization. This allows you to set the power capping values: • **Minimum (Allow Throttling)**—This is the lower power limit for the chassis, when the CPU throttling is enabled. **Note** You can use this minimum power limit value only when the **Allow Throttle** checkbox is enabled. • **Minimum (Efficient)** —This is the lower power limit for the chassis, when the CPU throttling is disabled. • **Maximum** —This is the upper power limit for the chassis.

Name	Description
Platform	Recommended values: • 526 W Minimum (Allow Throttling) • 732 W Minimum (Efficient) • 1139 W Maximum

Table 50: Standard Tab

Name	Description
Name field	The name of the profile selected to set the attributes for power capping.
Enable Profile toggle button	Enables the power profile for editing.
Allow Throttle toggle button	If checked, it 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.
Set Hard Cap toggle button	If checked, ensure that no platform consumption occurs beyond the set power capping value. The platform power consumption is maintained at a safe offset margin below the configured power cap value.
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.
Power Limit field	Allows you to set the power limit for the server.

Configuring Advanced Power Profile Settings

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

Before you begin

- You must enable power capping.

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

Procedure

Step 1 From the **Apps** drop-down list, select **System**.

Step 2 From the **System** menu, select **Power Management** tab.

Step 3 In the **Power Management** page, click the **Power Cap Configuration** tab.

Step 4 In the **Power Cap Configuration** page > **Power Capping** area, select the appropriate option in the following fields:

Name	Description
Power Capping toggle button	If enabled, then 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, then you cannot configure or modify individual power capping profiles in the **Power Profiles** area. **Note** You cannot enable Power Capping if **Enhanced CPU Performance** bios token is enabled.
Recommended Power Cap area	Recommended values to setup power cap for the server. The range is set by default for the server obtained after running power characterization. This allows you to set the power capping values: • **Minimum (Allow Throttling)**—This is the lower power limit for the chassis, when the CPU throttling is enabled. **Note** You can use this minimum power limit value only when the **Allow Throttle** checkbox is enabled. • **Minimum (Efficient)** —This is the lower power limit for the chassis, when the CPU throttling is disabled. • **Maximum** —This is the upper power limit for the chassis.
Platform	Recommended values: • 526 W Minimum (Allow Throttling) • 732 W Minimum (Efficient) • 1139 W Maximum

Table 51: Advanced Tab

Name	Description
Name field	The name of the profile selected to set the attributes for power capping.
Enable Profile toggle button	Enables the power profile for editing.
Allow Throttle toggle button	If selected, it 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. **Note** This is not available on Cisco UCS C220 and C240 M8 servers.
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. **Note** This is not available on Cisco UCS C220 and C240 M8 servers.
Set Hard Cap toggle button	If selected, ensure that no platform consumption occurs beyond the set power capping value. The platform power consumption is maintained at a safe offset margin below the configured power cap value. **Note** This is not available on Cisco UCS C220 and C240 M8 servers.
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.

Step 5 In the **Domain Specific Power Limit** area, complete the following fields:

Name	Description
CPU	Recommended value: (418-539) W
Memory	Recommended value: (14-46) W

Name	Description
Platform	Recommended value: (732-1139) W **Note** This is not available on Cisco UCS C220 and C240 M8 servers.

Resetting Power Profiles to Default

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.

Procedure

Step 1 From the **Apps** drop-down list, select **System**.

Step 2 From the **System** menu, select **Power Management** tab.

Step 3 In the **Power Management** page, click the **Power Cap Configuration** tab.

Step 4 In the **Power Cap Configuration** page > **Power Capping** area, click the **Power Restore Policy** drop-down list.

Name	Description
Power Restore Policy	The action to be taken when chassis power is restored after an unexpected power loss. This can be one of the following: • **Power 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.

Power Monitoring

Power monitoring is initiated from the time the host is either powered on or booted. This feature collects the power consumption statistics for a platform, CPU, and memory domains and provides a minimum, maximum, and averaged reading for the duration that is being collected. These readings can be used to calculate the power consumption trends of the domains. Cisco IMC collects and stores these power consumption statistic values to plot graphs for various time periods (such as an hour, a day, and a week).

Note You cannot create additional statistics collection policies or delete the existing monitoring policies. You can only modify the default policies.

Viewing Power Monitoring Summary

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

Procedure

Step 1 From the **Apps** drop-down list, select **Dashboard**.

Step 2 From the **Dashboard** menu, select **Performance Monitoring** under **Quick Actions**.

Step 3 In the **Power** tab, review the following information:

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

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

Table 52: Power Monitoring Summary Area

Name	Description
Monitoring Period	Shows the time period for monitoring in day HH:MM:SS format.
Platform	Shows the current, minimum, maximum, and average server power utilization.
CPU	Shows the current, minimum, maximum, and average CPU power utilization.
Memory	Shows the current, minimum, maximum, and average DIMM power utilization.

Step 5 In the **Chart Properties** area, review and update the chart, component, and view the power consumption details.

In the **Chart Properties** area, select the **Chart** tab.

Table 53: Chart Properties Area

Name	Description
Table/Chart toggle button	Allows you to toggle between table view or chart view.
Chart selection	Allows you to choose between **Last One Hour**, **Last One Day**, or **Last Week** data.
Download icon	Allows you to download the data in `.tar.gz` file format.

Name	Description
Component drop-down list	Allows you to select one or more of the following components: • CPU • Memory • Platform
Plot drop-down list	Allows you to select one or more of the following power data: • Current • Average • Minimum • Maximum

In the **Chart Properties** area, select the **Table** tab.

Table 54: Chart Properties Table Format

Name	Description
Time column	Shows the time at which the data was captured.
Platform-Minimum column	Shows the minimum power consumed by the server for the last one hour/day/week depending on the **Chart** selection made at a specific time-stamp.
Platform-Maximum column	Shows the maximum power consumed by the server for the last one hour/day/week depending on the **Chart** selection made at a specific time-stamp.
Platform-Average column	Shows the average power consumed by the server for the last one hour/day/week depending on the **Chart** selection made at a specific time-stamp.
Platform-Current column	Shows the current power consumed by the server for the last one hour/day/week depending on the **Chart** selection made at a specific time-stamp.
CPU-Minimum column	Shows the minimum power consumed by the CPU for the last one hour/day/week depending on the **Chart** selection made at a specific time-stamp.
CPU-Maximum column	Shows the maximum power consumed by the CPU for the last one hour/day/week depending on the **Chart** selection made at a specific time-stamp.

Name	Description
CPU-Average column	Shows the average power consumed by the CPU for the last one hour/day/week depending on the **Chart** selection made at a specific time-stamp.
CPU-Current column	Shows the current power consumed by the CPU for the last one hour/day/week depending on the **Chart** selection made at a specific time-stamp.
Memory-Minimum column	Shows the minimum power consumed by the DIMMs for the last one hour/day/week depending on the **Chart** selection made at a specific time-stamp.
Memory-Maximum column	Shows the maximum power consumed by the DIMMs for the last one hour/day/week depending on the **Chart** selection made at a specific time-stamp.
Memory-Average column	Shows the average power consumed by the DIMMs for the last one hour/day/week depending on the **Chart** selection made at a specific time-stamp.
Memory-Current column	Shows the current power consumed by the DIMMs for the last one hour/day/week depending on the **Chart** selection made at a specific time-stamp.

Viewing the Power Statistics in a Chart

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

Before you begin

- You must have enabled power capping.
- You must log in with admin privileges to perform this task.

Procedure

Step 1 From the **Apps** drop-down list, select **Dashboard**.

Step 2 From the **Dashboard** menu, select **Quick Actions** > **Performance Monitoring**.

Step 3 On the **Power** tab, review and update the chart, component, to view the power consumption details.

The **Chart** option shows the same data as in the below table in chart format. Hover your mouse over the chart data to see the legends, time-stamp, and data value.

Table 55: Chart Properties Table Format

Name	Description
Time column	Shows the time at which the data was captured.
Platform-Minimum column	Shows the minimum power consumed by the server for the last one hour/day/week depending on the **Chart** selection made at a specific time-stamp.
Platform-Maximum column	Shows the maximum power consumed by the server for the last one hour/day/week depending on the **Chart** selection made at a specific time-stamp.
Platform-Average column	Shows the average power consumed by the server for the last one hour/day/week depending on the **Chart** selection made at a specific time-stamp.
Platform-Current column	Shows the current power consumed by the server for the last one hour/day/week depending on the **Chart** selection made at a specific time-stamp.
CPU-Minimum column	Shows the minimum power consumed by the CPU for the last one hour/day/week depending on the **Chart** selection made at a specific time-stamp.
CPU-Maximum column	Shows the maximum power consumed by the CPU for the last one hour/day/week depending on the **Chart** selection made at a specific time-stamp.
CPU-Average column	Shows the average power consumed by the CPU for the last one hour/day/week depending on the **Chart** selection made at a specific time-stamp.
CPU-Current column	Shows the current power consumed by the CPU for the last one hour/day/week depending on the **Chart** selection made at a specific time-stamp.
Memory-Minimum column	Shows the minimum power consumed by the DIMMs for the last one hour/day/week depending on the **Chart** selection made at a specific time-stamp.
Memory-Maximum column	Shows the maximum power consumed by the DIMMs for the last one hour/day/week depending on the **Chart** selection made at a specific time-stamp.
Memory-Average column	Shows the average power consumed by the DIMMs for the last one hour/day/week depending on the **Chart** selection made at a specific time-stamp.
Memory-Current column	Shows the current power consumed by the DIMMs for the last one hour/day/week depending on the **Chart** selection made at a specific time-stamp.

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.

If choose the Standard profile, the trend line represent the power limit. If you choose the Advance profile, it represents the power limit for CPU, memory, and platform depending on your power profile configuration.

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

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.

SUMMARY STEPS

1. From the **Apps** drop-down list, select **System**.
2. From the **System** menu, select **Power Management** > **Power Policies**.
3. In the **Power Policies** area on the right pane, click and select the appropriate value from the **Power Restore Policy** drop-down list.
4. Click **Save**.

DETAILED STEPS

Procedure

Step 1 From the **Apps** drop-down list, select **System**.

Step 2 From the **System** menu, select **Power Management** > **Power Policies**.

Step 3 In the **Power Policies** area on the right pane, click and select the appropriate value from the **Power Restore Policy** drop-down list.

Name	Description
Power Restore Policy	The action to be taken when chassis power is restored after an unexpected power loss. This can be one of the following: • **Power 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.

Step 4 Click **Save**.

Configuring Fan Policies

Fan Control Policies

Fan Control Policies enable you to control the fan speed to bring down server power consumption and noise levels. Prior to these fan policies, the fan speed increased automatically when the temperature of any server component exceeded the set threshold. To ensure that the fan speeds were low, the threshold temperatures of components are usually set to high values. While this behavior suited most server configurations, it did not address the following situations:

- Maximum CPU performance

  For high performance, certain CPUs must be cooled substantially below the set threshold temperature. This required very high fan speeds which resulted in higher power consumption and increased noise levels.

- Low power consumption

  To ensure the lowest power consumption, fans must run very slowly, and in some cases, stop completely on servers that support it. But slow fan speeds resulted in servers overheating. To avoid this situation, it is necessary to run fans at a speed that is moderately faster than the lowest possible speed.

With the introduction of fan policies, you can determine the right fan speed for the server, based on the components in the server. In addition, it allows you to configure the fan speed to address problems related to maximum CPU performance and low power consumption.

Following are the fan policies that you can choose from:

- **Balanced**—This setting can cool almost any server configuration, but may not be suitable for servers with PCIe cards as these cards overheat easily.
- **Low Power**—This setting is ideal for minimal configuration servers that do not contain any PCIe cards.
- **High Power**—This policy is ideal for servers that contain PCIe cards that overheat easily and have high temperatures.
- **Maximum Power**—This setting can be used for server configurations that required extremely high fan speeds. This policy is ideal for servers that contain PCIe cards that overheat easily and have very high temperatures.
- **Acoustic**—This setting can be used for configuring the fan noise level, thereby enabling noise reduction in the servers.

  Application of this policy might result in performance throttling impacting system performance. If excessive thermal or performance events are recorded in the event logs, select a standard fan control policy like **Low Power**, which is a non-disruptive change.

Note This option is available only on Cisco UCS C220 M5, C240 SD M5, C240 M5, C220 M6, C240 M6, C245 M6 , C225 M6 , C220 M7, and C240 M7 servers. For these servers, **Acoustic** is the default fan policy.

For other servers, default fan policy depends on the server configuration and the number of PCIe cards present in the server.

Note For Cisco UCS M5 servers, although you set a fan policy in Cisco IMC, the actual speed that the fan runs at is determined by the configuration requirements of the server. PCIe cards are tagged with minimum fan speed depending on thermal requirements. If the server is equipped with these PCIe cards, you cannot configure the fan policy, which go below the tagged requirement.

The **Configuration Status** displays the status of the configured fan policy in Cisco UCS M5 servers. This can be one of the following:

- SUCCESS —The selected fan policy matches the actual fan speed that runs on the server.
- PENDING —The configured fan policy is not in effect yet. This can be due to one of the following:
  - The server is powered off
  - The BIOS POST is not complete
- FAN POLICY OVERRIDE—Overrides the specified fan speed with the actual speed determined by the configuration requirements of the server.

Note
- For Cisco UCS C220 M7, C240 M7, C220 M6, C240 M6, UCS C220 M5,C240 M5, C240 SD M5, C125 M5,C480 M5,C480-M5ML, **Applied fan policy** depends on the PCIe cards present in the server.
- For Cisco UCS C225 M6 and C245 M6, **Applied fan policy** depends on the PCIe cards or a specific CPU type present in the server.

Configuring the Fan Policy

You can determine the right fan policy based on the server configuration and server components.

Before you begin

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

Procedure

Step 1 From the **Apps** drop-down list, select **System**.

Step 2 From the **System** menu, select **Power Management** > **Power Policies**.

Step 3 In the **Power Policies** > **Fan Policies** area on the right pane, click and select the appropriate value from the **Fan Policy** drop-down list.

Name	Description
Fan Policy drop-down list	This can be one of the following: • **Maximum Cooling**—This setting configures the server fans to operate at their highest speeds to provide the maximum possible cooling. • **Balanced**—This setting can cool almost any server configuration, but may not be suitable for servers with PCIe cards as these cards overheat easily. • **Performance**—This setting can be used for server configurations where maximum fan speed is required for high performance. With this setting, the fan speeds run at the same speed or higher speed than that of the fan speed set with the Balanced fan policy. **Note** This option is available only on some C-Series servers. • **Low Power**—This setting is ideal for minimal configuration servers that do not contain any PCIe cards. • **High Power**—This policy is ideal for servers that contain PCIe cards that overheat easily and have high temperatures. • **Maximum Power**—This setting can be used for server configurations that required extremely high fan speeds. This policy is ideal for servers that contain PCIe cards that overheat easily and have very high temperatures. • **Acoustic**—This setting can be used for configuring the fan noise level, thereby enabling noise reduction in the servers. Application of this policy might result in performance throttling impacting system performance. If excessive thermal or performance events are recorded in the event logs, select a standard fan control policy like **Low Power**, which is a non-disruptive change. **Note** This option is available only on Cisco UCS C220 M7 and C240 M7 servers. For Cisco UCS C-Series M7 servers, **Acoustic** is the default fan policy. For all other servers, **Low Power** is the default fan policy.

Name	Description
Applied Fan Policy field	The actual speed of the fan that runs on the server. When the configured fan policy is not in effect, it displays N/A. The configured fan policy takes effect when the server is powered on and the POST is complete. **Note** • For Cisco UCS C220 M7, C240 M7, **Applied Fan Policy** depends on the PCIe cards present in the server.

Configuration Status field	The configuration status of the fan policy. This can be one of the following:
	• SUCCESS —The fan speed set by you matches the actual fan speed that runs on the server.
	• PENDING —The configured fan policy is not in effect yet. This can be due to one of the following:
	  • The server is powered off
	  • The BIOS POST is not complete
	• FAN POLICY OVERRIDE—Overrides the specified fan speed with the actual speed determined by the configuration requirements of the server.
	Note
	For Cisco UCS C220 M7, C240 M7, servers, **Applied Fan Policy** depends on the PCIe cards present in the server.

Enable Aggressive Cooling check-box	Check this option to enable aggressive cooling. **Note** This option is available only on Cisco UCS M7 and M8 servers.

Step 4 Click **Save**.

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 be logged in as an administrator.

Procedure

Step 1 From the **Apps**, select **System**.
Step 2 From the **System** page, select **Inventory**.
Step 3 From the **Inventory** tab, select **Memory**.
Step 4 Select the **Enable/Disable DIMM Block List** toggle button to enable **DIMM Block Listing**.
Step 5 Click **Save**.

After performing Restore Factory Default, DIMM block listing must be enabled, by default.

Configuring BIOS Settings

Configuring BIOS Settings

Before you begin

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

Procedure

Step 1 From the **Apps** drop-down list, select **Compute**.
Step 2 In the **Compute** page, select **BIOS** > **BIOS Tokens**.
Step 3 Refer Managing the Server, on page 23 to update the BIOS settings.

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.

Step 4 Click **Save**.

Entering BIOS Setup

Before you begin

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

Procedure

Step 1 From the **Apps** drop-down list, select **Compute**.
Step 2 In the **Compute** page, select **BIOS** > **BIOS Tokens**.
Step 3 In the **Actions** drop-down list on the right pane, click **BIOS** > **Enter BIOS Setup**.
Step 4 Click **OK** at the prompt.
Enables enter BIOS setup. On restart, the server enters the BIOS setup.

Clearing the BIOS CMOS

Before you begin

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

Procedure

Step 1 From the **Apps** drop-down list, select **Compute**.
Step 2 In the **Compute** page, select **BIOS** > **BIOS Tokens**.
Step 3 In the **Actions** area, click **BIOS** > **Clear BIOS CMOS**.
Step 4 Click **OK** to confirm.
Clears the BIOS CMOS.

Restoring BIOS Manufacturing Custom Settings

Before you begin

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

Procedure

Step 1 From the **Apps** drop-down list, select **Compute**.
Step 2 In the **Compute** page, select **BIOS** > **BIOS Tokens**.
Step 3 In the **Actions** drop-down list, click **BIOS** > **Restore Manufacturing Custom Settings**.
Step 4 Click **Yes** if you wish to reboot the server immediately.
Step 5 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.

Procedure

Step 1 From the **Apps** drop-down list, select **Compute**.
Step 2 In the **Compute** page, select **BIOS** > **BIOS Tokens**.
Step 3 In the **Actions** drop-down list on the right pane, click **Restore Defaults**.
Step 4 Click **Yes** if you wish to reboot the server immediately.
Step 5 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.

Procedure

Step 1 From the **Apps** drop-down list, select **Compute**.

Step 2 In the **Compute** page, select **BIOS** > **BIOS Profiles**.

Step 3 To upload the BIOS profile using a remote server location, in the **Profiles** area on the right pane, click the **Upload** button.

Step 4 To upload the BIOS profile using a remote server location, perform the following steps in the **Profiles** area:

a) Click the **Upload** button.

b) In the **Upload BIOS Profile** dialog box, update the following fields:

Table 56: Remote

Name	Description
Remote button	Select this option when you want to upload a BIOS profile from a remote location.
Server IP/Hostname	Server details from where you want to upload a BIOS profile.

Name	Description
Upload Protocol button	**Note** To comply with Cisco security standards, certain insecure protocols (TFTP, FTP, HTTP) will no longer be supported in upcoming releases. We recommend using secure protocols like SFTP or SCP moving forward. Select 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.
Path and Filename field	File path where BIOS profile resides on the server along with the filename.
Username field	User name for your remote server.
Password field	Password for your remote server.
Upload button	Allows you to upload the BIOS profile.

Step 5 To upload the BIOS profile using a browser client, perform the following steps in the **Profiles** area:

a) Click the **Upload** button.

b) In the **Upload BIOS Profile** dialog box, update the following fields:

Table 57: Local

Name	Description
Local button	Select this option when you want to upload a BIOS profile from your local machine. Click **Browse** and navigate to the BIOS profile that you want to upload.
Upload button	Allows you to upload the BIOS profile.

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.

Procedure

Step 1 From the **Apps** drop-down list, select **Compute**.
Step 2 In the **Compute** page, select **BIOS** > **BIOS Profiles**.
Step 3 Select a BIOS profile from the **BIOS Profile** area and click **Activate**.
Step 4 At the prompt, click **Yes** to activate the BIOS profile.

Deleting a BIOS Profile

Procedure

Step 1 From the **Apps** drop-down list, select **Compute**.
Step 2 In the **Compute** page, select **BIOS** > **BIOS Profiles**.
Step 3 Select a BIOS profile from the **Profiles** area on the right pane and click **Delete**.
Step 4 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.

Procedure

Step 1 From the **Apps** drop-down list, select **Compute**.
Step 2 In the **Compute** page, select **BIOS** > **BIOS Profiles**.
Step 3 Select a BIOS profile from the **Profiles** area on the right pane and click **Take Backup**.
Step 4 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.

Procedure

Step 1 From the **Apps** drop-down list, select **Compute**.

Step 2 In the **Compute** page, select **BIOS** > **BIOS Profiles**.

Step 3 Select a BIOS profile from the **Profiles** area on the right pane and click **Details**.

Step 4 Review the following information in the **Profile Details** window:

Table 58: BIOS Profile Details

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

Procedure

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

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

Step 3 Click the **Secure Boot Certificate Management** tab.

Step 4 From the certificates table, select the certificate, which you wish to view.

Step 5 Click the **View Secure Boot Certificate** icon above the table.

Step 6 **View Secure Boot Certificate** dialog box is displayed.

You can view the following information:

Table 59: 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 60: 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 61: 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.

Field	Description
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

Procedure

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

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

Step 3 Click the **Secure Boot Certificate Management** tab.

Step 4 To upload the boot certificate, click the upload button (+).

Step 5 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 62: 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.

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

Procedure

Step 1 In the **Navigation** pane, click the **Compute** menu.
Step 2 In the work pane, click the **BIOS** tab.
Step 3 Click the **Secure Boot Certificate Management** tab.
Step 4 From the certificates table, select the certificate, which you wish to delete.
Step 5 Click the **Delete Secure Boot Certificate** icon above the table.
Step 6 Click **Yes** to confirm.

Setting Dynamic Front Panel Temperature Threshold

The Dynamic Front Panel Temperature Threshold option allows you to set the upper critical threshold for the front panel temperature sensor.

Procedure

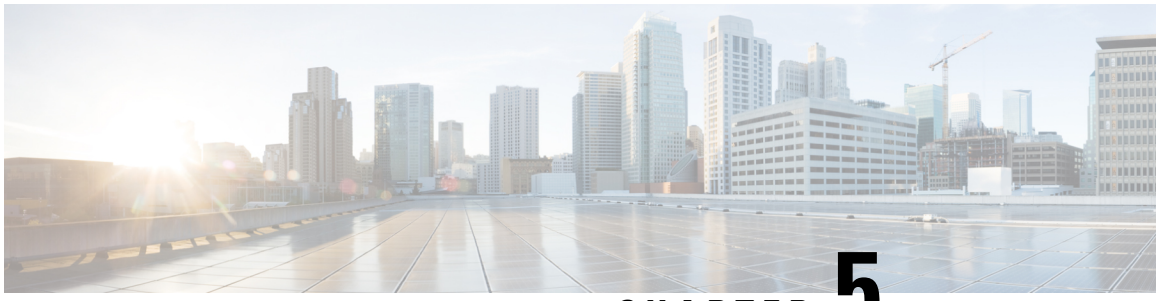
Step 1 From the **Apps** drop-down list, select **System**.
Step 2 In the **System** page, click the **Sensors** tab.
Step 3 In the **Sensors** pane, click the **Temperature** tab.
Step 4 In the **Dynamic Front Panel Temperature Threshold** area in the right pane, enter an upper critical threshold for the front panel temperature sensor in the **Critical** field. You can enter a value between 8 and 50.
Step 5 Click **Save**.

Persistent Memory Modules

Cisco UCS C-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

•
• Viewing Server Utilization, on page 167
• Viewing Server Components - Thermal Performance, on page 168
• Viewing CPU Properties, on page 170
• Viewing Memory Properties, on page 171
• Viewing PCI Adapter Properties, on page 174
• Viewing Storage Properties, on page 176
• Viewing TPM Properties, on page 177
• Viewing PID Catalog , on page 178

Viewing Server Utilization

Procedure

Step 1 From the **Apps** drop-down list, select **Dashboard**.

Step 2 In the **Dashboard Apps** page, under **Quick Actions** area, select **Performance Monitor**.

The **Performance Monitor** page shows information on **Overall Utilization**, **CPU Utilization**, **Memory Utilization**, and **IO Utilization** under **Usage** area.

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

Cisco servers monitor 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 **Usage** area, review the following properties:

Table 63: Server Utilization

Name	Description
Overall Utilization graphical representation	Shows the overall server resources utilization.
CPU Utilization (%)	Shows the overall CPU utilization in percentage.
Memory Utilization (%) graphical representation	Shows the overall DIMM utilization in percentage.
IO Utilization (%) graphical representation	Shows the overall input/output devices utilization in percentage.

Viewing Server Components - Thermal Performance

Beginning with the release 4.3(6), Cisco IMC allows you to view and monitor the thermal performance, such as temperature readings of the various components within the server.

The following temperature threshold parameters are set, by default, for the different components.

These thresholds are crucial for maintaining the balance between performance and safety, ensuring that the server operates efficiently without risking damage due to overheating.

- **Upper Non Recoverable**: This is a temperature limit set, beyond which the server is considered to be in a critical state.

  If the component's temperature exceeds this threshold, it might significantly impact the reliability of the component.

- **Upper Critical**: This threshold represents a temperature level that is higher than normal operating conditions but below the set value for the **Upper Non Recoverable** threshold.

  This threshold serves as a warning sign that the component is nearing unsafe operating temperatures.

Procedure

Step 1 From the **Apps** drop-down list, select **Dashboard**.

Step 2 From the **Dashboard** menu, select **Performance Monitoring** under **Quick Actions**.

Step 3 On the **Thermal** tab, review the following information:

The following table displays the various server components and the different durations over which thermal data is collected and monitored.

Table 64: Thermal Management - Chart Area

Name	Description
Component drop-down list	Allows you to select one of the following components: • Processor • Board • Memory • Add-in Card
Duration drop-down list	Allows you to select one of the following duration data: • Last Ten Minutes • Last One Hour • Last One Day • Last Week • Max Daily

Based on the values you select for the **Component** and **Duration** fields in the above fields, the data for thermal performance is displayed as a chart on the right pane.

Step 4 Based on the values you select for the **Component** and **Duration** fields in the above fields, the data for thermal performance is displayed as a chart on the right pane.

Step 5 View the peak values of the following parameters of the selected server component on the left pane of the page.

Table 65: Peak Values Area

Name	Description
Peak Time	Shows the time period for thermal monitoring in day HH:MM:SS format.
Temperature	Shows the temperature of the different sub-components under the component that you selected.

What to do next

Viewing CPU Properties

Procedure

Step 1 From the **Apps** drop-down list, select **Dashboard**.

Step 2 In the **Dashboard Apps** page, under **Processors & Memory** area, click the value below **CPUs** field.

Step 3 Review the following properties for each CPU:

Note
You can view the same properties from **System Apps** > **Inventory** > **CPUs**

Table 66: Processors

Name	Description
Name column	Processor number in the server.
Architecture column	CPU architecture used in the processor. This can be: • x86 • ARM • SPARC
Model column	Model of the CPU.
PID column	Cisco product ID.
Socket Designation column	The socket in which the CPU is installed.
Vendor column	Vendor for the CPU.

Table 67: Processors / CPU1 / CPU2

Name	Description
State	Overall status of the CPU. This can be: • Good • Fault • Severe Fault
CPU Stepping	
Speed(Mhz)	CPU speed, in megahertz.

Name	Description
Model	Model of the CPU.
Number of Threads	Maximum number of threads that the CPU can process concurrently.
Number of Cores	Number of cores in the CPU.
Number of Cores Enabled	Number of cores enabled out of the total cores.
Architecture	CPU architecture used in the processor. This can be: • x86 • ARM • SPARC
Socket Designation	The socket in which the CPU is installed.
Vendor	Vendor for the CPU.
Part Number	Vendor part number of the CPU.
PID	Cisco part number of the CPU.
Description	Additional vendor and CPU information.

Viewing Memory Properties

Procedure

Step 1 From the **Apps** drop-down list, select **Dashboard**.

Step 2 In the **Dashboard Apps** page, under **Processors & Memory** area, click the value below **Memory Capacity (MB)** field.

Step 3 In the **Memory Summary** area, click the drop-down arrow to view the status of memory installation.

Step 4 Choose the installation option for which you want to view the properties.

Step 5 In the **Memory Summary** area, review the following information about memory:

Note
You can view the same properties from **System Apps** > **Inventory** > **Memory**

Table 68: Memory Summary

Name	Description
Overall DIMM Status	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.
Memory Speed	The memory speed, in megahertz.
Total Memory	The total amount of memory available on the server if all DIMMs are fully functional.
Effective Memory (MB)	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	The amount of memory used for redundant storage.
Failed Memory	The amount of memory that is currently failing, in megabytes.
Ignored Memory	The amount of memory currently not available for use, in megabytes.
Number of Ignored DIMMs	The number of DIMMs that the server cannot access.
Number of Failed DIMMs	The number of DIMMs that have failed and cannot be used.
Memory RAS Possible	Details about the RAS memory configuration that the server supports

Name	Description
Memory Configuration	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.
Enable/Disable DIMM Block List toggle button	Check this option to enable DIMM block listing. **Note** After **Restore Factory Default** is performed, DIMM blocklisting should be enabled, by default.
Location column	DIMM location in the server.
Type column	The type of memory used in the device.
PID column	Cisco DIMM part number.
Serial column	The serial number of the DIMM.
Capacity (MB) column	The size of the DIMM.
Clock Speed (Mhz) column	The speed at which DIMM operates.

Step 6 To view the details of each DIMM, click the desired DIMM from the list.

Memory / DIMM_location page is displayed.

Step 7 In the **Memory / DIMM_location** page, review the following properties:

Table 69: Memory / DIMM_location

Name	Description
State	Shows whether the DIMM is enabled or disabled. By default, all installed DIMMs are typically enabled.
Capacity (MB)	The size of the DIMM.
Memory Type	The type of memory used in the device.

Name	Description
Channel Type	The type of memory channel.
Clock Speed (Mhz)	The speed at which the DIMM operates, typically set to the maximum supported speed for the installed DIMMs and compatible with the system.
Data Width (Bits)	The amount of data the DIMM supports, in bits.
Manufacturer	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	The serial number of the DIMM.
Part Number	The part number for the DIMM assigned by the vendor.
PID	Cisco DIMM part number.
Bank Locator	The location of the DIMM within the memory bank.
Memory Type Detail	The type of memory used in the device.
Visibility	Whether the DIMM is available to the server.
Operability	Whether the DIMM is currently operating correctly.
Description	Additional description about the DIMM.

Viewing PCI Adapter Properties

Before you begin

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

Procedure

Step 1 From the **Apps** drop-down list, select **System**.

Step 2 Select the **Inventory** tab.

Step 3 From the Navigation pane, select **PCIe Devices**.

Step 4 From the drop-down list, select the type of adatper which you wish to see.

Following options are available:

- All
- Storage
- Cisco VIC Adapters
- Network Adapters

  Beginning with the release 4.3(5.240021), you can view the properties of DPUs that are listed under **Network Adapters**.
- GPU

Step 5 You can view the following properties

Name	Description
ID column	The PCIe Device ID.
Name column	The name of the adapter.
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.

Name	Description
MAC Address	MAC Address of the Intel(R) Network Controller **Note** This field is displayed only for Intel(R) Network Controller.

Viewing Storage Properties

Before you begin

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

Procedure

Step 1 From the **Apps** drop-down list, select **Dashboard**.

Step 2 In the **Storage** area, review the following information:

Table 70: Storage Area

Name	Description
Controllers	Number of RAIDs available.
Capacity Available to OS	Storage space available to the installed OS in gigabytes.
Physical Drives	Total number of physical drives available in the server.
Virtual Drives	Total number of virtual drives available.

Step 3 Under the **Controllers**, click the number to view the following Storage Adapter properties:

Table 71: Storage Adapters

Name	Description
PCI Slot column	PCI slot in which the controller drive is located.
Name column	Name of the controller.
Firmware Version column	The active firmware package version number.
Serial Number column	The serial number of the storage controller.

Step 4 Under the **Physical Drives**, click the number to view the following Physical Drives properties:

Table 72: Physical Drives

Name	Description
Controllers column	Name of the RAID Controller.
Physical Drives column	Total number of physical drives available.
Total Capacity (GB) column	Total capacity of the physical disk present in the server.

Step 5 Under the **Virtual Drives**, click the number to view the following Virtual Drive properties:

Table 73: Virtual Drives

Name	Description
Controllers column	Name of the RAID Controller.
Virtual Drives column	Total number of virtual drives available.
Total Capacity (GB) column	Displays the total capacity of the virtual dirves.

Viewing TPM Properties

Procedure

Step 1 From the **Apps** drop-down list, select **System**.

Step 2 Select the **Inventory** tab.

Step 3 From the Navigation pane, select **TPM**.

Step 4 You can view the following properties:

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.

Name	Description
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.
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 PID Catalog

Procedure

Step 1 From the **Apps** drop-down list, select **System**.

Step 2 Select the **Inventory** tab.

Step 3 From the Navigation pane, select **PID Catalog**.

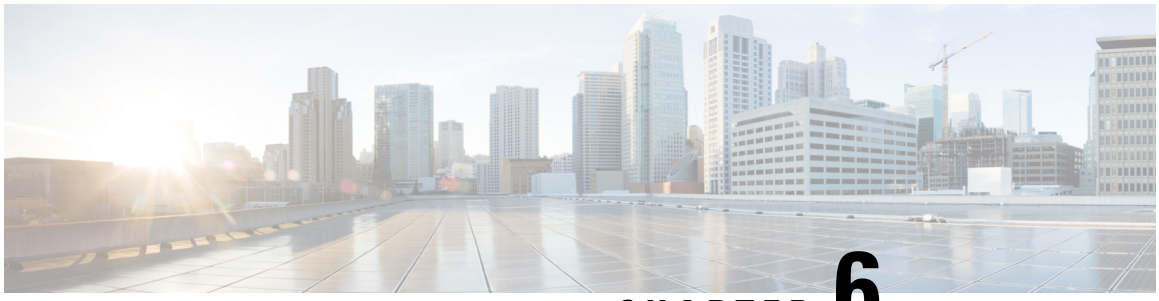
Step 4 You can view the following properties:

Table 74: PID Catalog Status

Name	Description
Upload Status	The upload status of the PID catalog. The value can be any of the following: • Upload in Progress • Upload Successful • Upload Error — TFTP File Not Found • Upload Error — Connection Failed • Upload Error — Access Denied • Upload Error — File Not Found • Upload Error — Download Failed • Activation Successful • Error — Unknown • N/A
Activation Status	Displays the PID catalog activation status.
Current Activated Status	Displays the current activated PID catalog.

