



Cisco UCS C240 SD M5 Server Installation and Service Guide

First Published: 2020-07-30

Last Modified: 2023-04-05

Americas Headquarters

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



CONTENTS

PREFACE

Preface	ix
Bias-Free Documentation	ix
Introduction	ix
Communications, Services, and Additional Information	xi

CHAPTER 1

Overview	1
Overview	1
External Features	1
Serviceable Component Locations	3
Summary of Server Features	5

CHAPTER 2

Installing the Server	9
Preparing for Installation	9
Installation Warnings and Guidelines	9
Rack Requirements	11
Installing 2-Post Rack Extender	12
Installing the Server in a Rack	13
Initial Server Setup	15
Connecting to the Server Locally For Setup	16
Connecting to the Server Remotely For Setup	17
Setting Up the System With the Cisco IMC Configuration Utility	18
NIC Mode and NIC Redundancy Settings	21
Updating the BIOS and Cisco IMC Firmware	22
Accessing the System BIOS	22
Smart Access Serial	23
Smart Access USB	23

CHAPTER 3**Maintaining the Server 25**

Status LEDs and Buttons	25
Front-Panel LEDs	26
Internal Diagnostic LEDs	29
Preparing For Component Installation	31
Required Equipment For Service Procedures	31
Shutting Down and Removing Power From the Server	31
Shutting Down Using the Power Button	31
Shutting Down Using The Cisco IMC GUI	32
Shutting Down Using The Cisco IMC CLI	32
Shutting Down Using The Cisco UCS Manager Equipment Tab	32
Shutting Down Using The Cisco UCS Manager Service Profile	33
Removing the Server Top Cover	33
Serial Number Location	34
Hot Swap vs Hot Plug	35
Removing and Replacing Components	35
Serviceable Component Locations	35
Replacing SAS/SATA Drives in PCIe Risers and Vertical Drive Bays	37
SAS/SATA Drive Population Guidelines	37
4K Sector Format SAS/SATA Drives Considerations	38
Setting Up UEFI Mode Booting in the BIOS Setup Utility	38
Setting Up UEFI Mode Booting in the Cisco IMC GUI	38
Replacing a SAS/SATA Drive	39
Replacing NVMe SSDs	40
Front-Loading NVMe SSD Population Guidelines	40
NVMe SSD Requirements and Restrictions	41
Enabling Hot-Plug Support in the System BIOS	41
Enabling Hot-Plug Support Using the BIOS Setup Utility	41
Enabling Hot-Plug Support Using the Cisco IMC GUI	42
Replacing a NVMe SSD	42
Replacing HHHL Form-Factor NVMe Solid State Drives	43
HHHL SSD Population Guidelines	44
HHHL Form-Factor NVMe SSD Requirements and Restrictions	44

Replacing an HHHL Form-Factor NVMe SSD	44
Replacing Fan Modules	46
Replacing CPUs and Heatsinks	47
Special Information For Upgrades to Second Generation Intel Xeon Scalable Processors	47
CPU Configuration Rules	48
Tools Required For CPU Replacement	49
Replacing a CPU and Heatsink	49
Additional CPU-Related Parts to Order with RMA Replacement CPUs	55
Additional CPU-Related Parts to Order with RMA Replacement System Chassis	56
Moving an M5 Generation CPU	56
Replacing Memory DIMMs	61
DIMM Population Rules and Memory Performance Guidelines	61
Replacing DIMMs	63
Replacing Intel Optane DC Persistent Memory Modules	64
Intel Optane DC Persistent Memory Module Population Rules and Performance Guidelines	64
Installing Intel Optane DC Persistent Memory Modules	66
Server BIOS Setup Utility Menu for DCPMM	67
Replacing a Micro SD Card	68
Replacing a USB Drive	71
Enabling or Disabling the Internal USB Port	72
Replacing the RTC Battery	73
Replacing Power Supplies	74
Replacing AC Power Supplies	75
Replacing DC Power Supplies	76
Installing DC Power Supplies (First Time Installation)	77
Grounding for DC Power Supplies	78
Replacing a PCIe Riser	79
Installing PCIe Risers 1C and 2E	80
Replacing a PCIe Card	83
PCIe Slot Specifications	83
Replacing a PCIe Card	86
Cisco Virtual Interface Card (VIC) Considerations	87
Replacing an mLOM Card	89
Replacing a SAS Storage Controller Card (RAID or HBA)	90

Storage Controller Card Firmware Compatibility	90
Replacing a SAS Storage Controller Card (RAID or HBA)	91
Replacing a Boot-Optimized M.2 RAID Controller Module	93
Cisco Boot-Optimized M.2 RAID Controller Considerations	93
Replacing a Cisco Boot-Optimized M.2 RAID Controller	94
Replacing a Chassis Intrusion Switch	96
Installing a Trusted Platform Module (TPM)	98
TPM Considerations	98
Installing and Enabling a TPM	99
Installing TPM Hardware	99
Enabling the TPM in the BIOS	100
Enabling the Intel TXT Feature in the BIOS	101
Service Headers and Jumpers	102
Using the Clear CMOS Header (J38, Pins 9 - 10)	104
Using the BIOS Recovery Header (J38, Pins 11 - 12)	104
Procedure 1: Reboot With bios.cap Recovery File	105
Procedure 2: Use BIOS Recovery Header and bios.cap File	105
Using the Clear Password Header (J38, Pins 13 - 14)	106
Using the Boot Alternate Cisco IMC Image Header (J39, Pins 1 - 2)	107
Using the Reset Cisco IMC Password to Default Header (J39, Pins 3 - 4)	108
Using the Reset Cisco IMC to Defaults Header (J39, Pins 5 - 6)	108
Recycling the PCB Assembly (PCBA)	109

APPENDIX A
Server Specifications 115

Server Specifications	115
Physical Specifications	115
Environmental Specifications	115
Power Specifications	116
1050 W AC Power Supply	117
1050 W DC Power Supply	117
Power Cord Specifications	118

APPENDIX B
Storage Controller Considerations 121

Supported Storage Controllers and Cables	121
--	-----

Storage Controller Card Firmware Compatibility	121
Write-Cache Policy for Cisco 12G SAS Modular RAID Controllers	122
For More RAID Utility Information	122

APPENDIX C

GPU Card Installation 123

Server Firmware Requirements	123
GPU Card Configuration Rules	123
Requirement For All GPUs: Memory-Mapped I/O Greater Than 4 GB	124
Installing a GPU Card	125
Using NVIDIA GRID License Server For T-Series GPUs	128
NVIDIA GRID License Server Overview	128
Registering Your Product Activation Keys With NVIDIA	129
Downloading the GRID Software Suite	130
Installing NVIDIA GRID License Server Software	130
Installing GRID License Server on Windows	130
Installing GRID License Server on Linux	131
Installing GRID Licenses From the NVIDIA Licensing Portal to the License Server	132
Reading Your License Server's MAC Address	132
Installing Licenses From the Licensing Portal	132
Viewing Available GRID Licenses	133
Viewing Current License Usage	133
Managing GRID Licenses	133
Acquiring a GRID License on Windows	133
Acquiring a GRID License on Linux	134
Using gpumodeswitch	134
Installing Drivers to Support the GPU Cards	135
1. Updating the Server BIOS	135
2. Updating the GPU Card Drivers	136

APPENDIX D

Installation For Cisco UCS Manager Integration 137

Installation For Cisco UCS Manager Integration	137
--	-----



Preface

This preface contains the following topics:

- [Bias-Free Documentation, on page ix](#)
- [Introduction, on page ix](#)
- [Communications, Services, and Additional Information, on page xi](#)

Bias-Free Documentation



Note

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

Introduction

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

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

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated

in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

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

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

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

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

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

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

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be

present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

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

Communications, Services, and Additional Information

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

Cisco Bug Search Tool

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



CHAPTER 1

Overview

- [Overview, on page 1](#)
- [External Features, on page 1](#)
- [Serviceable Component Locations, on page 3](#)
- [Summary of Server Features, on page 5](#)

Overview

Cisco UCS C240 SD M5 (UCSC-C240-M5SD) server is orderable in one version with two possible PCIe riser combinations.

- PCIe Riser 1 (UCSC-RIS-1-240M5) and PCIe Riser 2B (UCSC-RIS-2B-240M5)—This combination supports:
 - Two vertical drive bays with up to two 2.5-inch SAS/SATA drives; or up to two 2.5-inch NVMe SSDs.
 - Six PCIe slots
- PCIe Riser 1C (UCSC-RS1C-240M5SD) and PCIe Riser 2E (UCSC-RS2E-240M5SD)—This combination supports:
 - Four drive bays in the PCIe risers support 2.5-inch SAS/SATA drives; or up to two 2.5-inch NVMe SSDs.
 - Two vertical drive bays support up to two 2.5-inch SAS/SATA drives; or up to two 2.5-inch NVMe SSDs.
 - Two PCIe slots



Note Any other combination is not supported.

External Features

This topic shows the external features of the server versions.

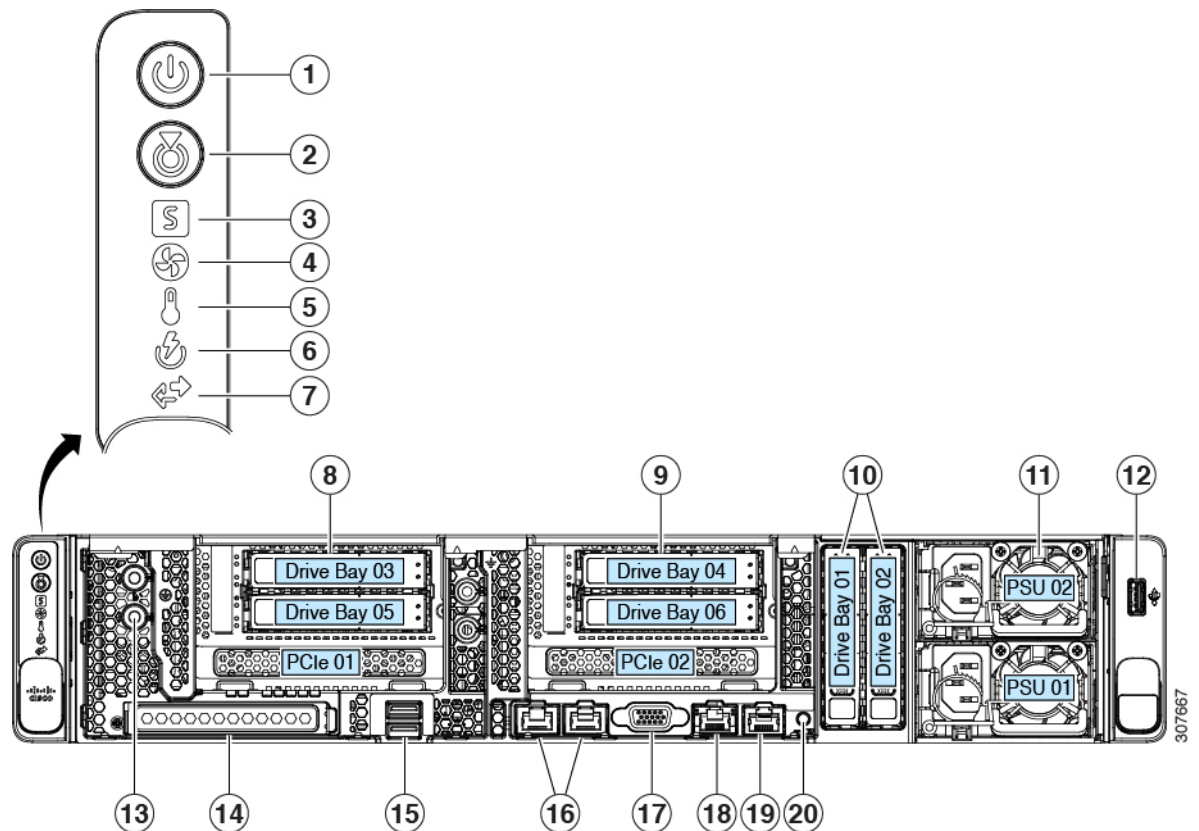
For definitions of LED states, see [Front-Panel LEDs, on page 26](#).

Cisco UCS C240 SD M5 Server Front Panel Features

The following figure shows the front panel features of Cisco UCS C240 SD M5 server.

For definitions of LED states, see [Front-Panel LEDs, on page 26](#).

Figure 1: Cisco UCS C240 SD M5 Server Front Panel



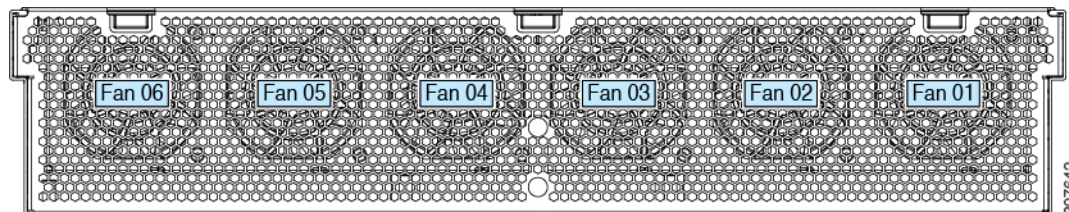
1 Power button/power status LED	11 Power supplies (two, redundant as 1+1) See Power Specifications, on page 116 for specifications and supported options.
2 Unit identification button/LED	2 USB 2.0 port
3 System health LED	3 Threaded holes for dual-hole grounding lug.
4 Fan status LED	4 Modular LAN-on-motherboard (mLOM) card slot (x16)
5 Temperature status LED	5 USB 3.0 ports (two)
6 Power supply status LED	6 Dual 1-Gb/10-Gb Ethernet ports (LAN1 and LAN2) The dual LAN ports can support 1 Gbps and 10 Gbps, depending on the link partner capability.

7 Network link activity LED	7 VGA video port (DB-15 connector)
8 PCIe riser 1 with the following options (Drive bays 03 and 05, and PCIe 01): <ul style="list-style-type: none"> • 1—Slots 1 (x8), 2 (x16), 3 (x8); slot 3 requires CPU2. • 1C—Drive bay 03 (x4), Drive bay 05 (x4), PCIe 1 (x16); all slots supported by CPU1 See PCIe Slot Specifications, on page 83 for slot specifications.	8 1-Gb Ethernet dedicated management port
9 PCIe riser 2 with the following options (Drive bays 04 and 06, and PCIe 02): <ul style="list-style-type: none"> • 2B—Slots 4 (x8), 5 (x16), 6 (x8); slot 3 requires CPU2. • 2E—Drive bay 04 (x4), Drive bay 06 (x4), PCIe 4 (x16); all slots supported by CPU2 	9 Serial port (RJ-45 connector)
0 Two 2.5-inch drive bays (Drive bays 01 and 02): <ul style="list-style-type: none"> • Supports only SAS/SATA HDD/SSD with SAS-backplane • Supports only NVME SSDs with NVMe-backplane 	0 Front panel identification button/LED

Cisco UCS C240 SD M5 Server Rear Panel Features

The following figure shows the rear panel features of Cisco UCS C240 SD M5 server.