Table 75: PID Catalog Detail

Name	Description
PCI Slot field	Slot where the PCIe device is located.
Vendor field	The vendor for the PCIe device.
Product ID field	The product ID for the PCIe device.
Description field	The model number of the PCIe device.



CHAPTER 6

Vewing Sensors

- Viewing Temperature Sensors, on page 181
- Viewing LED Sensors, on page 182
- Viewing Storage Sensors, on page 182
- Viewing Power Supply Sensors, on page 183
- Viewing Fan Sensors, on page 184

Viewing Temperature Sensors

Procedure

Step 1 From the **Apps** drop-down list, select **System**.

Step 2 Select the **Sensors** tab.

Step 3 From the Navigation pane, select **Temperature**.

Step 4 Review the following properties:

Name	Description
Name field	The name of the temperature sensor.
Status	The working status of the temperature sensor.
Temperature field	The current temperature, in Celsius/Fahrenheit.
Critical Threshold Min field	The minimum critical threshold.
Critical Threshold Max field	The maximum critical threshold.
Non-Recoverable Threshold Min field	The minimum non-recoverable threshold.
Non-Recoverable Threshold Max field	The maximum non-recoverable threshold.

Viewing LED Sensors

Procedure

Step 1 From the **Apps** drop-down list, select **System**.

Step 2 Select the **Sensors** tab.

Step 3 From the Navigation pane, select **LEDs**.

Step 4 Review the following properties:

Name	Description
Name column	The name of the sensor.
Status column	Whether the LED is on, blinking, or off.
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

Procedure

Step 1 From the **Apps** drop-down list, select **System**.

Step 2 Select the **Sensors** tab.

Step 3 From the Navigation pane, select **Storage**.

Step 4 Review the following properties:

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

Name	Description
LED Status field	The current LED color, if any. To make the physical LED on the storage device blink, select **Turn On** from the drop-down list. To let the storage device control whether the LED blinks, select **Turn Off**. **Note** This information is only available for some C-Series servers.

Viewing Power Supply Sensors

Procedure

Step 1 From the **Apps** drop-down list, select **System**.

Step 2 Select the **Sensors** tab.

Step 3 From the Navigation pane, select **Power Supply**.

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

Name	Description
Name field	The name of the power supply device.
Type field	The type of the power supply device.
Status	The working status of the power supply device.
Reading field	The current power usage, in watts.
Critical Threshold Min field	The minimum critical threshold.
Critical Threshold Max field	The maximum critical threshold.
Non-Recoverable Threshold Min field	The minimum non-recoverable threshold.
Non-Recoverable Threshold Max field	The maximum non-recoverable threshold.

Viewing Fan Sensors

Procedure

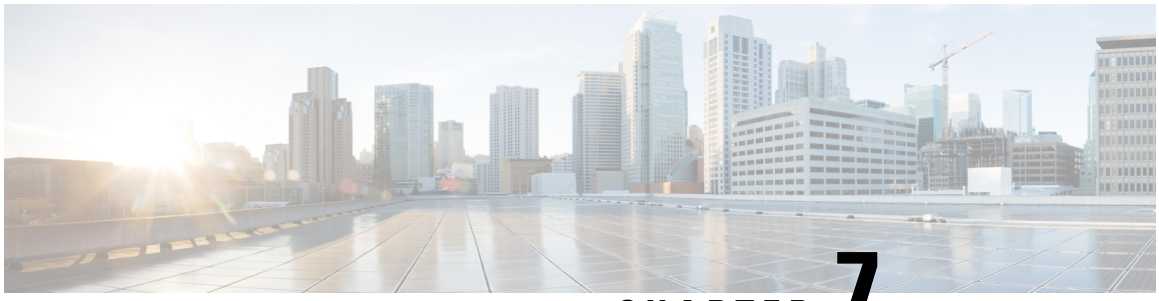
Step 1 From the **Apps** drop-down list, select **System**.

Step 2 Select the **Sensors** tab.

Step 3 From the Navigation pane, select **Fan**.

Step 4 Review the following sensor properties for the fan:

Name	Description
Name field	The name of the fan.
Status	The working status of the fan.
Reading field	The current power usage, in watts.
Non-Recoverable Threshold Min field	The minimum non-recoverable threshold.
PWM (%)	The Pulse Width Modulation (PWM) is the absolute measure of the fan on and off duration to control the speed. The ratio of on time compared to off time is known as **Duty cycle**.
Non-Recoverable Threshold Max field	The maximum non-recoverable threshold.



CHAPTER 7

Managing Remote Presence

•
• Configuring Serial Over LAN, on page 185
• Configuring Virtual Media, on page 186
• Virtual KVM Console, on page 194
• Launching KVM Console, on page 194
• Virtual KVM Console - Cisco UCS C-Series M6 and Later Servers, on page 195
• Configuring the Virtual KVM, on page 207

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.

Before you begin

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

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 In the **Navigation** pane, click **Communication Services** menu.

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

Table 76: Serial over LAN Area

Name	Description
Enabled toggle button	Allows you to enable/disable Serial over LAN (SoL) 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.
SSH Port filed	The port through which you can access Serial over LAN directly. The port enables you to by-pass the Cisco IMC shell to provide direct access to SoL. The valid range is 1024 to 65535. The default value is 2400. **Note** Changing the SSH Port setting disconnects any existing SSH sessions.

Step 4 Click **Save**.

Configuring Virtual Media

Before you begin

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

Procedure

Step 1 From the **Apps** drop-down list, select **Compute**.

Step 2 In the **Navigation** pane, click **Remote Management** menu.

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

Table 77: Properties Area

Name	Description
Enable Virtual KVM toggle button	Allows you to enable or disable virtual KVM.
Max Sessions drop-down list	The maximum number of concurrent vKVM sessions allowed. You can select any number between 1 and 4.
Remote Port field	The port used for vKVM communication.
Active Sessions	The number of vKVM sessions running on the server.
Enable Virtual Media toggle button	If checked, the server encrypts all video information sent through the vKVM.
Enable Local Server Video toggle button	If checked, the vKVM session is also displayed on any monitor attached to the server.
Lower Power USB Enabled toggle button	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. But, while mapping an ISO to a server that has a UCS VIC P81E card and the NIC is in Cisco Card mode, this option must be disabled for the virtual drives to appear on the boot selection menu.
Active Virtual Media Sessions	Displays the active virtual media sessions.

Creating a Cisco IMC Mapped vMedia Volume

Before you begin

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

Procedure

Step 1 From the **Apps** drop-down list, select **Compute**.

Step 2 In the **Navigation** pane, click **Remote Management** menu.

Step 3 In the **Virtual Media Mapping** area, click **Add New Mapping**.

Step 4 In the **Add Virtual Media** dialog box, update the following fields:

Name	Description
Virtual Media Type radio button	This is can be one of the following: • CDD • HDD
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.
File Location 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 5 Click **Save**.

Viewing Cisco IMC-Mapped vMedia Volume Properties

Before you begin

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

Procedure

Step 1 From the **Apps** drop-down list, select **Compute**.

Step 2 In the **Navigation** pane, click **Remote Management** menu.

Step 3 In the **Virtual Media Mapping** area, select a row from the mapping table.

Step 4 Click **Properties** and review the following information:

Table 78: Virtual Media Mapping

Name	Description
Add New Mapping button	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.
Remap button	Remaps the saved mapping.
Delete button	Deletes the saved mapping.
Volume column	The identity of the image.
Protocol column	Image protocol.
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.
Mapping Status	The status of the last mapping attempted.

Removing a Cisco IMC-Mapped vMedia Volume

Before you begin

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

Procedure

Step 1 From the **Apps** drop-down list, select **Compute**.
Step 2 In the **Navigation** pane, click **Remote Management** menu.
Step 3 In the **Virtual Media Mapping** area, select a row from the mapping table.
Step 4 In the **Virtual Media Mapping** area, click **Unmap**.

When you are prompted to save the mapping, click **Save**.

Remapping an Existing Cisco IMC vMedia Image

Before you begin

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

Procedure

Step 1 From the **Apps** drop-down list, select **Compute**.
Step 2 In the **Navigation** pane, click **Remote Management** menu.
Step 3 In the **Virtual Media Mapping** area, select a row from the mapping table.
Step 4 Click **Remap**.

Deleting a Cisco IMC vMedia Image

Before you begin

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

Procedure

Step 1 From the **Apps** drop-down list, select **Compute**.
Step 2 In the **Navigation** pane, click **Remote Management** menu.
Step 3 In the **Virtual Media Mapping** area, select a row from the mapping table.

Step 4 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.

Launching KVM Console

You can launch the KVM console from either the **Dashboard App** or **Actions**.

Procedure

Step 1 From the **Apps** drop-down list, select **Dashboard**.

Step 2 From the **KVM Console**, click the **Launch KVM** button.

Step 3 Alternatively, you can launch **KVM Console** from any page from **Actions** > **System** > **Launch KVM**.

Virtual KVM Console - Cisco UCS C-Series M6 and Later Servers

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.

Console Menu

Menu Item	Description
KVM	Selects KVM (Keyboard Video and Mouse) as the active console.
SOL	Selects SOL (Serial Over LAN) as the active console. **Note** **SOL** is not visible if SOL is inactive, instead **Activate SOL** is visible.
Activate SOL	Allows you to login to SOL session using user name and password. **Note** **Activate SOL** option is visible only when SOL session is not active for any reason.

File Menu

Menu Item	Description
Paste Clipboard Text	Opens the **Paste Clipboard Text** dialog box that allows you to paste content.
Paste Clipboard Text dialog box	**Paste Clipboard Text** dialog box has the following options: • **Settings** button—Opens the Settings dialog box. See Table 79: Settings dialog box, on page 196 for more information. • **Enter Text to Paste** field • **Send** button—Sends the text.
Capture to File	Opens the **Save** dialog box that allows you to save the current screen as a PNG image.

Table 79: Settings dialog box

Name	Description
When an unsupported character is found in pasted text: drop-down list	Allows you to select an action when an unsupported character is found in pasted text: • Ignore all unsupported characters—Ignores all the unsupported characters in the text. • Cancel the paste operation—Cancels the send operation. • Replace the character(s) with a mapped value—If the character is not mapped, opens the **Unsupported Character** dialog box. • Ask what to do with character—Opens the **Unsupported Character** dialog box.
Character Mapping button	**Character Mapping** button—Opens the sub-menu to edit/delete character mappings. Character mappings replace the unsupported character with a user-defined string (no character length).
Keyboard drop-down list	Layout of the keyboard being used to paste characters. This should be the same as the keyboard layout of the host.
Save button	Saves the configuration. **Note** This option is enabled only when the setting is updated.

Table 80: Unsupported Character dialog box

Option	Description
Character context	Group of 11 characters where the unsupported character is found. Five characters before and five characters after the unsupported character. However, more characters from before or after the unsupported character are pulled if enough characters after or before are not available to make 11 characters.

Option	Description
Choose what to do with the unsupported character drop-down list	Allows you to select one of the following actions: • Ignore the character(s)—Provides additional options to determine unsupported character(s) to ignore. • Cancel the paste operation—Cancels the operation. Replace the character(s)—Provides additional options to determine what to replace the unsupported character(s) with.
Replacement field	**Note** This option is visible only for **Replace the character(s)** option. Enter a replacement character.
Store a mapping of this replacement to the unsupported character check box	**Note** This option is visible only for **Replace the character(s)** option. Allows you to save the character mapping.
Repeat this action for all *unsupported_character* characters check box	Repeats the selected action for all instances of the unsupported character being evaluated.
Repeat this action for all unsupported characters check box	**Note** This option is not visible only for **Cancel the paste operation** option. Allows you to save the same action for the same unsupported character.

View Menu

Menu Item	Description
Refresh	Updates the console display with the current video output of the server. **Note** This option is supported only in KVM console.

Menu Item	Description
Video Quality	You can select one of the following from the sub-menu: • **High** • **Medium** • **Low** • **Ultra Low** **Note** This option is supported only in KVM console.
Clear SOL Console	Clears the Cisco SOL terminal. **Note** This option is supported only in SOL console.
Full Screen	Expands the vKVM console so that it fills the entire screen.

Macro menu

Note **Macro** menu is supported only in KVM console.

Menu Item	Description
Static Macros	Displays a predefined set of macros sub-menu.
User Defined Macros	Displays a user defined set of macros sub-menu.

Menu Item	Description
Manage	Opens the **Manage Macros** dialog box, which allows you to add, delete, edit macros; restore the predefined set of macros; and assign hotkey to a macro.
	To create a new macro, click **Macros** > **Manager Macros** > **Create New Macro** Opens the **Create New Macro** dialog box. • **Enter keystrokes for new user defined macro**—Enter the desired key(s). • **Special Characters** drop-down list—Select the desired special character and click **Add**. • **Create** button—Save the new macro.
	To restore predefined set of macros, click **Macros** > **Manager Macros** > **Restore Static Macros**.

Tools Menu

Menu Item	Description
Stats	

Menu Item	Description

	Opens the **Stats** dialog box:
	KVM Stats:
	• **Total Bytes Rec**—Total bytes received.
	• **Total Bytes Sent**—Total bytes sent.
	• **Rx Bandwidth**—Received bandwidth measured in the number of KBs per second.
	• **Tx Bandwidth**—Transmitted bandwidth measured in the number of KBs per second.
	• **Frame Rate**—Frame rate measured in the number of frames per second.
	• **Video Tile Rate**—Video tiles rendered per second.
	When vMedia is activated, the **vKVM-Mapped vMedia Stats** area displays the following:
	• **Total Bytes Rec**—Total bytes received.
	• **Total Bytes Sent**—Total bytes sent.
	• **Device**—The type of local device.
	• **Mapped File**—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 read from the vKVM media.
	• **Write Bytes**—The number of bytes written to the vKVM media.
	• **Owner**—The user who mapped the media to the browser.
	CIMC-Mapped vMedia Stats area displays the following:
	• **Device**—The type of local device.
	• **Mapped File**—The type of local device or image file to which the host server device is mapped.
	• **Device Status**—Possible device status:
	  • device mount in progress
	  • device mounted

Menu Item	Description
	• device eject in progress • ejected from host Following are the error status • mount failed • unmount failed • connection timed out • file server rejected connection • file server rejected credentials • file server path not found • file not found • file(s) still in use • open file as read only failed • open file as read/write failed • file input/output failed • HTTP server did not return content length • HTTP server does not support range request • invalid parameters • invalid device usage • invalid device type
Session User List	Opens the **Session User List** dialog box that shows all the user IDs that have an active vKVM session. The same can be accessed from the **Session User List** icon on top.
Keyboard	Displays the virtual keyboard for the vKVM console, which you can use to input data. **Note** This option is supported only in SOL console.
USB Reset	Provides you an option to reset keyboard, mouse, and virtual media. **Note** Resetting any USB connection affects all the input to the server including virtual media, keyboard, and mouse.

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	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	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	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	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. **Note** **Create Image** option is not available in Safari browser.

Name	Description
Activate vMedia	Allows you to login to vMedia session using user name and password. **Note** **Activate vMedia** option is visible only when vMedia session is not active for any reason. If **Activate vMedia** otion is visible, other vMedia options are not displayed.
vKVM-Mapped vDVD	Opens the **Map Virtual Media - CD/DVD** dialog box, which allows you to select an ISO image from your local computer and map the drive. **Note** Virtual Media is not available for read-only users.
vKVM-Mapped vHDD	Opens the **Map Virtual Media - Removable Disk** dialog box, which allows you to select an ISO image from your local computer and map the drive. **Note** Virtual Media is not available for read-only users.
vKVM-Mapped vFDD	Opens the **Map Virtual Media - Floppy Disk** dialog box, which allows you to select an ISO image from your local computer and map the drive. **Note** Virtual Media is not available for read-only users.
CIMC-Mapped vDVD	Opens the **Map Virtual Media - CD/DVD** dialog box, which allows you to select an ISO image from your local computer and map the drive. It also allows you to save, edit, and delete mappings. For more information on mount options, see Table 81: Add New Mapping Dialog Box, on page 205. **Note** Virtual Media is not available for read-only users.
CIMC-Mapped vHDD	Opens the **Map Virtual Media - CD/DVD** dialog box, which allows you to select an ISO image from your local computer and map the drive. It also allows you to save, edit, and delete mappings. For more information on mount options, see Table 81: Add New Mapping Dialog Box, on page 205. **Note** Virtual Media is not available for read-only users.

Table 81: Add New Mapping Dialog Box

Name	Description
Name field	User defined name of the virtual media.
NFS button	Network File System based mapping.
CIFS button	Common Internet File System based mapping.
HTTP/S	HTTP-based or HTTPS-based mapping.
File Location field	Location of the .iso file in the following format: • *<IP Address or DNS Name>*[:*Port*]/*.iso file path*
Username field	**Note** Available only for **CIFS** and **HTTP/S** based mappings. The username, if any.
Password field	**Note** Available only for **CIFS** and **HTTP/S** based mappings. The password for the selected username, if any.

Mount Options field	**Note**
	Available only for **CIFS** and **NFS** based mappings.
	
	The selected mount options.
	• NFS—For NFS, either leave the field blank or enter one or more of the following:
	  • wsize=VALUE
	  • vers=VALUE
	  • timeo=VALUE
	  • retrans=VALUE
	  • retry=VALUE
	  • rsize=VALUE
	• For CIFS, either leave the field blank or enter one or more of the following:
	  • nounix
	  • noserverino
	  • sec=VALUE
	  • vers=VALUE

Name	Description
Auto-remap check box	Cisco IMC automatically remaps the device when the host system ejects the media.
Stored vMedia button	Opens an additional area on the right to select stored vMedia from the respective list.
Save button	Saves the vMedia.
Map Drive button	Saves and maps the mounted vMedia.
CD/DVD panel	Provides a list of stored vMedia. If you are mapping using **CIMC-Mapped vDVD** option, then you can also edit or delete any vMedia from this list.
Removable Disk panel	Provides a list of stored vMedia. If you are mapping using **CIMC-Mapped vHDD** option, then you can also edit or delete any vMedia from this list.

Chat Menu

Menu Item	Description
Chat	Opens the **Chat** box to communicate with other users.

Help Icon

Name	Description
Take a Site Tour	Provides a quick interactive tour of the new console.
Help Topics	Clicking this option brings you back to this window.
About	Displays the version number of the Cisco vKVM console.

Language Icon

Shows a drop-down list of the supported languages. You can select desired language from the list.

Profile Menu Icon

The **Profile Menu** icon is located on the top right hand corner of the console.

Name	Description
Role	Displays your user role name.
Server	Displays the host name or IP address.

Name	Description

Settings	Opens the **Settings** dialog box:
	• **Maintain Aspect Ratio** toggle—Maintains the aspect ratio of the viewer window.
	• **Mouse Mode**
	  • **Absolute Positioning**—Cursor position in the view mirrors the local machine cursor position.
	  • **Relative Positioning**—Cursor position in the view is calculated relative to the previous position.
	• **Video Inactivity Timeout** drop-down list—Allows you to select preset time period or inactivity on the console after which the console video times out.
	• **Number of terminal scrollback lines** field—Allows you to configure the number of lines which can be scrolled for Cisco SOL terminal.
	• **Theme**—Allows you to toggle between dark and light theme.
	• **Save** button—Saves the settings for all users.

Sign Out	Signs out and closes the vKVM console.

Configuring the Virtual KVM

Before you begin

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

Procedure

Step 1 From the **Apps** drop-down list, select **Compute**.

Step 2 In the **Navigation** pane, click **Remote Management** menu.

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

Table 82: Properties Area

Name	Description
Enable Virtual KVM toggle button	Allows you to enable or disable virtual KVM.
Max Sessions drop-down list	The maximum number of concurrent vKVM sessions allowed. You can select any number between 1 and 4.
Remote Port field	The port used for vKVM communication.
Active Sessions	The number of vKVM sessions running on the server.
Enable Virtual Media toggle button	If checked, the server encrypts all video information sent through the vKVM.
Enable Local Server Video toggle button	If checked, the vKVM session is also displayed on any monitor attached to the server.
Lower Power USB Enabled toggle button	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. But, while mapping an ISO to a server that has a UCS VIC P81E card and the NIC is in Cisco Card mode, this option must be disabled for the virtual drives to appear on the boot selection menu.
Active Virtual Media Sessions	Displays the active virtual media sessions.

Enabling the Virtual KVM

Before you begin

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

Procedure

Step 1 From the **Apps** drop-down list, select **Compute**.

Step 2 In the **Navigation** pane, click **Remote Management** menu.

Step 3 In the **Properties** area, check the **Enabled Virtual KVM** check box.

Disabling the Virtual KVM

Before you begin

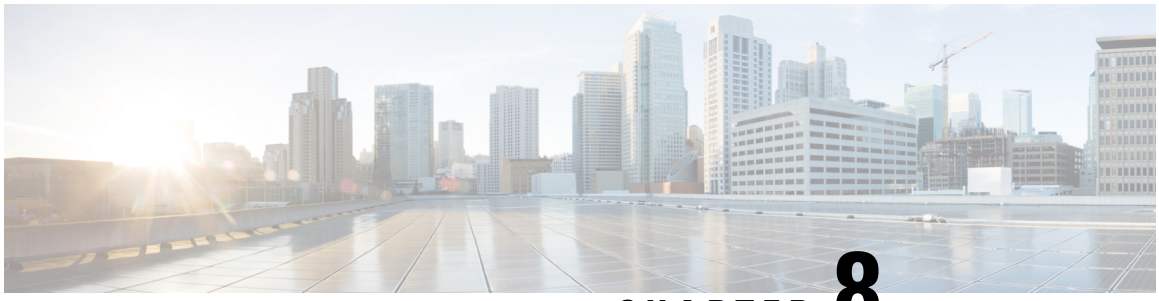
You must log in as a user with admin privileges to enable the virtual KVM.

Procedure

Step 1 From the **Apps** drop-down list, select **Compute**.

Step 2 In the **Navigation** pane, click **Remote Management** menu.

Step 3 In the **Properties** area, uncheck the **Enabled Virtual KVM** check box.



CHAPTER 8

Managing User Accounts

•
• Adding Local Users for Cisco UCS C-Series M7 and Later Servers, on page 211
• Modifying Local Users for Cisco UCS C-Series M7 and Later Servers, on page 214
• Managing SSH Keys in User Accounts, on page 218
• Password Expiry, on page 223
• Changing Password as a Non-Admin User, on page 225
• Configuring Account Lockout Details, on page 226
• Configuring User Authentication Precedence, on page 227
• Resetting User Credentials to Factory Default Values, on page 227
• LDAP Servers, on page 228
• LDAP Certificates Overview, on page 235
• TACACS+ Authentication, on page 239
• Viewing and Terminating User Sessions, on page 241

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.

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 In the **Navigation** pane, click **User Management** menu.

Step 3 Select the **User Management** tab.

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

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

Table 83: User Name and Role

Name	Description
User Name field	Enter a 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.

Role Played drop-down list	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
	  • 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.

Enabled toggle button	If checked, the user is enabled on the Cisco IMC.
CIMC/IPMI/SNMP toggle buttons	You may create the following types of user: • CIMC • SNMP • IPMI

Table 84: CIMC

Name	Description
Password field	Enter a suitable password. To know more about password requirements, hover the cursor over **?** icon beside the **Suggest** button.

Name	Description
Confirm Password field	The password repeated for confirmation.
Suggest button	You may use this option for a system generated password.

Table 85: IPMI

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 86: SNMP

Name	Description
Security Level drop-down list	**Note** In alignment with Cisco security policy, SNMP v3 without Authentication+Privacy (authPriv) is considered insecure and will not be supported in upcoming releases. Please enable **auth, priv**. 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 list	The authorization type. This can be one of the following: • **HMAC_SHA96** • **HMAC128_SHA224** • **HMAC192_SHA256** • **HMAC256_SHA384** • **HMAC384_SHA512**

Name	Description
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 list	The privacy type. This can be one of the following: • **CFB128_AES128** • **CFB128_AES192** • **CFB128_AES256**
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	The authorization password again for confirmation purposes.

Step 6 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.

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 In the **Navigation** pane, click **User Management** menu.

Step 3 Select the **User Management** tab.

Step 4 To modify a local user account, click a row and click **Modify User**.

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

Table 87: User Details

Name	Description
ID	System assigned user ID. You cannot edit this ID
User Name field	Enter a 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.

Role Played drop-down list	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
	  • 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.

Host Account field	This field is set to **No**, by default. When the bootstrap user is created using the Redfish API interface on the host, the **Host Account** field is set to **Yes** automatically.
Enabled toggle button	If checked, the user is enabled on the Cisco IMC.

Name	Description
CIMC/IPMI/SNMP toggle buttons	You may create the following types of user: • CIMC • SNMP • IPMI **Note** You cannot uncheck the default user type for the user, which you are modifying.
Change Password toggle button	Allows you to change the local user password. **Note** CIMC, IPMI, or SNMP properties are visible only when **Change Password** is enabled.

Table 88: CIMC

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 89: IPMI

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 90: SNMP

Name	Description
Security Level drop-down list	**Note** In alignment with Cisco security policy, SNMP v3 without Authentication+Privacy (authPriv) is considered insecure and will not be supported in upcoming releases. Please enable **auth, priv**. 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 list	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 list	The privacy type. This can be one of the following: • **CFB128_AES128** • **CFB128_AES192** • **CFB128_AES256**

Name	Description
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	The authorization password again for confirmation purposes.

Step 6 Click **Save**.

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.

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 In the **Navigation** pane, click **User Management** menu.

Step 3 Select the **User Management** tab.

Step 4 To view the details of the SSH keys for an account, select the a row in the pane and click **SSH Keys**.

The **SSH Keys** window is displayed.

Step 5 In the **SSH Keys** window, view the following properties:

Table 91: SSH Keys

Name	Description
ID checkbox	Allows you to select the SSH key.
Comment column	Displays the content describing the key.
Key column	Displays the key text.
Add icon	Allows you to add new SSH key. Check the **ID** checkbox for an empty SSH key row and click **Add**. You can then paste the key or upload a key from local or remote location.
Edit icon	Allows you to edit the SSH key. Check the **ID** checkbox for SSH key, which you wish to edit. Click the edit icon. You can then paste the key or upload a key from local or remote location.
Delete icon	Allows you to delete the SSH key. Click **OK** to proceed.

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.

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 In the **Navigation** pane, click **User Management** menu.

Step 3 Select the **User Management** tab.

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

The **SSH Keys** window is displayed.

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

Note
Add Keys icon is activated only for empty slots.

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

Step 7 Use one of the following information to upload the key:

Table 92: Paste

Name	Description
Paste SSH Key field	Allows you to copy the entire content of the key and paste it in the Paste text field.
Upload button	Allows you to upload the key.

Table 93: Local

Name	Description
Browse button	Click **Browse** and navigate to the key that you want to upload.
Upload button	Allows you to upload the key.

Table 94: Remote

Name	Description
Server IP/Hostname field	Server details from where you want to upload the key.
Upload Protocol button	**Note** To comply with Cisco security standards, certain insecure protocols (TFTP, FTP, HTTP) will no longer be supported in upcoming releases. We recommend using secure protocols like SFTP or SCP moving forward. Select 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. To comply with Cisco security standards, certain insecure protocols (TFTP, FTP, HTTP) will no longer be supported in upcoming releases. We recommend using secure protocols like SFTP or SCP moving forward.

Name	Description
Path and Filename field	File path where the key file resides on the server along with the filename.
Username field	User name for your remote server.
Password field	Password for your remote server.
Upload button	Allows you to upload the 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.

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 In the **Navigation** pane, click **User Management** menu.

Step 3 Select the **User Management** tab.

Step 4 To modify an SSH keys for an account, select the a row in the 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 **Edit Keys** icon in the **SSH Keys** window to edit the SSH key.

Step 7 Use one of the following information to upload the key:

Table 95: Paste

Name	Description
Paste SSH Key field	Allows you to copy the entire content of the key and paste it in the Paste text field.
Upload button	Allows you to upload the key.

Table 96: Local

Name	Description
Browse button	Click **Browse** and navigate to the key that you want to upload.
Upload button	Allows you to upload the key.

Table 97: Remote

Name	Description
Server IP/Hostname field	Server details from where you want to upload the key.
Upload Protocol button	**Note** To comply with Cisco security standards, certain insecure protocols (TFTP, FTP, HTTP) will no longer be supported in upcoming releases. We recommend using secure protocols like SFTP or SCP moving forward. Select 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. To comply with Cisco security standards, certain insecure protocols (TFTP, FTP, HTTP) will no longer be supported in upcoming releases. We recommend using secure protocols like SFTP or SCP moving forward.
Path and Filename field	File path where the key file resides on the server along with the filename.
Username field	User name for your remote server.
Password field	Password for your remote server.
Upload button	Allows you to upload the 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.

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 In the **Navigation** pane, click **User Management** menu.

Step 3 Select the **User Management** tab.

Step 4 To delete an SSH keys for an account, select the a row in the 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.

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

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.

Enabling and Configuring Password Expiry Duration

Before you begin

You must enable password expiry.

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 In the **Navigation** pane, click **User Management** menu.

Step 3 From the **Actions** drop-down list, select **User Management** > **Password Expiration Details**.

Password Expiration Details dialog box is displayed.

Step 4 In the **Password Expiration Details** dialog box, update the following properties:

Table 98: Password Expiration Details

Name	Description
Enable Password Expiry toggle button	Allows you to enable or disable the password expiry duration
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.
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.
Reset button	Allows you to reset the values.

Name	Description
Restore Defaults button	Allows you to restore factory default settings.

Step 5 Click **Save Changes**.

Changing Password as a Non-Admin User

Before you begin

You must log in as a non-admin user to change password.

Procedure

Step 1 From the right upper corner of the Cisco IMC GUI, click **Cisco IMC info** panel.

Step 2 From the **Cisco IMC info** panel, click **Reset**.

Note
This option is available only for non-admin user.

Change password dialog box is displayed.

Step 3 In the **Change password** dialog box, update the following properties:

Table 99: Change Password

Name	Description
User Name field	Displays the user name. You cannot edit this field.
User Type toggle button	Displays the user type. If you disable this, you cannot edit the password.
Current Password field	Enter the current password.
New Password field	Enter the new password.
Confirm New Password field	Enter the new password again.
Save button	Click to save the new password.

Configuring Account Lockout Details

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 In the **Navigation** pane, click **User Management** menu.

Step 3 From the **Actions** drop-down list, select **User Management** > **Account Lockout Details**.

Account Lockout Details dialog box is displayed.

Step 4 In the **Account Lockout Details** dialog box, update the following properties:

Table 100: Account Lockout Details

Name	Description
Allowed Attempts field	Allows you to set the maximum number of allowed failed login attempts due to incorrect password. 0 is the default value (Disabled). Enter an integer between 0 and 20.
Lockout Period field	Allows you to set the time in minutes for which you will be locked out. This happens when you exceed the allowed number of login attempts. 0 is the default value (Disabled). Enter an integer between 0 and 60.
Disable User on Lockout toggle button	When the **Disable User on Lockout** check box is selected, the user account is disabled on lockout. **Note** **Disable User on Lockout** is not applicable for default user (admin).

Beginning with the release 6.0, the number of attempts remaining to enter the passoword is not displayed anymore when the user tries to login to Cisco IMC. Also the message that the account is locked is also not displayed anymore during the login. The administrator can refer the IMC audit log to know about the number of attempts and the details of the locked account.

Configuring User Authentication Precedence

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 In the **Navigation** pane, click **User Management** menu.

Step 3 From the **Actions** drop-down list, select **User Management** > **Configure User Authentication Precedence**.

Configure User Authentication Precedence dialog box is displayed.

Step 4 In the **Configure User Authentication Precedence** dialog box, select the database for which you wish to update the priority.

Use the Up or the Down arrow to change the priority of the database.

Step 5 You can view the following properties:

Table 101: User Authentication Precedence

Name	Description
Database check box	Use the check box to select the desired database.
Name column	The user database name.
Priority column	This shows the priority of that database.
Up Arrow button	Use this arrow to move a database up the priority list.
Down Arrow button	Use this arrow to move a database down the priority list.

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.

SUMMARY STEPS

1. Login as an admin user.

2. In the **Navigation** pane, click the **Chassis** menu.
3. In the **Chassis** menu, click **Summary**.
4. From the tool bar, click **Launch KVM**.
5. Alternatively, in the **Navigation** pane, click the **Compute** menu.
6. From the **Power** menu, select **Reset System**.
7. When prompted, press **F8** to enter the Cisco IMC Configuration Utility. This utility opens in the KVM console window.
8. Check the **Factory Default** check box, the server reverts to the factory defaults.
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.
10. Press **F10** to save your settings and reboot the server.

DETAILED STEPS

Procedure

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 LDAP** 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, on page 232 section.

The following steps must be performed on the LDAP server.

Procedure

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

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

Properties	Value
Common Name	`CiscoAVPair`
LDAP Display Name	`CiscoAVPair`
Unique X500 Object ID	`1.3.6.1.4.1.9.287247.1`
Description	`CiscoAVPair`
Syntax	`Case Sensitive String`

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

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

Step 4 Add the following user role values to the CiscoAVPair attribute, for the users that you want to have access to 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 the LDAP Server on Cisco IMC

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.
Step 2 In the **Navigation** pane, click **User Management** menu.
Step 3 Select the **LDAP** tab.
Step 4 Select the **Configure LDAP Servers** tab.
Step 5 You can use one of the following methods to configure LDAP server:

- Pre-Configure LDAP Servers
- Use DNS to Configure LDAP Servers

Step 6 To configure using **Pre-Configure LDAP Servers**, select the radio button and click **Add LDAP Server**.
Step 7 Update the following properties:

Table 102: Configure LDAP Servers - Pre-Configure LDAP Servers

Name	Description
Add LDAP Server button	Allows you to add an LDAP server. A new row is added to the list of servers.

Name	Description
LDAP Servers column	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.
Port column	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.
Edit icon	To edit LDAP server details, click the icon for the respective row.

Step 8 To configure using **Use DNS to Configure LDAP Servers**, select the radio button and update the following properties:

Table 103: Configure LDAP Servers - Use DNS to Configure LDAP Servers

Name	Description
Source drop-down list	Allows you to select the source. It can be one of the following: • Extracted • Configured • Configured-Extracted
Domain To Search field	This setting specifies the domain name that the IMC will use to search for LDAP servers. When configured, the IMC queries DNS for SRV records in the specified domain to dynamically discover LDAP servers.
Forest to Search field	This setting specifies the Active Directory (AD) forest that the IMC will search to discover LDAP servers. When configured, the IMC queries DNS for SRV records within the specified forest to dynamically locate LDAP servers.

Configuring LDAP Settings and Group Authorization

Before you begin

You must log in as an admin to perform this procedure.

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 In the **Navigation** pane, click **User Management** menu.

Step 3 Select the **LDAP** tab.

Step 4 Select the **LDAP Settings** tab.

Step 5 In the **General Settings** area, update the following properties:

Table 104: General Settings Area

Name	Description
Enable LDAP toggle button	If enabled, 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 toggle button	**Note** For security reasons, starting with the upcoming releases, you will no longer be able to disable secure LDAP. If checked, the server enables secure LDAP and prompts you to download LDAP CA certificate. To delete an existing secure LDAP certificate, un-check this option. Follow the system prompts to confirm deletion.
Timeout (for each server) drop-down list	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.

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

Table 105: Binding Parameters Area

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 field	The distinguished name (DN) of the user. This field is editable only if you have selected **Configured Credentials** option as the binding method.
Password field	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:

Table 106: Search Parameters Area

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

Name	Description
Attribute field	An LDAP attribute that contains the role and locale information for the user. This property is always a name-value pair. The system queries the user record for the value that matches this attribute name. 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 field	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) Select the **Group Authorization** area and update the following properties:

Table 107: LDAP Group Authorization

Name	Description
LDAP Group Authorization toggle button	If enabled, user authentication is also done on the group level for LDAP users that are not found in the local user database. If you enable this option, 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. name of the group in the db
Group Domain column	The LDAP server domain the group must reside in. AD domain

Name	Description

Role column	The role assigned to all users in this LDAP server group. This can be one of the following: Role for these users
	• 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.

Edit icon	Allows you to edit the new row. Once configured, click **Save**.
Delete button	Allows you to delete the selected LDAP group.

LDAP Certificates Overview

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

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

Viewing LDAP CA Certificate Status

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 In the **Navigation** pane, click **User Management** menu.

Step 3 Select the **LDAP** tab.

Step 4 Select the **LDAP Settings** tab.

Step 5 In the **LDAP CA Certificate Status** area, view the following fields:

Table 108: LDAP CA Certificate Status

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 as admin to perform this procedure.

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

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 In the **Navigation** pane, click **User Management** menu.

Step 3 From the **Actions** drop-down list, select **Export LDAP CA Certificate**.

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

Step 4

Step 5 Click **Export**.

Uploading 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.

Before you begin

- You must log in as a user with admin privileges to perform this action.
- You must enable **Enable Secure LDAP** to perform this action.

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

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 In the **Navigation** pane, click **User Management** menu.

Step 3 Select the **LDAP** tab.

Step 4 Select the **LDAP Settings** tab.

Step 5 Enable **Enable Secure LDAP**.

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

Step 6 In the **Upload LDAP CA Certificate** dialog box, update the following properties:

Table 109: Remote

Name	Description
Remote button	Select this option when you want to upload the certificate from a remote location.
Server IP/Hostname	Server details from where you want to upload the certificate.
Upload Protocol button	Select 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. To comply with Cisco security standards, certain insecure protocols (TFTP, FTP, HTTP) will no longer be supported in upcoming releases. We recommend using secure protocols like SFTP or SCP moving forward.
Path and Filename field	File path where the certificate file resides on the server along with the filename.
Username field	User name for your remote server.
Password field	Password for your remote server.

Name	Description
Upload button	Allows you to upload the certificate.

Table 110: Local

Name	Description
Local button	Select this option when you want to upload the certificate from your local machine. Click **Browse** and navigate to the certificate that you want to upload.
Upload button	Allows you to upload the certificate.

Table 111: Paste

Name	Description
Paste button	Opens a text box that allows you to copy the entire content of the root CA certificate and paste it in the **Paste** text field.
Upload button	Allows you to upload the certificate.

Testing LDAP Binding

Before you begin

You must log in as an admin to perform this procedure.

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 In the **Navigation** pane, click **User Management** menu.

Step 3 Select the **LDAP** tab.

Step 4 Select the **LDAP Settings** tab.

Step 5 From the **Actions** drop-down list, select **User Management** > **Test LDAP Binding**.

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

Step 6 Click **Test**.

TACACS+ Authentication

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.

Cisco IMC also supports user authentication precedence in case TACACS+ remote servers are inaccessible.

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.

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 In the **Navigation** pane, click **User Management** menu.

Step 3 Select the **TACACS+** tab.

Step 4 Under the **TACACS+ Properties** area update the following properties:

Table 112: TACACS+ Properties

Name	Description
Enabled toggle button	If enabled, it enables TACACS+ based user authentication.

Name	Description
Fallback only on no connectivity toggle button	If enabled, 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.
Timeout (for each server): (5- 30) seconds drop-down list	Time duration, in seconds, for which Cisco IMC waits for a response from each of the TACACS+ servers

Step 5 Click **Save**.

Configuring TACACS+ Remote Server Settings

You can configure up to six TACACS+ remote servers.

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.
Step 2 In the **Navigation** pane, click **User Management** menu.
Step 3 Select the **TACACS+** tab.
Step 4 Under the **Server List** area, click the **Edit** icon for the server ID which you wish to configure.
Step 5 Update the following fields:

Table 113: Server List

Name	Description
ID column	The precedence that needs to be given for this TACACS+ server. This is also a unique identifier of the server.
IP Address or Host Name column	The IP address at which the TACACS+ server is running.
Port column	The port on which the TACACS+ server is running.
Server key column	The same key that is configured on the TACACS+ server.
Confirm Server Key column	Enter the server key again.

Step 6 Click **Save**.

Viewing and Terminating User Sessions

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 In the **Navigation** pane, click **User Management** menu.

Step 3 Select the **Sessions Management** tab.

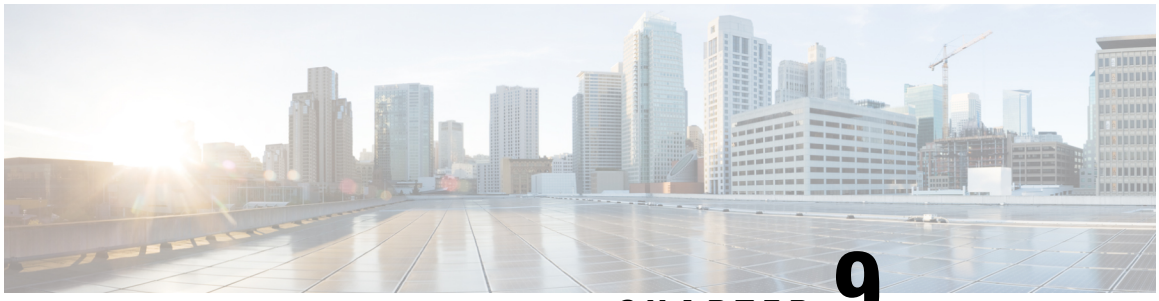
Step 4 View the following information about current user sessions:

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

Table 114: Session Management

Name	Description
Session ID column	The unique identifier for the session.
User Name column	The username for the user.
IP Address column	The IP address from which the user accessed the server. If this is a serial connection, it displays **N/A**.
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. • **XML API**— indicates the user is connected to the server using XML API. • **Redfish**— indicates the user is connected to the server using Redfish API.
Description column	Brief description of the session.
Terminate Session button	Allows you to a terminate a user session. Select a session from the table and click **Terminate Session**. Click **OK** to proceed.

Step 5 To terminate a session, select a session from the table and click **Terminate Session**. Click **OK** to proceed.



CHAPTER 9

Configuring Chassis-Related Settings

•
• Managing Server Power, on page 243
• Pinging a Hostname/IP Address from the Web UI, on page 244
• Toggling the Locator LEDs, on page 244
• Selecting a Time Zone, on page 245

Managing Server Power

Before you begin

You must be logged in as an admin to perform this procedure.

Procedure

Step 1

Step 2 From the **Apps** drop-down list, select **Dashboard**.

Step 3 From the Actions drop-down menu, select **Power**.

Step 4 Select a power option and perform the activities according to the following details:

Table 115: Power Options

Name	Description
Power Off	Allows you to power off the server. Click **Power Off** to proceed.
Power On	Allows you to power on the server.
Power Cycle	Allows you to perform an AC power cycle of the server. Click **Power Cycle** to proceed.
Hard Reset	Allows you to reset the server to factory settings. Click **Hard Reset** to proceed.

Name	Description
Shut Down	Allows you to gracefully shut down the server. Click **Shut Down** to proceed.

Pinging a Hostname/IP Address from the Web UI

Before you begin

You must be logged in as an admin to perform this procedure.

Procedure

Step 1 From the **Apps** drop-down list, select **Dashboard**.

Step 2 From the Actions drop-down menu, select **System** > **Ping**.

Step 3 In the **Ping Details** dialog box, perform the activities according to the details given in the table below.

Name	Description
Management IP Address field	Hostname or IP address you want to reach out to.
Number of Retries drop-down list	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 (in seconds) drop-down list	The maximum response time for a pinging activity. The default value is 10 seconds. The valid range is from 1 to 20 seconds.
Ping Status	Displays results of the pinging activity.
Details button	Displays details of the pinging activity.
Ping button	Performs the ping action of the IP address.

Step 4 Click **Ping**.

Toggling the Locator LEDs

Before you begin

You must be logged in as an admin to perform this procedure.

Procedure

Step 1 From the **Apps** drop-down list, select **Dashboard**.

Step 2 From the Actions drop-down menu, select **System** > **Turn On/Off LED**.

Step 3 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.
If the Turn On LED is selected, the locator LED on the physical drive is turned on.

If the Turn Off LED is selected, the locator LED on the physical drive is turned off.

Selecting a Time Zone

Before you begin

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

Procedure

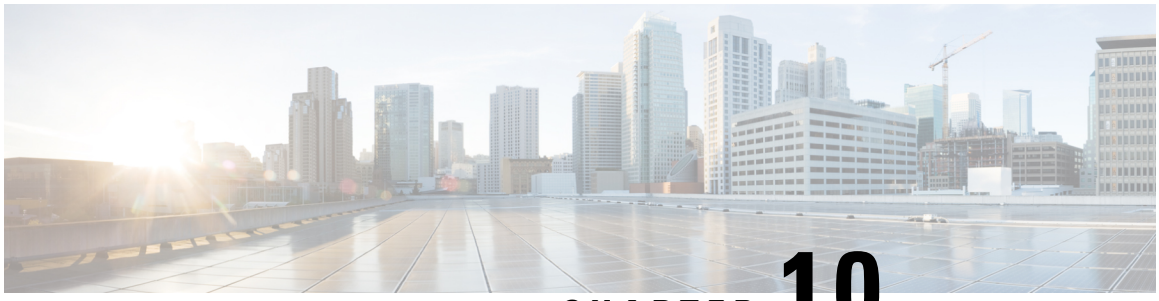
Step 1 From the **Apps** drop-down list, select **Dashboard**.

Step 2 In the **CIMC Information** area, click the value under **Timezone** field.

Select Timezone screen appears.

Step 3 Select the required time zone from the **Select Timezone** drop-down list or mouse over the map and click on the location to select the time zone.

Step 4 Click **Save**.



CHAPTER 10

Configuring Network-Related Settings

•
• Configuring Network-Related Settings, on page 247
• Server NICs, on page 247
• Configuring Server NICs, on page 250
• Cisco VIC mLOM and OCP Card Replacement Considerations, on page 254
• Single IP Configuration, on page 255
• Common Properties Configuration, on page 257
• Configuring IPv4, on page 259
• Configuring IPv6, on page 259
• Connecting to a VLAN, on page 261
• Network Security Configuration, on page 261
• Network Time Protocol Settings, on page 263

Configuring Network-Related Settings

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, M5, C220 M6, and C240 M6 servers, the NIC mode is set to **Shared LOM Extended** by default.

- **Shared OCP**—The OCP adapter card LOM ports are used to access Cisco IMC. You must select either the Active-Active or Active-standby NIC redundancy setting in the following step.
- **Shared OCP Extended**—In this NIC mode, DHCP replies are returned to both the OCP adapter card LOM ports and the Cisco virtual interface card (VIC) ports. If the system determines that the Cisco VIC connection is not getting its IP address from a Cisco UCS Manager system because the server is in standalone mode, further DHCP requests from the Cisco VIC are disabled.

Note **Shared OCP** and **Shared OCP Extended** ports are available only on Cisco UCS C225 M6, C245 M6, C220 M7, and C240 M7 servers.

Default NIC Mode Setting:

- For UCS C-Series C125 M5 servers and S3260 servers, the **NIC Mode** is set to **Cisco Card** by default.

For Cisco UCS C225 M6, C245 M6, C220 M7, and C240 M7 servers:

- if the server has a Cisco VIC card with OCP card, then the default NIC mode is **Shared OCP Extended** and **NIC Redundancy** is set to **active-active**.
- if the server has VIC card populated in NCSI supported slots and no OCP card, then the default NIC mode is **Cisco Card**.
- if the server does not have any VIC card and OCP card, the default NIC mode is **Dedicated** and **NIC Redundancy** is set to **None**.

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

VIC Slots

The VIC slot that can be used for management functions in Cisco card mode.

For C240 M6, C245 M6, and C240 M7, VIC slot options are as follows:

- **Riser 1**—Slot 1 and Slot 2
- **Riser 2**—Slot 4 and Slot 5
- **mLOM**

Note For C240 M6, C245 M6, and C240 M7, after resetting to factory default settings, the slot precedence is as follows:

1. mLOM
2. Riser 1 - Slot 2; and Riser 2 - Slot 5
3. Riser 1 - Slot 1; and Riser 2- Slot 4

For C220 M6, C225 M6, and C220 M7, VIC slot options are as follows:

- **Riser 1**—Slot 1 is selected.
- **Riser 3** —Slot 3 is selected.
- **mLOM**

Note For C220 M6, C225 M6, and C220 M7, after resetting to factory default settings, the slot precedence is as follows:

1. mLOM
2. Riser 1 - Slot 1
3. Riser 3 - Slot 3

For C125 M5, VIC slot option is **Riser 2**.

For C220 M4, C220 M5 and C240 M5 servers, VIC slot options are as follows:

- **Riser 1**—Slot 1 is selected.
- **Riser 2**—Slot 2 is selected.
- **FLEX LOM**—Slot 3 (MLOM) is selected.

For C240 M5 SD servers, VIC slot options are as follows:

- **Riser 2**— Slot 2 is selected.
- **mLOM**—VIC cards in mLOM slot is selected.

For C240 M4 servers, VIC slot options are as follows:

- **Riser 1**—Slot 2 is the primary slot, but you can also use slot 1.
- **Riser 2**—Slot 5 is the primary slot, but you can also use slot 4.
- **FLEX LOM**—Slot 7 (MLOM) is selected.

For C480 M5 ML servers, Cisco card mode slot is Slot 11 and Slot 12.

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.

Procedure

Step 1 From the **Apps** drop-down list, select **Networking**.

Step 2 From the **Apps** drop-down list, select **Administration**.

Step 3 From the **Administration** page, select **Networking**.

Step 4 From the **Networking** tab, select **Network**.

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

Table 116: NIC Properties Area

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). • **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. • **Shared OCP**—The OCP adapter card LOM ports are used to access Cisco IMC. You must select either the Active-Active or Active-standby NIC redundancy setting in the following step. • **Shared OCP Extended**—In this NIC mode, DHCP replies are returned to both the OCP adapter card LOM ports and the Cisco virtual interface card (VIC) ports. If the system determines that the Cisco VIC connection is not getting its IP address from a Cisco UCS Manager system because the server is in standalone mode, further DHCP requests from the Cisco VIC are disabled. **Default NIC Mode Setting**: • For UCS C-Series M7 servers: • if the server has a Cisco VIC card with OCP card, then the default NIC mode is **Shared OCP Extended** and **NIC Redundancy** is set to **active-active**. • if the server has VIC card populated in NCSI supported slots and no OCP card, then the default NIC mode is **Cisco Card**. • if the server does not have any VIC card and OCP card, the default NIC mode is **Dedicated** and **NIC Redundancy** is set to **None**.

Name	Description
VIC Slot drop-down list	The VIC slot that can be used for management functions in Cisco card mode. For C240 M7, VIC slot options are as follows: • **Riser 1**—Slot 1 and Slot 2 • **Riser 2**—Slot 4 and Slot 5 • **mLOM** **Note** For C240 M7, after resetting to factory default settings, the slot precedence is as follows: **a.** mLOM **b.** Riser 1 - Slot 2; and Riser 2 - Slot 5 **c.** Riser 1 - Slot 1; and Riser 2- Slot 4 For C220 M7, VIC slot options are as follows: • **Riser 1**—Slot 1 is selected. • **Riser 3** —Slot 3 is selected. • **mLOM** **Note** For C220 M7, after resetting to factory default settings, the slot precedence is as follows: **a.** mLOM **b.** Riser 1 - Slot 1 **c.** Riser 3 - Slot 3

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.
Port Profile field	The port profile that Cisco IMC uses to configure the management interface, the virtual Ethernet, and the VIF on supported adapter cards such as the Cisco UCS VIC 1225 Virtual Interface card. Enter up to 79 alphanumeric characters. You cannot use spaces or other special characters except for - (hyphen) and _ (underscore). In addition, the port profile name cannot begin with a hyphen. **Note** The port profile must be defined on the switch to which this server is connected.
Auto Negotiation toggle button	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 enabled, 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 disabled, you can configure the network port speed and duplex values.

Name	Description
Network Port Speed drop-down list	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**.

Step 6 Click **Save**.

Cisco VIC mLOM and OCP Card Replacement Considerations

In Cisco UCS C220 M7, C240 M7, C225 M8 and C245 M8 servers, Cisco IMC network connection may be lost in the following situations, while replacing Cisco VIC mLOM and OCP cards:

- If OCP card is replaced by Cisco VIC card in MLOM Slot and the NIC mode is set to **Shared OCP** or **Shared OCP Extended**.
- If Cisco VIC Card in MLOM Slot is replaced by OCP Card and NIC mode is set to **Cisco-card MLOM**.

Follow these recommendations while replacing Cisco VIC mLOM or OCP cards in Cisco UCS C220 M7, C240 M7, servers to avoid loss of connectivity:

- Before replacing the card, configure any of the NIC modes that has network connected, other than **Cisco card MLOM**, **Shared OCP**, or **Shared OCP Extended**. After replacing the card, configure the appropriate NIC mode.

  To set the NIC mode, refer *Server NIC Configuration* section in Configuration Guides for your Cisco IMC release.

- Or, after replacing the card, configure the appropriate NIC mode using Cisco IMC Configuration Utility/F8.

  Refer *Connecting to the Server Locally For Setup* section in Install and Upgrade Guides for your server.

- Or, after replacing the card, perform factory default settings using Cisco IMC Configuration Utility/F8 then perform the following steps:
  1. Once the server is rebooted, boot the system to Cisco IMC Configuration Utility/F8.

     Change the default password.
  2. Configure the appropriate NIC mode settings.

Table 117: Factory Default Settings

VIC in mLOM slot	Intel OCP 3.0 NIC in mLOM Slot	VIC in Riser Slot	Dedicated Management Port	NIC Mode for CIMC Access
Yes	No	No	Yes	**Cisco Card** mode with the card in mLOM Slot
No	Yes	No	Yes	**Shared OCP Extended**
No	Yes	Yes	Yes	**Shared OCP Extended**
No	No	Yes	Yes	**Cisco Card** with VIC SLOT based on precedence: **For C220 M7 and C225 M8:** **1.** Riser 1 - Slot 1 **2.** Riser 3 - Slot 3 **For C240 M7 and C245 M8:** **1.** Riser 1 - Slot 2 **2.** Riser 2 - Slot 5 **3.** Riser 1 - Slot 1 **4.** Riser 2 - Slot 4
No	No	No	Yes	**Dedicated**

Single IP Configuration

Single IP is an optional method to assign IPv4 for Cisco IMC management.

Note When **Single IP Mode** is enabled, the 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 you downgrade to the release 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.

Procedure

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**

Name	Description
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 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 . 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.

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 From the **Administration** page, select **Networking**.

Step 3 From the **Networking** tab, select **Network**.

Step 4 In the **Common Properties** area on the right pane, update the following properties:

Table 118: Common Properties Area

Name	Description
Management Hostname field	The user-defined management hostname of the system that manages the various components of Cisco IMC.
Enable Dynamic DNS toggle button	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.

Step 5 Click **Save**.

Configuring IPv4

Before you begin

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

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 From the **Administration** page, select **Networking**.

Step 3 From the **Networking** tab, select **Network**.

Step 4 In the **IPv4 Properties** area, update the following properties:

Table 119: IPv4 Properties Area

Name	Description
Enable IPv4 toggle button	If enabled, IPv4 is enabled.
DHCP toggle button	If enabled, Cisco IMC uses DHCP.
Management IP Address field	The management IP address. An external virtual IP address that helps manage the BMC.
Subnet Mask field	The subnet mask for the IP address.
IPv4 Gateway field	The gateway for the IP address.
Obtain DNS Server Addresses from DHCP toggle button	If enabled, Cisco IMC retrieves the DNS server addresses from DHCP.
IPv4 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 5 Click **Save**.

Configuring IPv6

Before you begin

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

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 From the **Administration** page, select **Networking**.

Step 3 From the **Networking** tab, select **Network**.

Step 4 In the **IPv6 Properties** area, update the following properties:

Table 120: IPv6 Properties Area

Name	Description
Enable IPv6 toggle button	If enabled, IPv6 is enabled.
Use DHCP toggle button	If enabled, 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.
IPv6 Gateway field	The gateway for the IPv6 address. **Note** Only global unicast addresses are supported.
Obtain DNS Server Addresses from DHCP toggle button	If enabled, the Cisco IMC retrieves the DNS server addresses from DHCP. **Note** You can use this option only when the **Use DHCP** option is enabled.
IPv6 Preferred DNS Server field	The IPv6 address of the primary DNS server.
IPv6 Alternate DNS Server field	The IPv6 address of the secondary DNS server.
Link Local Address field	The link local address for the IPv6 address.
Stateless Address Auto Configuration field	The Stateless Address Auto Configuration (SLAAC) depends on the Router Advertisement (RA) of the network.

Step 5 Click **Save**.

Connecting to a VLAN

Before you begin

You must be logged in as admin to connect to a VLAN.

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 From the **Administration** page, select **Networking**.

Step 3 In the **VLAN Properties** area on the right pane, update the following properties:

Table 121: VLAN Properties Area

Name	Description
Enable VLAN toggle button	If enabled, 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**.

Network Security Configuration

Network Security

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.

Procedure

Step 1 From the **Apps** drop-down list, select **Networking**.

Step 2 From the **Apps** drop-down list, select **Administration**.

Step 3 From the **Administration** page, select **Networking**.

Step 4 From the **Networking** tab, select **Settings**.

Step 5 In the **IP Blocking Properties** area, update the following properties:

Table 122: IP Blocking Properties Area

Name	Description
Enable IP Blocking toggle button	Allows you to enable or disable IP blocking feature.
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.
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.

Step 6 In the **IP Filtering (Allow listing)** area, update the following properties:

Table 123: IP Filtering Area

Name	Description
Enable IP Filtering toggle button	Allows you to enable or disable the IP filtering feature.
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 7 Click **Save**.

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

Procedure

Step 1 From the **Apps** drop-down list, select **Networking**.

Step 2 From the **Apps** drop-down list, select **Administration**.

Step 3 From the **Administration** page, select **Networking**.

Step 4 From the **Networking** tab, select **Settings**.

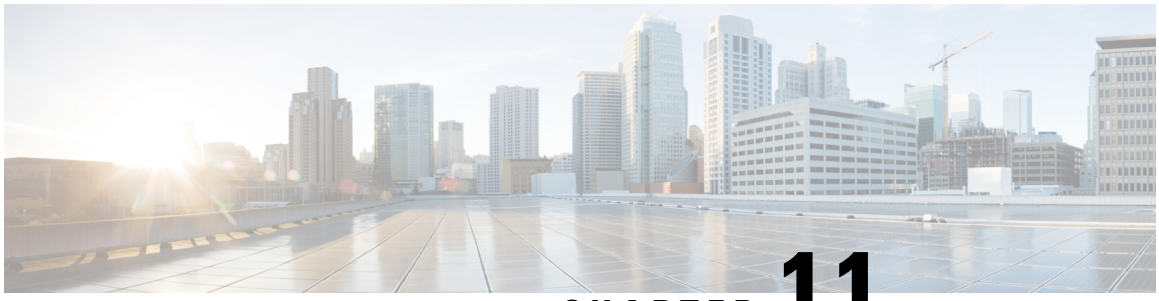
Step 5 In the **NTP Properties** area, update the following properties:

Table 124: NTP Properties Area

Name	Description
Enable NTP toggle button	Allows you to enable or disable NTP services.
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
Server Status message	If NTP is enabled, this field 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 6 Click **Save**.



CHAPTER 11

Managing Network Adapters

•
• Overview of the Cisco UCS C-Series Network Adapters, on page 265
• Viewing Cisco UCS Network Adapter Properties, on page 268
• Managing vHBAs, on page 276
• Managing vNICs, on page 291
• Backing Up and Restoring the Adapter Configuration, on page 327

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 1477 Virtual Interface Card
- Cisco UCS VIC 1467 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 1227T Virtual Interface Card
- Cisco UCS VIC 1225 Virtual Interface Card

- Cisco UCS P81E 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 15238 Virtual Interface Card

The Cisco UCS VIC 15238 is a dual-port quad small-form-factor pluggable (QSFP/QSFP28/QSFP56) mLOM card designed for designed for the M6 and M7 generation of Cisco UCS C-series Rack servers. The card supports 40/100/200-Gbps Ethernet or FCoE. The card can present PCIe standards-compliant interfaces to the host, and these can be dynamically configured as either NICs or HBAs.

Cisco UCS VIC 15428 Virtual Interface Card

The Cisco VIC 15428 is a quad-port Small Form-Factor Pluggable (SFP+/SFP28/SFP56) mLOM card designed for the M6 and M7 generation of Cisco UCS C-Series Rack servers. The card supports 10/25/50-Gbps Ethernet or FCoE. The card can present PCIe standards-compliant interfaces to the host, and these can be dynamically configured as either NICs or HBAs.

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 1477 Virtual Interface Card

The Cisco VIC 1477 is a dual-port Quad Small Form-Factor (QSFP28) mLOM card designed for the M6 generation of Cisco UCS C-Series Rack Servers. The card supports 40/100-Gbps Ethernet or FCoE. The card can present PCIe standards-compliant interfaces to the host, and these can be dynamically configured as NICs or HBAs.

Cisco UCS VIC 1467 Virtual Interface Card

The Cisco UCS VIC 1467 is a quad-port Small Form-Factor Pluggable (SFP28) mLOM card designed for the M6 generation of Cisco UCS C-Series Rack Servers. The card supports 10/25-Gbps Ethernet or FCoE. The card can present PCIe standards-compliant interfaces to the host, and these can be dynamically configured as either NICs or HBA.

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 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 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 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.

Cisco UCS P81E Virtual Interface Card

The Cisco UCS P81E Virtual Interface Card is optimized for virtualized environments, for organizations that seek increased mobility in their physical environments, and for data centers that want reduced costs through NIC, HBA, cabling, and switch reduction and reduced management overhead. This Fibre Channel over Ethernet (FCoE) PCIe card offers the following benefits:

- Allows up to 16 virtual Fibre Channel and 16 virtual Ethernet adapters to be provisioned in virtualized or nonvirtualized environments using just-in-time provisioning, providing tremendous system flexibility and allowing consolidation of multiple physical adapters.
- Delivers uncompromising virtualization support, including hardware-based implementation of Cisco VN-Link technology and pass-through switching.

- Improves system security and manageability by providing visibility and portability of network polices and security all the way to the virtual machine.

The virtual interface card makes Cisco VN-Link connections to the parent fabric interconnects, which allows virtual links to connect virtual NICs in virtual machines to virtual interfaces in the interconnect. In a Cisco Unified Computing System environment, virtual links then can be managed, network profiles applied, and interfaces dynamically reprovisioned as virtual machines move between servers in the system.

Viewing Cisco UCS 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.

Procedure

Step 1 From the **Apps** drop-down list, select **Networking**.

Step 2 Select the **General** tab.

Step 3 In the **Properties** area, review the following information:

Table 125: Properties Area

Name	Description
PCI Slot	The PCI slot in which the adapter is installed.
Vendor	The vendor for the adapter.
Product Name	The product name for the adapter.
Product ID	The product ID for the adapter.
Serial Number	The serial number for the adapter.
Version ID	The version ID for the adapter.
Hardware Revision	The hardware revision for the adapter.
Cisco IMC Management Enabled	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.
Configuration Pending	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.

Name	Description
ISCSI Boot Capable	Whether iSCSI boot is supported on the adapter.
CDN Capable	Whether CDN is supported on the adapter.
usNIC Capable	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.
Running Version	The firmware version that is currently active.
Backup Version	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	The firmware version that will become active the next time the adapter is rebooted.
Bootloader Version	The bootloader version associated with the adapter card.
Status	The status of the last firmware activation that was performed on this adapter. **Note** The status is reset each time the adapter is rebooted.

In the **Settings** area, review the following information:

Table 126: Settings Area

Name	Description
Description field	A user-defined description for the adapter. You can enter between 1 and 63 characters.

Name	Description
Enable FIP Mode toggle button	Allows you to enable or disable FCoE Initialization Protocol (FIP). 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 toggle button	**Note** For LLDP change to be effective, it is required that you reboot the server. If enabled, 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.
Enable VNTAG Mode toggle button	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 toggle button	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 toggle button	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**. **Note** Beginning with the release 4.3(6), when **Physical NIC mode** is enabled, you cannot create default vLANs using Cisco IMC user interfaces.
Transmit Enhanced Mode toggle button	Allows you to enable enhance TCP performance on the transmit side for 1500 byte packets.

Step 4 Select the **DCE Interfaces** tab.

Step 5 You can review the following information:

Table 127: DCE Interfaces

Name	Description
Port column	The uplink port ID.
MAC Address column	The MAC address of the uplink port.
Link Status column	The current operational state of the uplink port. This can be one of the following: • **Fault** • **Up** • **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.
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.
Encap column	The mode in which adapter operates. This can be one of the following: • **CE**—Classical Ethernet mode. • **NIV**—Network Interface Virtualization mode.

Name	Description
Operating Speed column	The operating rate for the port. This can be one of the following: • **1 Gbps** • **10 Gbps** • **25 Gbps** • **40 Gbps** • **50 Gbps** • **100 Gbps** • **4 x 10 Gbps** • **Auto**
Admin Speed column	The data transfer rate for the port. This can be one of the following: • **1 Gbps** • **10 Gbps** • **40 Gbps** • **4 x 10 Gbps** • **Auto** **Note** This option is available only on some of the adapters and servers.

Name	Description
Admin FEC Mode column	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.

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.

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
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.

Managing vHBAs

Guidelines for Managing vHBAs

When managing vHBAs, 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.

  The Cisco UCS 1455, 1457, 1455, and 1467 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 and Modifying vHBA Properties

Procedure

Step 1 From the **Apps** drop-down list, select **Networking**.

Step 2 Select the **vHBA Interfaces** tab.

Step 3 From the list of the vHBA, click the one for which you wish to view or modify the properties.

Step 4 In the **General Settings** tab, review or modify the following properties:

Table 128: Settings

Name	Description
Name field	The name of the virtual HBA. This name cannot be changed after the vHBA has been created.
Initiator WWNN toggle button and field	The WWNN associated with the vHBA. To let the system generate the WWNN, disable **Initiator WWNN**. To specify a WWNN, enable **Initiator WWNN** and enter the WWNN in the corresponding field.
Initiator WWPN toggle button and field	The WWPN associated with the vHBA. To let the system generate the WWPN, disable **Initiator WWPN**. To specify a WWPN, enable **Initiator WWPN** and enter the WWPN in the corresponding field.
PCI Order field	The order in which this vHBA will be used. Enter an integer between 0 and 17.
MAC Address toggle button and field	The MAC address associated with the vHBA. To let the system generate the MAC address, disable **MAC Address**. To specify a MAC address, enable **MAC Address** and enter the MAC address in the corresponding field.
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.
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.
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.

Name	Description
Default VLAN toggle button and field	If there is no default VLAN for this vHBA, disable **Default VLAN**. Otherwise, enable **Default VLAN** and enter a VLAN ID between 1 and 4094 in the field.
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.
vHBA Type drop-down list	**Note** This option is available only with Cisco UCS 14xx series VIC adapters and Cisco UCS 15428 VIC 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.
PCI Link field	It is read-only field.

Name	Description
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.
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.
Rate Limit toggle button and field	The data rate limit for traffic on this vHBA, in Mbps. If you want this vHBA to have an unlimited data rate, select disable **Rate Limit**. Otherwise, click the second radio button and enter an integer between 1 and 10,000. **Note** This option cannot be used in VNTAG mode.

Step 5 In the **Advanced Settings** tab, review or modify the following properties:

Table 129: Error Recovery Area

Name	Description
FCP Error Recovery toggle button	If enabled, 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.
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.

Name	Description
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.
FLOGI Retries toggle button and 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, enable **FLOGI Retries**. Otherwise disable **FLOGI Retries** 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.
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.

Table 130: Fiber Channel Port

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 1024.
LUNs per Target field	The maximum number of LUNs that the driver will export. This is usually an operating system platform limitation. For Linux OS, enter an integer between 1 and 16384. For Windows OS, enter an integer between 1 and 1024. For ESXi OS, enter an integer between 1 and 4096.
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. Enter an integer between 1 and 254.