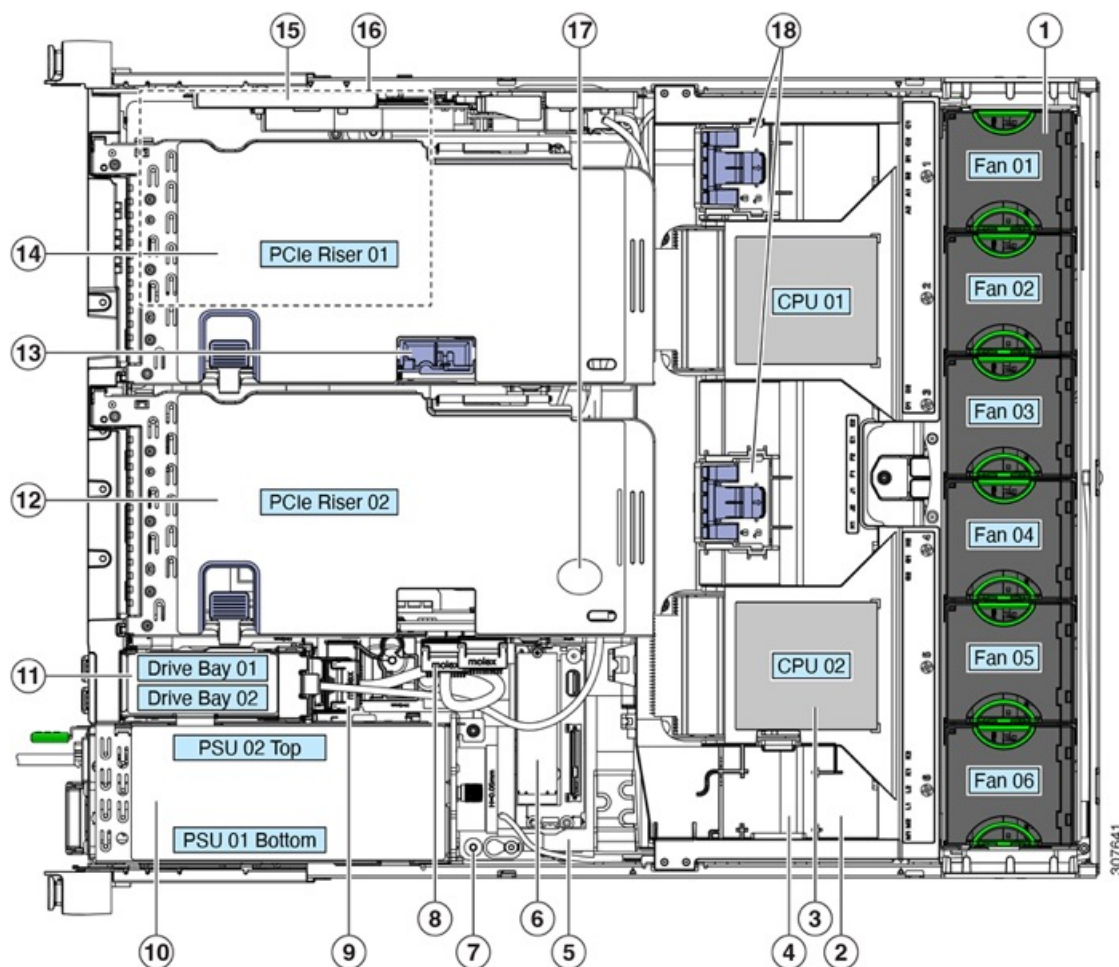
Figure 2: Cisco UCS C240 SD M5 Server Rear Panel



Serviceable Component Locations

This topic shows the locations of the field-replaceable components and service-related items. The view in the following figure shows the server with the top cover removed.

Figure 3: Cisco UCS C240 SD M5 Server, Serviceable Component Locations



<p>1 Cooling fan modules (six, hot-swappable)</p>	<p>11 Two 2.5-inch drive bays (Drive bays 01 and 02):</p> <ul style="list-style-type: none"> • Supports only SAS/SATA HDD/SSD with SAS-backplane • Supports only NVME SSDs with NVMe-backplane
<p>2 DIMM sockets on motherboard (up to 12 per CPU) Not visible under air baffle in this view. See DIMM Population Rules and Memory Performance Guidelines, on page 61 for DIMM slot numbering.</p>	<p>2 PCIe riser 2 with the following options (Drive bays 04 and 06, and PCIe 02):</p> <ul style="list-style-type: none"> • 2B—Slots 4 (x8), 5 (x16), 6 (x8); slot 3 requires CPU2. • 2E—Drive bay 04 (x4), Drive bay 06 (x4), PCIe 4 (x16); all slots supported by CPU2
<p>3 CPUs and heatsinks (up to two) Not visible under air baffle in this view.</p>	<p>3 Micro-SD socket on PCIe riser 01</p>

4 SuperCap power module mounting clip on air baffle (if applicable)	4 PCIe riser 1 with the following options (Drive bays 03 and 05, and PCIe 01): <ul style="list-style-type: none"> • 1—Slots 1 (x8), 2 (x16), 3 (x8); slot 3 requires CPU2. • 1C—Drive bay 03 (x4), Drive bay 05 (x4), PCIe 1 (x16); all slots supported by CPU1 See PCIe Slot Specifications, on page 83 for slot specifications.
5 Internal, vertical USB 3.0 port on motherboard	5 Storage controller dedicated slot
6 Mini-storage module socket. Options: <ul style="list-style-type: none"> • SD card module with two SD card slots • M.2 module with slots for two SATA M.2 drives 	6 On-Board LOM card socket on board
7 Chassis intrusion switch (optional)	7 RTC battery
8 PCIe cable connectors for NVMe SSDs.	8 Securing clips for GPU cards on air baffle
9 Vertical drive backplane assembly	
10 Power supplies (hot-swappable when redundant as 1+1)	

The Technical Specifications Sheets for all versions of this server, which include supported component part numbers, are at [Cisco UCS Servers Technical Specifications Sheets](#) (scroll down to *Technical Specifications*).

Summary of Server Features

The following table lists a summary of server features.

Feature	Description
Chassis	Two rack-unit (2RU) chassis
Central Processor	Up to two CPUs from the Intel Xeon Processor Scalable Family. This includes CPUs from the following series: <ul style="list-style-type: none"> • Intel Xeon Bronze 3XXX Processors • Intel Xeon Silver 4XXX Processors • Intel Xeon Gold 5XXX Processors • Intel Xeon Gold 6XXX Processors • Intel Xeon Platinum 8XXX Processors
Memory	24 DDR4 DIMM sockets on the motherboard (12 each CPU)
Multi-bit error protection	Multi-bit error protection is supported

Feature	Description
Baseboard management	BMC, running Cisco Integrated Management Controller (Cisco IMC) firmware. Depending on your Cisco IMC settings, Cisco IMC can be accessed through the 1-Gb dedicated management port, the 1-Gb/10-Gb Ethernet LAN ports, or a Cisco virtual interface card.
Network and management I/O	Front panel: <ul style="list-style-type: none"> • One 1-Gb Ethernet dedicated management port (RJ-45 connector) • Two 1-Gb/10-Gb BASE-T Ethernet LAN ports (RJ-45 connectors) <p>The dual LAN ports can support 1 Gbps and 10 Gbps, depending on the link partner capability.</p> <ul style="list-style-type: none"> • One RS-232 serial port (RJ-45 connector) • One VGA video connector port (DB-15 connector) • Two USB 3.0 ports • One USC 2.0 port
Modular LOM	One dedicated socket (x16 PCIe lane) that can be used to add an mLOM card for additional front-panel connectivity.
Power	Two power supplies, redundant as 1+1: <ul style="list-style-type: none"> • AC power supplies 1050 W AC each • DC power supplies 1050 W DC each <p>Do not mix power supply types or wattages in the server.</p>
ACPI	The advanced configuration and power interface (ACPI) 4.0 standard is supported.
Cooling	Six hot-swappable fan modules for front-to-rear cooling.
PCIe I/O	Two horizontal PCIe expansion slots on two PCIe riser assemblies. See PCIe Slot Specifications, on page 83 for specifications of the slots.
InfiniBand	The PCIe bus slots in this server support the InfiniBand architecture.
Storage, front-panel	Four 2.5-inch drive bays on risers 1 and 2; Two 2.5-inch vertical drive bays. <ul style="list-style-type: none"> • Supports only SAS/SATA HDD/SSD with SAS-backplane • Supports only NVMe SSDs with NVMe-backplane <p>SAS/SATA drives are hot-swappable. NVMe SSDs are hot-pluggable, meaning that they must be shut down in the operating system before hot-removal.</p>

Feature	Description
Storage, internal	<p>The server has these internal storage options:</p> <ul style="list-style-type: none">• One USB 3.0 port on the motherboard.• One micro-SD card socket on PCIe riser 1.• Mini-storage module socket, optionally with either:<ul style="list-style-type: none">• SD card carrier. Supports up to two SD cards.• M.2 SSD carrier. Supports two SATA M.2 SSDs.• Cisco Boot-Optimized M.2 RAID Controller (module with two slots for SATA M.2 drives, plus an integrated SATA RAID controller that can control the two SATA M.2 drives in a RAID 1 array)
Storage management	<p>Dedicated internal slot for Cisco 12G SAS HBA only</p> <p>For a detailed list of storage controller options, see Supported Storage Controllers and Cables, on page 121.</p>
RAID backup (if available)	<p>The server has a mounting bracket on the removable air baffle for one supercap unit that is used with the Cisco modular RAID controller card.</p>
Integrated video	<p>Integrated VGA video.</p>



CHAPTER 2

Installing the Server

- [Preparing for Installation, on page 9](#)
- [Installing 2-Post Rack Extender, on page 12](#)
- [Installing the Server in a Rack, on page 13](#)
- [Initial Server Setup, on page 15](#)
- [NIC Mode and NIC Redundancy Settings, on page 21](#)
- [Updating the BIOS and Cisco IMC Firmware, on page 22](#)
- [Accessing the System BIOS, on page 22](#)
- [Smart Access Serial, on page 23](#)
- [Smart Access USB, on page 23](#)

Preparing for Installation

This section contains the following topics:

Installation Warnings and Guidelines



Note

Before you install, operate, or service a server, review the [Regulatory Compliance and Safety Information for Cisco UCS C-Series Servers](#) for important safety information.



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.

Statement 1071

**Warning**

To prevent the system from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of: 35° C (95° F).

Statement 1047

**Warning**

The plug-socket combination must be accessible at all times, because it serves as the main disconnecting device.

Statement 1019

**Warning**

This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than: 250 V, 15 A.

Statement 1005

**Warning**

Installation of the equipment must comply with local and national electrical codes.

Statement 1074

**Warning**

This unit is intended for installation in restricted access areas. A restricted access area can be accessed only through the use of a special tool, lock, and key, or other means of security.

Statement 1017

**Caution**

To ensure proper airflow it is necessary to rack the servers using rail kits. Physically placing the units on top of one another or “stacking” without the use of the rail kits blocks the air vents on top of the servers, which could result in overheating, higher fan speeds, and higher power consumption. We recommend that you mount your servers on rail kits when you are installing them into the rack because these rails provide the minimal spacing required between the servers. No additional spacing between the servers is required when you mount the units using rail kits.

**Caution**

Avoid uninterruptible power supply (UPS) types that use ferroresonant technology. These UPS types can become unstable with systems such as the Cisco UCS, which can have substantial current draw fluctuations from fluctuating data traffic patterns.

When you are installing a server, use the following guidelines:

- Plan your site configuration and prepare the site before installing the server. See the [Cisco UCS Site Preparation Guide](#) for the recommended site planning tasks.

- Ensure that there is adequate space around the server to allow for accessing the server and for adequate airflow. The airflow in this server is from front to back.
- Ensure that the air-conditioning meets the thermal requirements listed in the [Environmental Specifications, on page 115](#).
- Ensure that the cabinet or rack meets the requirements listed in the [Rack Requirements, on page 11](#).
- Ensure that the site power meets the power requirements listed in the [Power Specifications, on page 116](#). If available, you can use an uninterruptible power supply (UPS) to protect against power failures.

Rack Requirements

The rack must be of the following type:

- A standard 19-in. (48.3-cm) wide, four-post EIA rack, with mounting posts that conform to English universal hole spacing, per section 1 of ANSI/EIA-310-D-1992.
- A standard 19-in. (48.3-cm) wide, two-post EIA rack (can be used only with Extender Bracket Kit)
- The rack-post holes can be square 0.38-inch (9.6 mm), round 0.28-inch (7.1 mm), #12-24 UNC, or #10-32 UNC when you use the Cisco-supplied slide rails.
- The minimum vertical rack space per server must be two rack units (RUs), equal to 3.5 in. (88.9 mm).

Supported Cisco Slide Rail Kits

The server supports the following rail kit options:

- Cisco part UCSC-RAILS-M5 (ball-bearing slide rail kit)
- Extender Bracket Kit (UCSC-C240SD-EXT) for 2-post rack rail installation

Rack Installation Tools Required

The slide rails sold by Cisco Systems for this server do not require tools for installation.

Slide Rail

The slide rails for this server have an adjustment range of 24 to 36 inches (610 to 914 mm).

Installing 2-Post Rack Extender



Warning

To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:

This unit should be mounted at the bottom of the rack if it is the only unit in the rack.

When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.

If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.

Statement 1006

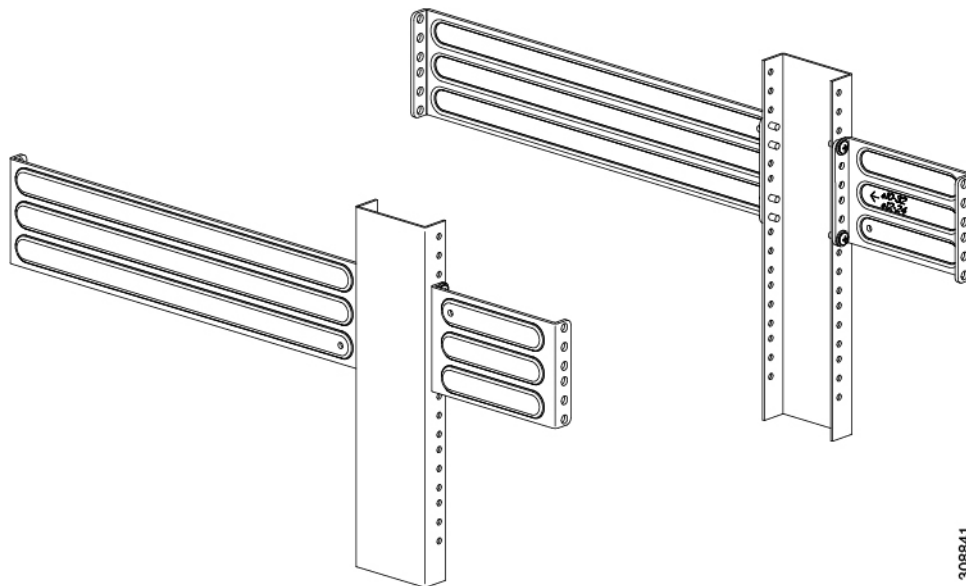
Step 1

Align one shorter bracket end with the front of the rack-post holes that you want to use. Ensure that the flanges are pointing inwards. See [Figure 4: 2-Post Rack Extender, on page 12](#).

Use one screw at the bottom and one at the top to fasten the bracket to the post.

Note For square hole rail posts, snap in the square nuts first before installing the bracket.