Name	Description
CDB Transmit Queue Count field	The number of SCSI I/O queue resources the system should allocate. 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.
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 6 In the **Boot Table** tab, review or modify the following properties:

Table 131: Boot Table

Name	Description
FC SAN Boot toggle button	If enabled, the vHBA can be used to perform a SAN boot.
Add Boot Entry button	Adds a new entry to the boot table.
Delete Boot Entry button	Allows you to delete the selected boot table row entry.
ID column	The default value for this field is **0**.
Target WWPN column and 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 column and field	The LUN ID that corresponds to the location of the boot image. Enter an ID between 0 and 255.
Edit icon	Allows you to edit the **Target WWPN** and **LUN ID** of the selected boot table row.

Step 7 In the **Persistent Bindings** tab, review or modify the following properties:

Table 132: Persistent Binding

Name	Description
Persistent LUN Bindings toggle button	Allows you to enable **Persistent LUN Bindings**.
Reset button	Allows you to reset to factory settings.

Name	Description
Save button	Saves the configuration after changing **Persistent LUN Bindings** settings.
Rebuild Persistent Bindings button	Clears all unused bindings and resets the ones that are in use.
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.

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, 1457, and 1467 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** is on.

Procedure

Step 1 From the **Apps** drop-down list, select **Networking**.

Step 2 From the **Actions** drop-down list, select **VIC** > **Create Virtual HBA Interface**.

Add vHBA dialog box is displayed.

Step 3 Under **Select Cisco VIC Adapter**, update the following properties and click **Next**.

Table 133: Select Cisco VIC Adapter

Name	Description
Slot drop-down list	Allows you to select the VIC slot. **Note** If there is one slot available, then this option is grayed out.

Name	Description
Next button	Click **Next** to proceed.

Step 4 Under **General Settings**, update the following properties and click **Next**.

Table 134: General Settings

Name	Description
Name field	Allows you to enter a user defined name.
PCIe Order field	This is the order in which the vHBA is used. Enter an integer between 0 and 4.
Uplink Port drop-down list	The uplink port associated with this vHBA. All traffic for this vHBA goes through this uplink port. Select 0 or 1.
Channel Number field	Select the channel number which is assigned to this vHBA. Enter an integer between 0 and 1000.
Advance Options toggle button	Enable this to update advance properites. **Note** All the other properties are visible only when **Advance Options** is enabled.
Initiator WWNN toggle button and field	The WWNN associated with the vHBA. To let the system generate the WWNN, disable **Initiator WWNN**. To specify a WWNN, enable **Initiator WWNN** and enter the WWNN in the corresponding field.
Initiator WWPN toggle button and field	The WWPN associated with the vHBA. To let the system generate the WWPN, disable **Initiator WWPN**. To specify a WWPN, enable **Initiator WWPN** and enter the WWPN in the corresponding field.
FC SAN Boot toggle button	If enabled, the vHBA can be used to perform a SAN boot.
Persistent LUN Binding toggle button	If enabled, any LUN ID associations are retained in memory until they are manually cleared.
MAC Address toggle button and field	The MAC address associated with the vHBA. To let the system generate the MAC address, disable **MAC Address**. To specify a MAC address, enable **MAC Address** and enter the MAC address in the corresponding field.
Default VLAN toggle button and field	If there is no default VLAN for this vHBA, disable **Default VLAN**. Otherwise, enable **Default VLAN** and enter a VLAN ID between 1 and 4094 in the field.

Name	Description
Rate Limit toggle button and field	The data rate limit for traffic on this vHBA, in Mbps. If you want this vHBA to have an unlimited data rate, select disable **Rate Limit**. Otherwise, click the second radio button and enter an integer between 1 and 10,000. **Note** This option cannot be used in VNTAG mode.
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.
vHBA Type drop-down list	**Note** This option is available only with Cisco UCS 14xx series VIC adapters and Cisco UCS 15428 VIC 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 • 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.
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.

Name	Description
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.
PCI Link field	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 5 Under **Error Recovery**, update the following properties and click **Next**.

Table 135: Error Recovery

Name	Description
FCP Error Recovery toggle button	If enabled, 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.
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.

Name	Description
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.

Step 6 Under **Fibre Channel Port**, update the following properties and click **Next**.

Table 136: Fibre Channel Port

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 1024.
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 4096.
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. Enter an integer between 1 and 254.
FLOGI Retries toggle button and 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, enable **FLOGI Retries**. Otherwise disable **FLOGI Retries** 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.
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 7 Under **I/O Receive & Transmit**, update the following properties and click **Next**.

Table 137: I/O Receive & Transmit Queues

Name	Description
CDB Transmit Queue Count field	The number of SCSI I/O queue resources the system should allocate. 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.
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 8 Under **Summary**, review the information and click **Save**.

What to do next

- Reboot the server to create the vHBA.

Cloning a vHBA

Procedure

Step 1 From the **Apps** drop-down list, select **Networking**.

Step 2 Select the **vHBA Interfaces** tab.

Step 3 Select the vHBA Interface which you wish to clone and click **Clone vHBA** button.

Clone vHBA dialog box is displayed.

Step 4 Update the following properties in the **Clone vHBA** dialog box.

Table 138: Clone vHBA

Name	Description
Name field	Allows you to enter a user defined name.
Uplink Port drop-down list	The uplink port associated with this vHBA. All traffic for this vHBA goes through this uplink port. Select 0 or 1.

Name	Description
vHBA Type drop-down list	**Note** This option is available only with Cisco UCS 14xx series VIC adapters and Cisco UCS 15428 VIC 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 • 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.
PCIe Order field	This is the order in which the vHBA is used. Enter an integer between 0 and 4.
Channel Number field	Select the channel number which is assigned to this vHBA. Enter an integer between 0 and 1000.

Step 5 Click **Clone vHBA** to save the changes.

Deleting a vHBA

Default vHBAs cannot be deleted. You can delete any other vHBAs created using VNTAG mode.

Procedure

Step 1 From the **Apps** drop-down list, select **Networking**.

Step 2 Select the **vHBA Interfaces** tab.

Step 3 Select the **vHBA Interfaces** which you wish to delete and click **Delete vHBAs** button.

Note
You cannot delete either of the two default vHBAs, **fc0** or **fc1**.

Step 4 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

Procedure

Step 1 From the **Apps** drop-down list, select **Networking**.

Step 2 Select the **vHBA Interfaces** tab.

Step 3 From the list of the vHBA, click the one for which you wish to view or modify the boot table.

Step 4 Select the **Boot Table** tab.

Step 5 Click the **Add Boot Entry** button.

This adds a new entry in the boot entry table.

Step 6 In the **Add Boot Entry** table, click the edit icon to update the following properties:

Name	Description
Target WWPN column and 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 column and field	The LUN ID that corresponds to the location of the boot image. Enter an ID between 0 and 255.

Step 7 Click **Save**.

Deleting a Boot Table Entry

Procedure

Step 1 From the **Apps** drop-down list, select **Networking**.

Step 2 Select the **vHBA Interfaces** tab.

Step 3 From the list of the vHBA, click the one for which you wish to view or modify the boot table.

Step 4 Select the **Boot Table** tab.

Step 5 From the boot entry table, select the entry which you wish to delete.

Step 6 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 and Enabling Persistent Bindings

Procedure

Step 1 From the **Apps** drop-down list, select **Networking**.

Step 2 Select the **vHBA Interfaces** tab.

Step 3 From the list of the vHBA, click the one for which you wish to view or modify the boot table.

Step 4 Select the **Persistent Binding** tab.

Step 5 In the **Persistent Bindings** area, review or modify the following properties:

Table 139: Persistent Binding

Name	Description
Persistent LUN Bindings toggle button	Allows you to enable **Persistent LUN Bindings**.
Reset button	Allows you to reset to factory settings.
Save button	Saves the configuration after changing **Persistent LUN Bindings** settings.
Rebuild Persistent Bindings button	Clears all unused bindings and resets the ones that are in use.
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.

Rebuilding Persistent Bindings

Procedure

Step 1 From the **Apps** drop-down list, select **Networking**.
Step 2 Select the **vHBA Interfaces** tab.
Step 3 From the list of the vHBA, click the one for which you wish to view or modify the boot table.
Step 4 Select the **Persistent Binding** tab.
Step 5 Click the **Rebuild Persistent Bindings** button.
Step 6 Click **Yes** 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, 1457, and 1467 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 and Modifying vNIC Properties

Procedure

Step 1 From the **Apps** drop-down list, select **Networking**.
Step 2 Select the **vNIC Interfaces** tab.
Step 3 From the list of the vNIC, click the one for which you wish to view or modify the properties.
Step 4 In the **General Settings** tab, review or modify the following properties:

Table 140: Settings Area

Name	Description
Name field	The name of the virtual NIC. You cannot change the name of default vNIC.
MTU field	The maximum transmission unit, or packet size, that this vNIC accepts. For Windows and Linux OS with Cisco UCS VIC 15xxx adapters, enter an integer between 1500 and 9158. For ESXi OS, enter an integer between 1500 and 9000.
VLAN Mode drop-down list	The mode for the associated VLAN. This can be one of the following: • TRUNK • ACCESS If you want to use VLAN trunking, select TRUNK. Otherwise, select ACCESS. In TRUNK mode: In addition to the Cisco VIC adapter policy configuration, you can configure sub-interface on bare metal RHEL Linux host with a specific vlan for the packets to be correctly VLAN tagged. You can also do this by creating Vswitch on ESXi Hypervisor and adding it to VM. Please work with the Host OS vendor accordingly.
PCI Order field	The order in which this vNIC will be used. To specify an order, enter an integer within the displayed range.
MAC Address toggle button	Allows you to enable automatic the MAC address for the vNIC.
MAC Address field	Allows you to enter MAC address manually.
Uplink Port drop-down list	The uplink port associated with the vNIC. All traffic for this vNIC goes through this uplink port.
Class of Service field	The Class of Service assigned to the vNIC.
Trust Host CoS toggle button	Allows you to enable class of service provided by the host operating system.

Name	Description
Default VLAN toggle button	Allows you to enable the number of the default VLAN associated with the vNIC. **Note** Beginning with the release 4.3(6), if **Physical NIC mode** is enabled, then this option is disabled.
Number of Default VLAN field	Enter the number of default VLAN.
Rate Limit toggle button	Allows you to enable or disable unlimited data rate. If you want vNIC to have an unlimited data rate, select OFF. Otherwise, enable the toggle button and enter a rate limit in the associated Rate Limit field.
Rate Limit field	Enter a rate limit value between 1 and 50000.
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.
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.
Channel Number field	Select the channel number that will be assigned to this vNIC. Enter an interger between 1 and 1000. **Note** VNTAG mode is required for this option.
Port Profile field	The port profile associated with the vNIC, if any. **Note** VNTAG mode is required for this option. :
Enable Uplink Failover toggle button	Allows you to enable or disable whether the traffic on this vNIC should fail over to the secondary interface if there are communication problems.

Name	Description
Failback Timeout field	After a vNIC has started using the 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 an integer between 0 and 600.

Table 141: Resources Area

Name	Description
Receive Queue Count field	The number of receive queue resources to allocate. Enter an integer between 1 and 256.
Transmit Queue Count field	The number of transmit 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.
Receive Queue 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.
Transmit Queue 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.
Completion Queue Ring Size field	The number of descriptors in each completion queue. This value cannot be changed.
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 5 In the **Features** tab, review or modify the following properties:

Table 142: Offload Feature Area

Name	Description
TCP Segmentation Offload toggle button	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 NVGRE toggle button	Allows you to enable or disable Network Virtualization using Generic Routing Encapsulation.

Name	Description
Geneve Offload toggle button	

Name	Description
	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. 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** Cisco UCS C220 M7 and C240 M7 servers do not support Cisco VIC 14xx series. **Note** You cannot enable the following when **Geneve Offload** is enabled in a setup with Cisco VIC 15xxx: • aRFS

Name	Description
	• 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 4.2(2a).
TCP Large Receive toggle button	If enabled, 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.
aRFS toggle button	Allows yout to enable or disable Accelerated Receive Flow steering (aRFS).
Advanced Filter toggle button	Enable this feature for advanced filter options in vNICs.
TCP Tx Offload Checksum Generation toggle button	If enabled, 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.
Enable PTP toggle button	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.

Name	Description
Receive Side Scaling toggle button	Receive Side Scaling (RSS) distributes network receive processing across multiple CPUs in multiprocessor systems. If enabled, 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.
TCP Rx Offload Checksum Validation toggle button	If enabled, 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.
VXLAN toggle button	Allows you to enable Virtual Extensible LAN.

Name	Description
QinQ Offload toggle button	Cisco IMC provides VIC QinQ Tunneling support for Cisco UCS M7 servers with Cisco UCS VIC 14xx series and 15xxx series VIC adapters. Check this box to enable the **QinQ Offload** option on the specified vNIC. **Note** VIC QinQ Tunneling is not supported on 13xx adapters. You cannot enable the following when **QinQ Offload** 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 **QinQ Offload** 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.

Beginning with the release 4.3(6) onwards, you can configure Receive Side Scaling (RSS) and multiple transmit (Tx) and receive (Rx) queues to enable improved network performance in VMware ESXi 8.0 U3 and later.

This configuration is supported on the following:

- Cisco IMC: Release 4.3(6) or later
- VMware ESXi: Version 8.0 U3 or later
- nenic driver on ESXi: Minimum required nenic driver version is 2.0.17.0-1OEM.800.1.0.20613240 (for ESXi 8.0U3).
- Hardware: Supported on Cisco UCS 1400, 14000, and 15000 series adapters.

In the **Offload Feature Area**, set the following options:

- Transmit Queues = n (up to 16)
- Receive Queues = n (up to 16)
- Completion Queues = # of Transmit Queues + # of Receive Queues
- Interrupts = (# Completion Queues +2) rounded up to the nearest power of 2

Note
Ensure the following:

- **Receive Side Scaling (RSS)** option is enabled.
- **VMQ Connection Policy** option is disabled.

When VMQ is disabled, RSS engines handle the queue distribution, which may result in the Rx netqueue count appearing as 1 in ESXi command outputs.

If VMQ is enabled, then the Rx queue count will reflect the VMQ queues, and RSS engines may not be reported as active. Hence, to support RSS with multiple transmit queues, VMQ must be disabled and RSS must be enabled.

Table 143: VMQ Properties

Name	Description
Enable VMQ toggle button	Allows you to enable Virtual Machine Queue (VMQ).
Enable Multi Queue toggle button	Allows you 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
No. of Sub vNICs field	Number of sub vNICs available to the host when the multi queue option is enabled. Enter an integer between 1 and 64.
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.

Table 144: RoCE Properties

Name	Description
RDMA Mode 1/2 toggle button	Check the check box to change the RoCE Properties. **Note** If **Enable Multi Queue** is enabled, ensure that **RDMA Mode 2** is also enabled.
Queue Pairs field	The number of queue pairs per adapter. Enter an integer between 1 and 8192. 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 256. 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 drop-down list	This field is read-only and is set to 5. **Note** This option is available only on some of the adapters.

Table 145: SR-IOV Properties

Name	Description
Enable SR-IOV toggle button	Allows you to enable or disable SR-IOV feature.
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.

Name	Description
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 Per VF 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 6 In the **iSCSI Boot Properties** tab, review or modify the following properties:

Table 146: PXE Boot/iSCSI Boot

Name	Description
PXE Boot toggle button	If enabled, the PXE boot device is visible to BIOS in a boot order configuration.
iSCSI Boot toggle button	If enabled, the iSCSI boot device is visible to BIOS in a boot order configuration.

Table 147: iSCSI Settings

Name	Description
DHCP Network toggle button	Whether DHCP Network is enabled for the vNIC. If enabled, the initiator network configuration is obtained from the DHCP server.
DHCP iSCSI toggle button	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.

Name	Description
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.

Table 148: Initiator Area

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.
Initiator Priority drop-down list	Allows you to select one of the following: • Primary • Secondary
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.
IP Address field	The IP address of the iSCSI initiator.

Name	Description
Subnet Mask field	The subnet mask for the iSCSI initiator.
Gateway field	The default gateway.
Primary DNS field	The primary DNS server address.
Secondary DNS field	The secondary DNS server address.

Table 149: Primary Target

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.

Table 150: Secondary Target

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 7 In the **usNIC Properties** tab, review or modify the following properties:

Table 151: usNIC Properties

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.
Receive Queue Count field	The number of receive queue resources to allocate. Enter an integer between 1 and 256.
Transmit Queue Count field	The number of transmit 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.
Large Receive toggle button	If enabled, 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 Segment Offload toggle button	If enabled, 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).
TCP Tx Checksum toggle button	If enabled, 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 toggle button	If enabled, 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.

What to do next

Reboot the server to create the vHBA.

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, 1457, and 1467 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 Beginning with the release 4.3(6), you cannot create a vNIC if **Physical NIC Mode** is enabled.

Procedure

Step 1 From the **Apps** drop-down list, select **Networking**.

Step 2 From the **Actions** drop-down list, select **VIC** > **Create Virtual NIC Interface**.

Add vNIC dialog box is displayed.

Step 3 Under **Select Cisco VIC Adapter**, update the following properties and click **Next**.

Table 152: Select Cisco VIC Adapter

Name	Description
Slot drop-down list	
Next button	Click **Next** to continue.

Step 4 Under **General Settings**, update the following properties and click **Next**.

Table 153: General Settings

Name	Description
Name field	The name of the virtual NIC.
PCI Order field	The order in which this vNIC will be used. To specify an order, enter an integer within the displayed range.
Uplink Port drop-down list	The uplink port associated with the vNIC. All traffic for this vNIC goes through this uplink port.
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.

Name	Description
Channel field	The channel associated with the vNIC, if any. **Note** VNTAG mode is required for this option. :
Advance Options toggle button	Allows yout to enable or disable advance properties.
MAC Address toggle button	Allows you to enable automatic the MAC address for the vNIC.
MAC Address field	Allows you to enter MAC address manually.
NVGRE toggle button	Allows you to enable or disable Network Virtualization using Generic Routing Encapsulation.
VXLAN toggle button	Allows you to enable Virtual Extensible LAN.
PTP toggle button	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.
aRFS toggle button	Allows yout to enable or disable Accelerated Receive Flow steering (aRFS).

Name	Description
Geneve Offload toggle button	

Name	Description
	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. 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** Cisco UCS C220 M7 and C240 M7 servers do not support Cisco VIC 14xx series. **Note** You cannot enable the following when **Geneve Offload** is enabled in a setup with Cisco VIC 15xxx: • aRFS

Name	Description
	• 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 4.2(2a).
Advanced Filter toggle button	Enable this feature for advanced filter options in vNICs.
PXE Boot toggle button	Whether PXE boot is enabled for this vNIC.
Uplink Failover toggle button	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. :

Name	Description
QinQ Offload toggle button	Cisco IMC provides VIC QinQ Tunneling support for Cisco UCS M7 servers with Cisco UCS VIC 14xx series and 15xxx series VIC adapters. Check this box to enable the **QinQ Offload** option on the specified vNIC. **Note** VIC QinQ Tunneling is not supported on 13xx adapters. You cannot enable the following when **QinQ Offload** 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 **QinQ Offload** 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.
Default VLAN toggle button	Allows you to enable the number of the default VLAN associated with the vNIC.
Number of Default VLAN field	Enter the number of default VLAN.
Rate Limit toggle button	Allows you to enable or disable unlimited data rate. If you want vNIC to have an unlimited data rate, select OFF. Otherwise, enable the toggle button and enter a rate limit in the associated Rate Limit field.
Rate Limit field	Enter a rate limit value between 1 and 50000.

Name	Description
MTU field	The maximum transmission unit, or packet size, that this vNIC accepts. Enter an integer between 1500 and 9000.
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.
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.
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.
Port Profile field	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.
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.
Next button	Click **Next** to continue.

Step 5 Under **Ethernet Interrupt**, update the following properties and click **Next**.

Table 154: Ethernet Interrupt

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.
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.
Next button	Click **Next** to continue.

Step 6 Under **TCP Offload**, update the following properties and click **Next**.

Table 155: TCP Offload

Name	Description
TCP Large Receive toggle button	If enabled, 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.

Name	Description
TCP Segmentation Offload toggle button	If enabled, 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).
TCP Rx Offload Checksum Validation toggle button	If enabled, 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.
TCP Tx Offload Checksum Generation toggle button	If enabled, 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.
Next button	Click **Next** to continue.

Step 7 Under **VMQ Settings**, update the following properties and click **Next**.

Table 156: VMQ Settings

Name	Description
VMQ toggle button	Allows you to enable or disable Virtual Machine Queue (VMQ).
Multi Queue toggle button	Allows you 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 toggle button	Enable this option 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.

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.
Next button	Click **Next** to continue.

Step 8 Under **RoCE Properties**, update the following properties and click **Next**.

Table 157: RoCE Properties

Name	Description
RoCEv2 toggle button	Check the check box to change the RoCE Properties. **Note** If **Enable Multi Queue** is enabled, ensure that **RDMA Mode 2** is also enabled.
Queue Pairs field	The number of queue pairs per adapter. Enter an integer between 1 and 8192. 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 256. 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 drop-down list	This field is read-only and is set to 5. **Note** This option is available only on some of the adapters.
Next button	Click **Next** to continue.

Step 9 Under **Queue Settings**, update the following properties and click **Next**.

Table 158: Queue Settings

Name	Description
Receive Queue Count field	The number of receive queue resources to allocate. Enter an integer between 1 and 256.
Transmit Queue Count field	The number of transmit 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.
Receive Queue Ring Size field	The number of descriptors in each receive queue. Enter an integer between 64 and 4096.
Transmit Queue Ring Size field	The number of descriptors in each transmit queue. Enter an integer between 64 and 4096.
Completion Queue Ring Size field	The number of descriptors in each completion queue. This value cannot be changed.
Next button	Click **Next** to continue.

Step 10 Under **SR-IOV Properties**, update the following properties and click **Next**.

Table 159: SR-IOV Properties

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.

Name	Description
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 Per VF 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.
Next button	Click **Next** to continue.

Step 11 Under **Summary**, review the information and click **Next**.

Cloning a vNIC

Procedure

Step 1 From the **Apps** drop-down list, select **Networking**.

Step 2 Select the **vNIC Interfaces** tab.

Step 3 Select the vNIC Interface which you wish to clone and click **Clone vNIC** button.

Clone vNIC dialog box is displayed.

Step 4 Update the following properties in the **Clone vNIC** dialog box.

Table 160: Clone vNIC

Name	Description
Name field	Allows you to enter a user defined name.
Uplink Port drop-down list	The uplink port associated with this vNIC. All traffic for this vNIC goes through this uplink port. Select 0 or 1.
PCIe Order field	This is the order in which the vNIC is used. Enter an integer between 0 and 4.

Name	Description
VLAN Mode drop-down list	The mode for the associated VLAN. This can be one of the following: • TRUNK • ACCESS If you want to use VLAN trunking, select TRUNK. Otherwise, select ACCESS.
Default VLAN toggle button and field	If there is no default VLAN for this vNIC, disable Default VLAN. Otherwise, enable Default VLAN and enter a VLAN ID between 1 and 4094 in the field.
Channel Number field	Select the channel number which is assigned to this vNIC. Enter an integer between 0 and 1000.
Clone vNIC button	Allows you to clone a vNIC.

Step 5 Click **Clone vNIC** to save the changes.

Deleting a vNIC

Procedure

Step 1 From the **Apps** drop-down list, select **Networking**.

Step 2 Select the **vNIC Interfaces** tab.

Step 3 Select the **vNIC Interfaces** which you wish to delete and click **Delete vNIC** button.

Note
You cannot delete either of the two default vNIC, **eth0** or **eth1**.

Step 4 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 as an admin to perform this procedure.
- 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

Before you begin

You must log in as an admin to perform this procedure.

Beginning with the Cisco IMC release 6.0, you can configure iSCSI boot capability for **IPv6** in a vNIC.

Note The following list are the requirements to configure iSCSI boot capability for IPv6 in a vNIC:

- The minimum supported versions to enable iSCSI boot capability for IPv6 in a vNIC are Cisco IMC 6.0 release components (Cisco IMC, BIOS, VIC).
- Supported servers: Cisco UCS M6 servers and later (only in UEFI boot mode).
- Default iSCSI port number must be 3260 for iSCSI Boot.
- iSCSI DHCP vendor options 43 and 17 are not supported for IPv6.
- iSCSI supported Boot LUN ID <=255 in the LUN ID filed for primary and secondary targets.

Procedure

Step 1 From the **Apps** drop-down list, select **Networking**.

Step 2 Select the **vNIC Interfaces** tab.

Step 3 Select the vNIC Interface which you wish to modify the properties and click the Name column.

vNIC Properties dialog box is displayed.

Step 4 Select the **iSCSI Boot Properties** tab.

You can view or modify the following properties:

Table 161: PXE Boot/iSCSI Boot

Name	Description
PXE Boot toggle button	If enabled, the PXE boot device is visible to BIOS in a boot order configuration.
iSCSI Boot toggle button	If enabled, the iSCSI boot device is visible to BIOS in a boot order configuration.

Table 162: iSCSI Settings

Name	Description
DHCP Network toggle button	Whether DHCP Network is enabled for the vNIC. If enabled, the initiator network configuration is obtained from the DHCP server.
DHCP iSCSI toggle button	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.

Table 163: Initiator Area

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.
Initiator Priority drop-down list	Allows you to select one of the following: • Primary • Secondary
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.
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.
Secondary DNS field	The secondary DNS server address.

Table 164: Primary Target

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.

Name	Description
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.

Table 165: Secondary Target

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 5 Click **Save**.

Removing iSCSI Boot Configuration from a vNIC

Before you begin

You must log in as an admin to perform this procedure.

Procedure

Step 1 From the **Apps** drop-down list, select **Networking**.

Step 2 Select the **vNIC Interfaces** tab.

Step 3 Select the vNIC Interface which you wish to modify the properties and click the Name column.

vNIC Properties dialog box is displayed.

Step 4 Select the **iSCSI Boot Properties** tab.

Step 5 Click the **iSCSI Boot** toggle button to disable iSCSI boot.

What to do next

Reboot the server to remove the iSCSI Boot Configuration.

Managing Cisco usNIC

Viewing and Configuring Cisco usNIC on a vNIC

Before you begin

You must log in as an admin to perform his procedure.

Procedure

Step 1 From the **Apps** drop-down list, select **Networking**.

Step 2 Select the **vNIC Interfaces** tab.

Step 3 Select the vNIC Interface which you wish to modify the properties and click the Name column.

vNIC Properties dialog box is displayed.

Step 4 Select the **usNIC Properties** tab.

Step 5 In the **usNIC Properties** area, review and update the following fields.

Table 166: usNIC Properties

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.
Receive Queue Count field	The number of receive queue resources to allocate. Enter an integer between 1 and 256.
Transmit Queue Count field	The number of transmit queue resources to allocate. Enter an integer between 1 and 256.

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 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.
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.
Large Receive toggle button	If enabled, 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.

Name	Description
TCP Segment Offload toggle button	If enabled, 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).
TCP Tx Checksum toggle button	If enabled, 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 toggle button	If enabled, 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 6 Click **Save Changes**.

The changes take effect upon the next server reboot.

Backing Up and Restoring the Adapter Configuration

Exporting the Adapter Configuration

Before you begin

Obtain the remote server IP address.

Procedure

Step 1 From the **Apps** drop-down list, select **Networking**.

Step 2 From the **Actions** drop-down list, select **VIC** > **Export vNIC**.

Export vNIC dialog box is displayed.

Step 3 In the **Export vNIC** dialog box, update the following properties:

Table 167: Export vNIC

Name	Description
Server IP/Hostname field	The IP address or hostname of the server to which you wish to export the file.
Upload Protocol button	**Note** To comply with Cisco security standards, certain insecure protocols (TFTP, FTP, HTTP) will no longer be supported in upcoming releases. We recommend using secure protocols like SFTP or SCP moving forward. The remote server type. This can be one of the following: • **TFTP** • **FTP** • **SFTP** • **SCP** • **HTTP** **Note** If you chose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message *Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*. Click Yes or No depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.
Path and Filename field	The path and filename of the configuration file on the remote server.
Username 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.

Step 4 Click **Export Configuration**.

Importing the Adapter Configuration

Procedure

Step 1 From the **Apps** drop-down list, select **Networking**.

Step 2 From the **Actions** drop-down list, select **VIC** > **Import vNIC**.

Import vNIC dialog box is displayed.

Step 3 In the **Import vNIC** dialog box, update the following properties:

Table 168: Import vNIC

Name	Description
Server IP/Hostname field	The IP address or hostname of the server on which the configuration file resides.
Upload Protocol button	**Note** To comply with Cisco security standards, certain insecure protocols (TFTP, FTP, HTTP) will no longer be supported in upcoming releases. We recommend using secure protocols like SFTP or SCP moving forward. The remote server type. This can be one of the following: • **TFTP** • **FTP** • **SFTP** • **SCP** • **HTTP** **Note** If you chose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message *Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*. Click Yes or No depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.
Path and Filename field	The path and filename of the configuration file on the remote server.
Username 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.

Step 4 Click **Import Configuration**.

What to do next

Reboot the server to apply the imported configuration.

Restoring Adapter Defaults

Procedure

Step 1 From the **Apps** drop-down list, select **Networking**.

Step 2 From the **Actions** drop-down list, select **VIC** > **Reset To Defaults**.

Reset To Defaults dialog box is displayed.

Step 3 Click **Yes** to confirm.

Resetting the Adapter

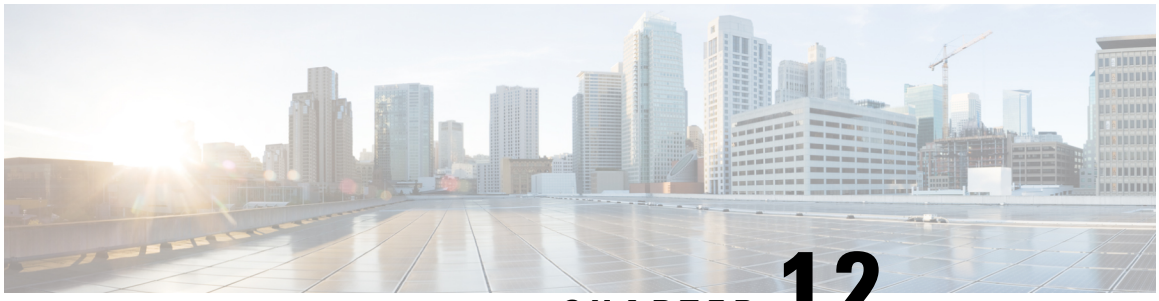
Procedure

Step 1 From the **Apps** drop-down list, select **Networking**.

Step 2 From the **Actions** drop-down list, select **VIC** > **Reset**.

Reset dialog box is displayed.

Step 3 Click **OK** to confirm.



CHAPTER 12

Managing Storage Adapters

•

• Self Encrypting Drives (Full Disk Encryption), on page 332
• Create Virtual Drive from Unused Physical Drives, on page 335
• Create Virtual Drive from an Existing Drive Group, on page 338
• Setting a Virtual Drive as Transport Ready, on page 341
• Importing Foreign Configuration, on page 341
• Clearing Foreign Configuration, on page 342
• Clearing a Boot Drive, on page 343
• Enabling a JBOD, on page 344
• Disabling a JBOD, on page 344
• Retrieving TTY Logs for a Controller, on page 344
• Clearing Controller Configuration, on page 345
• Restoring Storage Controller to Factory Defaults, on page 345
• Preparing a Drive for Removal, on page 346
• Making a Dedicated Hot Spare, on page 347
• Making a Global Hot Spare, on page 348
• Removing a Drive from Hot Spare Pools, on page 348
• Toggling Physical Drive Status, on page 349
• Setting a Physical Drive as a Controller Boot Drive, on page 349
• Initializing a Virtual Drive, on page 350
• Set as Boot Drive, on page 351
• Editing a Virtual Drive, on page 352
• Deleting a Virtual Drive, on page 354
• Hiding a Virtual Drive, on page 355
• Starting Learn Cycles for a Battery Backup Unit, on page 355
• Viewing Storage Controller Logs, on page 356
• Viewing SSD Smart Information for MegaRAID Controllers, on page 357
• Viewing NVMe Controller Details, on page 358
• Viewing NVMe Physical Drive Details, on page 359
• Viewing PCI Switch Details, on page 361
• Starting Copyback Operation, on page 365
• Managing the Flexible Flash Controller, on page 366
• Managing the FlexUtil Controller, on page 382

• Cisco Boot Optimized M.2 Raid Controller, on page 395
• Cisco FlexMMC, on page 407

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

Before you begin

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

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.

Step 2 From **Storage** > **Controllers**, click the appropriate LSI MegaRAID controller.

Step 3 In the **Actions** drop-down list on the right pane, click **Storage** > **Enable Drive Security**.

The **Enable Drive Security** dialog box appears.

Step 4 In the **Enable Drive Security** dialog box, review the following information:

Name	Description
Controller Security field	Indicates whether or not controller security is enabled. This can be one of the following: • **True**— Controller security is enabled. • **False**— 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.
Confirm Security Key field	Re-enter the security key.
Suggest button	Suggests the security key or key ID that can be used.
Save button	Saves the data.
Cancel button	Cancels the action.

Step 5 Click **Save**.

Modifying Controller Security

Before you begin

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

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.

Step 2 From **Storage** > **Controllers**, click the appropriate LSI MegaRAID controller.

Step 3 In the **Actions** drop-down list on the right pane, click **Storage** > **Modify Drive Security**.

The **Modify Drive Security** dialog box appears.

Step 4 In the **Modify Drive Security** dialog box, review the following information:

Name	Description
Controller Security field	Indicates whether or not controller security is enabled. This can be one of the following: • **True**— Controller security is enabled. • **False**— 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.
Confirm Security Key field	Re-enter the security key.
Suggest button	Suggests the security key or key ID that can be used.
Save button	Saves the data.
Cancel button	Cancels the action.

Step 5 Click **Save**.

Disabling Controller Security

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.

Step 2 From **Storage** > **Controllers**, click the appropriate LSI MegaRAID controller.

Step 3 In the **Actions** drop-down list on the right pane, click **Storage** > **Disable Drive Security**.

Click **Yes** or **No** at the prompt.

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.

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.

Step 2 From **Storage** > **Controllers**, click the appropriate LSI MegaRAID controller.