Figure 4: 2-Post Rack Extender



Step 2

Repeat the same to attach the second shorter bracket to the other post. Ensure that the two brackets are at the same height and are level.

Step 3

Align one longer bracket end with the back of the rack-post holes. Ensure that the flanges are pointing inwards, and that the long bracket is at the same height as the short bracket. See [Figure 4: 2-Post Rack Extender, on page 12](#).

Use two screws at the bottom and two at the top to fasten the bracket to the post.

Note For square hole rail posts, snap in the square nuts first before installing the bracket.

What to do next

Perform [Installing the Server in a Rack, on page 13](#) procedure to install the slide rails and the server in the rack.

Installing the Server in a Rack



Warning

To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:

This unit should be mounted at the bottom of the rack if it is the only unit in the rack.

When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.

If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.

Statement 1006

Before you begin

If you are installing the server on a 2-post rack, ensure that you have installed the extender kit. See [Installing 2-Post Rack Extender, on page 12](#).

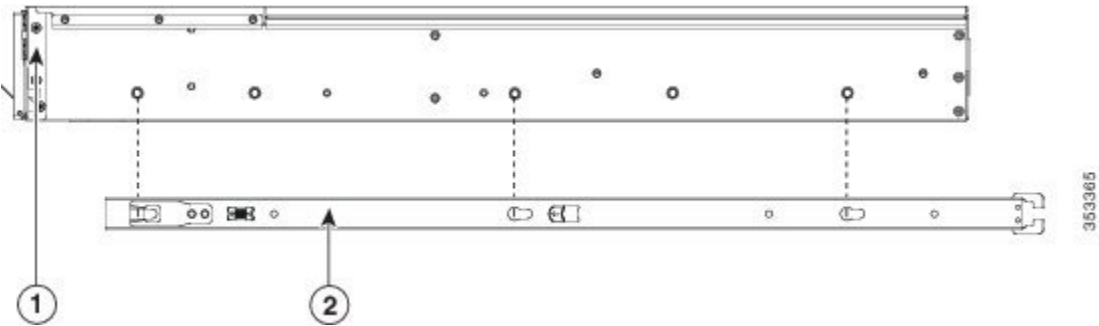
Step 1 Inner and outer rails are shipped as an assembled unit. Separate the inner and the outer rail:

- a. Slide the internal rail out till it hits the internal stop.
- b. Slide the spring loaded locking button in the direction of the arrow (shown on the button) to release it from the outer rail and pull the rail out at the same time.

Step 2 Attach the inner rails to the sides of the server:

- a) Align an inner rail with one side of the server so that the three keyed slots in the rail align with the three pegs on the side of the server.
- b) Set the keyed slots over the pegs, and then slide the rail toward the front to lock it in place on the pegs. The front slot has a metal clip that locks over the front peg.
- c) Install the second inner rail to the opposite side of the server.

Figure 5: Attaching the Inner Rail to the Side of the Server

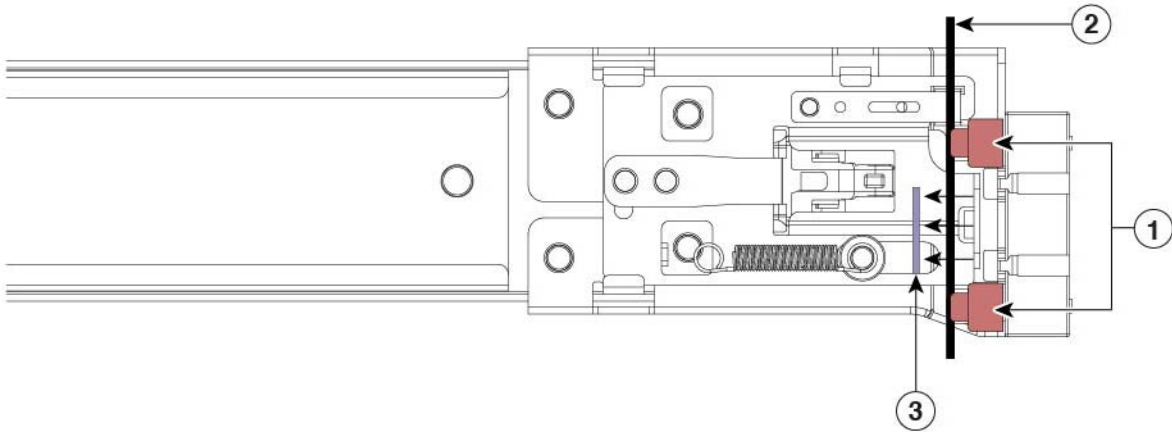


Front of server	Inner rail
-----------------	------------

Step 3 Open the front securing plate on both slide-rail assemblies. The front end of the slide-rail assembly has a spring-loaded securing plate that must be open before you can insert the mounting pegs into the rack-post holes.

On the *outside* of the assembly, push the green-arrow button toward the rear to open the securing plate.

Figure 6: Front Securing Mechanism, Inside of Front End



Front mounting pegs	Securing plate shown pulled back to the open position
Rack post between mounting pegs and opened securing plate	-

Step 4 Install the outer slide rails into the rack:

a) Align one slide-rail assembly front end with the front rack-post holes that you want to use.

The slide rail front-end wraps around the outside of the rack post and the mounting pegs enter the rack-post holes from the outside-front. See [Figure 6: Front Securing Mechanism, Inside of Front End, on page 14](#).

Note The rack post must be between the mounting pegs and the *open* securing plate.

b) Push the mounting pegs into the rack-post holes from the outside-front.

c) Press the securing plate release button, marked PUSH. The spring-loaded securing plate closes to lock the pegs in place.

- d) Adjust the slide-rail length, and align the slide-rail assembly rear end with the corresponding rear rack-post holes. The slide rail must be level front-to-rear.
The rear mounting pegs enter the rear rack-post holes from the *inside* of the rack post.
- e) Push the locking lever inwards and at the same time push the rear mounting pegs in the corresponding rear rack post holes.
- f) Once the mounting pegs are in place, release the locking lever.
- g) Attach the second slide-rail assembly to the opposite side of the rack. Ensure that the two slide-rail assemblies are at the same height and are level front-to-back.
- h) Pull the inner slide rails on each assembly out toward the rack front until they hit the internal stops and lock in place.

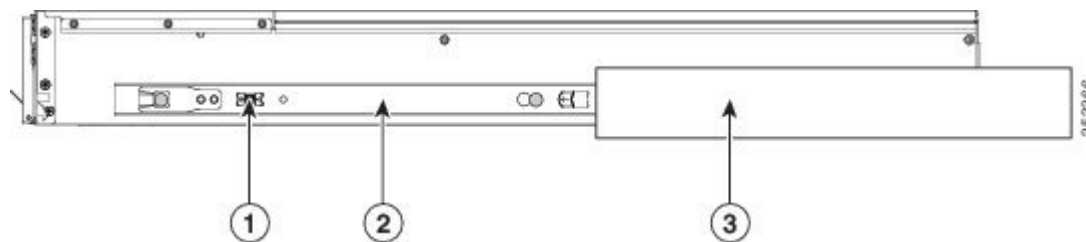
Step 5

Insert the server into the slide rails:

Caution This server can weigh up to 40 pounds (18 kilograms) when fully loaded with components. We recommend that you use a minimum of two people or a mechanical lift when lifting the server. Attempting this procedure alone could result in personal injury or equipment damage.

- a) Align the rear ends of the inner rails that are attached to the server sides with the front ends of the empty slide rails on the rack.
- b) Push the inner rails into the slide rails on the rack until they stop at the internal stops.
- c) Slide the inner-rail release clip toward the rear on both inner rails, and then continue pushing the server into the rack until the front slam-latches engage with the rack posts.

Figure 7: Inner-Rail Release Clip



Inner-rail release clip	Outer slide rail attached to rack post
Inner rail attached to server and inserted into outer slide rail	-

Initial Server Setup



Note

This section describes how to power on the server, assign an IP address, and connect to server management when using the server in standalone mode. To use the server in Cisco UCS Manager integration, specific cabling and settings are required. See [Installation For Cisco UCS Manager Integration, on page 137](#).

Server Default Settings

The server is shipped with these default settings:

- The NIC mode is *Shared LOM EXT*.

Shared LOM EXT mode enables the 1-Gb/10-Gb Ethernet ports *and* the ports on any installed Cisco virtual interface card (VIC) to access the Cisco Integrated Management Interface (Cisco IMC). If you want to use the 10/100/1000 dedicated management ports to access Cisco IMC, you can connect to the server and change the NIC mode as described in [Setting Up the System With the Cisco IMC Configuration Utility, on page 18](#).

- The NIC redundancy is *Active-Active*. All Ethernet ports are utilized simultaneously.
- DHCP is enabled.
- IPv4 is enabled.

Connection Methods

There are two methods for connecting to the system for initial setup:

- Local setup—Use this procedure if you want to connect a keyboard and monitor directly to the system for setup. This procedure can use the VGA and USB ports on the front of the server.
- Remote setup—Use this procedure if you want to perform setup through your dedicated management LAN.

**Note**

To configure the system remotely, you must have a DHCP server on the same network as the system. Your DHCP server must be preconfigured with the range of MAC addresses for this server node. The MAC address is printed on a label that is on the pull-out asset tag on the front panel. This server node has a range of six MAC addresses assigned to the Cisco IMC. The MAC address printed on the label is the beginning of the range of six contiguous MAC addresses.

Connecting to the Server Locally For Setup

This procedure requires the following equipment:

- VGA monitor
- USB keyboard
- Supported USB cable and VGA DB-15 cable

Step 1

Attach a power cord to each power supply in your server, and then attach each power cord to a grounded AC power outlet.

If you are using DC power supplies, see [Installing DC Power Supplies \(First Time Installation\), on page 77](#).

Wait for approximately two minutes to let the server boot to standby power during the first bootup. You can verify system power status by looking at the system Power Status LED on the front panel. The system is in standby power mode when the LED is amber.

Step 2 Connect a USB keyboard and mouse, and VGA monitor to the corresponding connectors on the front panel.

Step 3 Open the Cisco IMC Configuration Utility:

- a) Press and hold the front panel power button for four seconds to boot the server.
- b) During bootup, press **F8** when prompted to open the Cisco IMC Configuration Utility.

Note The first time that you enter the Cisco IMC Configuration Utility, you are prompted to change the default password. The default password is *password*. **Strong Password** feature is enabled.

Following are the requirements for **Strong Password**:

- The password can have minimum 8 characters; maximum 14 characters.
- The password must not contain the user name.
- The password must contain characters from three of the following four categories:
 - English uppercase letters (A through Z)
 - English lowercase letters (a through z)
 - Base 10 digits (0 through 9)
 - Non-alphabetic characters !, @, #, \$, %, ^, &, *, -, _, =, “

Step 4 Continue with [Setting Up the System With the Cisco IMC Configuration Utility, on page 18](#).

Connecting to the Server Remotely For Setup

This procedure requires the following equipment:

- One RJ-45 Ethernet cable that is connected to your management LAN.

Before you begin



Note To configure the system remotely, you must have a DHCP server on the same network as the system. Your DHCP server must be preconfigured with the range of MAC addresses for this server node. The MAC address is printed on a label that is on the pull-out asset tag on the front panel. This server node has a range of six MAC addresses assigned to the Cisco IMC. The MAC address printed on the label is the beginning of the range of six contiguous MAC addresses.

Step 1 Attach a power cord to each power supply in your server, and then attach each power cord to a grounded AC power outlet. If you are using DC power supplies, see [Installing DC Power Supplies \(First Time Installation\), on page 77](#).

Wait for approximately two minutes to let the server boot to standby power during the first bootup. You can verify system power status by looking at the system Power Status LED on the front panel. The system is in standby power mode when the LED is amber.

Step 2 Plug your management Ethernet cable into the dedicated management port on the front panel.

- Step 3** Allow your preconfigured DHCP server to assign an IP address to the server node.
- Step 4** Use the assigned IP address to access and log in to the Cisco IMC for the server node. Consult with your DHCP server administrator to determine the IP address.
- Note** The default user name for the server is *admin*. The default password is *password*.
- Step 5** From the Cisco IMC Server Summary page, click **Launch KVM Console**. A separate KVM console window opens.
- Step 6** From the Cisco IMC Summary page, click **Power Cycle Server**. The system reboots.
- Step 7** Select the KVM console window.
- Note** The KVM console window must be the active window for the following keyboard actions to work.
- Step 8** When prompted, press **F8** to enter the Cisco IMC Configuration Utility. This utility opens in the KVM console window.
- Note** The first time that you enter the Cisco IMC Configuration Utility, you are prompted to change the default password. The default password is *password*. **Strong Password** feature is enabled.
- Following are the requirements for **Strong Password**:
- The password can have minimum 8 characters; maximum 14 characters.
 - The password must not contain the user's name.
 - The password must contain characters from three of the following four categories:
 - English uppercase letters (A through Z)
 - English lowercase letters (a through z)
 - Base 10 digits (0 through 9)
 - Non-alphabetic characters !, @, #, \$, %, ^, &, *, -, _, =, “
- Step 9** Continue with [Setting Up the System With the Cisco IMC Configuration Utility, on page 18](#).

Setting Up the System With the Cisco IMC Configuration Utility

Before you begin

The following procedure is performed after you connect to the system and open the Cisco IMC Configuration Utility.

- Step 1** Set the NIC mode to choose which ports to use to access Cisco IMC for server management:
- *Shared LOM EXT* (default)—This is the shared LOM extended mode, the factory-default setting. With this mode, the Shared LOM and Cisco Card interfaces are both enabled. You must select the default *Active-Active* NIC redundancy setting in the following step.
- In this NIC mode, DHCP replies are returned to both the shared LOM ports and the Cisco card ports. If the system determines that the Cisco card 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 card are disabled. Use the Cisco Card NIC mode if you want to connect to Cisco IMC through a Cisco card in standalone mode.

- *Shared LOM*—The 1-Gb/10-Gb Ethernet ports are used to access Cisco IMC. You must select either the *Active-Active* or *Active-standby* NIC redundancy setting in the following step.
- *Dedicated*—The dedicated management port is used to access Cisco IMC. You must select the *None* NIC redundancy setting in the following step.
- *Cisco Card*—The ports on an installed Cisco UCS Virtual Interface Card (VIC) are used to access the Cisco IMC. You must select either the *Active-Active* or *Active-standby* NIC redundancy setting in the following step.

See also the required VIC Slot setting below.

- *VIC Slot*—Only if you use the Cisco Card NIC mode, you must select this setting to match where your VIC is installed. The choices are Riser1, Riser2, or Flex-LOM (the mLOM slot).
 - For servers with PCIe Riser 1 and 2B combination:
 - If you select Riser1, you must install the VIC in slot 2.
 - If you select Riser2, you must install the VIC in slot 5.
 - For servers with PCIe Riser 1C and 2E combination:
 - If you select Riser1, you must install the VIC in slot 1.
 - If you select Riser2, you must install the VIC in slot 2.
 - If you select Flex-LOM, you must install an mLOM-style VIC in the mLOM slot.

Step 2

Set the NIC redundancy to your preference. This server has three possible NIC redundancy settings:

- *None*—The Ethernet ports operate independently and do not fail over if there is a problem. This setting can be used only with the Dedicated NIC mode.
- *Active-standby*—If an active Ethernet port fails, traffic fails over to a standby port. Shared LOM and Cisco Card modes can each use either Active-standby or Active-active settings.
- *Active-active* (default)—All Ethernet ports are utilized simultaneously. The Shared LOM EXT mode must use only this NIC redundancy setting. Shared LOM and Cisco Card modes can each use either Active-standby or Active-active settings.

Step 3

Choose whether to enable DHCP for dynamic network settings, or to enter static network settings.

Note Before you enable DHCP, you must preconfigure your DHCP server with the range of MAC addresses for this server. The MAC address is printed on a label on the rear of the server. This server has a range of six MAC addresses assigned to Cisco IMC. The MAC address printed on the label is the beginning of the range of six contiguous MAC addresses.

The *static* IPv4 and IPv6 settings include the following:

- The Cisco IMC IP address.
For IPv6, valid values are 1 - 127.
- The gateway.
For IPv6, if you do not know the gateway, you can set it as none by entering :: (two colons).
- The preferred DNS server address.

For IPv6, you can set this as none by entering :: (two colons).

Step 4 (Optional) Make VLAN settings.

Step 5 Press **F1** to go to the second settings window, then continue with the next step.

From the second window, you can press **F2** to switch back to the first window.

Step 6 (Optional) Set a hostname for the server.

Step 7 (Optional) Enable dynamic DNS and set a dynamic DNS (DDNS) domain.

Step 8 (Optional) If you check the Factory Default check box, the server reverts to the factory defaults.

Step 9 (Optional) Set a default user password.

Note The factory default username for the server is *admin*. The default password is *password*.

Step 10 (Optional) Enable auto-negotiation of port settings or set the port speed and duplex mode manually.

Note Auto-negotiation is applicable only when you use the Dedicated NIC mode. Auto-negotiation sets the port speed and duplex mode automatically based on the switch port to which the server is connected. If you disable auto-negotiation, you must set the port speed and duplex mode manually.

Step 11 (Optional) Reset port profiles and the port name.

Step 12 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 13 Press **F10** to save your settings and reboot the server.

Note If you chose to enable DHCP, the dynamically assigned IP and MAC addresses are displayed on the console screen during bootup.

What to do next

Use a browser and the IP address of the Cisco IMC to connect to the Cisco IMC management interface. The IP address is based upon the settings that you made (either a static address or the address assigned by your DHCP server).



Note The factory default username for the server is *admin*. The default password is *password*.

To manage the server, see the *Cisco UCS C-Series Rack-Mount Server Configuration Guide* or the *Cisco UCS C-Series Rack-Mount Server CLI Configuration Guide* for instructions on using those interfaces for your Cisco IMC release. The links to the configuration guides are in the [Cisco UCS C-Series Documentation Roadmap](#).

NIC Mode and NIC Redundancy Settings

Table 1: Valid NIC Redundancy Settings For Each NIC Mode

NIC Mode	Valid NIC Redundancy Settings
Shared LOM EXT	Active-active
Dedicated	None
Shared LOM	Active-active Active-standby
Cisco Card	Active-active Active-standby

This server has the following NIC mode settings that you can choose from:

- *Shared LOM EXT* (default)—This is the shared LOM extended mode, the factory-default setting. With this mode, the Shared LOM and Cisco Card interfaces are both enabled. You must select the default *Active-Active* NIC redundancy setting in the following step.

In this NIC mode, DHCP replies are returned to both the shared LOM ports and the Cisco card ports. If the system determines that the Cisco card 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 card are disabled. Use the Cisco Card NIC mode if you want to connect to Cisco IMC through a Cisco card in standalone mode.

- *Shared LOM*—The 1-Gb/10-Gb Ethernet ports are used to access Cisco IMC. You must select either the *Active-Active* or *Active-standby* NIC redundancy setting in the following step.
- *Dedicated*—The dedicated management port is used to access Cisco IMC. You must select the *None* NIC redundancy setting in the following step.
- *Cisco Card*—The ports on an installed Cisco UCS Virtual Interface Card (VIC) are used to access the Cisco IMC. You must select either the *Active-Active* or *Active-standby* NIC redundancy setting in the following step.

See also the required VIC Slot setting below.

- *VIC Slot*—Only if you use the Cisco Card NIC mode, you must select this setting to match where your VIC is installed. The choices are Riser1, Riser2, or Flex-LOM (the mLOM slot).
 - For servers with PCIe Riser 1 and 2B combination:
 - If you select Riser1, you must install the VIC in slot 2.
 - If you select Riser2, you must install the VIC in slot 5.
 - For servers with PCIe Riser 1C and 2E combination:
 - If you select Riser1, you must install the VIC in slot 1.

- If you select Riser2, you must install the VIC in slot 2.
- If you select Flex-LOM, you must install an mLOM-style VIC in the mLOM slot.

This server has the following NIC redundancy settings that you can choose from:

- *None*—The Ethernet ports operate independently and do not fail over if there is a problem. This setting can be used only with the Dedicated NIC mode.
- *Active-standby*—If an active Ethernet port fails, traffic fails over to a standby port. Shared LOM and Cisco Card modes can each use either Active-standby or Active-active settings.
- *Active-active* (default)—All Ethernet ports are utilized simultaneously. The Shared LOM EXT mode must use only this NIC redundancy setting. Shared LOM and Cisco Card modes can each use either Active-standby or Active-active settings.

Updating the BIOS and Cisco IMC Firmware



Caution

When you upgrade the BIOS firmware, you must also upgrade the Cisco IMC firmware to the same version or the server does not boot. Do not power off the server until the BIOS and Cisco IMC firmware are matching or the server does not boot.

Cisco provides the *Cisco Host Upgrade Utility* to assist with simultaneously upgrading the BIOS, Cisco IMC, and other firmware to compatible levels.

The server uses firmware obtained from and certified by Cisco. Cisco provides release notes with each firmware image. There are several possible methods for updating the firmware:

- **Recommended method for firmware update:** Use the Cisco Host Upgrade Utility to simultaneously upgrade the Cisco IMC, BIOS, and component firmware to compatible levels.

See the *Cisco Host Upgrade Utility Quick Reference Guide* for your firmware release at the documentation roadmap link below.

- You can upgrade the Cisco IMC and BIOS firmware by using the Cisco IMC GUI interface.

See the *Cisco UCS C-Series Rack-Mount Server Configuration Guide*.

- You can upgrade the Cisco IMC and BIOS firmware by using the Cisco IMC CLI interface.

See the *Cisco UCS C-Series Rack-Mount Server CLI Configuration Guide*.

For links to the documents listed above, see the [Cisco UCS C-Series Documentation Roadmap](#).

Accessing the System BIOS

Step 1 Enter the BIOS Setup Utility by pressing the **F2** key when prompted during bootup.

Note The version and build of the current BIOS are displayed on the Main page of the utility.

- Step 2** Use the arrow keys to select the BIOS menu page.
- Step 3** Highlight the field to be modified by using the arrow keys.
- Step 4** Press **Enter** to select the field that you want to change, and then modify the value in the field.
- Step 5** Press the right arrow key until the Exit menu screen is displayed.
- Step 6** Follow the instructions on the Exit menu screen to save your changes and exit the setup utility (or press **F10**). You can exit without saving changes by pressing **Esc**.
-

Smart Access Serial

This server supports the Smart Access Serial feature. This feature allows you to switch between host serial and Cisco IMC CLI.

- This feature has the following requirements:
 - A serial cable connection, which can use the RJ-45 serial connector on the server front panel.
 - Console redirection must be enabled in the server BIOS.
 - Terminal type must be set to VT100+ or VTUFT8.
 - Serial-over-LAN (SOL) must be disabled (SOL is disabled by default).
- To switch from host serial to Cisco IMC CLI, press **Esc+9**.

You must enter your Cisco IMC credentials to authenticate the connection.
- To switch from Cisco IMC CLI to host serial, press **Esc+8**.



Note You cannot switch to Cisco IMC CLI if the serial-over-LAN (SOL) feature is enabled.

- After a session is created, it is shown in the CLI or web GUI by the name `serial`.

Smart Access USB

This server supports the Smart Access USB feature. The board management controller (BMC) in this server can accept a USB mass storage device and access the data on it. This feature allows you to use the front-panel USB device as a medium to transfer data between the BMC and the user without need for network connectivity. This can be useful, for example, when remote BMC interfaces are not yet available, or are not accessible due to network misconfiguration.

- This feature has the following requirements:
 - Connect a USB keyboard and mouse, and VGA monitor to the corresponding connectors on the front panel.
 - A USB storage device connected to one of the USB 3.0 connectors on the front panel.

- You can use USB 3.0-based devices, but they will operate at USB 2.0 speed.
- We recommend that the USB device have only one partition.
- The file system formats supported are: FAT16, FAT32, MSDOS, EXT2, EXT3, and EXT4. NTFS is not supported.
- Smart Access USB can be enabled or disabled using any of the BMC user interfaces. For example, you can use the Cisco IMC Configuration Utility that is accessed by pressing **F8** when prompted during bootup.
 - Enabled: the front-panel USB device is connected to the BMC.
 - Disabled: the front-panel USB device is connected to the host.
- In a case where no management network is available to connect remotely to Cisco IMC, a Device Firmware Update (DFU) shell over serial cable can be used to generate and download technical support files to the USB device that is attached to front panel USB port.



CHAPTER 3

Maintaining the Server

This chapter contains the following sections:

- [Status LEDs and Buttons, on page 25](#)
- [Preparing For Component Installation, on page 31](#)
- [Removing and Replacing Components, on page 35](#)
- [Serviceable Component Locations, on page 35](#)
- [Replacing SAS/SATA Drives in PCIe Risers and Vertical Drive Bays, on page 37](#)
- [Replacing NVMe SSDs, on page 40](#)
- [Replacing HHHL Form-Factor NVMe Solid State Drives, on page 43](#)
- [Replacing Fan Modules, on page 46](#)
- [Replacing CPUs and Heatsinks, on page 47](#)
- [Replacing Memory DIMMs, on page 61](#)
- [Replacing Intel Optane DC Persistent Memory Modules, on page 64](#)
- [Replacing a Micro SD Card, on page 68](#)
- [Replacing a USB Drive, on page 71](#)
- [Replacing the RTC Battery, on page 73](#)
- [Replacing Power Supplies, on page 74](#)
- [Replacing a PCIe Riser, on page 79](#)
- [Installing PCIe Risers 1C and 2E, on page 80](#)
- [Replacing a PCIe Card, on page 83](#)
- [Replacing a SAS Storage Controller Card \(RAID or HBA\), on page 90](#)
- [Replacing a Boot-Optimized M.2 RAID Controller Module, on page 93](#)
- [Replacing a Chassis Intrusion Switch, on page 96](#)
- [Installing a Trusted Platform Module \(TPM\), on page 98](#)
- [Service Headers and Jumpers, on page 102](#)
- [Recycling the PCB Assembly \(PCBA\), on page 109](#)

Status LEDs and Buttons

This section contains information for interpreting LED states.

Front-Panel LEDs

Figure 8: Front Panel LEDs

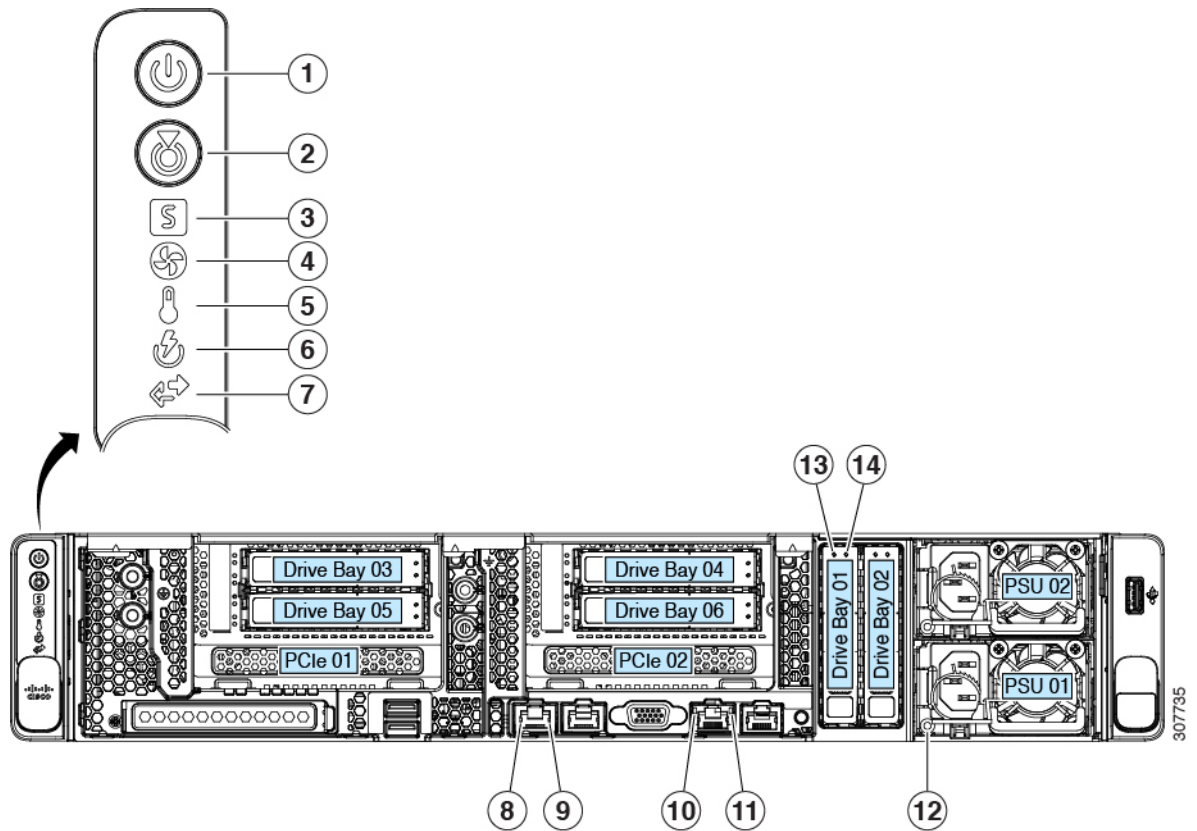


Table 2: Front Panel LEDs, Definition of States

LED Name	States
Power button/LED	<ul style="list-style-type: none"> Off—There is no AC power to the server. Amber—The server is in standby power mode. Power is supplied only to the Cisco IMC and some motherboard functions. Green—The server is in main power mode. Power is supplied to all server components.
Unit identification	<ul style="list-style-type: none"> Off—The unit identification function is not in use. Blue, blinking—The unit identification function is activated.

System health	<ul style="list-style-type: none"> • Green—The server is running in normal operating condition. • Green, blinking—The server is performing system initialization and memory check. • Amber, steady—The server is in a degraded operational state (minor fault). For example: <ul style="list-style-type: none"> • Power supply redundancy is lost. • CPUs are mismatched. • At least one CPU is faulty. • At least one DIMM is faulty. • At least one drive in a RAID configuration failed. • Amber, 2 blinks—There is a major fault with the system board. • Amber, 3 blinks—There is a major fault with the memory DIMMs. • Amber, 4 blinks—There is a major fault with the CPUs.
Fan status	<ul style="list-style-type: none"> • Green—All fan modules are operating properly. • Amber, blinking—One or more fan modules breached the non-recoverable threshold.
Temperature status	<ul style="list-style-type: none"> • Green—The server is operating at normal temperature. • Amber, steady—One or more temperature sensors breached the critical threshold. • Amber, blinking—One or more temperature sensors breached the non-recoverable threshold.
Power supply status	<ul style="list-style-type: none"> • Green—All power supplies are operating normally. • Amber, steady—One or more power supplies are in a degraded operational state. • Amber, blinking—One or more power supplies are in a critical fault state.
Network link activity	<ul style="list-style-type: none"> • Off—The Ethernet LOM port link is idle. • Green—One or more Ethernet LOM ports are link-active, but there is no activity. • Green, blinking—One or more Ethernet LOM ports are link-active, with activity.