Step 3 In the **Controller Info** tab on the right pane, from the **Actions** drop-down list, select **Switch to Local Key Management** to switch the controller security from remote to local 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, select **Switch to Remote Key Management**.

Step 5 Click **OK** to confirm.

Create Virtual Drive from Unused Physical Drives

Before you begin

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

This is available only on some C-series servers.

Note Cisco IMC now supports single drive support in M.2 RAID controller along with existing dual drive support. With single drive support, you cannot create a virtual disk.

SUMMARY STEPS

1. From the **Apps** drop-down list, select **Storage**.
2. From **Storage** > **Controllers**, click the appropriate LSI MegaRAID controller.
3. On the right pane, click the **Virtual Drive Info** tab.
4. From the **Actions** drop-down list on the right pane, click **Storage** > **Create Virtual Drive**.
5. In the **Select Controller**
6. In the **Create / Carve VD** page, enter the following information:
7. In the **RAID Type & PDs** page, enter the following information:
8. In the **VD Properties** page, enter the following information:
9. In the **Summary** page, review the information and click **Create**.

DETAILED STEPS

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.

Step 2 From **Storage** > **Controllers**, click the appropriate LSI MegaRAID controller.

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

Step 4 From the **Actions** drop-down list on the right pane, click **Storage** > **Create Virtual Drive**.

The **Create Virtual Drive** pane is displayed.

Step 5 In the **Select Controller**

Name	Description
MRAID drop-down list	Select the MRAID from the drop-down list and click **Next**.

Step 6 In the **Create / Carve VD** page, enter the following information:

Name	Description
From Unused Physical Drives radio button	Select this option to create a VD from unused physical drives
From Existing Drive Group radio button	Select this option to create a VD from existing groups.
Virtual Drive drop-down list	This option is available only with **From Existing Drive Group**. Select the VD from the list and click **Next**.

Step 7 In the **RAID Type & PDs** page, enter the following information:

RAID Type

Table 169: RAID Type

Name	Description
RAID Type drop-down list	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. • **Raid 00**—Spanned striping.

Note
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.

Physical Drives

Table 170: Physical Drives

Name	Description
Physical Drives table	A list of physical drives that are not already included in a drive group.
ID column	The ID of the physical drive.
Size (GB) column	The size of the physical drive in MB.
Model column	The drive vendor name.
Interface Type column	Whether the drive is SAS or SATA
Type column	Type of the drive SSD or HDD.
> button	Adds the drive selected in the **Physical Drives** table to the drive group.
< button	Removes the drive selected in the **Drive Groups** table from the drive group.
Drives/Span table	A list of drive groups
Name column	The name of the drive group to be created.

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.

Step 8 In the **VD Properties** page, enter the following information:

Table 171: Virtual Drives in this group

Name	Description
ID column	The ID of the virtual drive.
Name column	The name of the virtual drive.
Size (MB) column	The size of the virtual drive.

Step 9 In the **Summary** page, review the information and click **Create**.

Create Virtual Drive from an Existing Drive Group

Before you begin

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

SUMMARY STEPS

1. From the **Apps** drop-down list, select **Storage**.
2. From **Storage** > **Controllers**, click the appropriate LSI MegaRAID controller.
3. On the right pane, click the **Virtual Drive Info** tab.
4. From the **Actions** drop-down list on the right pane, click **Storage** > **Create Virtual Drive**.
5. In the **Select Controller**
6. In the **Create / Carve VD** page, enter the following information:
7. In the **RAID Type & PDs** page, enter the following information:
8. In the **VD Properties** page, enter the following information:
9. In the **Summary** page, review the information and click **Create**.

DETAILED STEPS

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.

Step 2 From **Storage** > **Controllers**, click the appropriate LSI MegaRAID controller.

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

Step 4 From the **Actions** drop-down list on the right pane, click **Storage** > **Create Virtual Drive**.

The **Create Virtual Drive** pane is displayed.

Step 5 In the **Select Controller**

Name	Description
MRAID drop-down list	Select the MRAID from the drop-down list and click **Next**.

Step 6 In the **Create / Carve VD** page, enter the following information:

Name	Description
From Unused Physical Drives radio button	Select this option to create a VD from unused physical drives
From Existing Drive Group radio button	Select this option to create a VD from existing groups.
Virtual Drive drop-down list	This option is available only with **From Existing Drive Group**. Select the VD from the list and click **Next**.

Step 7 In the **RAID Type & PDs** page, enter the following information:

RAID Type

Table 172: RAID Type

Name	Description
RAID Type drop-down list	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. • **Raid 00**—Spanned striping.

Note

- **Configure RAID Type** is available only when **From Existing Drive Group** is selected.
- 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.

Physical Drives

Table 173: Physical Drives

Name	Description
Physical Drives table	A list of physical drives that are not already included in a drive group.
ID column	The ID of the physical drive.
Size (GB) column	The size of the physical drive in MB.
Model column	The drive vendor name.
Interface Type column	Whether the drive is SAS or SATA
Type column	Type of the drive SSD or HDD.
> button	Adds the drive selected in the **Physical Drives** table to the drive group.
< button	Removes the drive selected in the **Drive Groups** table from the drive group.
Drives/Span table	A list of drive groups
Name column	The name of the drive group to be created.

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.

Size is available only when **From Existing Drive Group** is selected.

Table 174: Size

Name	Description
Size drop-down list	The size of the virtual drive you want to create.

Step 8 In the **VD Properties** page, enter the following information:

Table 175: Virtual Drives in this group

Name	Description
ID column	The ID of the virtual drive.
Name column	The name of the virtual drive.
Size (MB) column	The size of the virtual drive.

Virtual Drives in this group is available only when **From Existing Drive Group** is selected.

Step 9 In the **Summary** page, review the information and click **Create**.

Setting a Virtual Drive as Transport Ready

Before you begin

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

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.

Step 2 From **Storage** > **Controllers**, click the appropriate LSI MegaRAID controller.

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

Step 4 In the **Virtual Drives** area, choose the drive and click **Set Transport Ready**.

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

Step 5 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**.

Importing Foreign Configuration

When a set of physical drives hosting a secured drive group are inserted into a different server or controller (or the same controller but whose security-key has been changed while they were not present), they become foreign configurations. Since they are secured, these foreign configurations must be unlocked by verifying their security key information before they can be imported.

Complete the following steps to verify the security key for a foreign configuration and import the configuration:

Before you begin

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

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.

Step 2 From **Storage** > **Controllers**, click the appropriate LSI MegaRAID controller.

Step 3 On the **Storage** tab, click the appropriate LSI MegaRAID controller.

Step 4 On the right pane, click the **Controller Info** tab.

Step 5 In the **Actions** drop-down list, click **Storage** > **Import Foreign Config**.

The **Import Foreign Config** window is displayed with the following message:

Are you sure you want import foreign config?

Click **OK**.

This action opens the **Secure Key Verification** dialog box. Review the following information before proceeding:

Table 176: Secure Key Verification Area

Name	Description
Security Key field	Unique key ID assigned to a controller.
Verify button	Verifies if the key you entered matches the stored key information. If the secure key is verified to be correct, the requested action is completed.
Cancel button	Cancels the action.

Step 6 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.

SUMMARY STEPS

1. From the **Apps** drop-down list, select **Storage**.
2. From **Storage** > **Controllers**, click the appropriate LSI MegaRAID controller.
3. On the **Storage** tab, click the appropriate LSI MegaRAID controller.
4. On the right pane, click the **Controller Info** tab.
5. In the **Actions** drop-down list on the right pane, click **Storage** > **Clear Foreign Config**.
6. Click **OK** to confirm.

DETAILED STEPS

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.
Step 2 From **Storage** > **Controllers**, click the appropriate LSI MegaRAID controller.
Step 3 On the **Storage** tab, click the appropriate LSI MegaRAID controller.
Step 4 On the right pane, click the **Controller Info** tab.
Step 5 In the **Actions** drop-down list on the right pane, click **Storage** > **Clear Foreign Config**.
Step 6 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.

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.
Step 2 From **Storage** > **Controllers**, click the appropriate LSI MegaRAID controller.
Step 3 In the **Actions** drop-down list on the right pane, click **Storage** > **Clear Boot Drive**.
Step 4 Click **OK** to confirm.

Enabling a JBOD

Note You can enable Just a Bunch Of Disks (JBOD) only on some UCS C-Series servers.

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.
Step 2 From **Storage** > **Controllers**, click the appropriate LSI MegaRAID controller.
Step 3 On the right pane, click the **Controller Info** tab.
Step 4 In the **Actions** drop-down list on the right pane, select **Enable JBOD**.
Step 5 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.

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.
Step 2 From **Storage** > **Controllers**, click the appropriate LSI MegaRAID controller.
Step 3 On the right pane, click the **Controller Info** tab.
Step 4 In the **Actions** drop-down list on the right pane, click **Disable JBOD**.
Step 5 Click **OK** to confirm.

Retrieving TTY Logs for a Controller

This task retrieves the TTY 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.

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.

Step 2 From **Storage** > **Controllers**, click the appropriate LSI MegaRAID controller.

Step 3 On the right pane, click the **Controller Info** tab.

Step 4 In the **Actions** area, click **Get TTY Log**.

Step 5 Click **OK** to confirm.

Important
Retrieving TTY 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.

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.

Step 2 From **Storage** > **Controllers**, click the appropriate LSI MegaRAID controller.

Step 3 In the **Actions** drop-down list on the right pane, click **Storage** > **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.

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.
Step 2 From **Storage** > **Controllers**, click the appropriate LSI MegaRAID controller.
Step 3 In the **Actions** drop-down list on the right pane, click **Storage** > **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.

SUMMARY STEPS

1. From the **Apps** drop-down list, select **Storage**.
2. From **Storage** > **Controllers**, click the appropriate LSI MegaRAID controller.
3. On the right pane, click the **Physical Drive Info** tab.
4. Select the drive you want to remove.
5. Click the 3 horizontal dots near the selected drive and select **Prepare for Removal** from the drop-down list.
6. Click **OK** to confirm.

DETAILED STEPS

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.
Step 2 From **Storage** > **Controllers**, click the appropriate LSI MegaRAID controller.
Step 3 On the right pane, click the **Physical Drive Info** tab.
Step 4 Select the drive you want to remove.
Step 5 Click the 3 horizontal dots near the selected drive and select **Prepare for Removal** from the drop-down list.
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.

SUMMARY STEPS

1. From the **Apps** drop-down list, select **Storage**.
2. From **Storage** > **Controllers**, click the appropriate LSI MegaRAID controller.
3. On the right pane, click the **Physical Drive Info** tab.
4. In the **Physical Drive Info** tab, select the physical drive you want to make a dedicated hot spare.
5. Click the 3 horizontal dots and select **Make Dedicated Hot Spare** from the drop-down list.
6. In the **Virtual Drive Details** area, update the following properties:
7. Click **Make Dedicated Hot Spare** to confirm.

DETAILED STEPS

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.

Step 2 From **Storage** > **Controllers**, click the appropriate LSI MegaRAID controller.

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

Step 4 In the **Physical Drive Info** tab, select the physical drive you want to make a dedicated hot spare.

Step 5 Click the 3 horizontal dots and select **Make Dedicated Hot Spare** from the drop-down list.

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.
Physical Drive Number field	The number of the physical drive.

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.

SUMMARY STEPS

1. From the **Apps** drop-down list, select **Storage**.
2. From **Storage** > **Controllers**, click the appropriate LSI MegaRAID controller.
3. On the right pane, click the **Physical Drive Info** tab.
4. In the **Physical Drive Info** tab, select the physical drive you want to make a global hot spare.
5. Click the 3 horizontal dots and select **Make Global Hot Spare** from the drop-down list.

DETAILED STEPS

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.

Step 2 From **Storage** > **Controllers**, click the appropriate LSI MegaRAID controller.

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

Step 4 In the **Physical Drive Info** tab, select the physical drive you want to make a global hot spare.

Step 5 Click the 3 horizontal dots and select **Make Global Hot Spare** from the drop-down list.

Removing a Drive from Hot Spare Pools

Before you begin

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

SUMMARY STEPS

1. From the **Apps** drop-down list, select **Storage**.
2. From **Storage** > **Controllers**, click the appropriate LSI MegaRAID controller.
3. On the right pane, click the **Physical Drive Info** tab.
4. In the **Physical Drive Info** tab, select the global or dedicated hot spare you want to remove from the hot spare pools.
5. Click **Remove From Hot Spare Pools**.

DETAILED STEPS

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.
Step 2 From **Storage** > **Controllers**, click the appropriate LSI MegaRAID controller.
Step 3 On the right pane, click the **Physical Drive Info** tab.
Step 4 In the **Physical Drive Info** tab, select the global or dedicated hot spare you want to remove from the hot spare pools.
Step 5 Click **Remove From Hot Spare Pools**.

Toggling Physical Drive Status

Before you begin

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

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.
Step 2 From **Storage** > **Controllers**, click the appropriate LSI MegaRAID controller.
Step 3 On the right pane, click the **Physical Drive Info** tab.
Step 4 In the **Physical Info** tab, select the drive you want to set as unconfigured good.
Step 5 Click the three horizontal dots near the selected drive and click **Set State as Unconfigured Good** from the drop-down list.
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.

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.
Step 2 From **Storage** > **Controllers**, click the appropriate LSI MegaRAID controller.
Step 3 On the right pane, click the **Physical Drive Info** tab.
Step 4 In the **Physical Drive Info** tab, select the drive you want to set as boot drive for the controller.
Step 5 Click the three horizontal dots near the selected drive and select **Set as Boot Drive** from the drop-down list.
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.

SUMMARY STEPS

1. From the **Apps** drop-down list, select **Storage**.
2. From **Storage** > **Controllers**, click the appropriate LSI MegaRAID controller.
3. On the right pane, click the **Virtual Drive Info** tab.
4. In the **Virtual Drive Info** tab, choose the drive that you want to initialize.
5. Click the 3 horizontal dots near the selected drive and click **Initialize** from the drop-down list.
6. Choose the type of initialization you want to use for the virtual drive.
7. Click **Initialize VD** to initialize the drive, or **Cancel** to close the dialog box without making any changes.
8. To view the status of the task running on the drive, in the **Operations** area, click **Refresh**.

DETAILED STEPS

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.
Step 2 From **Storage** > **Controllers**, click the appropriate LSI MegaRAID controller.
Step 3 On the right pane, click the **Virtual Drive Info** tab.
Step 4 In the **Virtual Drive Info** tab, choose the drive that you want to initialize.
Step 5 Click the 3 horizontal dots near the selected drive and click **Initialize** from the drop-down list.

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

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

This can be one of the following:

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

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

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

The following details are displayed:

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

Set as Boot Drive

Before you begin

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

SUMMARY STEPS

1. From the **Apps** drop-down list, select **Storage**.
2. From **Storage** > **Controllers**, click the appropriate LSI MegaRAID controller.
3. On the right pane, click the **Physical Drive Info** tab.
4. In the **Physical Drive Info** tab, choose the drive from which the controller must boot.
5. Click the 3 horizontal dots near the selected drive and click **Set as Boot Drive**.
6. Click **OK** to confirm.

DETAILED STEPS

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.

Step 2 From **Storage** > **Controllers**, click the appropriate LSI MegaRAID controller.

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

Step 4 In the **Physical Drive Info** tab, choose the drive from which the controller must boot.

Step 5 Click the 3 horizontal dots near the selected drive and click **Set as Boot Drive**.

Step 6 Click **OK** to confirm.

Editing a Virtual Drive

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.

Step 2 From **Storage** > **Controllers**, click the appropriate LSI MegaRAID controller.

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

Step 4 Click the 3 horizontal dots near the selected drive and click **Edit Virtual Drive**.

Step 5 Review the instructions, and then click **OK**.
The Edit Virtual Drive dialog box displays.

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.

SUMMARY STEPS

1. From the **Apps** drop-down list, select **Storage**.
2. From **Storage** > **Controllers**, click the appropriate LSI MegaRAID controller.
3. On the right pane, click the **Virtual Drive Info** tab.
4. In the **Virtual Drive Info** tab, select the virtual drive you want to delete.
5. Click the 3 horizontal dots near the selected drive and click **Delete Virtual Drive**.
6. Click **OK** to confirm.

DETAILED STEPS

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.

Step 2 From **Storage** > **Controllers**, click the appropriate LSI MegaRAID controller.

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

Step 4 In the **Virtual Drive Info** tab, select the virtual drive you want to delete.

Step 5 Click the 3 horizontal dots near the selected drive and click **Delete Virtual Drive**.

Step 6 Click **OK** to confirm.

Hiding a Virtual Drive

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.
Step 2 From **Storage** > **Controllers**, click the appropriate LSI MegaRAID controller.
Step 3 On the right pane, click the **Virtual Drive Info** tab.
Step 4 In the **Virtual Drive Info** tab, select the virtual drive you want to hide.
Step 5 Click the 3 horizontal dots near the selected drive and 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.

SUMMARY STEPS

1. From the **Apps** drop-down list, select **Storage**.
2. From **Storage** > **Controllers**, click the appropriate LSI MegaRAID controller.
3. On the **Storage** tab, click the appropriate LSI MegaRAID controller.
4. On the right pane, click the **Battery Backup Unit** tab.
5. From the **Actions** pane, click **Start Learn Cycle**.
6. Click **OK**.

DETAILED STEPS

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.
Step 2 From **Storage** > **Controllers**, click the appropriate LSI MegaRAID controller.
Step 3 On the **Storage** tab, click the appropriate LSI MegaRAID controller.
Step 4 On the right pane, click the **Battery Backup Unit** tab.
Step 5 From the **Actions** pane, click **Start Learn Cycle**.

A dialog prompts you to confirm the task.

Step 6 Click **OK**.

Viewing Storage Controller Logs

Before you begin

You must log in with admin privileges to perform this task

SUMMARY STEPS

1. From the **Apps** drop-down list, select **Storage**.
2. From **Storage** > **Controllers**, click the appropriate LSI MegaRAID controller.
3. On the right pane, click **Storage Log** tab and review the following information:

DETAILED STEPS

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.

Step 2 From **Storage** > **Controllers**, click the appropriate LSI MegaRAID controller.

Step 3 On the right pane, 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.

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.

Step 2 From **Storage** > **Controllers**, click the appropriate LSI MegaRAID controller.

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

Step 4 Select the drive under the column **Slot ID**.

A new pane is displayed with the drive details.

Step 5 Click the **Details** tab and review the following information:

Table 177: Product Details

Name	Description
Power Cycle Count	Number of power cycles that the drive went through from the time it was manufactured.
Power on Hours	Total number of hours that the drive is in the 'Power On' mode.
Percentage Life Left	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	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	The current temperature of the drive at which the selected SSD operates at the time of selection.
Maximum Operating Temperature	Allowable maximum temperature in which the drive can operate without errors.
Percentage Reserved Capacity Consumed	The total capacity (out of the percentage reserved for it) consumed by the drive.

Step 6 Click **Close**.

Viewing NVMe Controller Details

Before you begin

- The server must be powered on.

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.

Step 2 From **Storage** > **Controllers**, click the appropriate NVMe controller.

Step 3 In the **Controller Info** tab on the right pane, review the following information under the **General** tab.

Name	Description
Product Name	The name of the MegaRAID controller.
Product ID	Cisco part number of the RAID controller.
Composite Health	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	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. • **Unresponsive** — The controller is down.
Security	Displays the controller lock key depending on its current state. **Note** • This option is available only on some C-Series servers. • Disabling the drive security makes the data on all secure drives unusable.

Name	Description
Serial Number field	The serial number of the MegaRAID controller.
RAID Chip Temperature field	Temperature of the controller in degree centigrade.
Firmware Package Build field	The active firmware package version number. For the firmware component version numbers, see the **Running Firmware Images** area.
Consistency Check Rate field	The rate at which the controller scans the virtual drives looking for redundant data inconsistencies and fixing them. This rate is shown as a percentage of the total bandwidth available.
PCI Slot	The name of the PCIe slot in which the controller is located.
Vendor ID	The PCI vendor ID, in hexadecimal.
SubVendor ID	The PCI subvendor ID, in hexadecimal.
Device ID	The PCI device ID, in hexadecimal.
Sub Device ID	The PCI subdevice ID, in hexadecimal.
Manufactured Date	The date the MegaRAID card was manufactured, in the format yyy-mm-dd.
Revision	The board revision number, if any.
Boot Drive(s)	The number of the boot drive.
Interface Type	Whether the drive is SAS or SATA

Viewing NVMe Physical Drive Details

Before you begin

- The server must be powered on.

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.

Step 2 From **Storage** > **Controllers**, click the appropriate NVMe controller.

Step 3 Click the **Physical Drive Info** tab on the right pane and review the following information:

Name	Description
Slot ID	The name of the PCIe slot in which the controller drive is located.
Disk Type	Whether the drive is a hard drive (HDD) or a solid state drive (SSD).
Status	The physical drive status. This can be one of the following: • Copyback—The drive is busy performing a copyback operation. • Failed—The drive was in use, but it has failed. • Foreign configuration—The drive contains a foreign configuration. • Global hot spare—The drive is designated as a global spare drive. • Dedicated hot spare—The drive is designated as a dedicated spare drive. • 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. • Ready to remove—The drive is prepared for removal. • Rebuild—The drive is currently being rebuilt. • System—The drive is visible to the host and cannot be used for virtual drives. • Unconfigured bad—The drive has failed and is not in use. • Unconfigured good—The drive is ready to be assigned to a drive group or hot spare pool.
Capacity (GB)	The capacity of the drive in gigabytes.
Model	The drive vendor name.
Firmware	The firmware version running on the drive.

Step 4 Select a drive under the column **Slot ID**.

A new pane is displayed with the drive details.

View the drive details in the **General** tab.

Table 178: General Tab

Name	Description
Media Type	Whether the drive is a hard drive (HDD) or a solid state drive (SSD).
Interface Type	The drive interface type.
Sequence Number	The sequence number used by the controller to track drive changes.
Security Enabled	If this field displays **Yes**, full disk encryption is enabled on the physical drive.
Physical Block Size	Indicates the physical block size of the drive.
Slot Number	The slot number in which the physical drive resides.
Device ID	The device ID for the drive.
Product ID	The drive product ID. This field generally displays the drive model number.
UCS Product ID	
Vendor	The vendor for the drive.
Drive Firmware	The active firmware version on the drive.
Drive Serial Number	The serial number for the drive.
Raw Size	The capacity of drive in megabytes, including the space used for formatting.
Non Coerced Size	The capacity in megabytes, including space lost to coercion.
Coerced Size	The capacity in megabytes after any coercion rounding has been performed.
Negotiated Link Speed	The speed of the link between the drive and the controller.

Viewing PCI Switch Details

Before you begin

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

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.

Step 2 From **Storage** > **Controllers**, click the appropriate **PCI Switch** controller.

Step 3 Review the following information:

General Tab

Name	Description
Product Name	The name of the MegaRAID controller.
Product ID	Cisco part number of the RAID controller.
Composite Health	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	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. • **Unresponsive** — The controller is down.
Security	Displays the controller lock key depending on its current state. **Note** • This option is available only on some C-Series servers. • Disabling the drive security makes the data on all secure drives unusable.
Serial Number field	The serial number of the MegaRAID controller.
RAID Chip Temperature field	Temperature of the controller in degree centigrade.
Firmware Package Build field	The active firmware package version number. For the firmware component version numbers, see the **Running Firmware Images** area.

Name	Description
Consistency Check Rate field	The rate at which the controller scans the virtual drives looking for redundant data inconsistencies and fixing them. This rate is shown as a percentage of the total bandwidth available.
PCI Slot	The name of the PCIe slot in which the controller is located.
Vendor ID	The PCI vendor ID, in hexadecimal.
SubVendor ID	The PCI subvendor ID, in hexadecimal.
Device ID	The PCI device ID, in hexadecimal.
Sub Device ID	The PCI subdevice ID, in hexadecimal.
Manufactured Date	The date the MegaRAID card was manufactured, in the format yyy-mm-dd.
Revision	The board revision number, if any.
Boot Drive(s)	The number of the boot drive.
Interface Type	Whether the drive is SAS or SATA

Settings Area

Table 179: Settings Area

Name	Description
Physical Drive Status Auto Config Mode	The physical drive status auto config mode that you select for the controller. This can be one of the following: • Unconfigured Good - The default option. Select this option if you are using the server for RAID volume and mixed JBOD. • RAID-0 Write Back - Select this option if you are using the server for per drive R0 WB. • JBOD - Select this option if you are using the server for JBOD only.
Rebuild Rate	The rate at which the controller rebuilds degraded RAID volumes. This rate is shown as a percentage of the total bandwidth available.

Name	Description
Patrol Read Rate	The rate at which the controller performs a background read of the physical drives looking for inconsistent data. This rate is shown as a percentage of the total bandwidth available.
Consistency Check Rate	The rate at which the controller scans the virtual drives looking for redundant data inconsistencies and fixing them. This rate is shown as a percentage of the total bandwidth available.
ECC Bucket Leak Rate	The error correcting code (ECC) single-bit error bucket leak rate, in minutes. With ECC, the controller increments an error counter when it encounters a single bit error while reading from a physical drive. The controller decrements the error counter each time the number of minutes defined in this field passes. If the error counter reaches a system-defined maximum, the controller sends an event message to the system.
JBOD	If this field displays true, JBOD is enabled.
Maintain PD Fail History	If this field displays true, the controller remembers which physical drives were determined to be bad across server reboots.
Battery Warning	If this field displays true, missing battery warnings are disabled.

Table 180: HW Config Area

Name	Description
Controller SAS Address	A MegaRAID controller can have up to 16 serial-attached SCSI (SAS) addresses. This field displays the first 8 SAS addresses, if they are in use.
BBU Present	If this field displays true, the battery backup unit is present.
Memory Present	If this field displays true, memory is present.
Flash Present	If this field displays true, flash memory is present.

Table 181: Capabilities Area

Name	Description
RAID Levels Supported	The RAID levels supported by the controller. This can be one or more of the following: • Raid 0—Simple striping. • Raid 1—Simple mirroring. • Raid 5—Striping with parity. • Raid 1E—Integrated offset strip mirroring • 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. • Raid srl-03—Spanned secondary RAID level • Raid 00—Spanned striping. • Raid 1e-rlq0—Integrated adjacent strip mirroring with no span. • Raid 1e0-rlq0—Integrated adjacent strip mirroring with span.

Table 182: Error Counters Area

Name	Description
Memory Correctable Errors	The number of correctable errors in the controller memory.

Starting Copyback Operation

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.
Step 2 From **Storage** > **Controllers**, click the appropriate LSI MegaRAID or HBA controller.
Step 3 Click the **Physical Drive Info** tab on the right pane and select a drive, which is in online state.
Step 4 In the **Actions** drop-down list, click **Start Copyback**.
Step 5 A **Start Copyback Operation** dialog box is displayed.

Step 6 Select the **Destination Physical Drive** to which the copyback operation needs to be done.

Step 7 Click **Start Copyback**.

Step 8 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 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 Cisco IMC version, or you can switch back to the FlexFlash 1.4(x) configuration. If you choose to revert to the latest 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 controller properties before using any virtual drives, or power down the host prior to starting this task

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.

Step 2 On the **Storage** > **Cisco FlexFlash**.

Step 3 In the **Controller Info** tab on the right pane, click **Configure Operational Profile**.

Step 4 In the **Operational Profile** dialog box, update the following fields:

Table 183: Operational Profile Fields for Cisco UCS M5 Servers

Name	Description
Controller field	The system-defined name of the selected Cisco Flexible Flash controller. This name cannot be changed.
Firmware Operating Mode field	System displayed message. Displays the firmware operating mode as Mirror.
SLOT-1 Read Error Threshold field	The number of read errors that are permitted while accessing Slot 1 of the Cisco Flexible Flash card. If the number of read errors exceeds this threshold on a card, the card is marked unhealthy. To specify a read error threshold, enter an integer between 1 and 255. To specify that the card should never be disabled regardless of the number of errors encountered, enter `0` (zero).
SLOT-1 Write Error Threshold field	The number of write errors that are permitted while accessing Slot 1 of the Cisco FlexFlash card. If the number of write errors exceeds this threshold on a card, the card is marked unhealthy. To specify a write error threshold, enter an integer between 1 and 255. To specify that the card should never be disabled regardless of the number of errors encountered, enter `0` (zero).

Step 5 Click **Save**.

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.

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.

Step 2 From **Storage** > **Controllers**, click the appropriate Cisco Flexible Flash controller.

Step 3 In the **Actions** drop-down list, 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.

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.

Step 2 From **Storage** > **Controllers**, click **Cisco FlexFlash**.

Step 3 In the **Actions** drop-down list, click **Configure Cards**.
Configure Cards dialog box appears.

Step 4 In the **Configure Cards** dialog box, update the following fields:

Name	Description
Mode field	Displays the mode type as Mirror.
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 syncs 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 **Virtual Drive** 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**
Virtual Drive drop-down	The virtual drive type. This can be one of the following: • **Removable** • **Non Removable**

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 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 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 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.

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.

Step 2 From **Storage** > **Controllers**, click **FlexFlash**.

Step 3 In the **Actions** drop-down list on the right pane, 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.

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.

Step 2 From **Storage** > **Controllers**, click the appropriate Cisco FlexFlash controller.

Step 3 In the **Cisco FlexFlash** pane, click the **Controller Info** tab.

Step 4 In the **Actions** drop-down list on the right pane, click **Reset FlexFlash Controller**.

Step 5 Click **OK** to confirm.

Editing a Virtual Drive

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.

Step 2 From **Storage** > **Controllers**, click the appropriate LSI MegaRAID controller.

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

Step 4 Click the 3 horizontal dots near the selected drive and click **Edit Virtual Drive**.

Step 5 Review the instructions, and then click **OK**.
The Edit Virtual Drive dialog box displays.

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**.

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.

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.
Step 2 From **Storage** > **Controllers**, click the appropriate Cisco FlexFlash controller.
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.

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.
Step 2 From **Storage** > **Controllers**, click the appropriate Cisco FlexFlash controller.
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.

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.
Step 2 From **Storage** > **Controllers**, click the appropriate Cisco Flexible Flash controller.
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.
Step 5 Click **Add Image**.
Step 6 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**
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`**

Name	Description
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**.

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.

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.

Step 2 From **Storage** > **Controllers**, click the appropriate Cisco Flexible Flash controller.

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.

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.
Step 2 From **Storage** > **Controllers**, click the appropriate Cisco Flexible Flash controller.
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.

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.
Step 2 From **Storage** > **Controllers**, click the appropriate Cisco Flexible Flash controller.
Step 3 Click the **Controller Info** tab.
Step 4 In the **Actions** drop-down list on the right pane, click **Reset Partition Defaults**.
Step 5 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 6 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 Cisco Flexible Flash cards.
- 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.

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.

Step 2 From **Storage** > **Controllers**, click the appropriate Cisco Flexible Flash controller.

Step 3 Click the **Controller Info** tab.

Step 4 In the **Actions** drop-down list on the right pane, click **Synchronize Card Configuration**.

Step 5 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.

Name	Description
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 6 Click **Yes**.

Viewing FlexFlash Log Details

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.

Step 2 From **Storage** > **Controllers**, click the appropriate Cisco Flexible Flash controller.

Step 3 In the **FlexFlash Logs** tab > **FlexFlash LogTable** area, review the following fields:

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 • Info • Notice • Debug
Description column	A description of the event.

Step 4 In the **FlexFlash Logs** tab > **Actions** area, review the following fields:

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 + to add new filtering criteria. 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.
Filter icon	Displays or hides the quick filter fields.
Column drop-down list	Allows you to choose the columns you want to view.

Step 5 In the **FlexFlash Logs** tab > **Log Navigation Toolbar** area, review the following fields:

Name	Description
<<Newest	If there are more events than can fit on a single page, click this link to view the newest entries. The total number of entries displayed depends on the setting in the **Entries per Page** drop-down list.
<Newer	If there are more events than can fit on a single page, click this link to view the next page of entries that are newer than the set you are currently viewing.
Log Entries field	This field displays which log entries are currently being shown in the table.
Older>	If there are more events than can fit on a single page, click this link to view the next page of entries that are older than the set you are currently viewing.

Name	Description
Oldest>>	If there are more events than can fit on a single page, click this link to view the oldest entries.
Page Number drop-down list	Allows you to navigate to a specific page. Select the page number from the drop-down list.
Number of Rows field	Displays the rows displayed in the current page.

Managing the FlexUtil Controller

The Cisco UCS M5 servers support microSD memory card for storage of server software tools and utilities. Riser 1 has this microSD memory card slot. Cisco FlexUtil supports only 32GB microSD card.

The following user visible partitions are present on the microSD card:

- Server Configuration Utility (SCU) – 1.25 GB
- Diagnostics – 0.25 GB
- Host Update Utility (HUU) – 1.5 GB
- Drivers – 8 GB
- User

Note The number of partitions and size of each partition on microSD is fixed.

At any time, two partitions can be mapped onto the host. These partitions (except the user partition) can also be updated through a CIFS or NFS share. A second level BIOS boot order support is also available for all the bootable partitions.

Note User partition must be used only for storage. This partition does not support OS installations.

Configuring FlexUtil Controller Properties

Before you begin

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

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.

Step 2 From **Storage** > **Controllers**, click the appropriate Cisco FlexUtil controller.

Step 3 In the **General** tab > **Actions** area, click **Configure Operational Profile**.

Step 4 In the **Operational Profile** dialog box, update the following fields.

Name	Description
Controller field	The system-defined name of the selected Flex Util controller. This name cannot be changed.
Read Error Threshold field	The number of read errors that are permitted while accessing the Flex Util card. If the number of read errors exceeds this threshold on a card, the card is marked unhealthy. To specify a read error threshold, enter an integer between 1 and 255. To specify that the card should never be disabled regardless of the number of errors encountered, enter `0` (zero).
Write Error Threshold field	The number of write errors that are permitted while accessing the Flex Util card. If the number of write errors exceeds this threshold on a card, the card is marked unhealthy. To specify a write error threshold, enter an integer between 1 and 255. To specify that the card should never be disabled regardless of the number of errors encountered, enter `0` (zero).

Resetting FlexUtil Card Configuration

Before you begin

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

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.

Step 2 From **Storage** > **Controllers**, click the appropriate FlexUtil controller.

Step 3 In the **General** tab > **Actions** area, click **Reset Card Configuration**.

This action resets the FlexUtil card configuration to its default settings.

Viewing Cisco FlexUtil Controller Properties

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.