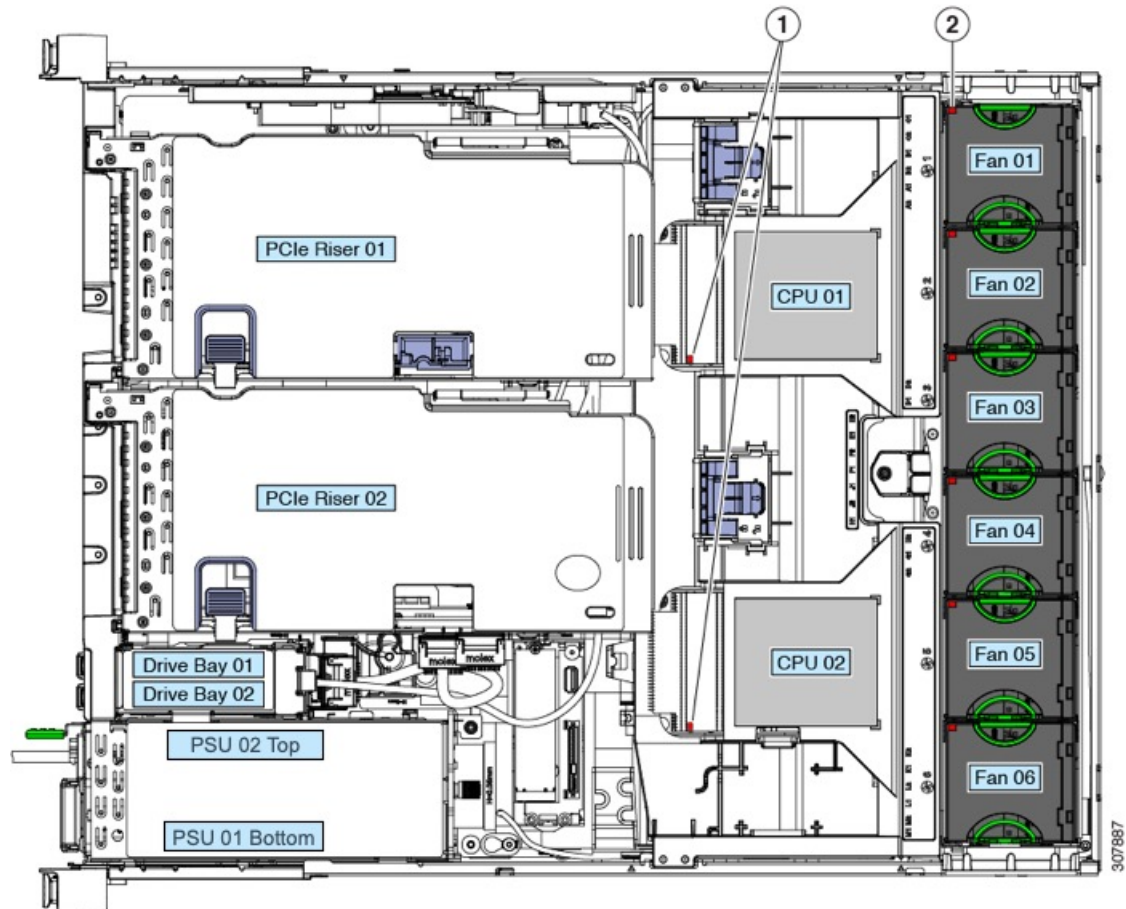
80-Gb Ethernet link speed (on both LAN1 and LAN2)	<ul style="list-style-type: none"> • Off—Link speed is 10 Mbps. • Amber—Link speed is 1 Gbps/100 Mbps. • Green—Link speed is 10 Gbps.
90-Gb Ethernet link status (on both LAN1 and LAN2)	<ul style="list-style-type: none"> • Off—No link is present. • Green—Link is active. • Green, blinking—Traffic is present on the active link.
01-Gb Ethernet dedicated management link speed	<ul style="list-style-type: none"> • Off—Link speed is 10 Mbps. • Amber—Link speed is 100 Mbps. • Green—Link speed is 1 Gbps.
11-Gb Ethernet dedicated management link status	<ul style="list-style-type: none"> • Off—No link is present. • Green—Link is active. • Green, blinking—Traffic is present on the active link.
2Power supply status (one LED each power supply unit)	<p>AC power supplies:</p> <ul style="list-style-type: none"> • Off—No AC input (12 V main power off, 12 V standby power off). • Green, blinking—12 V main power off, 12 V standby power on. • Green, solid—12 V main power on; 12 V standby power on. • Amber, blinking—Warning threshold detected but 12 V main power on. • Amber, solid—Critical error detected; 12 V main power off (for example, over-current, over-voltage, or over-temperature failure). <p>DC power supply (UCSC-PSUF-1050WDC):</p> <ul style="list-style-type: none"> • Off—No DC input (12 V main power off, 12 V standby power off). • Green, blinking—12 V main power off, 12 V standby power on. • Green, solid—12 V main power on; 12 V standby power on. • Amber, blinking—Warning threshold detected but 12 V main power on. • Amber, solid—Critical error detected; 12 V main power off (for example, over-current, over-voltage, or over-temperature failure).

<p>SAS/SATA drive fault</p> <p>Note NVMe solid state drive (SSD) drive tray LEDs have different behavior than SAS/SATA drive trays.</p>	<ul style="list-style-type: none"> • Off—The hard drive is operating properly. • Amber—Drive fault detected. • Amber, blinking—The device is rebuilding. • Amber, blinking with one-second interval—Drive locate function activated in the software.
<p>SAS/SATA drive activity LED</p>	<ul style="list-style-type: none"> • Off—There is no hard drive in the hard drive tray (no access, no fault). • Green—The hard drive is ready. • Green, blinking—The hard drive is reading or writing data.
<p>NVMe SSD drive fault</p> <p>Note NVMe solid state drive (SSD) drive tray LEDs have different behavior than SAS/SATA drive trays.</p>	<ul style="list-style-type: none"> • Off—The drive is not in use and can be safely removed. • Green—The drive is in use and functioning properly. • Green, blinking—the driver is initializing following insertion or the driver is unloading following an eject command. • Amber—The drive has failed. • Amber, blinking—A drive Locate command has been issued in the software.
<p>NVMe SSD activity</p>	<ul style="list-style-type: none"> • Off—No drive activity. • Green, blinking—There is drive activity.

Internal Diagnostic LEDs

The server has internal fault LEDs for CPUs, DIMMs, and fan modules.

Figure 9: Internal Diagnostic LED Locations



CPU fault LEDs (one behind each CPU socket on the motherboard).

These LEDs operate only when the server is in standby power mode.

- Amber—CPU has a fault.
- Off—CPU is OK.

Note Visible after removing the air baffle.

DIMM fault LEDs (one behind each DIMM socket on the motherboard)

These LEDs operate only when the server is in standby power mode.

- Amber—DIMM has a fault.
- Off—DIMM is OK.

Fan module fault LEDs (one on the top of each fan module)

- Amber—Fan has a fault or is not fully seated.
- Green—Fan is OK.

-

Preparing For Component Installation

This section includes information and tasks that help prepare the server for component installation.

Required Equipment For Service Procedures

The following tools and equipment are used to perform the procedures in this chapter:

- T-30 Torx driver (supplied with replacement CPUs for heatsink removal)
- #1 flat-head screwdriver (used during CPU or heatsink replacement)
- #1 Phillips-head screwdriver (for M.2 SSD and intrusion switch replacement)
- Electrostatic discharge (ESD) strap or other grounding equipment such as a grounded mat

Shutting Down and Removing Power From the Server

The server can run in either of two power modes:

- Main power mode—Power is supplied to all server components and any operating system on your drives can run.
- Standby power mode—Power is supplied only to the service processor and certain components. It is safe for the operating system and data to remove power cords from the server in this mode.

**Caution**

After a server is shut down to standby power, electric current is still present in the server. To completely remove power, you must disconnect all power cords from the power supplies in the server, as directed in the service procedures.

You can shut down the server by using the front-panel power button or the software management interfaces.

Shutting Down Using the Power Button

Step 1 Check the color of the Power button/LED:

- Amber—The server is already in standby mode and you can safely remove power.
- Green—The server is in main power mode and must be shut down before you can safely remove power.

Step 2 Invoke either a graceful shutdown or a hard shutdown:

Caution To avoid data loss or damage to your operating system, you should always invoke a graceful shutdown of the operating system.

- Graceful shutdown—Press and release the **Power** button. The operating system performs a graceful shutdown and the server goes to standby mode, which is indicated by an amber Power button/LED.

- Emergency shutdown—Press and hold the **Power** button for 4 seconds to force the main power off and immediately enter standby mode.

Step 3 If a service procedure instructs you to completely remove power from the server, disconnect all power cords from the power supplies in the server.

Shutting Down Using The Cisco IMC GUI

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

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

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

Step 3 In the Actions area, click **Power Off Server**.

Step 4 Click **OK**.

The operating system performs a graceful shutdown and the server goes to standby mode, which is indicated by an amber Power button/LED.

Step 5 If a service procedure instructs you to completely remove power from the server, disconnect all power cords from the power supplies in the server.

Shutting Down Using The Cisco IMC CLI

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

Step 1 At the server prompt, enter:

Example:

```
server# scope chassis
```

Step 2 At the chassis prompt, enter:

Example:

```
server/chassis# power shutdown
```

The operating system performs a graceful shutdown and the server goes to standby mode, which is indicated by an amber Power button/LED.

Step 3 If a service procedure instructs you to completely remove power from the server, disconnect all power cords from the power supplies in the server.

Shutting Down Using The Cisco UCS Manager Equipment Tab

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

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

Step 2 Expand **Equipment > Rack Mounts > Servers**.

Step 3 Choose the server that you want to shut down.

Step 4 In the Work pane, click the **General** tab.

Step 5 In the Actions area, click **Shutdown Server**.

Step 6 If a confirmation dialog displays, click **Yes**.

The operating system performs a graceful shutdown and the server goes to standby mode, which is indicated by an amber Power button/LED.

Step 7 If a service procedure instructs you to completely remove power from the server, disconnect all power cords from the power supplies in the server.

Shutting Down Using The Cisco UCS Manager Service Profile

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

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

Step 2 Expand **Servers > Service Profiles**.

Step 3 Expand the node for the organization that contains the service profile of the server that you are shutting down.

Step 4 Choose the service profile of the server that you are shutting down.

Step 5 In the **Work** pane, click the **General** tab.

Step 6 In the **Actions** area, click **Shutdown Server**.

Step 7 If a confirmation dialog displays, click **Yes**.

The operating system performs a graceful shutdown and the server goes to standby mode, which is indicated by an amber Power button/LED.

Step 8 If a service procedure instructs you to completely remove power from the server, disconnect all power cords from the power supplies in the server.

Removing the Server Top Cover



Caution

To maintain proper cooling, Cisco recommends not to operate the server for more than one minute without the top cover.

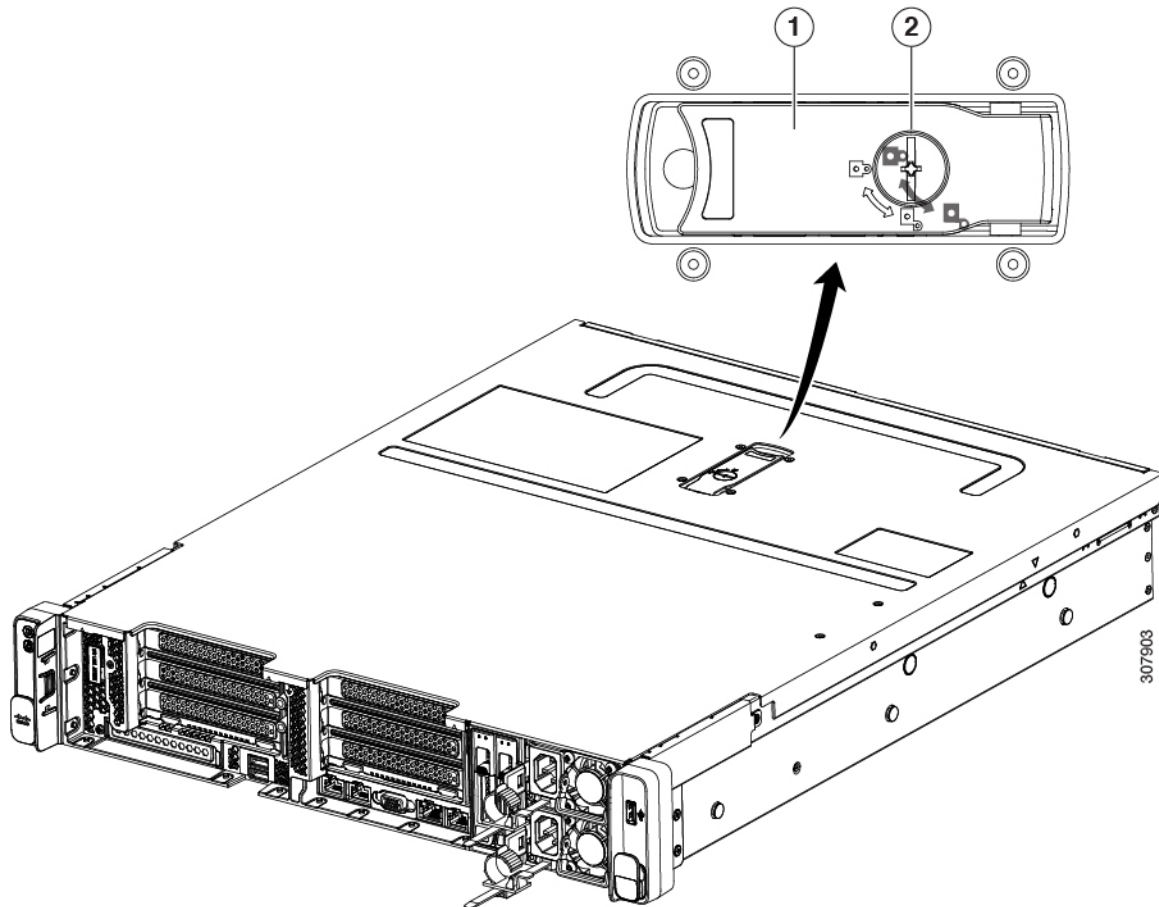
Step 1 Remove the top cover:

- a) If the cover latch is locked, use a screwdriver to turn the lock 90-degrees counterclockwise to unlock it.
- b) Lift on the end of the latch that has the green finger grip. The cover is pushed back to the open position as you lift the latch.
- c) Lift the top cover straight up from the server and set it aside.

Step 2 Replace the top cover:

- With the latch in the fully open position, place the cover on top of the server about one-half inch (1.27 cm) behind the lip of the front cover panel. The opening in the latch should fit over the peg that sticks up from the fan tray.
- Press the cover latch down to the closed position. The cover is pushed forward to the closed position as you push down the latch.
- If desired, lock the latch by using a screwdriver to turn the lock 90-degrees clockwise.

Figure 10: Removing the Top Cover



Cover latch	Serial number label location
Cover lock	

Serial Number Location

The serial number for the server is printed on a label on the top of the server, near the front. See [Removing the Server Top Cover, on page 33](#).

Hot Swap vs Hot Plug

Some components can be removed and replaced without shutting down and removing power from the server. This type of replacement has two varieties: hot-swap and hot-plug.

- Hot-swap replacement—You do not have to shut down the component in the software or operating system. This applies to the following components:
 - SAS/SATA hard drives
 - SAS/SATA solid state drives
 - Cooling fan modules
 - Power supplies (when redundant as 1+1)
- Hot-plug replacement—You must take the component offline before removing it for the following component:
 - NVMe PCIe solid state drives

Removing and Replacing Components



Warning

Blank faceplates and cover panels serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place.

Statement 1029



Caution

When handling server components, handle them only by carrier edges and use an electrostatic discharge (ESD) wrist-strap or other grounding device to avoid damage.



Tip

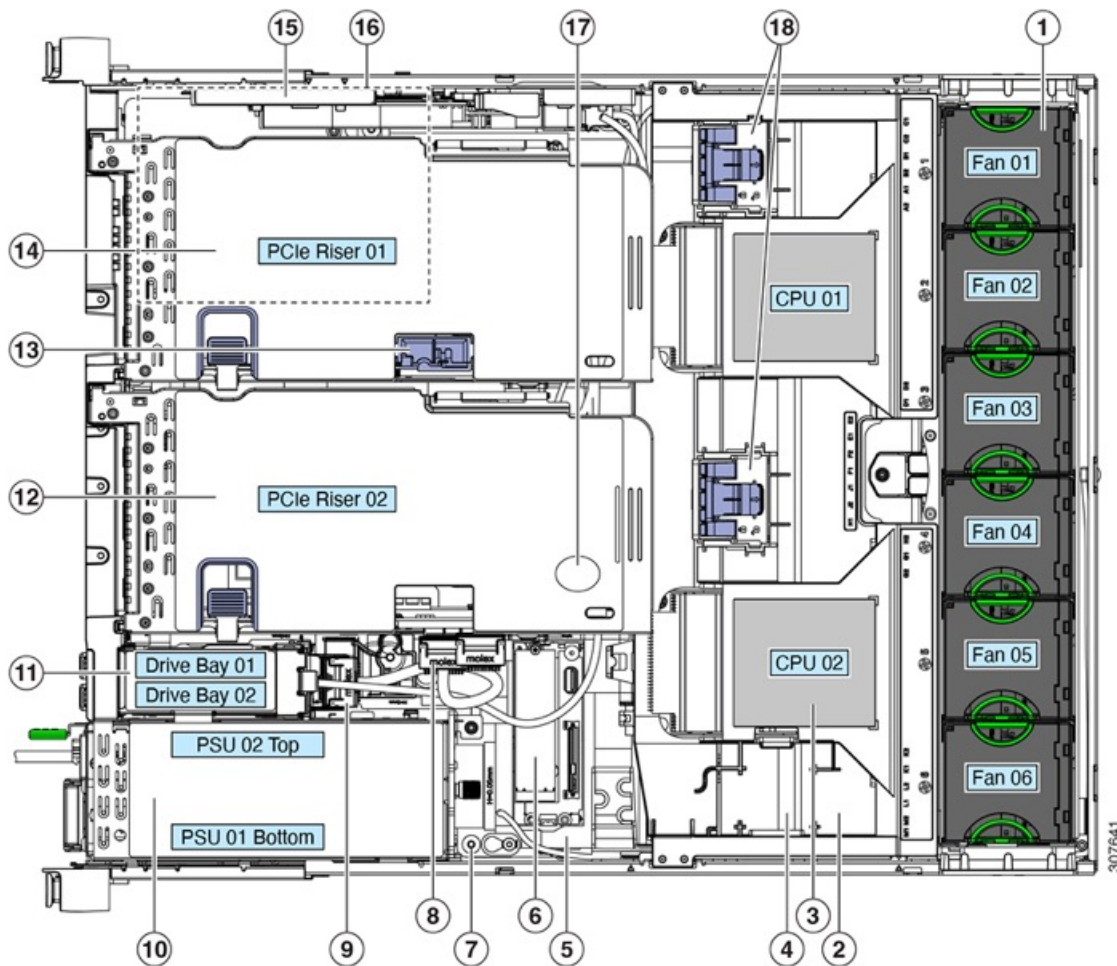
You can press the unit identification button on the front panel or rear panel to turn on a flashing, blue unit identification LED on both the front and rear panels of the server. This button allows you to locate the specific server that you are servicing when you go to the opposite side of the rack. You can also activate these LEDs remotely by using the Cisco IMC interface.

This section describes how to install and replace server components.

Serviceable Component Locations

This topic shows the locations of the field-replaceable components and service-related items. The view in the following figure shows the server with the top cover removed.

Figure 11: Cisco UCS C240 SD M5 Server, Serviceable Component Locations



<p>1 Cooling fan modules (six, hot-swappable)</p>	<p>11 Two 2.5-inch drive bays (Drive bays 01 and 02):</p> <ul style="list-style-type: none"> • Supports only SAS/SATA HDD/SSD with SAS-backplane • Supports only NVME SSDs with NVMe-backplane
<p>2 DIMM sockets on motherboard (up to 12 per CPU) Not visible under air baffle in this view. See DIMM Population Rules and Memory Performance Guidelines, on page 61 for DIMM slot numbering.</p>	<p>2 PCIe riser 2 with the following options (Drive bays 04 and 06, and PCIe 02):</p> <ul style="list-style-type: none"> • 2B—Slots 4 (x8), 5 (x16), 6 (x8); slot 3 requires CPU2. • 2E—Drive bay 04 (x4), Drive bay 06 (x4), PCIe 4 (x16); all slots supported by CPU2
<p>3 CPUs and heatsinks (up to two) Not visible under air baffle in this view.</p>	<p>3 Micro-SD socket on PCIe riser 01</p>

4 SuperCap power module mounting clip on air baffle (if applicable)	4 PCIe riser 1 with the following options (Drive bays 03 and 05, and PCIe 01): <ul style="list-style-type: none"> • 1—Slots 1 (x8), 2 (x16), 3 (x8); slot 3 requires CPU2. • 1C—Drive bay 03 (x4), Drive bay 05 (x4), PCIe 1 (x16); all slots supported by CPU1 See PCIe Slot Specifications , on page 83 for slot specifications.
5 Internal, vertical USB 3.0 port on motherboard	5 Storage controller dedicated slot
6 Mini-storage module socket. Options: <ul style="list-style-type: none"> • SD card module with two SD card slots • M.2 module with slots for two SATA M.2 drives 	6 OnLOM card socket on board
7 Chassis intrusion switch (optional)	7 RTC battery
8 PCIe cable connectors for NVMe SSDs.	8 Securing clips for GPU cards on air baffle
9 Vertical drive backplane assembly	
10 Power supplies (hot-swappable when redundant as 1+1)	

The Technical Specifications Sheets for all versions of this server, which include supported component part numbers, are at [Cisco UCS Servers Technical Specifications Sheets](#) (scroll down to *Technical Specifications*).

Replacing SAS/SATA Drives in PCIe Risers and Vertical Drive Bays



Note You do not have to shut down the server or drive to replace SAS/SATA hard drives or SSDs because they are hot-swappable.

SAS/SATA Drive Population Guidelines

Cisco UCS C240 SD M5 supports 2.5 inch SAS/SATA in the following combinations:

- PCIe Riser 1 and PCIe Riser 2B—This combination supports:
 - Two vertical drive bays with up to two 2.5-inch SAS/SATA drives
- PCIe Riser 1C and PCIe Riser 2E—This combination supports:
 - Four drive bays in the PCIe risers support 2.5-inch SAS/SATA drives
 - Two vertical drive bays support up to two 2.5-inch SAS/SATA drives

Observe these drive population guidelines for optimum performance:

- You can mix SAS/SATA hard drives and SAS/SATA SSDs in the same server. However, you cannot configure a logical volume (virtual drive) that contains a mix of hard drives and SSDs. That is, when you create a logical volume, it must contain all SAS/SATA hard drives or all SAS/SATA SSDs.

4K Sector Format SAS/SATA Drives Considerations

- You must boot 4K sector format drives in UEFI mode, not legacy mode. See the procedures in this section.
- Do not configure 4K sector format and 512-byte sector format drives as part of the same RAID volume.
- For operating system support on 4K sector drives, see the interoperability matrix tool for your server: [Hardware and Software Interoperability Matrix Tools](#)

Setting Up UEFI Mode Booting in the BIOS Setup Utility

- Step 1** Enter the BIOS setup utility by pressing the **F2** key when prompted during bootup.
- Step 2** Go to the **Boot Options** tab.
- Step 3** Set **UEFI Boot Options** to **Enabled**.
- Step 4** Under **Boot Option Priorities**, set your OS installation media (such as a virtual DVD) as your **Boot Option #1**.
- Step 5** Go to the **Advanced** tab.
- Step 6** Select **LOM** and **PCIe Slot Configuration**.
- Step 7** Set the **PCIe Slot ID: HBA Option ROM** to **UEFI Only**.
- Step 8** Press **F10** to save changes and exit the BIOS setup utility. Allow the server to reboot.
- Step 9** After the OS installs, verify the installation:
- a) Enter the BIOS setup utility by pressing the **F2** key when prompted during bootup.
 - b) Go to the **Boot Options** tab.
 - c) Under **Boot Option Priorities**, verify that the OS you installed is listed as your **Boot Option #1**.
-

Setting Up UEFI Mode Booting in the Cisco IMC GUI

- Step 1** Use a web browser and the IP address of the server to log into the Cisco IMC GUI management interface.
- Step 2** Navigate to **Server > BIOS**.
- Step 3** Under **Actions**, click **Configure BIOS**.
- Step 4** In the **Configure BIOS Parameters** dialog, select the **Advanced** tab.
- Step 5** Go to the **LOM** and **PCIe Slot Configuration** section.
- Step 6** Set the **PCIe Slot: HBA Option ROM** to **UEFI Only**.
- Step 7** Click **Save Changes**. The dialog closes.
- Step 8** Under **BIOS Properties**, set **Configured Boot Order** to **UEFI**.
- Step 9** Under **Actions**, click **Configure Boot Order**.

- Step 10** In the Configure Boot Order dialog, click **Add Local HDD**.
- Step 11** In the Add Local HDD dialog, enter the information for the 4K sector format drive and make it first in the boot order.
- Step 12** Save changes and reboot the server. The changes you made will be visible after the system reboots.
-

Replacing a SAS/SATA Drive

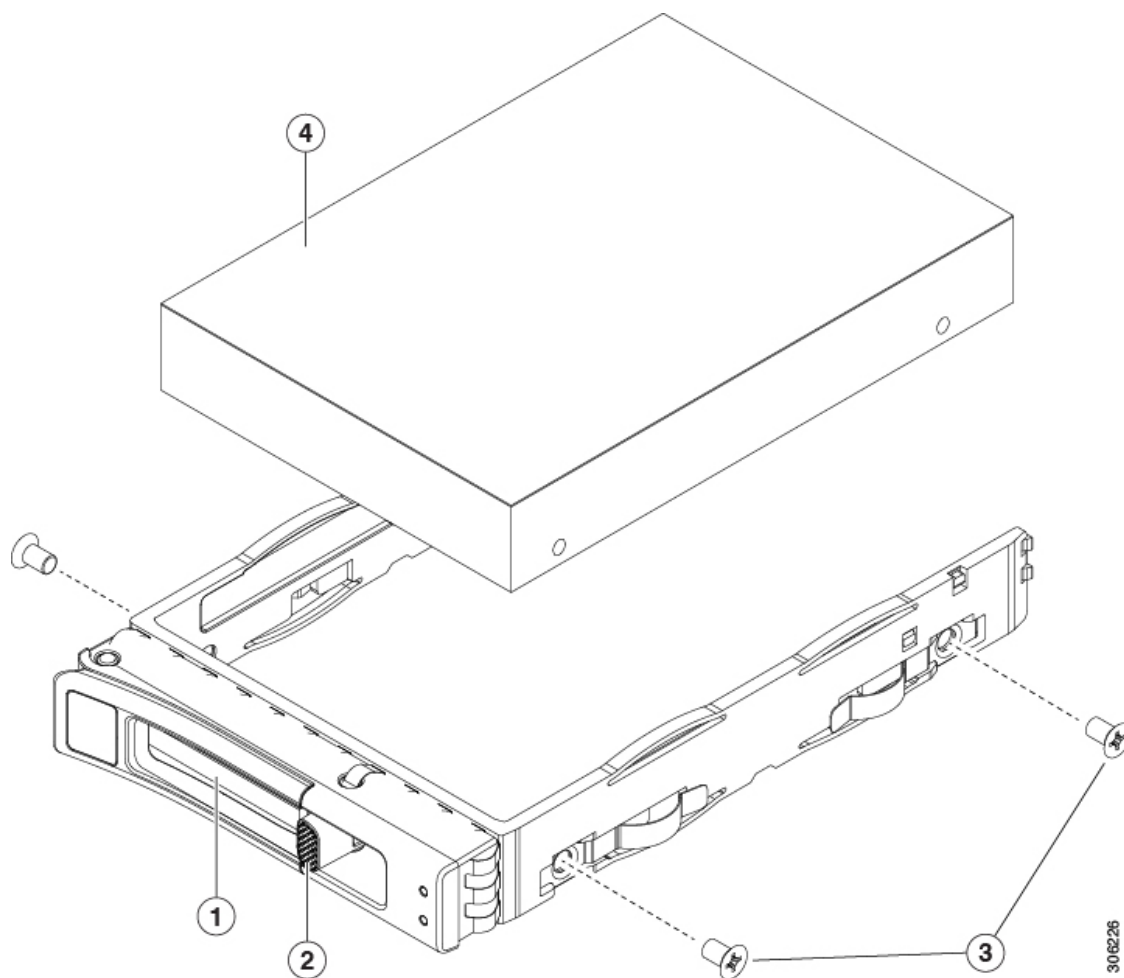


Note You do not have to shut down the server or drive to replace SAS/SATA hard drives or SSDs because they are hot-swappable.

Follow this procedure to remove a SAS/SATA drive from a PCIe Riser or from a vertical drive bay.

- Step 1** Remove the drive that you are replacing or remove a blank drive tray from the front of the server:
- Press the release button on the face of the drive tray.
 - Grasp and open the ejector lever and then pull the drive tray out of the slot.
 - If you are replacing an existing drive, remove the four drive-tray screws that secure the drive to the tray and then lift the drive out of the tray.
- Step 2** Install a new drive:
- Place a new drive in the empty drive tray and install the four drive-tray screws.
 - With the ejector lever on the drive tray open, insert the drive tray into the empty drive bay.
 - Push the tray into the slot until it touches the backplane, and then close the ejector lever to lock the drive in place.