Step 2 From **Storage** > **Controllers**, click the appropriate FlexUtil controller.

Step 3 In the **General** tab > **General** area, review the following fields:

Name	Description
Product Name field	The name of the product.
Controller Name field	The name for the controller.
Controller Status field	The current status of the FlexUtil card. This can be one of the following: • **Card is absent** • **Card is Unhealthy** • **Metadata Read Error** • **Card access error** • **Invalid Card size** • **Metadata is in failed state** • **No partition, reset required** • **Invalid partition, reset required** • **Card is write protected**

Name	Description
Internal State field	The internal state of the controller. This can be one of the following: • **Uninitialized**—FlexUtil monitoring is not initialized. • **Initializing**—FlexUtil monitoring is initializing. • **Configuring**—The controller is determining the FlexUtil card configuration. • **OK**—The FlexUtil card is not connected to the host. • **Connecting**—The controller is connecting to the host. • **Connected**—The controller is connected to the host. • **Failed**—The controller has failed. See the **Controller Status** field for more details. • **Erasing**—The FlexUtil card is being erased. • **Updating**—The FlexUtil card is being updated. • **Resetting**—The configuration on the card is reset.

Step 4 In the **General** tab's **Physical Drive Count** area, review the following fields:

Name	Description
Physical Drive Count field	The number of FlexUtil cards detected in the server.

Step 5 In the **General** tab's **Virtual Drive Count** area, review the following fields:

Name	Description
Virtual Drive Count field	The number of virtual drives configured on the FlexUtil cards installed in the server.

Viewing Physical Drive Properties

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.

Step 2 From **Storage** > **Controllers**, click the appropriate FlexUtil controller.

Step 3 In the **Physical Drive Info** tab on the right pane, review the following fields:

Name	Description
Slot ID	The name of the PCIe slot in which the controller drive is located.
Disk Type	Whether the drive is a hard drive (HDD) or a solid state drive (SSD).
Status	The physical drive status. This can be one of the following: • Copyback—The drive is busy performing a copyback operation. • Failed—The drive was in use, but it has failed. • Foreign configuration—The drive contains a foreign configuration. • Global hot spare—The drive is designated as a global spare drive. • Dedicated hot spare—The drive is designated as a dedicated spare drive. • 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. • Ready to remove—The drive is prepared for removal. • Rebuild—The drive is currently being rebuilt. • System—The drive is visible to the host and cannot be used for virtual drives. • Unconfigured bad—The drive has failed and is not in use. • Unconfigured good—The drive is ready to be assigned to a drive group or hot spare pool.
Capacity (GB)	The capacity of the drive in gigabytes.
Model	The drive vendor name.
Firmware	The firmware version running on the drive.

Step 4 Select a drive and review the following information in the new pane:

Table 184: Product Details

Name	Description
Power Cycle Count	Number of power cycles that the drive went through from the time it was manufactured.
Power on Hours	Total number of hours that the drive is in the 'Power On' mode.
Percentage Life Left	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	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	The current temperature of the drive at which the selected SSD operates at the time of selection.
Maximum Operating Temperature	Allowable maximum temperature in which the drive can operate without errors.
Percentage Reserved Capacity Consumed	The total capacity (out of the percentage reserved for it) consumed by the drive.

Table 185: General Tab

Name	Description
Media Type	Whether the drive is a hard drive (HDD) or a solid state drive (SSD).
Interface Type	The drive interface type.
Sequence Number	The sequence number used by the controller to track drive changes.
Security Enabled	If this field displays **Yes**, full disk encryption is enabled on the physical drive.
Physical Block Size	Indicates the physical block size of the drive.
Slot Number	The slot number in which the physical drive resides.
Device ID	The device ID for the drive.

Name	Description
Product ID	The drive product ID. This field generally displays the drive model number.
UCS Product ID	
Vendor	The vendor for the drive.
Drive Firmware	The active firmware version on the drive.
Drive Serial Number	The serial number for the drive.
Raw Size	The capacity of drive in megabytes, including the space used for formatting.
Non Coerced Size	The capacity in megabytes, including space lost to coercion.
Coerced Size	The capacity in megabytes after any coercion rounding has been performed.
Negotiated Link Speed	The speed of the link between the drive and the controller.

Table 186: Health Status

Name	Description
Locator LED toggle button	Allows you to turn on or off the drive LED.
Health	This field displays the health of the physical drive.

Name	Description
State	The drive status. This can be one of the following: • **Cache degraded**—A virtual drive with a **Write Policy** of **Write Back** was changed by the controller to **Write Through** because the BBU could not guarantee the coherency of the cache. • **Copyback**—The drive is busy performing a copyback operation. • **Failed**—The drive was in use, but it has failed. • **Foreign configuration**—The drive contains a foreign configuration. • **Global hot spare**—The drive is designated as a global spare drive. • **Dedicated hot spare**—The drive is designated as a dedicated spare drive. • **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. • **Ready to remove**—The drive is prepared for removal. • **Rebuild**—The drive is currently being rebuilt. • **System**—The drive is visible to the host and cannot be used for virtual drives. • **Unconfigured bad**—The drive has failed and is not in use. • **Unconfigured good**—The drive is ready to be assigned to a drive group or hot spare pool.
Status	The physical drive status. This can be one of the following: • **JBOD**— The drive is in JBOD state. • **Predicted Failure**—The drive is marked as due to fail soon by the controller. • **Unconfigured bad**—The drive has failed and is not in use.

Name	Description
Copyback Operation Status	Copyback operation status. This can be one of the following: • **Unknown**— Percentage completed is not known. • **In Progress**— The rebuild process as seen in the **Copyback Percent Complete** field. When a hot spare is configured, and you remove a disk from the RAID group, and subsequently replace it, the rebuild occurs releasing the hot space. • **Completed**— Copyback operation is completed.
Copyback Percent Complete	Copyback operation completed, in percentage.
Power State field	The current power state. This can be one of the following: • **active**—The drive is running normally. • **powersave**—The drive has been spun down. • **transitioning**—The drive is spinning up.

Table 187: Error Count

Name	Description
Media Error Count	The number of media errors encountered since the drive was first installed or the host was rebooted.
Other Error Count	The number of non media errors encountered since the drive was first installed or the host was rebooted.
Predictive Failure Count	The number of times that the controller has predicted that the drive could fail.

Step 5 Click **Close**.

Viewing Virtual Drive Properties

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.

Step 2 From **Storage** > **Controllers**, click the appropriate FlexUtil controller.

Step 3 In the **Virtual Drive Info** tab on the right pane, review the following fields.

Table 188: Virtual Drive Info

Name	Description
ID	The number of the virtual drive. Click to see more details.
Name	The name of the virtual drive.
Status	The virtual drive state. This can be one of the following: • **Cache degraded**—The requested Write-cache policy for this drive is **Write Back**, but it is running in **Write Through** mode because the BBU is defective or is undergoing a learn cycle. • **Degraded**—One or more spans of the drive has no redundancy. • **Off Line**—The drive is not visible to the host. • **Partially Degraded**—The drive has lost some redundancy but still has partial redundancy. For example, if a 3-way RAID 1 mirrored drive lost one disk, it would still have 2-way redundancy. • **Optimal**—The drive has full redundancy.
Size (GB)	The capacity of the drive in megabytes.
RAID Level	The RAID level on the virtual drive. 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**—Striping with parity. • **Raid 60**—Spanned striping with two parity drives. • **Raid 00**—Spanned striping.
Boot Drive(s)	Whether the virtual drive has been designated as a boot drive.

Mapping an Image to a Virtual Drive

Before you begin

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

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.

Step 2 From **Storage** > **Controllers**, click the appropriate FlexUtil controller.

Step 3 Click the **Virtual Drive Info** tab on the right pane.

Step 4 Select the virtual drive and click **Add Image**.

Step 5 In the **Add New 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** • **Diagnostics** • **HUU** • **Drivers**
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. • **WWW(HTTP/HTTPS)**—HTTP-based or HTTPS-based 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`**. • **WWW(HTTP/HTTPS)**—Use http[s]://serverip/share.
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`** • **WWW(HTTP/HTTPS)** — **`http[s]://softwares/ucs-cxx-scu-3.1.9.iso`**

Name	Description
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** If you are using **WWW(HTTP/HTTPS)**, leave the field blank or enter the following: • **noauto** **Note** Before mounting the image, Cisco IMC tries to verify reachability to the end server by pinging the server. • **username=VALUE** • **password=VALUE**

Updating an Image on the Virtual Drive

Before you begin

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

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.
Step 2 From **Storage** > **Controllers**, click the appropriate FlexUtil controller.
Step 3 Click the **Virtual Drive Info** tab on the right pane.
Step 4 Click the **Virtual Drives** tab.
Step 5 In the **Virtual Drives** area, select the virtual drive for which you want to update an image and click **Update Image**.
Step 6 Optional: If you want to cancel an ongoing update operation, click **Cancel Update**.

Unmapping an Image From a Virtual Drive

Before you begin

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

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.
Step 2 From **Storage** > **Controllers**, click the appropriate FlexUtil controller.
Step 3 Click the **Virtual Drive Info** tab on the right pane.
Step 4 Select the virtual drive for which you want to delete the image and click **Unmap Image**.

Erasing a Virtual Drive

Before you begin

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

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.
Step 2 From **Storage** > **Controllers**, click the appropriate FlexUtil controller.
Step 3 Click the **Virtual Drive Info** tab on the right pane.
Step 4 In the **Virtual Drive Info** area, select the virtual drive you want to erase, and click **Erase Virtual Drive**.

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.

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.

Step 2 From **Storage** > **Controllers**, click the appropriate M.2 Raid controller controller.

Step 3 In the **Controller Info** tab > **General** tab on the right pane, review the following information:

Name	Description
Product Name	The name of the MegaRAID controller.
Product ID	Cisco part number of the RAID controller.
Composite Health	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	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. • **Unresponsive** — The controller is down.
Security	Displays the controller lock key depending on its current state. **Note** • This option is available only on some C-Series servers. • Disabling the drive security makes the data on all secure drives unusable.

Name	Description
Serial Number field	The serial number of the MegaRAID controller.
RAID Chip Temperature field	Temperature of the controller in degree centigrade.
Firmware Package Build field	The active firmware package version number. For the firmware component version numbers, see the **Running Firmware Images** area.
Consistency Check Rate field	The rate at which the controller scans the virtual drives looking for redundant data inconsistencies and fixing them. This rate is shown as a percentage of the total bandwidth available.
PCI Slot	The name of the PCIe slot in which the controller is located.
Vendor ID	The PCI vendor ID, in hexadecimal.
SubVendor ID	The PCI subvendor ID, in hexadecimal.
Device ID	The PCI device ID, in hexadecimal.
Sub Device ID	The PCI subdevice ID, in hexadecimal.
Manufactured Date	The date the MegaRAID card was manufactured, in the format yyy-mm-dd.
Revision	The board revision number, if any.
Boot Drive(s)	The number of the boot drive.
Interface Type	Whether the drive is SAS or SATA

Step 4 In the **Controller Info** tab > **Settings** tab on the right pane, review the following information:

Table 189: Settings Area

Name	Description
Physical Drive Status Auto Config Mode	The physical drive status auto config mode that you select for the controller. This can be one of the following: • Unconfigured Good - The default option. Select this option if you are using the server for RAID volume and mixed JBOD. • RAID-0 Write Back - Select this option if you are using the server for per drive R0 WB. • JBOD - Select this option if you are using the server for JBOD only.

Name	Description
Rebuild Rate	The rate at which the controller rebuilds degraded RAID volumes. This rate is shown as a percentage of the total bandwidth available.
Patrol Read Rate	The rate at which the controller performs a background read of the physical drives looking for inconsistent data. This rate is shown as a percentage of the total bandwidth available.
Consistency Check Rate	The rate at which the controller scans the virtual drives looking for redundant data inconsistencies and fixing them. This rate is shown as a percentage of the total bandwidth available.
ECC Bucket Leak Rate	The error correcting code (ECC) single-bit error bucket leak rate, in minutes. With ECC, the controller increments an error counter when it encounters a single bit error while reading from a physical drive. The controller decrements the error counter each time the number of minutes defined in this field passes. If the error counter reaches a system-defined maximum, the controller sends an event message to the system.
JBOD	If this field displays true, JBOD is enabled.
Maintain PD Fail History	If this field displays true, the controller remembers which physical drives were determined to be bad across server reboots.
Battery Warning	If this field displays true, missing battery warnings are disabled.

Table 190: HW Config Area

Name	Description
Controller SAS Address	A MegaRAID controller can have up to 16 serial-attached SCSI (SAS) addresses. This field displays the first 8 SAS addresses, if they are in use.
BBU Present	If this field displays true, the battery backup unit is present.
Memory Present	If this field displays true, memory is present.
Flash Present	If this field displays true, flash memory is present.

Table 191: Capabilities Area

Name	Description
RAID Levels Supported	The RAID levels supported by the controller. This can be one or more of the following: • Raid 0—Simple striping. • Raid 1—Simple mirroring. • Raid 5—Striping with parity. • Raid 1E—Integrated offset strip mirroring • 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. • Raid srl-03—Spanned secondary RAID level • Raid 00—Spanned striping. • Raid 1e-rlq0—Integrated adjacent strip mirroring with no span. • Raid 1e0-rlq0—Integrated adjacent strip mirroring with span.

Table 192: Error Counters Area

Name	Description
Memory Correctable Errors	The number of correctable errors in the controller memory.

Viewing Physical Drive Info for Cisco Boot Optimized M.2 Raid Controller

Before you begin

The server must be powered on.

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.

Step 2 From **Storage** > **Controllers**, click the appropriate M.2 raid controller.

Step 3 Click **Physical Drive Info** tab on the right pane and review the following information:

Name	Description
Slot ID	The name of the PCIe slot in which the controller drive is located.
Disk Type	Whether the drive is a hard drive (HDD) or a solid state drive (SSD).
Status	The physical drive status. This can be one of the following: • Copyback—The drive is busy performing a copyback operation. • Failed—The drive was in use, but it has failed. • Foreign configuration—The drive contains a foreign configuration. • Global hot spare—The drive is designated as a global spare drive. • Dedicated hot spare—The drive is designated as a dedicated spare drive. • 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. • Ready to remove—The drive is prepared for removal. • Rebuild—The drive is currently being rebuilt. • System—The drive is visible to the host and cannot be used for virtual drives. • Unconfigured bad—The drive has failed and is not in use. • Unconfigured good—The drive is ready to be assigned to a drive group or hot spare pool.
Capacity (GB)	The capacity of the drive in gigabytes.
Model	The drive vendor name.
Firmware	The firmware version running on the drive.

Step 4 Select a drive and review the following information that is displayed on a new pane:

Table 193: General Tab

Name	Description
Media Type	Whether the drive is a hard drive (HDD) or a solid state drive (SSD).
Interface Type	The drive interface type.
Sequence Number	The sequence number used by the controller to track drive changes.
Security Enabled	If this field displays **Yes**, full disk encryption is enabled on the physical drive.
Physical Block Size	Indicates the physical block size of the drive.
Slot Number	The slot number in which the physical drive resides.
Device ID	The device ID for the drive.
Product ID	The drive product ID. This field generally displays the drive model number.
UCS Product ID	
Vendor	The vendor for the drive.
Drive Firmware	The active firmware version on the drive.
Drive Serial Number	The serial number for the drive.
Raw Size	The capacity of drive in megabytes, including the space used for formatting.
Non Coerced Size	The capacity in megabytes, including space lost to coercion.
Coerced Size	The capacity in megabytes after any coercion rounding has been performed.
Negotiated Link Speed	The speed of the link between the drive and the controller.

Table 194: Health Status

Name	Description
Locator LED toggle button	Allows you to turn on or off the drive LED.
Health	This field displays the health of the physical drive.

Name	Description
State	The drive status. This can be one of the following: • **Cache degraded**—A virtual drive with a **Write Policy** of **Write Back** was changed by the controller to **Write Through** because the BBU could not guarantee the coherency of the cache. • **Copyback**—The drive is busy performing a copyback operation. • **Failed**—The drive was in use, but it has failed. • **Foreign configuration**—The drive contains a foreign configuration. • **Global hot spare**—The drive is designated as a global spare drive. • **Dedicated hot spare**—The drive is designated as a dedicated spare drive. • **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. • **Ready to remove**—The drive is prepared for removal. • **Rebuild**—The drive is currently being rebuilt. • **System**—The drive is visible to the host and cannot be used for virtual drives. • **Unconfigured bad**—The drive has failed and is not in use. • **Unconfigured good**—The drive is ready to be assigned to a drive group or hot spare pool.
Status	The physical drive status. This can be one of the following: • **JBOD**— The drive is in JBOD state. • **Predicted Failure**—The drive is marked as due to fail soon by the controller. • **Unconfigured bad**—The drive has failed and is not in use.

Name	Description
Copyback Operation Status	Copyback operation status. This can be one of the following: • **Unknown**— Percentage completed is not known. • **In Progress**— The rebuild process as seen in the **Copyback Percent Complete** field. When a hot spare is configured, and you remove a disk from the RAID group, and subsequently replace it, the rebuild occurs releasing the hot space. • **Completed**— Copyback operation is completed.
Copyback Percent Complete	Copyback operation completed, in percentage.
Power State field	The current power state. This can be one of the following: • **active**—The drive is running normally. • **powersave**—The drive has been spun down. • **transitioning**—The drive is spinning up.

Table 195: Error Count

Name	Description
Media Error Count	The number of media errors encountered since the drive was first installed or the host was rebooted.
Other Error Count	The number of non media errors encountered since the drive was first installed or the host was rebooted.
Predictive Failure Count	The number of times that the controller has predicted that the drive could fail.

Table 196: Product Details

Name	Description
Power Cycle Count	Number of power cycles that the drive went through from the time it was manufactured.
Power on Hours	Total number of hours that the drive is in the 'Power On' mode.
Percentage Life Left	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%.

Name	Description
Wear Status in Days	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	The current temperature of the drive at which the selected SSD operates at the time of selection.
Maximum Operating Temperature	Allowable maximum temperature in which the drive can operate without errors.
Percentage Reserved Capacity Consumed	The total capacity (out of the percentage reserved for it) consumed by the drive.

Step 5 Click **Close**.

Viewing the Virtual Drive Info for Cisco Boot Optimized M.2 Raid Controller

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.

Step 2 From **Storage** > **Controllers**, click the appropriate M.2 Raid controller.

Step 3 Select the **Virtual Drive Info** tab and review the following information:

Table 197: Virtual Drive Info

Name	Description
ID	The number of the virtual drive. Click to see more details.
Name	The name of the virtual drive.

Name	Description
Status	The virtual drive state. This can be one of the following: • **Cache degraded**—The requested Write-cache policy for this drive is **Write Back**, but it is running in **Write Through** mode because the BBU is defective or is undergoing a learn cycle. • **Degraded**—One or more spans of the drive has no redundancy. • **Off Line**—The drive is not visible to the host. • **Partially Degraded**—The drive has lost some redundancy but still has partial redundancy. For example, if a 3-way RAID 1 mirrored drive lost one disk, it would still have 2-way redundancy. • **Optimal**—The drive has full redundancy.
Size (GB)	The capacity of the drive in megabytes.
RAID Level	The RAID level on the virtual drive. 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**—Striping with parity. • **Raid 60**—Spanned striping with two parity drives. • **Raid 00**—Spanned striping.
Boot Drive(s)	Whether the virtual drive has been designated as a boot drive.

Step 4 Select a virtual drive and review the following information:

Table 198: RAID Details

Name	Description
Name	The name of the virtual drive.
Strip Size	The size of each strip, in KB.
Drives Per Span	The number of drives included in each span.

Name	Description
Span Depth	The number of spans that comprise the virtual drive.
Dedicated Hot Spare Drives	
Access Policy field	The method the host operating system can use to access the virtual drive. This can be one of the following: • **Blocked**—The host cannot access the drive. • **Read-Write**—The host has full access to the drive. • **Read-Only**—The host can only read data from the drive.
Cache Policy field	The cache policy. This can be one of the following: • **Allow**—Reads and writes are cached in the controller. • **Allow Read**—Only reads are cached in the controller. • **Allow Write**—Only writes are cached in the controller. • **Direct**—Neither reads or writes are cached in the controller.
Read Ahead Policy field	How the controller uses the read-ahead feature. This can be one of the following: • **Adaptive**—Read-ahead is enabled and used when the controller thinks it will improve performance. • **Always**—Read-ahead is enabled and always used. • **None**—Read-ahead is disabled.
Security Capable	If this field displays Yes, it indicates that the physical drive is security-capable.
Consistency Check Operation Status	

Name	Description
Requested Write Cache Policy	How the controller handles caching. This can be one of the following: • **Write Through**—Data written is stored in the cache and also written through to the physical drives. The transaction is not marked complete until data is written to the physical drives. • **Write Back**—Data written is stored in the cache and will be written to the physical drives when bandwidth is available. This policy has higher write performance than the **Write Through** mode, but it falls back to the **Write Through** mode when the BBU is defective or is in a learn cycle. • **Write Back Even If Bad BBU**—Caching remains in **Write Back** mode even if the BBU is bad. Data can be lost in this mode if there is a power failure.
Current Write Cache Policy	The currently running cache policy. This can be one of the following: • **Write Through**—Data written is stored in the cache and also written through to the physical drives. The transaction is not marked complete until data is written to the physical drives. • **Write Back**—Data written is stored in the cache and will be written to the physical drives when bandwidth is available. This policy has higher write performance than the **Write Through** mode, but it falls back to the **Write Through** mode when the BBU is defective or is in a learn cycle. • **Write Back Even If Bad BBU**—Caching remains in **Write Back** mode even if the BBU is bad. Data can be lost in this mode if there is a power failure.

Name	Description
Disk Cache Policy	How the controller handles physical disk caching. This can be one of the following: • **Disable**—Caching is disabled on the physical drives. • **Enable**—Caching is enabled on the physical drives. • **Unchanged**—The controller uses the caching policy specified on the physical drive. **Note** If several virtual drives share a drive group, they must all use the same disk cache policy. Otherwise the caching policy may be randomly assigned to the physical drives.
Boot Drive	If this field displays **true**, then the virtual drive is designated as a boot drive.
Security Enable	If this field displays Yes, full disk encryption is enabled on the physical drive.

Step 5 Click **Close**.

Cisco FlexMMC

Viewing Cisco FlexMMC Details

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.

Step 2 In the **Storage** page, click **Cisco FlexMMC**.

Step 3 In the **Storage for IMC Images** area, view the following:

Table 199: Storage for IMC Images Area

Name	Description
Storage for IMC Images pie chart	Helps you analyze the total, available, and used spaces for the Cisco IMC images.
File Name column	Cisco IMC image file names.
File Size column	Cisco IMC image file size.

Name	Description
File Type column	Cisco IMC image file type.
Status column	Status of the Cisco IMC image file.

Step 4 In the **Storage for User Files Area** area, view the following:

Table 200: Storage for User Files Area

Name	Description
Storage for User Files pie chart	Helps you analyze the total, available, and used spaces for the user files.
File Name column	User file names.
File Size column	User file size.
File Type column	User file type.
Status column	Status of the user file.

Uploading New Image File

Before you begin

Ensure that there are no file upload in progress. You can upload only one image file at any time. To upload a new file, you should first un-map and delete the existing file.

SUMMARY STEPS

1. From the **Apps** drop-down list, select **Storage**.
2. In the **Storage** page, click **Cisco FlexMMC**.
3. In the **Storage for IMC Images** area, click **Upload File**.
4. In the **Upload File to IMC Images partition** dialog box, complete the following:
5. Click **Save**.

DETAILED STEPS

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.

Step 2 In the **Storage** page, click **Cisco FlexMMC**.

Step 3 In the **Storage for IMC Images** area, click **Upload File**.

The **Upload File to IMC Images partition** dialog box is displayed.

Step 4 In the **Upload File to IMC Images partition** dialog box, complete the following:

Name	Description
File Location 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`**.

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`**
Username field	**Note** This field is not available for NFS mount. The username for the specified **Mount Type**, if required.
Password field	**Note** This field is not available for NFS mount. The password for the selected username, if required.
Add button	Allows you to add the file in the system.

Step 5 Click **Save**.

You can view the file upload status under **Files Copied** area.

Note
If you wish to cancel the upload process before it is completed, select the file and click **Cancel Upload**.

Deleting an Image File

Before you begin

- Ensure that there are no file uploads in progress. You cannot delete a file for which the upload is in progress.
- Ensure that there are no files mapped. You cannot delete a file which is already mapped. You should first un-map the file before deleting the file.

SUMMARY STEPS

1. In the **Navigation** pane, click the **Storage** menu.
2. From the **Apps** drop-down list, select **Storage**.
3. In the **Storage** page, click **Cisco FlexMMC**.
4. In the **Storage for IMC Images** area > **Files Copied** area, select an image file.
5. Click **Delete File**.

DETAILED STEPS

Procedure

Step 1 In the **Navigation** pane, click the **Storage** menu.
Step 2 From the **Apps** drop-down list, select **Storage**.
Step 3 In the **Storage** page, click **Cisco FlexMMC**.
Step 4 In the **Storage for IMC Images** area > **Files Copied** area, select an image file.
Step 5 Click **Delete File**.

Mapping or Un-mapping an Image

SUMMARY STEPS

1. From the **Apps** drop-down list, select **Storage**.
2. In the **Storage** page, click **Cisco FlexMMC**.
3. In the **Storage for IMC Images** area > **Files Copied** area, select an image file.
4. Click **Map Image** or **UnMap Image**.

DETAILED STEPS

Procedure

Step 1 From the **Apps** drop-down list, select **Storage**.

Step 2 In the **Storage** page, click **Cisco FlexMMC**.

Step 3 In the **Storage for IMC Images** area > **Files Copied** area, select an image file.

Step 4 Click **Map Image** or **UnMap Image**.

Resetting FlexMMC to Default Settings

Perform this procedure to reset FlexMMC to default Cisco IMC settings.

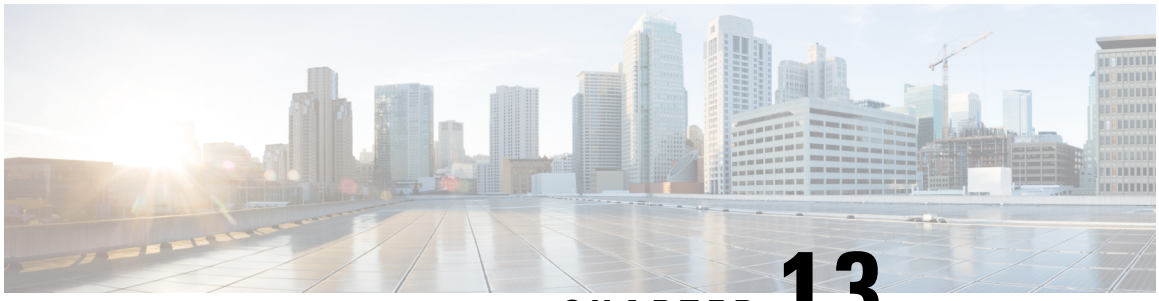
Note Performing this procedure deletes all the uploaded images.

Before you begin

- Ensure that there are no file uploads in progress. You cannot reset FlexMMC to default settings while a file upload is in progress.
- Ensure that there are no files mapped. You cannot reset FlexMMC if a file is already mapped. You should first un-map the file before resetting FlexMMC.

Procedure

	Command or Action	Purpose
Step 1	From the **Apps** drop-down list, select **Storage**.	
Step 2	In the **Storage** page, click **Cisco FlexMMC**.	
Step 3	In the **Actions** drop-down list on the right pane, select **Reset to Defaults**.	
Step 4	Click **Yes** to confirm.	



CHAPTER 13

Configuring Communication Services

•
• Enabling or Disabling TLS v1.2, on page 415
• Configuring HTTP, on page 417
• Configuring SSH, on page 419
• Configuring XML API, on page 419
• Enabling Redfish, on page 420
• Configuring IPMI, on page 421
• Configuring SNMP, on page 422
• Configuring a Server to Send Email Alerts Using SMTP, on page 427

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.

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 In the **Navigation** pane, click **Communication Services** menu.

Step 3 Select the **Communication Services** tab.

Step 4 In the **TLS Configuration** area, update the following properties:

Table 201: TLS Configuration Area

Name	Description
Enable TLS v1.2 toggle button	Allows you to enable/disable TLS v1.2 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.
Configured TLS Version	TLS versions supported by Cisco IMC (TLSv1.2, TLSv1.3)
TLS v1.2 Cipher Mode drop-down list	**Note** For security reasons, from upcoming releases, low, medium and custom strength ciphers in TLS v1.2 will no longer be supported. Please ensure you are using high strength ciphers to maintain security and compatibility. 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.

Step 5 Click **Save**.

Configuring HTTP

Before you begin

You must be logged in as as admin to perform this procedure.

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.
Step 2 In the **Navigation** pane, click **Communication Services** menu.
Step 3 Select the **Communication Services** tab.
Step 4 In the **HTTP Properties** area, update the following properties:

Table 202: HTTP Properties Area

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. Allows you to enable/disable HTTPS services to access Cisco IMC. This option enables only HTTPS services to access Cisco IMC.
HTTP Enabled toggle button	**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. Allows you to enable/disable 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 toggle button	**Note** This option is applicable only when HTTP Enabled is checked. Allows you to enable/disable feature when all attempts to communicate via HTTP are redirected to the equivalent HTTPS address. Cisco strongly recommends 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 Cisco IMC times out and terminates the session. Enter an integer between 60 and 10,800. The default is 1,800 seconds.
Max Sessions	Displays the maximum number of concurrent HTTP and HTTPS sessions allowed on Cisco IMC.
Active Sessions	Displays the number of HTTP and HTTPS sessions currently running on Cisco IMC.

Step 5 Click **Save**.

Configuring SSH

Before you begin

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

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 In the **Navigation** pane, click **Communication Services** menu.

Step 3 Select the **Communication Services** tab.

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

Table 203: SSH Properties Area

Name	Description
SSH Enabled toggle button	Allows you to enable/disable SSH on 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	Displays the maximum number of concurrent SSH sessions allowed on Cisco IMC.
Active Sessions	Displays the number of SSH sessions currently running on Cisco IMC.

Step 5 Click **Save**.

Configuring XML API

XML API for Cisco IMC

The 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 XML API Programmer's Guide*.

Enabling the XML API

Before you begin

You must be logged in as an admin to perform this procedure.

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 In the **Navigation** pane, click **Communication Services** menu.

Step 3 Select the **Communication Services** tab.

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

Table 204: XML API Properties Area

Name	Description
XML API Enabled toggle button	Allows you to enable/disable API access on this server.
Max Sessions	Displays the maximum number of concurrent API sessions allowed on Cisco IMC.
Active Sessions	Displays the number of API sessions currently running on Cisco IMC.

Step 5 Click **Save**.

Enabling Redfish

Before you begin

You must be logged in as admin to perform this action.

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 In the **Navigation** pane, click **Communication Services** menu.

Step 3 Select the **Communication Services** tab.

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

Table 205: Redfish Properties Area

Name	Description
Redfish Enabled toggle button	Allows you to enable/disable Redfish access on the Cisco IMC.

Name	Description
Max Sessions	Displays the maximum number of concurrent Redfish sessions allowed on Cisco IMC.
Active Sessions	Displays the number of Redfish sessions currently running on Cisco IMC.

Step 5 Click **Save**.

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 be logged in as as admin to perform this procedure.

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 In the **Navigation** pane, click **Communication Services** menu.

Step 3 Select the **Communication Services** tab.

Step 4 In the **IPMI over LAN Properties** area, update the following properties:

Table 206: IPMI over LAN Properties Area

Name	Description
Enabled check box	Whether IPMI access is allowed on this server.
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 5 Click **Save**.

Configuring SNMP

SNMP

The Cisco IMC 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 be logged in as an admin to perform this procedure.

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 In the **Navigation** pane, click **Communication Services** menu.

Step 3 Select the **SNMP** tab.

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

Table 207: Properties Area

Name	Description
SNMP Enabled toggle button	Enables/disables the feature in which, server sends SNMP traps to the designated host. **Note** After you check this enable SNMP, 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.
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.

Step 5 In the **v2c Properties** area, update the following properties:

Table 208: v2c Properties Area

Name	Description
SNMP v2c Enabled toggle button	To comply with Cisco security standards, support for SNMP v2c and earlier implementations will not be supported in upcoming releases. Please use a protocol that provides a higher level of security, such as SNMPv3. Allows you to enable or disable SNMP v2c version.
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.

Step 6 In the **v3 Properties** area, update the following properties:

Table 209: v3 Properties Area

Name	Description
SNMP v3 Enabled toggle button	Allows you to enable or disable SNMP v3 version.
SNMP Engine ID field	Unique string to identify the device for administration purpose. This is generated from the SNMP Input Engine ID if it is already defined, else it is derived from the BMC serial number.
SNMP Input Engine ID field	User-defined unique identification of the static engine.

Step 7 Click **Save**.

What to do next

Configure SNMP trap settings.

Configuring SNMP Trap Settings

Before you begin

You must be logged in as an admin to perform this procedure.

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 In the **Navigation** pane, click **Communication Services** menu.

Step 3 Select the **SNMP** tab.

Step 4 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 5 In the **Trap Details** dialog box, complete the following fields:

Table 210: Add/Modify Trap

Name	Description
Version drop-down list	The SNMP version and model used for the trap. This can be one of the following: • **V2** • **V3**
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, an acknowledgment is sent to the SNMP engine.

Name	Description
User drop-down list	The drop-down list displays all available users, select a user from the list.
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.
SNMP Port field	The port the server uses to communicate with the trap destination. Enter a trap destination port number within the range 1 to 65535.
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.

Step 6 Click **Save**.

Step 7 (Optional) Additionally, 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 be logged in as an admin to perform this procedure.

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 In the **Navigation** pane, click **Communication Services** menu.

Step 3 Select the **SNMP** tab.

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

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 In the **Navigation** pane, click **Communication Services** menu.

Step 3 Select the **SNMP** tab.

Step 4 In the **v3 User Settings** area, you can view the following properties:

Table 211: v3 User Settings Area

Name	Description
ID column	The system-assigned identifier for the SNMP user.
Name column	The SNMP user name.
Auth Type column	The user authentication type.
Privacy Type column	The user privacy type.

Step 5 Click **CLICK HERE to change the Users configurations**. Refer Adding Local Users for Cisco UCS C-Series M7 and Later Servers, on page 211

Configuring a Server to Send Email Alerts Using SMTP

Configuring SMTP Server For Receiving Email Alerts

Before you begin

You must be logged in as an admin to perform this procedure.