Figure 12: Replacing a Drive in a Drive Tray



Ejector lever	Drive tray screws (two on each side)
Release button	Drive removed from drive tray

Replacing NVMe SSDs

This section is for replacing 2.5-inch form-factor NVMe solid-state drives (SSDs) in vertical drive bays.

To replace HHHL form-factor NVMe SSDs in the PCIe slots, see [Replacing HHHL Form-Factor NVMe Solid State Drives](#), on page 43.

Front-Loading NVMe SSD Population Guidelines

Cisco UCS C240 SD M5 supports 2.5 inch NVMe SSDs in the following combinations:

- PCIe Riser 1 and PCIe Riser 2B—This combination supports:
 - Two vertical drive bays with up to two 2.5-inch NVMe SSDs.
- PCIe Riser 1C and PCIe Riser 2E—This combination supports:
 - Four drive bays in the PCIe risers support up to two 2.5-inch NVMe
 - Two vertical drive bays support up to two 2.5-inch NVMe

NVMe SSD Requirements and Restrictions

Observe these requirements:

- Hot-plug support must be enabled in the system BIOS. If you ordered the system with NVMe drives, hot-plug support is enabled at the factory.

Observe these restrictions:

- NVMe 2.5 inch SSDs support booting only in UEFI mode. Legacy boot is not supported. For instructions on setting up UEFI boot, see [Setting Up UEFI Mode Booting in the BIOS Setup Utility, on page 38](#) or [Setting Up UEFI Mode Booting in the Cisco IMC GUI, on page 38](#).
- You cannot control NVMe PCIe SSDs with a SAS RAID controller because NVMe SSDs interface with the server via the PCIe bus.
- You can combine NVMe 2.5 inch SSDs and HHHL form-factor SSDs in the same system, but the same partner brand must be used. For example, two *Intel* NVMe SFF 2.5-inch SSDs and two *HGST* HHHL form-factor SSDs is an invalid configuration. A valid configuration is two HGST NVMe SFF 2.5-inch SSDs and two HGST HHHL form-factor SSDs.
- UEFI boot is supported in all supported operating systems. Hot-insertion and hot-removal are supported in all supported operating systems except VMWare ESXi.

Enabling Hot-Plug Support in the System BIOS

Hot-plug (OS-informed hot-insertion and hot-removal) is disabled in the system BIOS by default.

- If the system was ordered with NVMe PCIe SSDs, the setting was enabled at the factory. No action is required.
- If you are adding NVMe PCIe SSDs after-factory, you must enable hot-plug support in the BIOS. See the following procedures.

Enabling Hot-Plug Support Using the BIOS Setup Utility

-
- | | |
|---------------|--|
| Step 1 | Enter the BIOS setup utility by pressing the F2 key when prompted during bootup. |
| Step 2 | Navigate to Advanced > PCI Subsystem Settings > NVMe SSD Hot-Plug Support . |
| Step 3 | Set the value to Enabled . |

Step 4 Save your changes and exit the utility.

Enabling Hot-Plug Support Using the Cisco IMC GUI

- Step 1** Use a browser to log in to the Cisco IMC GUI for the server.
- Step 2** Navigate to **Compute > BIOS > Advanced > PCI Configuration**.
- Step 3** Set NVME SSD Hot-Plug Support to **Enabled**.
- Step 4** Save your changes.
-

Replacing a NVMe SSD

This topic describes how to replace 2.5 inch form-factor NVMe SSDs in the PCIe Risers or the vertical drive bays.



Note OS-surprise removal is not supported. OS-informed hot-insertion and hot-removal are supported on all supported operating systems except VMware ESXi.



Note OS-informed hot-insertion and hot-removal must be enabled in the system BIOS. See [Enabling Hot-Plug Support in the System BIOS, on page 41](#).

Step 1 Remove an existing NVMe SSD:

- a) Shut down the NVMe SSD to initiate an OS-informed removal. Use your operating system interface to shut down the drive, and then observe the drive-tray LED:
 - Green—The drive is in use and functioning properly. Do not remove.
 - Green, blinking—the driver is unloading following a shutdown command. Do not remove.
 - Off—The drive is not in use and can be safely removed.
- b) Press the release button on the face of the drive tray.
- c) Grasp and open the ejector lever and then pull the drive tray out of the slot.
- d) Remove the four drive tray screws that secure the SSD to the tray and then lift the SSD out of the tray.

Note If this is the first time that NVMe SSDs are being installed in the server, you must install a PCIe cable with PCIe riser. See [Installing PCIe Risers 1C and 2E, on page 80](#).

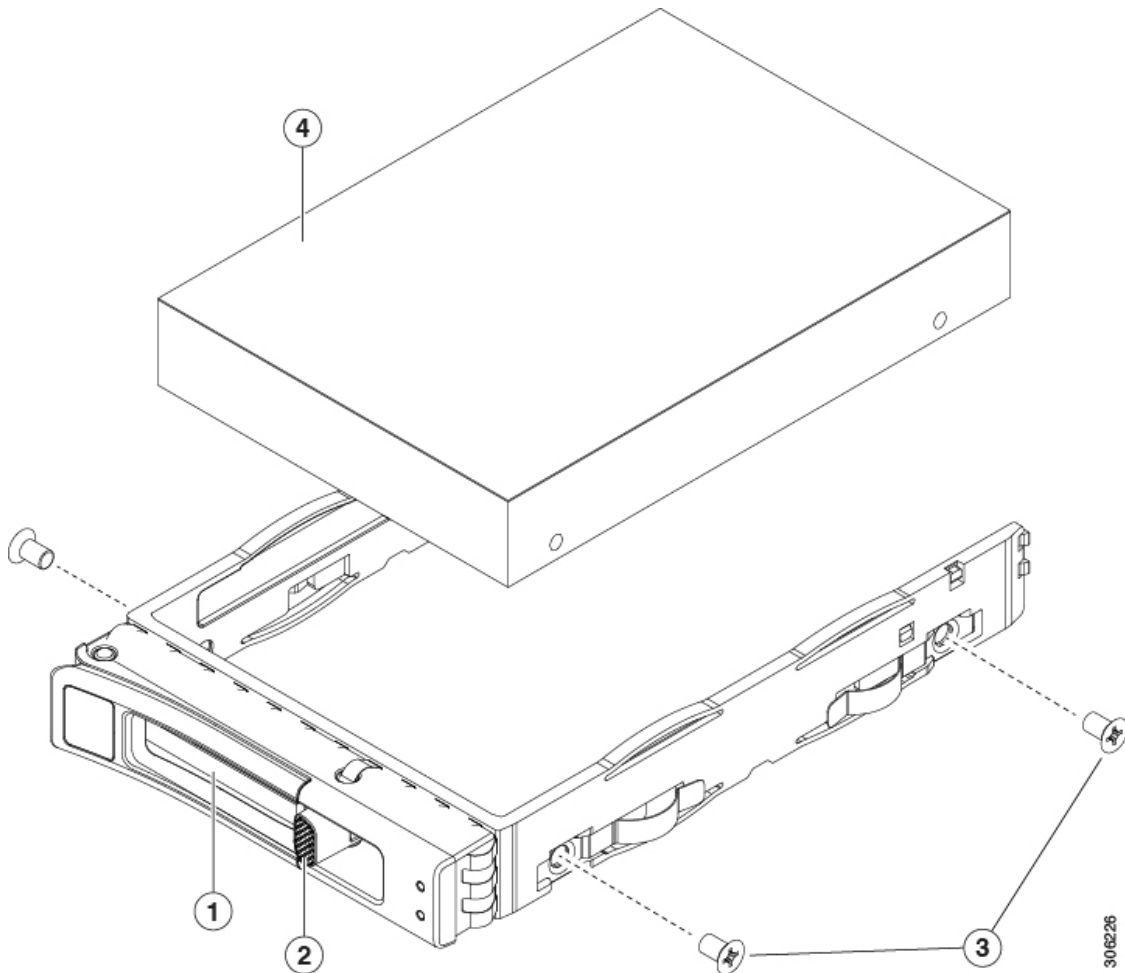
Step 2 Install a new NVMe SSD:

- a) Place a new SSD in the empty drive tray and install the four drive-tray screws.
- b) With the ejector lever on the drive tray open, insert the drive tray into the empty drive bay.
- c) Push the tray into the slot until it touches the backplane, and then close the ejector lever to lock the drive in place.

Step 3 Observe the drive-tray LED and wait until it returns to solid green before accessing the drive:

- Off—The drive is not in use.
- Green, blinking—the driver is initializing following hot-plug insertion.
- Green—The drive is in use and functioning properly.

Figure 13: Replacing a Drive in a Drive Tray



Ejector lever	Drive tray screws (two on each side)
Release button	Drive removed from drive tray

Replacing HHHL Form-Factor NVMe Solid State Drives

This section is for replacing half-height, half-length (HHHL) form-factor NVMe SSDs in the PCIe risers.

HHHL SSD Population Guidelines

Observe the following population guidelines when installing HHHL form-factor NVMe SSDs:

- Two-CPU systems—You can populate up to 6 HHHL form-factor SSDs, using PCIe slots 1 – 6.
- One-CPU systems—In a single-CPU system, PCIe riser 2 is not available. Therefore, the maximum number of HHHL form-factor SSDs you can populate is 3, using PCIe slots 1 - 3.

HHHL Form-Factor NVMe SSD Requirements and Restrictions

Observe these requirements:

- All versions of the server support HHHL form-factor NVMe SSDs.

Observe these restrictions:

- You cannot boot from an HHHL form-factor NVMe SSD.
- You cannot control HHHL NVMe SSDs with a SAS RAID controller because NVMe SSDs interface with the server via the PCIe bus.
- You can combine NVMe SFF 2.5- or 3.5-inch SSDs and HHHL form-factor SSDs in the same system, but the same partner brand must be used. For example, two *Intel* NVMe SFF 2.5-inch SSDs and two *HGST* HHHL form-factor SSDs is an invalid configuration. A valid configuration is two HGST NVMe SFF 2.5-inch SSDs and two HGST HHHL form-factor SSDs.

Replacing an HHHL Form-Factor NVMe SSD



Note In a single-CPU server, PCIe riser 2 (PCIe slot 2) is not available.

Step 1

Remove an existing HHHL form-factor NVMe SSD (or a blank filler panel) from the PCIe riser:

- Shut down and remove power from the server as described in [Shutting Down and Removing Power From the Server, on page 31](#).
- Slide the server out the front of the rack far enough so that you can remove the top cover. You might have to detach cables from the rear panel to provide clearance.

Caution If you cannot safely view and access the component, remove the server from the rack.

- Remove the top cover from the server as described in [Removing the Server Top Cover, on page 33](#).
- Use two hands to flip up and grasp the blue riser handle and the blue fingergrasp area on the front edge of the riser, and then lift straight up.
- On the bottom of the riser, push the release latch that holds the securing plate, and then swing the hinged securing plate open.
- Open the hinged card-tab retainer that secures the rear-panel tab of the card.
- Pull evenly on both ends of the HHHL form-factor NVMe SSD to remove it from the socket on the PCIe riser.

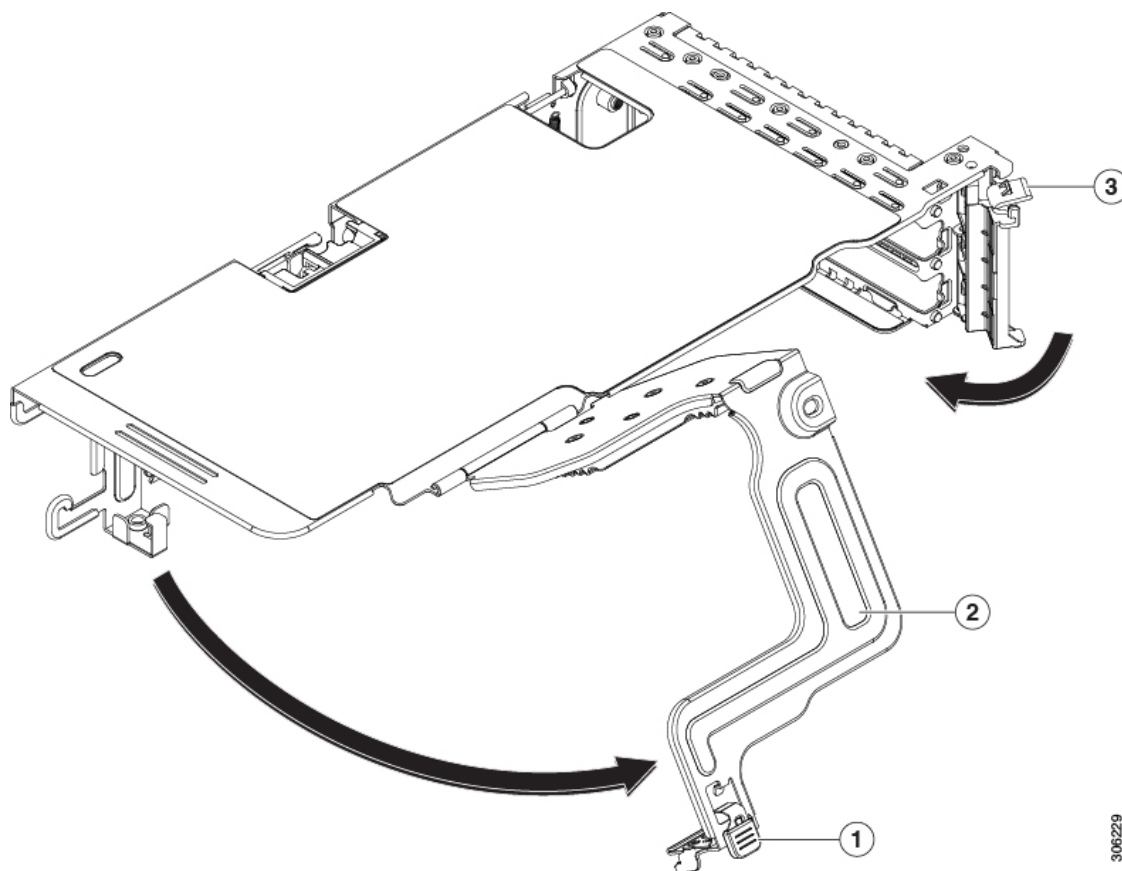
If the riser has no SSD, remove the blanking panel from the rear opening of the riser.

Step 2

Install a new HHHL form-factor NVMe SSD:

- a) Open the hinged, plastic card-tab retainer.
- b) Align the new SSD with the empty socket on the PCIe riser.
- c) Push down evenly on both ends of the card until it is fully seated in the socket.
- d) Ensure that the SSD's rear panel tab sits flat against the riser rear-panel opening and then close the hinged card-tab retainer over the rear-panel tab.
- e) Close the hinged securing plate.
- f) Position the PCIe riser over its socket on the motherboard and over the chassis alignment channels.
- g) Carefully push down on both ends of the PCIe riser to fully engage its connector with the sockets on the motherboard.
- h) Replace the top cover to the server.
- i) Replace the server in the rack, replace cables, and then fully power on the server by pressing the Power button.

Figure 14: PCIe Riser Card Securing Mechanisms



Release latch on hinged securing plate	Hinged card-tab retainer
Hinged securing plate	-

Replacing Fan Modules

The six fan modules in the server are numbered as shown in [Serviceable Component Locations, on page 3](#).