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 In the **Navigation** pane, click **Communication Services** menu.

Step 3 Select the **Mail Alert** tab.

Step 4 In the **SMTP Properties** area, update the following properties.

Table 212: SMTP Properties Area

Name	Description
SMTP Enabled toggle button	Allows you to enable/disable 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).

What to do next

Refer Adding SMTP Email Recipients, on page 428 to add SMTP email recipients.

Adding SMTP Email Recipients

Add email recipients on the **Mail Alert** tab to receive email notifications for server faults.

Before you begin

- You must be logged in as an admin to perform this procedure.
- Configure the SMTP server properties in the SMTP Properties area. See Configuring SMTP Server For Receiving Email Alerts, on page 427

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 In the **Navigation** pane, click **Communication Services** menu.

Step 3 Select the **Mail Alert** tab.

Step 4 In the **SMTP Recipients** area, do the following:

- You can add a recipient.
- You can delete a recipient.

Step 5 To add a recipient, click **+ Add Recipient**, and enter the email ID and select severity from the **Minimum Severity to Report** drop-down list.

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.

Step 6 Click **Save**.

Step 7 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)

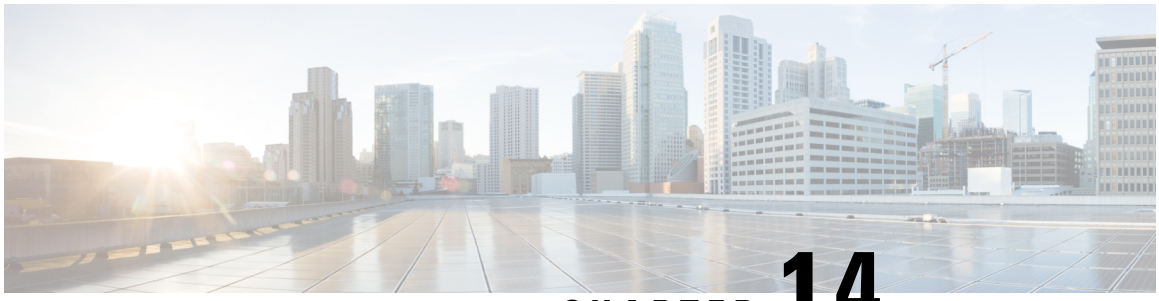
Step 8 (Optional) To delete an email recipient, select the email recipient and click **Delete Rows**.

Step 9 (Optional) Click **OK** to confirm.

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.



CHAPTER 14

Managing Certificates and Server Security

- Managing the mTLS Certificate, on page 431
- Managing the Server Certificate, on page 433
- Managing the External Certificate, on page 444
- SPDM Security - MCTP SPDM, on page 449
- Key Management Interoperability Protocol, on page 456
- FIPS 140-2 Compliance in Cisco IMC, on page 469

Managing the mTLS Certificate

Uploading an mTLS Certificate

- You must be logged in as an admin to perform this procedure.
- The certificate file to be uploaded must reside on a locally accessible file system.
- The following certificate formats are supported:
  - .pem

You can upload an mTLS Client CA Certificate from the following locations:

- Remote
- Local
- Paste

1. From the **Apps** drop-down list, select **Administration**.
2. In the **Navigation** pane, click **Security Management** menu.
3. From the **Security Management** menu, select **Certificate Management**.
4. In the **mTLS Client CA** area, click **Add Certificate**.

   The **Add mTLS Client CA Certificate** dialog box is displayed.

5. In the **Add mTLS Client CA Certificate** dialog box, select the appropriate method to upload the certificate and enter the relevant details:

Table 213: Remote

Name	Description
Server IP/Hostname field	The IP address or hostname of the server on which the mTLS Client CA certificate file is available.
Upload Protocol option	The remote server type. This can be one of the following: • SFTP • SCP
Path and Filename field	The path and filename of the mTLS Client CA certificate file on the remote server.
Username field	User name for your remote server.
Password field	Password for your remote server.
Upload mTLS Client CA Certificate button	Allows you to upload the mTLS Client CA certificate.

Table 214: Local

Name	Description
Local tab	Select this tab when you want to upload the mTLS Client CA Certificate from your local machine. Click **Browse** and navigate to the mTLS Client CA Certificate that you want to upload.
Upload mTLS Client CA Certificate button	Allows you to upload the mTLS Client CA Certificate.

Table 215: Paste

Name	Description
Paste tab	Opens a text box that allows you to copy the entire content of the mTLS Client CA Certificate and paste in the text field.
Upload mTLS Client CA Certificate button	Allows you to upload the mTLS Client CA Certificate.

Viewing mTLS Certificate

1. From the **Apps** drop-down list, select **Administration**.

2. In the **Navigation** pane, click **Security Management** menu.
3. From the **Security Management** menu, select **Certificate Management**.
4. In the **Certificate Management** tab > **mTLS Client CA** area, the following details are displayed:

Name	Description
Common Name field	The fully qualified (FQDN or domain name of the server) hostname of the server for which the certificate was issued.
Issued By	Contains identifying information about the Certificate Authority (CA) that issued the certificate to the client or server.
Expires	The date on which the certificate expires.
+ Add Certificate button	Allows you to add mTLS Client certificates.

Managing the Server Certificate

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.

Procedure

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 an admin to perform this procedure.
- Ensure that the Cisco IMC time is set to the current time.

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 In the **Navigation** pane, click **Security Management** menu.

Step 3 From the **Security Management** menu, select **Certificate Management**.

Step 4 From the **Actions** drop-down list, select **Generate Certificate Signing Request**.

The **Generate Certificate Signing Request** dialog box appears.

Step 5 In the **Generate Certificate Signing Request** dialog box, update the following properties:

Table 216: Generate Certificate Signing Request

Name	Description
Common Name	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	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 types include: • 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.

Name	Description
Organization Name field	The organization requesting the certificate.
Organization Unit field	The organizational unit.
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: • 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 toggle button	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 toggle button	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 6 Click **Generate CSR**.

The **Opening csr.txt** dialog box appears.

Step 7 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**.

Certificate a Self 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 an admin to perform this procedure.
- Ensure that the Cisco IMC time is set to the current time.

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.
Step 2 In the **Navigation** pane, click **Security Management** menu.
Step 3 From the **Security Management** menu, select **Certificate Management**.
Step 4 In the **Actions** area, click the **Generate New Certificate Signing Request**.

The **Generate Certificate Signing Request** dialog box appears.

Step 5 From the **Actions** drop-down list, select **Generate Certificate Signing Request**.

The **Generate Certificate Signing Request** dialog box appears.

Step 6 In the **Generate Certificate Signing Request** dialog box, update the following properties:

Note
Ensure that **Self Signed Certificate** toggle button is enabled.

Table 217: Generate Certificate Signing Request

Name	Description
Common Name	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	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 types include: • 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.
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.

Name	Description
Signature Algorithm	Allows you to select the signature algorithm for generating certificate signing request. This can be one of the following: • 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
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

Name	Description
Challenge Password toggle button	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 toggle button	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.

Step 7 Click **Generate CSR**.

The **Opening csr.txt** dialog box appears.

Step 8 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 using Linux

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* **Example:** `# openssl req -new -x509 -days 365 -key ca.key -out ca.crt`	This command generates a new self-signed certificate for the CA using the specified key. The certificate is valid for the specified period. The command prompts the user for additional certificate information. The certificate server is an active CA.
Step 3	**echo "nsCertType = server" > openssl.conf** **Example:** `# echo "nsCertType = server" > openssl.conf`	This command adds a line to the OpenSSL configuration 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".

	Command or Action	Purpose
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 an admin to perform this procedure.
- Ensure that the Cisco IMC time is set to the current time.

Procedure

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 an admin to perform this procedure.
- 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.

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 In the **Navigation** pane, click **Security Management** menu.

Step 3 From the **Security Management** menu, select **Certificate Management**.

Step 4 From the **Actions** drop-down list, select **Upload Server Certificate**.

The **Upload Server Certificate** dialog box appears.

Step 5 In the **Upload Server Certificate** dialog box, update the following properties:

Name	Description
Local/Paste toggle button	Allows you to select the certificate file from the local machine or paste the certificate.
Browse button	Opens a dialog box that allows you to navigate to the appropriate certificate file. Applicable only when **Local** option is selected.
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. Applicable only when **Paste** option is selected.
Upload button	Click **Upload** to upload the certificate.

Managing the External Certificate

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 be logged in as an admin to perform this procedure.
- The certificate file to be uploaded must reside on a locally accessible file system.
- The following certificate formats are supported:
  - .crt
  - .cer
  - .pem

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 In the **Navigation** pane, click **Security Management** menu.

Step 3 From the **Security Management** menu, select **Certificate Management**.

Step 4 From the **Actions** drop-down list, select **Upload External Certificate**.

The **Upload External Certificate** dialog box appears.

Step 5 In the **Upload External Certificate** dialog box, select the appropriate method to upload the certificate and enter the relevant details:

Table 218: Remote

Name	Description
Remote button	Select this option when you want to upload the external certificate from a remote location.
Server IP/Hostname	Server details from where you want to upload the external certificate.

Name	Description
Upload Protocol button	Select 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. To comply with Cisco security standards, certain insecure protocols (TFTP, FTP, HTTP) will no longer be supported in upcoming releases. We recommend using secure protocols like SFTP or SCP moving forward.
Path and Filename field	File path where the external certificate file resides on the server along with the filename.
Username field	User name for your remote server.
Password field	Password for your remote server.
Upload button	Allows you to upload the external certificate.

Table 219: Local

Name	Description
Local button	Select this option when you want to upload the external certificate from your local machine. Click **Browse** and navigate to the external certificate that you want to upload.
Upload button	Allows you to upload the external certificate.

Table 220: Paste

Name	Description
Paste button	Opens a text box that allows you to copy the entire content of the external certificate and paste it in the **Paste External Certificate Content** text field.
Upload button	Allows you 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** action is enabled. From the **Actions** drop-down list, 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 be logged in as an admin to perform this procedure.
- Ensure that you have uploaded an external certificate.

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 In the **Navigation** pane, click **Security Management** menu.

Step 3 From the **Security Management** menu, select **Certificate Management**.

Step 4 From the **Actions** drop-down list, select **Upload External Private Key**.

The **Upload External Private Key** dialog box appears.

Step 5 In the **Upload External Private Key** dialog box, select the appropriate method to upload the certificate and enter the relevant details:

Table 221: Remote

Name	Description
Remote button	Select this option when you want to upload the external private key from a remote location.
Server IP/Hostname field	Server details from where you want to upload the external private key
Upload Protocol button	Select one of the following protocols. • SFTP • SCP
Username field	User name for your remote server.
Password field	Password for your remote server.

Name	Description
Upload button	Allows you to upload the external private key.

Table 222: Local

Name	Description
Local button	Select this option when you want to upload the external private key from your local machine. Click **Browse** and navigate to the external private key file that you want to upload.
Upload button	Allows you to upload the external private key.

Table 223: Paste

Name	Description
Paste button	Opens a text box that allows you to copy the entire content of the external private key and paste it in the **Paste External Private Key Content** text field.
Upload button	Allows you to upload the external private key.

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** action is enabled. From the **Actions** drop-down list, 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 be logged in as an admin to perform this procedure.
- Ensure that you have uploaded the external certificate and external private key.

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 In the **Navigation** pane, click **Security Management** menu.

Step 3 From the **Security Management** menu, select **Certificate Management**.

Step 4 From the **Actions** drop-down list, select **Activate External Certificate**.

Note
Activating the external certificate overwrites any existing certificate and key pair, and disconnects any existing HTTPS and SSH sessions.

SPDM Security - MCTP SPDM

SPDM Security

Cisco UCS C-Series Servers might contain mutable components that could provide vectors for attack against a device itself or use of a device to attack another device within the system. To defend against these attacks, SPDM (Security Protocol and Data Model) specification defines messages, data objects, and sequences for performing message exchanges between devices over a variety of transport and physical media. It orchestrates message exchanges between management controllers and end-point devices over Management Component Transport Protocol (MCTP).

Message exchanges include authentication of hardware identities accessing the controller. The SPDM enables access to low-level security capabilities and operations by specifying a managed level for device authentication and certificate management.

Endpoint certificates and authorites (Root CA) certificates are listed on all user interfaces on the server. You can also upload the content of one or more external device certificates into Cisco IMC. Using a SPDM policy allows you to change or delete external Root CA certificate or settings as desired. You can also delete or replace the root CA certificate when no longer needed.

A SPDM security policy allows you to specify any one of the three security level settings, as listed below:

- Full Security:

  This is the highest MCTP security setting. When you select this setting, a fault is generated when any endpoint authentication failure is detected. A fault will also be generated if any of the endpoints do not support endpoint authentication.

- Partial Security:

  When you select this setting, a fault is generated when any endpoint authentication failure is detected. There will NOT be a fault generated when the endpoint doesn’t support endpoint authentication. This is chosen as the default setting.

- No Security

  When you select this setting, no fault will be generated for any failure (endpoint measurement).

Configuring and Viewing the MCTP SPDM Fault Alert Settings

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 In the **Navigation** pane, click **Security Management** menu.

Step 3 From the **Security Management** menu, select **MCTP SPDM**.

Step 4 Under the **Properties** area, review or update the following properties:

Table 224: Properties Area

Name	Description
Fault Alert Setting drop-down list	Select the fault alert setting from the drop-down list. This can be one of the following: • **Full** - If you select this option, then a fault is generated when there is any endpoint authentication failure. If you select this option, then a fault is generated when the endpoints do not support endpoint authentication. • **Partial** - The default option. If you select this option, then a fault is generated when there is any endpoint authentication failure. If you select this option, no fault is generated when the endpoints do not support endpoint authentication. • **Disabled** - If you select this option, no fault is generated for endpoint authentication failure.
Certificate Upload Progress	Displays the certificate upload progress.
Certificate Upload Status	Displays the certificate upload status.
SPDM Status	Displays the overall SDPM authentication status.

What to do next

When a fault is generated in case of device attestation failure, you can view the respective fault details in the **Faults and Logs** tab under the **System** Apps.

Viewing SPDM Authentication Status

Procedure

	Command or Action	Purpose
Step 1	From the **Apps** drop-down list, select **Administration**.	
Step 2	In the **Navigation** pane, click **Security Management** menu.	
Step 3	From the **Security Management** menu, select **MCTP SPDM**.	
Step 4	Under the **Properties** area, review the following properties:	*Table 225: Properties Area*

Name	Description
Fault Alert Setting drop-down list	Select the fault alert setting from the drop-down list. This can be one of the following: • **Full** - If you select this option, then a fault is generated when there is any endpoint authentication failure. If you select this option, then a fault is generated when the endpoints do not support endpoint authentication. • **Partial** - The default option. If you select this option, then a fault is generated when there is any endpoint authentication failure. If you select this option, no fault is generated when the endpoints do not support endpoint authentication. • **Disabled** - If you select this option, no fault is generated for endpoint authentication failure.
Certificate Upload Progress	Displays the certificate upload progress.
Certificate Upload Status	Displays the certificate upload status.
SPDM Status	Displays the overall SDPM authentication status.

Adding Authorities Certificate

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 In the **Navigation** pane, click **Security Management** menu.

Step 3 From the **Security Management** menu, select **MCTP SPDM**.

Step 4 Under the **Certificates** area, click **+ Add Certificate**.

Add Authorities Certificate dialog box is displayed.

Step 5 In the **Add Authorities Certificate** dialog box, use of the following method to add certificate:

Table 226: Remote

Name	Description
Remote button	Select this option when you want to add authorities certificate from a remote location.
Server IP/Hostname	Server details from where you want to add authorities certificate.
Upload Protocol button	Select 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.
Path and Filename field	File path where the root CA certificate file resides on the server along with the filename.
Username field	User name for your remote server.
Password field	Password for your remote server.
Upload Authorities Certificate button	Allows you to add authorities certificate.

Table 227: Local

Name	Description
Local button	Select this option when you want to add authorities certificate from your local machine. Click **Browse** and navigate to the authorities certificate that you want to add.
Upload Authorities Certificate button	Allows you to add authorities certificate.

Table 228: Paste

Name	Description
Paste field	Opens a text box that allows you to copy the entire content of the root CA certificate and paste it in the **Paste Authorities Certificate** text field.
Upload Authorities Certificate button	Allows you to add authorities certificate.

You can view the upload progress and status from the following fields in MCTP SPDM tab.

After the upload is complete and successful, the authorities certificate is uploaded and the details are displayed in the **Authorities** tab.

Viewing the List of Certificates and Certificate Details

Procedure

	Command or Action	Purpose
Step 1	From the **Apps** drop-down list, select **Administration**.	
Step 2	In the **Navigation** pane, click **Security Management** menu.	
Step 3	From the **Security Management** menu, select **MCTP SPDM**.	
Step 4	Under the **Certificates** area, click **Endpoints** tab.	
Step 5	You can view the following properties:	*Table 229: Endpoints*

Name	Description
Common Name column	Displays the endpoint's Root CA certificate common name.
Endpoint ID column	Displays the PCIe Slot ID.
Status column	Displays the endpoint's final SPDM handshake status.

<table>
<tr><th></th><th>Command or Action</th><th>Purpose</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>View Certificate Details icon</td><td>Allows you to view the endpoint certificate details.</td></tr>
</table>
</td></tr>
<tr><td>Step 6</td><td>Under the Certificates area, click Authorities tab.</td><td></td></tr>
<tr><td>Step 7</td><td>You can view the following properties:</td><td>
Table 230: Authorities
<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>Add Certificate + button</td><td>Allows you to add authorities certificates.</td></tr>
<tr><td>Delete button</td><td>Allows you to delete the authorities certificate.
Select the check box on any row in the table and click the Delete button.
Note
A lock icon is displayed next to the certificates that are shipped from the factory. You cannot delete the certificates with the lock icon.</td></tr>
<tr><td>Common Name column</td><td>Displays the authorities certificate common name.</td></tr>
<tr><td>Issued By column</td><td>Displays the details of who issued the authorities certificate.</td></tr>
<tr><td>Expires column</td><td>Displays the validity of the authorities certificate.</td></tr>
<tr><td>View Certificate Details icon</td><td>Allows you to view the authorities certificate details.</td></tr>
</table>
Note
A lock icon is displayed next to the certificates that are shipped from the factory. You cannot delete the certificates with the lock icon.
</td></tr>
<tr><td>Step 8</td><td>To view the details of a specific certificate, click the View icon.</td><td>
The following details of the authorities certificate are displayed in View Certificate dialog box:
<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>Name</td><td>Displays the authorities certificate common name.</td></tr>
<tr><td>Issued By</td><td>Displays the details of who issued the authorities certificate.</td></tr>
</table>
</td></tr>
</table>

	Command or Action	Purpose

Name	Description
Serial Number field	Displays the serial number of the certificate.
Valid from	Displays the start of validity period of the certificate.
Valid To	Displays the end of validity period of the certificate.

Table 231: Subject Area

Name	Description
Common Name	Displays the authorities certificate common name.
City	Displays the issuer city of the certificate.
State field	Displays the issuer state of the certificate.
Country Code	Displays the issuer country code of the certificate.
Organization Unit	Displays the issuer organization unit of the certificate.
Organization	Displays the issuer organization name.

Table 232: Issuer Area

Name	Description
Common Name	Displays the issuer common name of the certificate.
City	Displays the issuer city of the certificate.
State	Displays the issuer state of the certificate.
Country Code	Displays the issuer country code of the certificate.
Organization Unit	Displays the issuer organization unit of the certificate.

	Command or Action	Purpose
		<table><tr><th>Name</th><th>Description</th></tr><tr><td>Organization</td><td>Displays the issuer organization name.</td></tr></table>

Deleting Certificates

Procedure

	Command or Action	Purpose
Step 1	From the **Apps** drop-down list, select **Administration**.	
Step 2	In the **Navigation** pane, click **Security Management** menu.	
Step 3	From the **Security Management** menu, select **MCTP SPDM**.	
Step 4	Under the **Certificates** area, click **Authorities** tab.	
Step 5	In the **Authorities** tab, select the check box on any row in the table.	**Note** A lock icon is displayed next to the certificates that are shipped from the factory. You cannot delete the certificates with the lock icon.
Step 6	Click the **Delete** to delete the endpoint certificate.	The following message is displayed in a pop-window: **The certificate has deleted successfully. CIMC will re-authenticate all devices.**
Step 7	Click **OK**.	

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.

Viewing Secure Key Management Settings

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 In the **Navigation** pane, click **Security Management** menu.

Step 3 From the **Security Management** menu, select **Secure Key Management**.

Step 4 You can review the following properties:

Table 233: Secure Key Management

Name	Description
Enable Secure Key Management toggle button	Allows you to enable or disable the secure key management feature.

Step 5 In the **KMIP Servers** area, review the following fields:

Table 234: KMIP Servers

Name	Description
KMIP Login Details button	Displays the KMIP Login Details dialog box.
+ Add Server button	Allows you to add a row with serve details. Click and enter the server properties in the new row.
ID field	ID for the KMIP server configuration.
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	Allows you to delete the KMIP server configuration. Select a row from the table and click **Delete**. **Note** **Delete** button is visible when you select a row.
Test Connection button	Tests whether or not the KMIP connection was successful. **Note** **Test Connection** button is visible when you select a row.

Step 6 In the **Certificate and Key Status** area, review the following fields:

Table 235: Certificate and Key Status

Name	Description
Name column	Displays the name of the certificate/key.
Status column	Indicates the availability of the certificate/key.
Download column	Displays the download status of the certificate/key.
Export column	Displays the export status of the certificate/key.

Creating a Client Private Key and Client Certificate for KMIP Configuration

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.

SUMMARY STEPS

1. **openssl genrsa -out** *Client_Privatekeyfilename keysize*
2. **openssl req -new -x509 -days** *numdays* **-key** *Client_Privatekeyfilename* **-out** *Client_certfilename*
3. Obtain the KMIP root CA certificate from the KMIP server.

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**openssl genrsa -out** *Client_Privatekeyfilename keysize* **Example:** `# openssl genrsa -out client_private.pem 2048`	This command generates a client private key that will be used to generate the client certificate. The specified file name contains an RSA key of the specified key size.
Step 2	**openssl req -new -x509 -days** *numdays* **-key** *Client_Privatekeyfilename* **-out** *Client_certfilename*	This command generates a new self-signed client certificate using the client private key obtained from the previous step.

	Command or Action	Purpose
	Example: `# openssl req -new -x509 -key client_private.pem -out client.pem -days 365`	The certificate is valid for the specified period. The command prompts the user for additional certificate information. A new self-signed client certificate is created.
Step 3	Obtain the KMIP root CA certificate from the KMIP server.	Refer to the KMIP vendor documentation for details on obtaining the root CA certificate.

What to do next

Upload the new certificate to the Cisco IMC.

Root CA Certificate

Downloading a Root CA Certificate

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 In the **Navigation** pane, click **Security Management** menu.

Step 3 From the **Security Management** menu, select **Secure Key Management**.

Step 4 From the **Actions** drop-down list, select **Download Root CA Certificate**.

Step 5 In the **Download Root CA Certificate** dialog box, use one of the following methods to download the Root CA certificate:

Table 236: Remote

Name	Description
Remote button	Select this option when you want to download the root CA certificate from a remote location.
Server IP/Hostname	Server details from where you want to download the root CA certificate.

Name	Description
Upload Protocol button	Select 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. To comply with Cisco security standards, certain insecure protocols (TFTP, FTP, HTTP) will no longer be supported in upcoming releases. We recommend using secure protocols like SFTP or SCP moving forward.
Path and Filename field	File path where the root CA certificate file resides on the server along with the filename.
Username field	User name for your remote server.
Password field	Password for your remote server.
Download Root CA Certificate button	Allows you to download the root CA certificate.

Table 237: Local

Name	Description
Local button	Select this option when you want to download the root CA certificate from your local machine. Click **Browse** and navigate to the root CA certificate that you want to download.
Download Root CA Certificate button	Allows you to download the root CA certificate.

Table 238: Paste

Name	Description
Paste field	Opens a text box that allows you to copy the entire content of the root CA certificate and paste it in the **Paste root CA Certificate Content** text field.
Download Root CA Certificate button	Allows you to download the root CA certificate.

Exporting a Root CA Certificate

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 In the **Navigation** pane, click **Security Management** menu.

Step 3 From the **Security Management** menu, select **Secure Key Management**.

Step 4 From the **Actions** drop-down list, select **Export Root CA Certificate**.

Step 5 In the **Export Root CA Certificate** dialog box, use one of the following methods to export Root CA certificate:

Table 239: Remote

Name	Description
Remote button	Select this option when you want to export root CA certificate from a remote location.
Server IP/Hostname	Server details where you want to export root CA certificate.
Upload Protocol button	Select 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. To comply with Cisco security standards, certain insecure protocols (TFTP, FTP, HTTP) will no longer be supported in upcoming releases. We recommend using secure protocols like SFTP or SCP moving forward.
Path and Filename field	File path where the root CA certificate file resides on the server along with the filename.
Username field	User name for your remote server.
Password field	Password for your remote server.
Export Root CA Certificate button	Allows you to export root CA certificate.

Table 240: Local

Name	Description
Local button	Select this option when you want to export root CA certificate from your local machine. Click **Browse** and navigate to the export root CA certificate that you want to export.
Export Root CA Certificate button	Allows you to export the root CA certificate.

Deleting a Root CA Certificate

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.
Step 2 In the **Navigation** pane, click **Security Management** menu.
Step 3 From the **Security Management** menu, select **Secure Key Management**.
Step 4 From the **Actions** drop-down list, select **Delete Root CA Certificate**.
Step 5 Click **OK** to confirm.

Downloading a Client Certificate

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.
Step 2 In the **Navigation** pane, click **Security Management** menu.
Step 3 From the **Security Management** menu, select **Secure Key Management**.
Step 4 From the **Actions** drop-down list, select **Download Client Certificate**.
Step 5 In the **Download Client Certificate** dialog box, use one of the following methods to download the client certificate:

Table 241: Remote

Name	Description
Remote button	Select this option when you want to download the client certificate from a remote location.
Server IP/Hostname	Server details from where you want to download the client certificate.

Name	Description
Upload Protocol button	Select 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. To comply with Cisco security standards, certain insecure protocols (TFTP, FTP, HTTP) will no longer be supported in upcoming releases. We recommend using secure protocols like SFTP or SCP moving forward.
Path and Filename field	File path where the client certificate file resides on the server along with the filename.
Username field	User name for your remote server.
Password field	Password for your remote server.
Download Client Certificate button	Allows you to download the client certificate.

Table 242: Local

Name	Description
Local button	Select this option when you want to download client certificate from your local machine. Click **Browse** and navigate to the client certificate that you want to download.
Download Client Certificate button	Allows you to download the client certificate.

Table 243: Paste

Name	Description
Paste field	Opens a text box that allows you to copy the entire content of the client certificate and paste it in the **Paste Client Certificate Content** text field.
Download Client Certificate button	Allows you to download the client certificate.

Client Certificate

Exporting a Client Certificate

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 In the **Navigation** pane, click **Security Management** menu.

Step 3 From the **Security Management** menu, select **Secure Key Management**.

Step 4 From the **Actions** drop-down list, select **Export Client Certificate**.

Step 5 In the **Export Client Certificate** dialog box, use one of the following methods to export the client certificate:

Table 244: Remote

Name	Description
Remote button	Select this option when you want to export client certificate from a remote location.
Server IP/Hostname	Server details where you want to export client certificate.
Upload Protocol button	Select 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. To comply with Cisco security standards, certain insecure protocols (TFTP, FTP, HTTP) will no longer be supported in upcoming releases. We recommend using secure protocols like SFTP or SCP moving forward.
Path and Filename field	File path where the client certificate file resides on the server along with the filename.
Username field	User name for your remote server.
Password field	Password for your remote server.
Export Client Certificate button	Allows you to export client certificate.

Table 245: Local

Name	Description
Local button	Select this option when you want to export client certificate from your local machine. Click **Browse** and navigate to the export client certificate that you want to export.
Export Client Certificate button	Allows you to export the client certificate.

Deleting a Client Certificate

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.
Step 2 In the **Navigation** pane, click **Security Management** menu.
Step 3 From the **Security Management** menu, select **Secure Key Management**.
Step 4 From the **Actions** drop-down list, select **Delete Client Certificate**.
Step 5 Click **OK** to confirm.

Downloading a Client Private Key

Procedure

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 **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 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

Client Private Key

Downloading a Client Private Key

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 In the **Navigation** pane, click **Security Management** menu.

Step 3 From the **Security Management** menu, select **Secure Key Management**.

Step 4 From the **Actions** drop-down list, select **Download Client Private Key**.

Step 5 In the **Download Client Private Key** dialog box, update the following properties:

Table 246: Remote

Name	Description
Remote button	Select this option when you want to download the client private key from a remote location.
Server IP/Hostname	Server details from where you want to download the client private key.
Upload Protocol button	Select 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.
Path and Filename field	File path where the client private key file resides on the server along with the filename.
Username field	User name for your remote server.
Password field	Password for your remote server.
Download Root CA Certificate button	Allows you to download the client private key.

Table 247: Local

Name	Description
Local button	Select this option when you want to download the client private key from your local machine. Click **Browse** and navigate to the client private key that you want to download.
Download Client Private Key button	Allows you to download the client private key.

Table 248: Paste

Name	Description
Paste field	Opens a text box that allows you to copy the entire content of the client private key and paste it in the **Download Client Private Key** text field.
Download Client Private Key button	Allows you to download client private key.

Deleting a Client Private Key

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.
Step 2 In the **Navigation** pane, click **Security Management** menu.
Step 3 From the **Security Management** menu, select **Secure Key Management**.
Step 4 From the **Actions** drop-down list, select **Delete Client Private Key**.
Step 5 Click **OK** to confirm.

Testing the KMIP Server Connection

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.
Step 2 In the **Navigation** pane, click **Security Management** menu.
Step 3 From the **Security Management** menu, select **Secure Key Management**.
Step 4 In the **KMIP Servers** area, select a row by checking the check box and click **Test Connection**.
Step 5 If the connection is successful, a success message is displayed.

Restoring the KMIP Server to Default Settings

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.
Step 2 In the **Navigation** pane, click **Security Management** menu.
Step 3 From the **Security Management** menu, select **Secure Key Management**.
Step 4 In the **KMIP Servers** area, 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.

Deleting KMIP Login Details

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.
Step 2 In the **Navigation** pane, click **Security Management** menu.
Step 3 From the **Security Management** menu, select **Secure Key Management**.
Step 4 From the **Actions** drop-down list, select **Delete KMIP Login**.
Step 5 Click **OK** to confirm.

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.

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 In the **Navigation** pane, click **Security Management** menu.

Step 3 From the **Security Management** menu, select **Security Configuration**.

Step 4 In the **Federal Information Processing Standard Configuration (FIPS) and Common Criteria (CC) Configuration** pane, toggle **Enable FIPS** button.

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 be logged in as an admin to perform this procedure.

Note If **Configured TLS Version** is set to **Custom**, then you cannot enable FIPS.

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 In the **Navigation** pane, click **Security Management** menu.

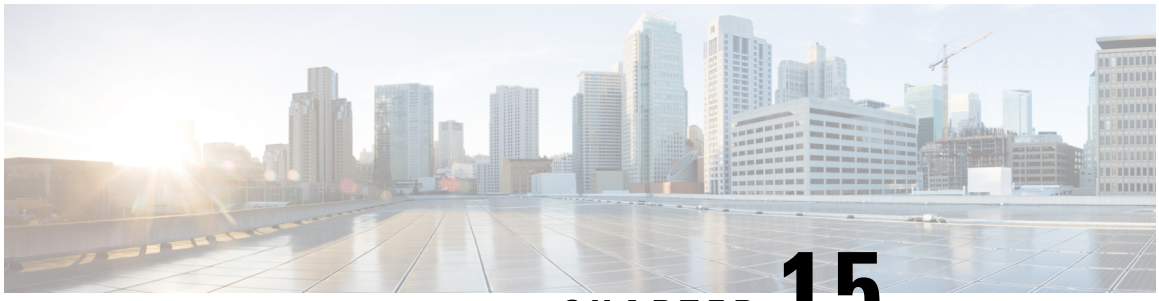
Step 3 From the **Security Management** menu, select **Security Configuration**.

Step 4 In the **Federal Information Processing Standard Configuration (FIPS) and Common Criteria (CC) Configuration** pane, toggle **Enable CC** button.

Step 5 Click **Save**.

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

- Firmware Management Overview, on page 471
- Viewing Firmware Components, on page 471
- Updating the Firmware, on page 472
- Activating the Firmware, on page 474
- Canceling Firmware Activation, on page 475

Firmware Management Overview

Firmware for the following individual components can be updated:

- CIMC
- BIOS
- RAID Controllers
- Cisco UCS VICs

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

Viewing Firmware Components

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 In the **Navigation** pane, click **Firmware Management** menu.

Step 3 In the **Firmware Management** area, review the following information for CIMC, BIOS, and other components:

Table 249: Firmware Management

Name	Description
Component checkbox	Allows you to select one ore more components.
Upload 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. **Note** **Upload** button is visible only when you select a component.
Activate button	Allows you to activate the firmware for the selected component. **Note** **Activate** button is visible only when you select a component.
Component column	List of components available for which you can update the firmware.
Running Version column	The firmware version of the component that is currently active.
Backup Version column	The alternate firmware version installed on the server, if any. The backup version is not currently running. To activate it, click **Activate**. **Note** When you install new firmware, any existing backup version is deleted and the new firmware becomes the backup version. You must manually activate the new firmware if you want the server to run the new version.
Bootloader Version column	The bootloader version associated with the boot-loader software of the component.
Status column	The status of the firmware activation on this server.
Progress in % column	The progress of the operation, in percentage.

Updating the Firmware

You can install the firmware package from a local disk, remote server, or a USB storage device connected to a server. After you confirm the installation, BMC replaces the firmware version in the component's backup memory slot with the selected version.

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 In the **Navigation** pane, click **Firmware Management** menu.

Step 3 In the **Firmware Management** area, select a component from the **Component** column and click **Upload**.
The **Update Firmware** dialog box appears.

Step 4 In the **Update Firmware** dialog box, update the following properties:

Table 250: Remote

Name	Description
Remote button	Select this option when you want to upload the firmware from a remote location.
Server IP/Hostname	Server details from where you want to download the client certificate.
Upload Protocol button	**Note** To comply with Cisco security standards, certain insecure protocols (TFTP, FTP, HTTP) will no longer be supported in upcoming releases. We recommend using secure protocols like SFTP or SCP moving forward. Select 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. • **Note** **Front Panel USB** option is visible only if **Smart Access USB** is enabled and a USB storage device is connected to the server. **Front Panel USB**—This allows you to install the firmware through a USB storage device connected to the server. Enter the firmware file name and location in the **Image Path and Filename** field, and click **Install Firmware**.
Path and Filename field	File path where the firmware file resides on the server along with the filename.
Username field	User name for your remote server.
Password field	Password for your remote server.

Name	Description
Upload button	Allows you to upload the firmware file. **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.

Table 251: Local

Name	Description
Local button	Select this option when you want to updated the firmware from your local machine. Click **Browse** and navigate to the firmware file you wish to use.
Upload button	Allows you to upload the firmare file.

Activating the Firmware

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 In the **Navigation** pane, click **Firmware Management** menu.

Step 3 In the **Firmware Management** area, select a component from the **Component** column and click **Activate**.
The **Activate Firmware** dialog box appears.

Step 4 In the **Activate Firmware** dialog box, update the following properties:

Table 252: Activate Firmware

Name	Description
Firmware Version list	A list of the firmware versions available for activating the firmware.

Name	Description
Activate Firmware button	Activates the selected firmware version depending on the component you choose. **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 **Note** You can activate the BIOS firmware when the host is On. When you do this, **Activation Pending** is displayed in the **Status** field. After the next host boot, the BIOS activation that is in the pending state is activated.

Canceling Firmware Activation

Before you begin

BIOS firmware must be in **Activation Pending** state for you to cancel the activation.

Procedure

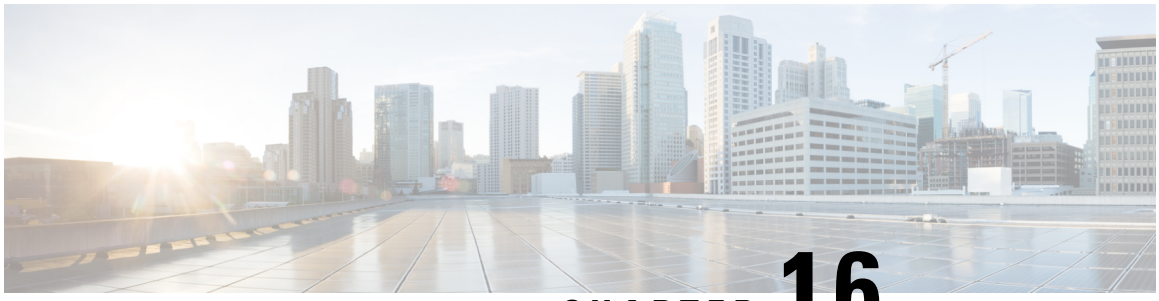
Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 In the **Navigation** pane, click **Firmware Management** menu.

Step 3 In the **Firmware Management** area, select the firmware for which you want to cancel the activation.

Step 4 Click **Cancel Activation**.

Cancel Activation button is displayed only when you choose a firmware that is in **Activation Pending** state.



CHAPTER 16

Viewing Faults and Logs

- Viewing the Fault Summary, on page 477
- Viewing Faults History, on page 478
- Viewing System Event Logs, on page 479
- Viewing the Cisco IMC Log, on page 480
- Logging Controls, on page 481

Viewing the Fault Summary

Procedure

Step 1 From the **Apps** drop-down list, select **System**.

Step 2 Select the **Faults and Logs** tab.

Step 3 In the **Navigation** pane, click **Fault Summary** menu.

Step 4 In the **Faults Summary** area, review the following properties:

Note
To view the exact summary, in the **Search Logs** field, enter the text related to the faults. Alternatively, from the **Severity** drop-down list, choose the specific severity type.

Name	Description
Time	The time when the fault occurred.
Severity	This can be one of the following: • **Critical** • **Informational** • **Major** • **Minor** • **Warning**

Name	Description
Code	The unique identifier assigned to the fault.
Domain Name	The distinguished name (Domain Name) 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.

Viewing Faults History

Procedure

Step 1 From the **Apps** drop-down list, select **System**.

Step 2 Select the **Faults and Logs** tab.

Step 3 In the **Navigation** pane, click **Fault History** menu.

Step 4 In the **Faults History** area, review the following properties:

Tip
To view the exact fault history, in the **Search Logs** field, enter the text related to the faults. Alternatively, from the **Severity** drop-down list, choose the specific severity type.

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
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.

Viewing System Event Logs

Procedure

Step 1 From the **Apps** drop-down list, select **System**.

Step 2 Select the **Faults and Logs** tab.

Step 3 In the **Navigation** pane, click **System Event Log** menu.

Step 4 In the **System Event Log** area, review the following information:

Tip
To view the exact system event log, in the **Search Logs** field, enter the text related to the system event. Alternatively, from the **Severity** drop-down list, choose the specific severity type.

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.
SEL Fullness Indicator	Displays, in percentage, the used space in the **System Event Log** tab. The percentage is calculated with 3008 entries as the reference (the System Event Log tab always displays only the most recent 3008 system events). For example, if there are 1504 entries, then the percentage is shown as 50. After the first set of 3008 entries are reached, the status is always displayed as 100% until the SEL is cleared.
Clear Logs button	Allows you to clear the system even log entries.

Viewing the Cisco IMC Log

Procedure

Step 1 From the **Apps** drop-down list, select **System**.

Step 2 Select the **Faults and Logs** tab.

Step 3 In the **Navigation** pane, click **Cisco IMC Log** menu.

Step 4 In the **Cisco IMC Log** tab, review the following information:

Tip
To view the exact Cisco IMC log, in the **Search Logs** field, enter the text related to the Cisco IMC logs. Alternatively, from the **Severity** drop-down list, choose the specific severity type.

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**
Source column	The software module that logged the event.
Description column	A description of the event.
Clear Logs button	Allows you to clear Cisco IMC log entries.

Logging Controls

Viewing Logging Controls

Procedure

Step 1 From the **Apps** drop-down list, select **System**.

Step 2 Select the **Faults and Logs** tab.

Step 3 In the **Navigation** pane, click **Logging Controls** menu.

Step 4 In the **Logging Controls** area, review the following information:

Table 253: Local Logging Area

Name	Description
Minimum Severity to Report drop-down list	The drop-down list lets you specify the lowest level of messages that will be included in the local log. You can select one of the following: • **Emergency** • **Alert** • **Critical** • **Error** • **Warning** • **Notice** • **Informational** • **Debug**

Table 254: Upload Status Area

Name	Description
Certificate Upload Status	Displays the status of the certificate upload. By default, the value is **NONE**. When the certificate upload is complete, the value is displayed as **COMPLETED**.

Name	Description
Certificate Upload Progress	Displays the progress of the certificate upload. By default, the value is **None**. When the certificate upload is complete, the value is displayed as **100%**.

Table 255: Remote Logging Area

Name	Description
+Add Server button	Allows you to add a row for a new server. Once you click **+Add Server**, you can enter the values to create a server and click **Save**.
Delete button	Allows you to delete an entry. Select the entry which you wish to delete, and click **Delete**.
Secure Syslog toggle button or column	If the status is **Enabled**, Cisco IMC makes a secure, encrypted outbound connection to remote syslog servers supporting secure connectivity for logging. **Note** If the status is **Enabled**, then the **Protocol** field is disabled by default. This property functions as a toggle button when creating or editing a server entry.
Host Name/IP Address field or column	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. This property functions as a field when creating or editing a server entry.
Port field or column	A destination port number of the Syslog server, which ranges from 1 to 65535. The default port number is 514. This property functions as a field when creating or editing a server entry.
Protocol drop-down list or column	The transport layer protocol for transmission of Syslog messages. The protocol can be one of the following: • TCP • UDP This property functions as a drop-down list when creating or editing a server entry.
Handshake Status field	If **Secure Syslog** featurs is enabled, then Cisco IMC performs SSL handshake to verify if the certificate is for the correct Syslog server.

Name	Description
Minimum Severity drop-down list or column	Specifies the lowest level of messages that will be included in the remote logs. This can be one of the following severity levels: • **Emergency** • **Alert** • **Critical** • **Error** • **Warning** • **Notice** • **Informational** • **Debug** This property functions as a drop-down list when creating or editing a server entry.
Send Test SysLog button	Allows you to send a test Cisco IMC log to the configured remote Syslog servers.
Edit icon	Allows you to edit the properties of Remote Syslog server. You can edit and save the following properties: • Host Name/IP Address • Port • Protocol • Minimum Severity
Delete button	Allows you to delete the Syslog server.

Sending the Cisco IMC Log to a Remote Server

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

Before you begin

- The remote syslog server must be configured to receive logs from a remote host.
- The remote syslog server must be configured to receive all types of logs, including authentication-related logs.
- The remote syslog server's firewall must be configured to allow syslog messages to reach the syslog server.

Procedure

Step 1 From the **Apps** drop-down list, select **System**.

Step 2 Select the **Faults and Logs** tab.

Step 3 In the **Navigation** pane, click **Logging Controls** menu.

Step 4 In the **Remote Logging** area, you can either create a new server entry or edit an entry to enable secure syslog.

Step 5 To add a new server and enable secure syslog, click **Add Server** and to edit an existing server entry, click the edit icon at the end of the row and update the following properties:

Table 256: Remote Logging Area

Name	Description
+Add Server button	Allows you to add a row for a new server. Once you click **+Add Server**, you can enter the values to create a server and click **Save**.
Delete button	Allows you to delete an entry. Select the entry which you wish to delete, and click **Delete**.
Secure Syslog toggle button or column	If the status is **Enabled**, Cisco IMC makes a secure, encrypted outbound connection to remote syslog servers supporting secure connectivity for logging. **Note** If the status is **Enabled**, then the **Protocol** field is disabled by default. This property functions as a toggle button when creating or editing a server entry.
Host Name/IP Address field or column	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. This property functions as a field when creating or editing a server entry.
Port field or column	A destination port number of the Syslog server, which ranges from 1 to 65535. The default port number is 514. This property functions as a field when creating or editing a server entry.
Protocol drop-down list or column	The transport layer protocol for transmission of Syslog messages. The protocol can be one of the following: • TCP • UDP This property functions as a drop-down list when creating or editing a server entry.
Handshake Status field	If **Secure Syslog** featurs is enabled, then Cisco IMC performs SSL handshake to verify if the certificate is for the correct Syslog server.

Name	Description
Minimum Severity drop-down list or column	Specifies the lowest level of messages that will be included in the remote logs. This can be one of the following severity levels: • **Emergency** • **Alert** • **Critical** • **Error** • **Warning** • **Notice** • **Informational** • **Debug** This property functions as a drop-down list when creating or editing a server entry.
Send Test SysLog button	Allows you to send a test Cisco IMC log to the configured remote Syslog servers.
Edit icon	Allows you to edit the properties of Remote Syslog server. You can edit and save the following properties: • Host Name/IP Address • Port • Protocol • Minimum Severity
Delete button	Allows you to delete the Syslog server.

Step 6 Click **Save Changes**.

Configuring the Cisco IMC Log Threshold

Procedure

Step 1 From the **Apps** drop-down list, select **System**.

Step 2 Select the **Faults and Logs** tab.

Step 3 In the **Navigation** pane, click **Logging Controls** menu.

Step 4 In the **Local Logging** area, use the **Minimum Severity to Report** drop-down list to specify the lowest level of messages that will be included in the log.

Table 257: Local Logging Area

Name	Description
Minimum Severity to Report drop-down list	The drop-down list lets you specify the lowest level of messages that will be included in the local log. You can select one of the following: • **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 log will contain all messages with the severity Emergency, Alert, Critical, or Error. It will not show Warning, Notice, Informational, or Debug messages.

Sending a Test Cisco IMC Log to a Remote Server

Before you begin

- The remote syslog server must be configured to receive logs from a remote host.
- The remote syslog server must be configured to receive all types of logs, including authentication-related logs.
- The remote syslog server's firewall must be configured to allow syslog messages to reach the syslog server.

Procedure

Step 1 From the **Apps** drop-down list, select **System**.
Step 2 Select the **Faults and Logs** tab.
Step 3 In the **Navigation** pane, click **Logging Controls** menu.
Step 4 In the **Remote Logging** area, click **Send Test Syslog**.

A test log is sent to the configured remote servers.

Managing the Remote Syslog Certificate

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 the Remote Syslog Certificate to one or two Cisco UCS C-series servers.

Before you begin

- You must be logged is as an admin to perform this procedure.
- If you select **Local** option, the certificate file to be uploaded must reside on a locally accessible file system.
- The following certificate formats are supported:
  - .crt
  - .cer
  - .pem

Procedure

	Command or Action	Purpose
Step 1	From the **Apps** drop-down list, select **System**.	
Step 2	Select the **Faults and Logs** tab.	
Step 3	In the **Navigation** pane, click **Logging Controls** menu.	
Step 4	In the **Remote Logging** area, select the Syslog server for which the Remote Syslog Certificate must be uploaded.	
Step 5	Click the **Upload Certificate** button.	The **Upload Remote Syslog Certificate** dialog box opens.
Step 6	Select any of the following options to select the certificate:	• Remote • Local • Paste

	Command or Action	Purpose

Table 258: Remote

Name	Description
Remote button	Select this option when you want to upload the certificate from a remote location.
Server IP/Hostname field	Server details from where you want to upload the certificate.
Upload Protocol button	**Note** To comply with Cisco security standards, certain insecure protocols (TFTP, FTP, HTTP) will no longer be supported in upcoming releases. We recommend using secure protocols like SFTP or SCP moving forward. Select 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.
Path and Filename field	File path where the certificate file resides on the server along with the filename.
Username field	User name for your remote server.
Password field	Password for your remote server.

	Command or Action	Purpose

Name	Description
Upload button	Allows you to upload the certificate.

Table 259: Local

Name	Description
Local button	Select this option when you want to upload the certificate from your local machine. Click **Browse** and navigate to the certificate that you want to upload.
Upload button	Allows you to upload the certificate.

Table 260: Paste

Name	Description
Paste button	Opens a text box that allows you to copy the entire content of the Syslog certificate and paste it in the **Paste** text field.
Upload button	Allows you to upload the certificate.

You can view the **Certificate Upload Status** and **Certificate Upload Progress** in the **Upload Status** area.

Deleting a Remote Syslog Certificate

You can delete a Remote Syslog Certificate from the server.

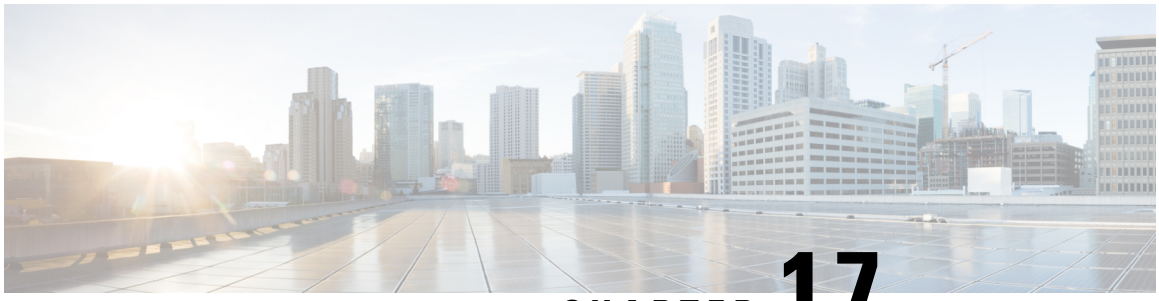
Before you begin

You must be logged is as an admin to perform this procedure.

Procedure

	Command or Action	Purpose
Step 1	From the **Apps** drop-down list, select **System**.	
Step 2	Select the **Faults and Logs** tab.	

	Command or Action	Purpose
Step 3	In the **Navigation** pane, click **Logging Controls** menu.	
Step 4	In the **Remote Logging** area, select the Syslog server for which the Syslog certificate to be deleted.	
Step 5	Click **Delete Certificate**.	
Step 6	Follow the system prompts to confirm deletion.	



CHAPTER 17

Server Utilities

- Exporting Technical Support Data, on page 491
- Downloading Technical Support Data to a Local File, on page 494
- Resetting to Factory Default, on page 495
- Exporting and Importing the Cisco IMC Configuration, on page 499
- Generating Non Maskable Interrupts to the Host, on page 503
- Adding or Updating the Cisco IMC Banner, on page 504
- Viewing Cisco IMC Last Reset Reason, on page 504
- Downloading Hardware Inventory to a Local File, on page 505
- Exporting Hardware Inventory Data to a Remote Server, on page 506
- PID Catalog, on page 507
- Enabling Smart Access USB, on page 510
- Device Connector Configuration, on page 511

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.

Important If any firmware or BIOS updates are in progress, do not export the technical support data until those tasks are complete.

Procedure

	Command or Action	Purpose
Step 1	From the **Apps** drop-down list, select **Administration**.	
Step 2	In the **Navigation** pane, click **Utilities** menu.	
Step 3	From the Actions drop-down menu, select **Admin Utilities** > **Export Technical Support Data**.	

	Command or Action	Purpose
Step 4	In the **Export Technical Support Data** dialog box, update the following properties:	*Table 261: Export Technical Support Data*

Name	Description
Server IP/Hostname field	

	Command or Action	Purpose	
		Name	**Description**
			The IP address or hostname of the server on which the support data file should be stored. **Note** **Front Panel USB** option is visible only if **Smart Access USB** is enabled and a USB storage device is connected to the server. You can export the technical support data to a remote server or to a USB storage device connected to a server. You can choose one of the following: • **Remote**— This allows you to export the technical support data to a remote server using one of the following protocols: • **TFTP** • **FTP** • **SFTP** • **SCP** • **HTTP** **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. • **Front Panel USB**—This allows you to export the technical

	Command or Action	Purpose

Name	Description
	support data to a USB storage device connected to the server.
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 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 button	Allows you to export the technical support data.

Downloading Technical Support Data to a Local File

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

Procedure

	Command or Action	Purpose
Step 1	From the **Apps** drop-down list, select **Administration**.	
Step 2	In the **Navigation** pane, click **Utilities** menu.	
Step 3	From the Actions drop-down menu, select **Admin Utilities** > **Generate Technical Support Data for Local Download**.	

	Command or Action	Purpose
Step 4	In the **Generate Technical Support Data for Local Download** dialog box, select the following options:	*Table 262: Generate Technical Support Data for Local Download*

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.
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.
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.

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.

Important When you move VIC adapters from other generation C-Series servers, you must reset the adapters to factory defaults.

Before you begin

You must be logged in as an admin to reset the server components to factory defaults.

Procedure

	Command or Action	Purpose
Step 1	From the **Apps** drop-down list, select **Administration**.	
Step 2	In the **Navigation** pane, click **Utilities** menu.	
Step 3	From the Actions drop-down menu, select **Admin Utilities** > **Reset to Factory Default**.	

	Command or Action	Purpose
Step 4	In the **Reset to Factory Default** dialog box, select the following options:	*Table 263: Reset to factory default* **Name** / **Description** **Reset to Factory Default Setting of** drop-down list

	Command or Action	Purpose	
		Name	**Description**
			Expand to select the specific component that you want to reset to factory settings. This can be one of the following: • BMC—If checked, it resets the BMC to factory settings. **Note** After 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. After factory defaults of BMC NIC Mode, **Shared LOM Extended** is configured by default. • Storage Controllers—If checked, it resets the specific storage adapters that you want to reset to factory settings. When you reset a storage adapter, the data on the disk is not modified but the virtual drive meta data will be erased which may result in data loss. Expand to select • VIC—If checked, it resets the specific VICs that you want to reset to factory settings. **Note** The host must be powered on to reset VIC adapters to

	Command or Action	Purpose

Name	Description
	factory defaults.
Reset button	Resets the selected components 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 C125 M5 servers. For other C-Series servers, NIC mode is set to Shared LOM Extended by default.

A reboot of Cisco IMC powers down the host for a short amount of time while the host is performing BIOS POST (Power on Self Test) or is in EFI shell. The 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 the Cisco IMC Configuration

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

Important If any firmware or BIOS updates are in progress, do not export the Cisco IMC configuration until those tasks are complete.

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

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

Step 3 From the Actions drop-down menu, select **Admin Utilities** > **Export Configuration**.

Step 4 In the **Export CIMC configuration** dialog box, select any of the following options to export the Cisco IMC configuration:

- Remote
- Local

Table 264: Remote

Name	Description
Remote button	Select this option to export the JSON configuration file to a remote server.
Server IP/Hostname field	The IP address or hostname of the server to which the configuration file has to be exported.
Upload Protocol button	**Note** To comply with Cisco security standards, certain insecure protocols (TFTP, FTP, HTTP) will no longer be supported in upcoming releases. We recommend using secure protocols like SFTP or SCP moving forward. The remote server type. This can be one of the following: • **TFTP** • **FTP** • **SFTP** • **SCP** • **HTTP** **Note** If you chose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message *Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*. Click Yes or No depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.
Path and Filename field	The path and filename of the configuration file on the remote server.
Username 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.

Name	Description
Passphrase field	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: ! # $ & < > ? ; ' | ` ~ \ % ^ ( )" **Note** If you edit the encrypted sections in the configuration file and try to export it, the edits will be ignored and the export operation displays a partially successful message.

Table 265: Local

Name	Description
Local button	Select this option to export the JSON configuration file to a drive that is local to the computer running Cisco IMC.
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: ! # $ & < > ? ; ' | ` ~ \ % ^ ( )" **Note** If you edit the encrypted sections in the configuration file and try to export it, the edits will be ignored and the export operation displays a partially successful message.

Importing the Cisco IMC Configuration

Important If any firmware or BIOS updates are in progress, do not import the Cisco IMC configuration until those tasks are complete.

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.

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

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

Step 3 From the Actions drop-down menu, select **Admin Utilities** > **Import Configuration**.

Step 4 The **Import CIMC configuration** dialog box, select any of the following options to import the Cisco IMC configuration:

- Remote
- Local

Table 266: Remote

Name	Description
Remote button	Select this option to import the JSON configuration file from a remote server.
Server IP/Hostname field	The IP address or hostname of the server on which the configuration file resides.
Upload Protocol button	**Note** To comply with Cisco security standards, certain insecure protocols (TFTP, FTP, HTTP) will no longer be supported in upcoming releases. We recommend using secure protocols like SFTP or SCP moving forward. The remote server type. This can be one of the following: • **TFTP** • **FTP** • **SFTP** • **SCP** • **HTTP** **Note** If you choose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message *Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*. Click Yes or No depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.
Path and Filename field	The path and filename of the configuration file on the remote server.
Username field	The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP.
Password field	The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP.

Name	Description
Passphrase field	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.

Table 267: Local

Name	Description
Local button	Select this option to import the JSON configuration file to a drive that is local to the computer running Cisco IMC. Click **Browse** and navigate to the configuration file that you want to import.
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.

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.

Before you begin

- You must be logged in as an admin to perform this procedure
- The server must be powered on.

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

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

Step 3 From the Actions drop-down menu, select **Admin Utilities** > **Generate NMI to Host**.

Step 4 In the **Generate NMI to Host** dialog box, click **OK** to proceed.
An NMI signal is sent to the host, which might restart the OS.

Adding or Updating the Cisco IMC Banner

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

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

Step 3 From the Actions drop-down menu, select **Admin Utilities** > **Add/Update Cisco IMC Banner**.

Step 4 In the **Add/Update Cisco IMC Banner** dialog box, update the following properties:

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 Cisco IMC Web UI or the command line interface.
Restart SSH toggle button	When enabled, the active SSH sessions are terminated after you click the **Save Banner** button.
Save banner button	Saves the banner changes. Click **Ok** to proceed.
Clear banner button	Clears the banner information. Click **Ok** to proceed.

Viewing Cisco IMC Last Reset Reason

Procedure

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

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

Step 3 Under the **Operations** area of the **Utilities** pane, view the following information under the **Cisco IMC Last Reset** row.

Name	Description
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. • **OOM-reset**—Cisco IMC reboots when memory reaches full capacity (without watchdog-timer).

Downloading Hardware Inventory to a Local File

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

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

Step 3 From the Actions drop-down menu, select **Admin Utilities** > **Download Hardware Inventory Data to Local Download**.

Step 4 In the **Download inventory data to local file** dialog box, select the following options:

Name	Description
Generate Inventory Data radio button	Cisco IMC disables this radio button when there is no inventory data file to download. 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.
Download Inventory Data to local file radio button	Cisco IMC enables this radio button when an inventory data file is available for download. To download the existing file, select this option and click **Download**.

Exporting Hardware Inventory Data to a Remote Server

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 From the Actions drop-down menu, select **Admin Utilities** > **Export Hardware Inventory Data to Remote**.

Step 3 In the **Export Hardware Inventory Data to Remote** dialog box, update the following properties:

Table 268: Export Hardware Inventory Data to Remote

Name	Description
Server IP/Hostname field	The IP address or hostname of the server to which the data file has to be exported.
Upload Protocol button	**Note** To comply with Cisco security standards, certain insecure protocols (TFTP, FTP, HTTP) will no longer be supported in upcoming releases. We recommend using secure protocols like SFTP or SCP moving forward. The remote server type. This can be one of the following: • **TFTP** • **FTP** • **SFTP** • **SCP** • **HTTP** **Note** If you chose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message *Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*. Click Yes or No depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.
Path and Filename field	The path and filename of the data file on the remote server.
Username field	The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP.
Password field	The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP.

Name	Description
Export button	Click to export the data file.

PID Catalog

Uploading a PID Catalog

Before you begin

You must be logged in as an admin to perform this procedure.

Procedure

Step 1 From the **Apps** drop-down list, select **System**.

Step 2 Select the **Inventory** tab.

Step 3 From the Actions drop-down menu, select **PID Catalog** > **Upload PID Catalog**.

Step 4 In the **Upload PID Catalog** dialog box, select any of the following options to select the PID catalog:

- Remote
- Local

Table 269: Remote Tab

Name	Description
Server IP/Hostname field	The IP address or hostname of the server on which the PID catalog information is available.

Name	Description
Upload Protocol button	**Note** To comply with Cisco security standards, certain insecure protocols (TFTP, FTP, HTTP) will no longer be supported in upcoming releases. We recommend using secure protocols like SFTP or SCP moving forward. Select one of the following protocols. • FTP • SFTP • SCP • TFTP • HTTP **Note** If you select FTP, SCP or SFTP, you will be prompted to enter your username and password.
Path and Filename field	The path and filename of the configuration file on the remote server.
Username field	User name of the remote server.
Password field	Password of the remote server.
Upload button	Allows you to upload the 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.

Local: Click **Browse** and navigate to the PID catalog file that you want to update on the browser client. After you select the file, click **Upload**.

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 be logged in as an admin to perform this procedure.

Procedure

Step 1 From the **Apps** drop-down list, select **System**.

Step 2 Select the **Inventory** tab.

Step 3 From the Actions drop-down menu, select **PID Catalog** > **Activate PID Catalog**.

Step 4 In the **Activate PID Catalog** dialog box, click the **Activate** button.

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 the PID catalog, the link remains active and you can activate the PID catalog 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 be logged in as an admin to perform this procedure.

SUMMARY STEPS

1. From the **Apps** drop-down list, select **System**.
2. Select the **Inventory** tab.
3. From the Actions drop-down menu, select **PID Catalog** > **Delete PID Catalog**.
4. Click **OK** to confirm.

DETAILED STEPS

Procedure

Step 1 From the **Apps** drop-down list, select **System**.

Step 2 Select the **Inventory** tab.

Step 3 From the Actions drop-down menu, select **PID Catalog** > **Delete PID Catalog**.

Step 4 Click **OK** to confirm.

Note
The **Delete PID Catalog** option is visible only if a PID catalog has already been uploaded and activated.

Enabling Smart Access USB

When you enable the smart access USB feature, the front panel USB devices are disconnected from the host operating system and connected to Cisco IMC. After enabling the smart access USB feature, you can use the front panel USB devices to export technical support data, import or export Cisco IMC configuration, or update Cisco IMC, BIOS, and VIC firmware.

The supported file systems for smart access USB are as follows:

- EXT2
- EXT3
- EXT4
- FAT32
- FAT16
- DOS

Note Huge file support is not supported in BMC. For EXT4 file system, huge file support has to be turned off.

Before you begin

You must be logged in as an admin to perform this procedure.

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

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

Step 3 From the Actions drop-down menu, select **Admin Utilities** > **Enable Smart Access USB**.

Step 4 In the **Enable Smart Access USB** dialog box, click **OK** to proceed.

Device Connector Configuration

Enabling or Disabling Cisco Intersight Management

You can enable or disable the Cisco Intersight management.

When you enable the Cisco Intersight management, it establishes a bi-directional communication between the Intersight Cloud application and the server.

Note Port numbers 8888-8889 are reserved for Intersight communication.

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 In the **Navigation** pane, click **Device Connector** menu.

Step 3 In the **Device Connector** window, click the **Settings** icon.
The **General** settings page opens.

Step 4 Enable or disable the **Device Connector** toggle button.

Name	Description
Enable	Enables the Intersight management. You can claim this system and leverage the capabilities of Cisco Intersight.
Disable	Disables the Intersight management. When disabled, no communication will be allowed to Cisco Intersight.

Viewing Intersight Device Connector Properties

Intersight Infrastructure Service License

Cisco IMC displays the following warning if the Device Connector does not detect a connection to Cisco Intersight Services:

```
The Device Connector is unable to detect a connection to Cisco Intersight.
Please check your settings and ensure that the server is claimed in
Intersight with an Intersight Infrastructure Services license to be in
compliance.( 1/5 )
```

You may click **OK** to go to **Device Connector** and configure the settings or click **Cancel** to continue.

Note The warning counter (1/5) continues to increment till it reaches (5/5). The prompt stops after it reaches (5/5) or if the Device Connector is configured, whichever is first. If the Device Connector is configured once, and later disabled, the warning is displayed again and the counter continues from the last count. The counter is reset only in case restore factory default is performed.

Apart from the warning, Cisco IMC also shows the following static ribbon at the top of screen:

```
Please note: Intersight Infrastrucutre Services license is required with
this server. Learn More.
```

You may click **Help Center** to get more information from Intersight Help Center.

Note This message is not displayed if the Device Connector is configured. If the Device Connector is configured once, and later disabled, the message is displayed again.

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 In the **Navigation** pane, click **Device Connector** menu.

Step 3 In the **Device Connector** window, review and update the following properties:

Table 270: Device Connector

Action	Description
Retry Connection or **Refresh** button	Allows you to retry the connection to Intersight. This option appears only when there are Intersight connection issues.
Open Settings button for Connection settings	Opens the Connection settings. Click Connection to see more details.
Open Settings button for General settings	Opens the General settings. Click General to see more details.

Action	Description
Settings button	Opens the following settings: • General. See General for more details. • DNS Configuration. See DNS Configuration for more details. • NTP Configuration. See NTP Configuration for more details. • Proxy Configuration. See Proxy Configuration for more details. • Cerificate Manager. See Certificate Manager for more details. • Connection. See Connection for more details.
Connection Status	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.
Device ID	Unique identifier assigned to a device managed by the Cisco IMC.
Claim ID	Unique identifier assigned to a device that is used to register and associate the device with Cisco Intersight.

Table 271: General

Name	Description
Device Connector toggle 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.
Access Mode radio button	This can be one of the following: • **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 toggle button	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.
Tunneled vKVM toggle button	This setting enables the use of a secure tunnel to access the server's KVM interface. When enabled, the KVM traffic is routed through a secure tunnel, typically via the Device Connector, enhancing the security of remote management sessions by encrypting the data transmitted between the client and the server

Table 272: DNS Configuration

Name	Description
Domain Name field	The fully qualified domain name (FQDN) or hostname of the server for Cisco IMC.
DNS Server field	IP address of the FQDN.

Table 273: NTP Configuration

Name	Description
NTP Server field	The IP/DNS address of one of the servers that act as an NTP server.

Table 274: Proxy Configuration

Name	Description
Enable Proxy toggle button	Allows you to enable or disable 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.
Username field	The credentials for the proxy server.
Password field	
Save button	Saves the proxy settings.

Table 275: Certificate Manager

Name	Description
Import button	Allows you to select and import a CA signed certificate. **Note** The imported certificates must be in the *.pem (base64 encoded) format.
Name column	Common name of the CA certificate.
In User column	Whether the certificate in the trust store was used to successfully verify the remote server.
Issued By column	The issuing authority for the certificate.
Expires column	The expiry date of the certificate.

Name	Description
View Certificate icon	Click to see certificate details.
Delete Certificate button	Allows you to delete a certificate. **Note** You cannot delete bundled certificates (certificates with the lock icon).

Table 276: View Certificate Details

Name	Description
Name	Name of the certificate.
Issued By	Name of the organization.
Expires	Expiry date of the certificate.
Fingerprints	The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.
Subject	
Country	The country in which the company resides.
Organization	The organization requesting the certificate.
Common Name	The fully qualified (FQDN or domain name of the server) hostname of the server for which the certificate was issued.
Issuer	
Country	The country in which the company that issued the certificate resides.
Organization	The organization within the company that issued the certificate.
Common Name	The fully qualified hostname of the issuing company.

Table 277: Connection

Name	Description
Check Connection	Allows you to check the connection. Click **Check Connection** to proceed.
View All Details	Opens the **View Details** window. You can view complete details of the connection under.
View Details	Allows you to view the **Addresses** and **Latency** values under DNS Resolution.

Name	Description
View Remediations	Allows administrators to view remediation actions that need to be taken on the server. Remediations typically include updates, patches, or configuration changes required to bring the server into compliance with security policies or operational standards.

Configuring HTTPS Proxy Settings for Device Connector

You can manually configure the HTTPS proxy settings for the server.

Procedure

Step 1 From the **Apps** drop-down list, select **Administration**.

Step 2 In the **Navigation** pane, click **Device Connector** menu.

Step 3 In the **Device Connector** window, click the **Settings** button.

Step 4 In the **Settings** area, select **Proxy Configuration**.

Step 5 In the **Configure proxy settings** dialog box, update the following properties:

Table 278: Proxy Configuration

Name	Description
Enable Proxy toggle button	Allows you to enable or disable 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.
Username field	The credentials for the proxy server.
Password field	
Save button	Saves the proxy settings.