**Tip**

There is a fault LED on the top of each fan module. This LED lights green when the fan is correctly seated and is operating OK. The LED lights amber when the fan has a fault or is not correctly seated.

**Caution**

You do not have to shut down or remove power from the server to replace fan modules because they are hot-swappable. However, to maintain proper cooling, do not operate the server for more than one minute with any fan module removed.

Step 1

Remove an existing fan module:

- a) Slide the server out the front of the rack far enough so that you can remove the top cover. You might have to detach cables from the rear panel to provide clearance.

Caution

If you cannot safely view and access the component, remove the server from the rack.

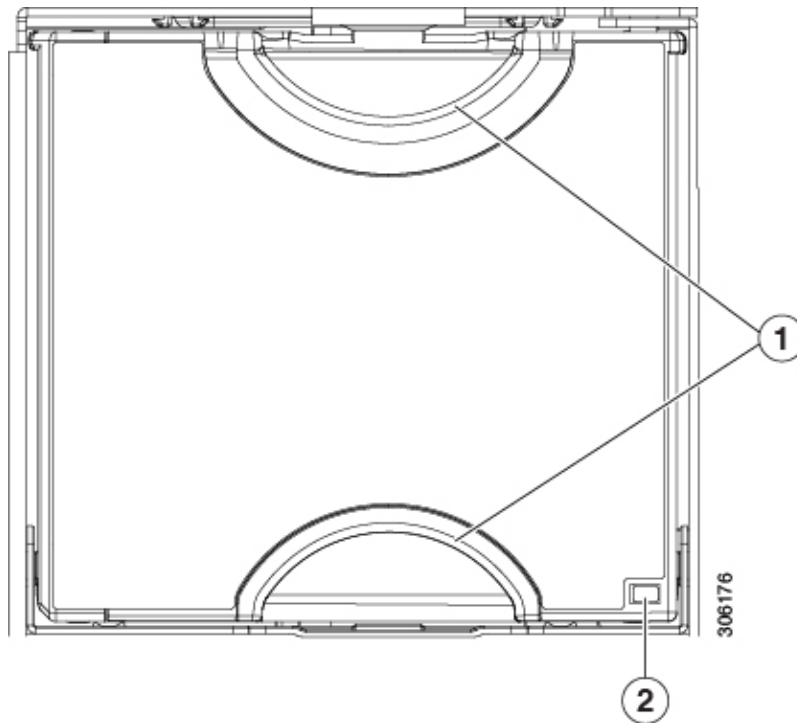
- b) Remove the top cover from the server as described in [Removing the Server Top Cover, on page 33](#).
- c) Grasp and squeeze the fan module release latches on its top. Lift straight up to disengage its connector from the motherboard.

Step 2

Install a new fan module:

- a) Set the new fan module in place. The arrow printed on the top of the fan module should point toward the rear of the server.
- b) Press down gently on the fan module to fully engage it with the connector on the motherboard.
- c) Replace the top cover to the server.
- d) Replace the server in the rack, replace cables, and then fully power on the server by pressing the Power button.

Figure 15: Top View of Fan Module



Fan module release latches

Fan module fault LED

Replacing CPUs and Heatsinks

This section contains the following topics:

- [CPU Configuration Rules, on page 48](#)
- [Tools Required For CPU Replacement, on page 49](#)
- [Replacing a CPU and Heatsink, on page 49](#)
- [Additional CPU-Related Parts to Order with RMA Replacement CPUs, on page 55](#)

Special Information For *Upgrades* to Second Generation Intel Xeon Scalable Processors



Caution

You must upgrade your server firmware to the required minimum level before you upgrade to the Second Generation Intel Xeon Scalable processors that are supported in this server. Older firmware versions cannot recognize the new CPUs and this would result in a non-bootable server.

The minimum software and firmware versions required for this server to support Second Generation Intel Xeon Scalable processors are as follows:

Table 3: Minimum Requirements For Second Generation Intel Xeon Scalable processors

Software or Firmware	Minimum Version
Server Cisco IMC	4.0(4)
Server BIOS	4.0(4)

CPU Configuration Rules

This server has two CPU sockets on the motherboard. Each CPU supports six DIMM channels (12 DIMM slots). See [DIMM Population Rules and Memory Performance Guidelines](#), on page 61.

- The server can operate with one CPU or two identical CPUs installed.
- The minimum configuration is that the server must have at least CPU 1 installed. Install CPU 1 first, and then CPU 2.
- **For Intel Xeon Scalable processors (first generation):** The maximum combined memory allowed in the 12 DIMM slots controlled by any one CPU is 768 GB. To populate the 12 DIMM slots with more than 768 GB of combined memory, you must use a high-memory CPU that has a PID that ends with an "M", for example, UCS-CPU-6134M.
- **For Second Generation Intel Xeon Scalable processors:** These Second Generation CPUs have three memory tiers. These rules apply on a *per-socket* basis:
 - If the CPU socket has up to 1 TB of memory installed, a CPU with no suffix can be used (for example, Gold 6240).
 - If the CPU socket has 1 TB or more (up to 2 TB) of memory installed, you must use a CPU with an M suffix (for example, Platinum 8276M).
 - If the CPU socket has 2 TB or more (up to 4.5 TB) of memory installed, you must use a CPU with an L suffix (for example, Platinum 8270L).
- The following restrictions apply when using a single-CPU configuration:
 - Any unused CPU socket must have the socket dust cover from the factory in place.
 - The maximum number of DIMMs is 12 (only CPU 1 channels A, B, C, D, E, F).
 - PCIe riser 2 (slots 4, 5, 6) is unavailable.
 - You must use PCIe riser 1 (UCSC-RSI-1-240M5) to have support for all three slots (PCIe 1, 2, 3). In PCIe riser 1C (UCSC-RS1C-240M5SD), slot 3 is unavailable because it is controlled by CPU 2.
 - Front loading NVMe drives are unavailable (they require PCIe rise 2E or 1C).
- The following NVIDIA GPUs are not supported with Second Generation Intel Xeon Scalable processors:
 - NVIDIA Tesla P4
 - NVIDIA Tesla P100 12G

- NVIDIA Tesla P100 16G

Tools Required For CPU Replacement

You need the following tools and equipment for this procedure:

- T-30 Torx driver—Supplied with replacement CPU.
- #1 flat-head screwdriver—Supplied with replacement CPU.
- CPU assembly tool—Supplied with replacement CPU. Orderable separately as Cisco PID UCS-CPUAT=.
- Heatsink cleaning kit—Supplied with replacement CPU. Orderable separately as Cisco PID UCSX-HSCK=.

One cleaning kit can clean up to four CPUs.

- Thermal interface material (TIM)—Syringe supplied with replacement CPU. Use only if you are reusing your existing heatsink (new heatsinks have a pre-applied pad of TIM). Orderable separately as Cisco PID UCS-CPU-TIM=.

One TIM kit covers one CPU.

See also [Additional CPU-Related Parts to Order with RMA Replacement CPUs, on page 55](#).

Replacing a CPU and Heatsink

**Caution**

CPUs and their sockets are fragile and must be handled with extreme care to avoid damaging pins. The CPUs must be installed with heatsinks and thermal interface material to ensure cooling. Failure to install a CPU correctly might result in damage to the server.

An instructive video is available for this procedure: [CPU and Heatsink Replacement in Cisco UCS M5 Servers](#)

Step 1

Remove the existing CPU/heatsink assembly from the server:

- a) Shut down and remove power from the server as described in [Shutting Down and Removing Power From the Server, on page 31](#).
- b) Slide the server out the front of the rack far enough so that you can remove the top cover. You might have to detach cables from the rear panel to provide clearance.

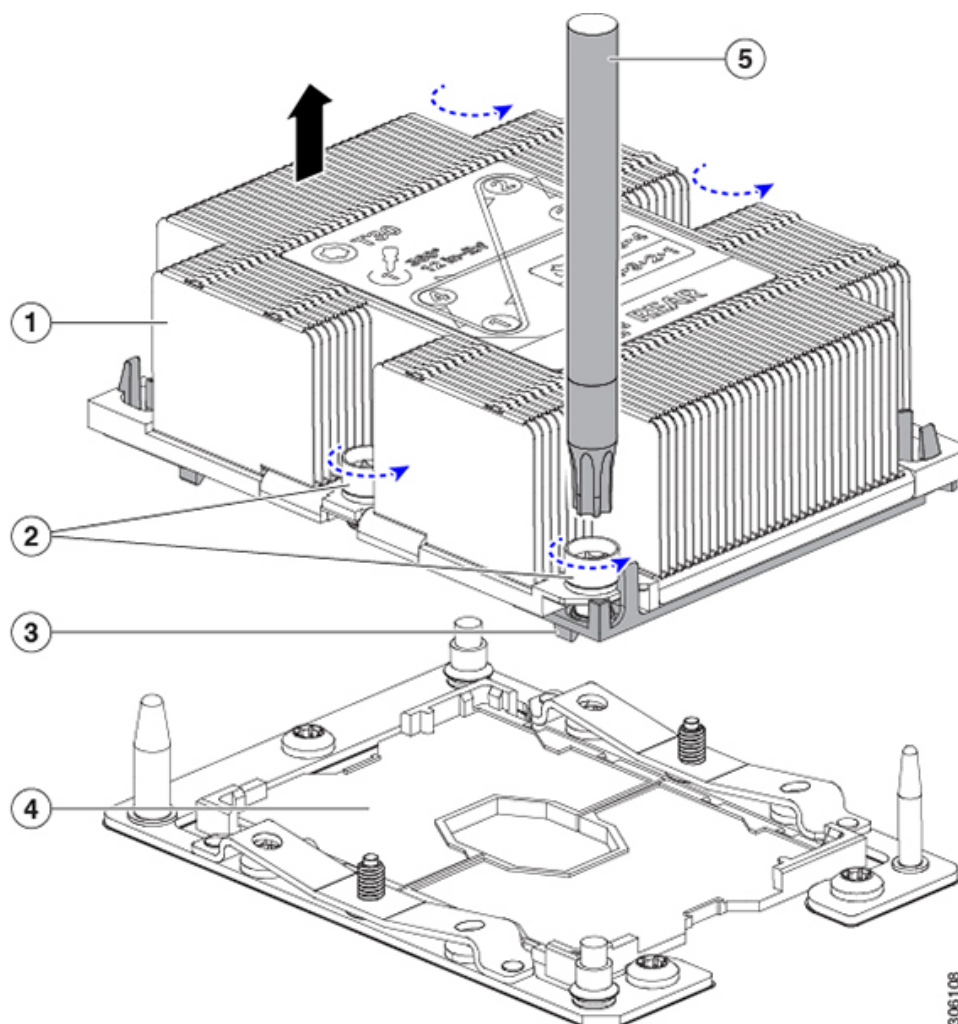
Caution If you cannot safely view and access the component, remove the server from the rack.

- c) Remove the top cover from the server as described in [Removing the Server Top Cover, on page 33](#).
- d) Use the T-30 Torx driver that is supplied with the replacement CPU to loosen the four captive nuts that secure the assembly to the motherboard standoffs.

Note Alternate loosening the heatsink nuts evenly so that the heatsink remains level as it is raised. Loosen the heatsink nuts in the order shown on the heatsink label: 4, 3, 2, 1.

- e) Lift straight up on the CPU/heatsink assembly and set it heatsink-down on an antistatic surface.

Figure 16: Removing the CPU/Heatsink Assembly



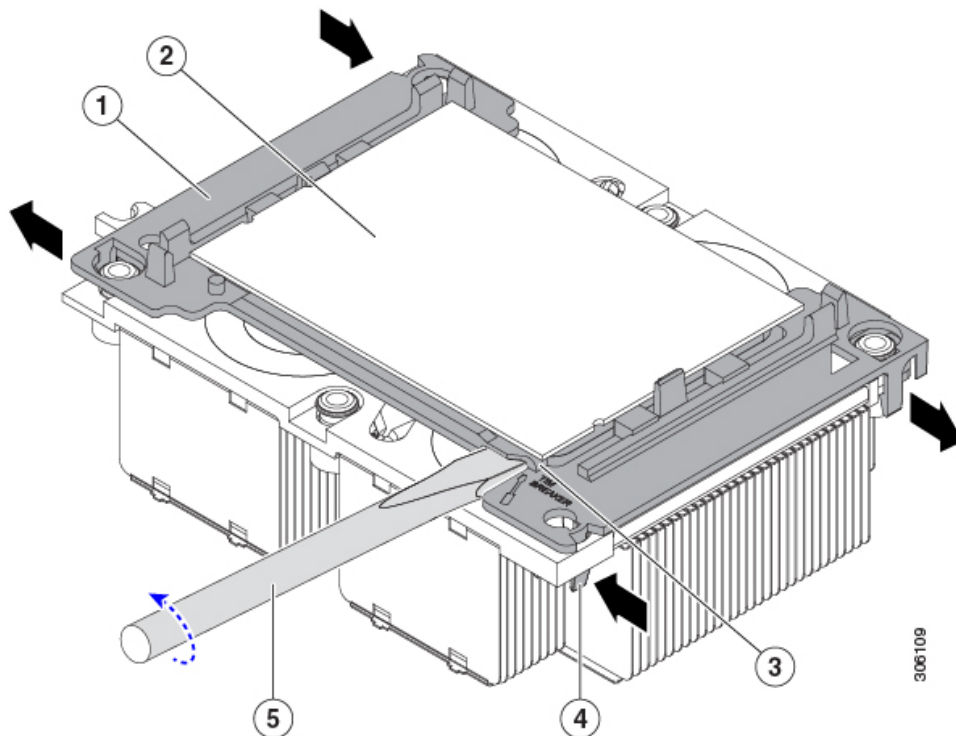
1 Heatsink	4 CPU socket on motherboard
2 Heatsink captive nuts (two on each side)	5 T-30 Torx driver
3 CPU carrier (below heatsink in this view)	-

Step 2 Separate the heatsink from the CPU assembly (the CPU assembly includes the CPU and the plastic CPU carrier):

- a) Place the heatsink with CPU assembly so that it is oriented upside-down.

Note the thermal-interface material (TIM) breaker location. TIM BREAKER is stamped on the CPU carrier next to a small slot.

Figure 17: Separating the CPU Assembly From the Heatsink



1 CPU carrier	4 CPU-carrier inner-latch nearest to the TIM breaker slot
2 CPU	5 #1 flat-head screwdriver inserted into TIM breaker slot
3 TIM BREAKER slot in CPU carrier	-

- b) Pinch inward on the CPU-carrier clip that is nearest the TIM breaker slot and then push up to disengage the clip from its slot in the heatsink corner.
- c) Insert the blade of a #1 flat-head screwdriver into the slot marked TIM BREAKER.

Note In the following step, do not pry on the CPU surface. Use gentle rotation to lift on the plastic surface of the CPU carrier at the TIM breaker slot. Use caution to avoid damaging the heatsink surface.

- d) Gently rotate the screwdriver to lift up on the CPU until the TIM on the heatsink separates from the CPU.

Note Do not allow the screwdriver tip to touch or damage the green CPU substrate.

- e) Pinch the CPU-carrier clip at the corner opposite the TIM breaker and push up to disengage the clip from its slot in the heatsink corner.
- f) On the remaining two corners of the CPU carrier, gently pry outward on the outer-latches and then lift the CPU-assembly from the heatsink.

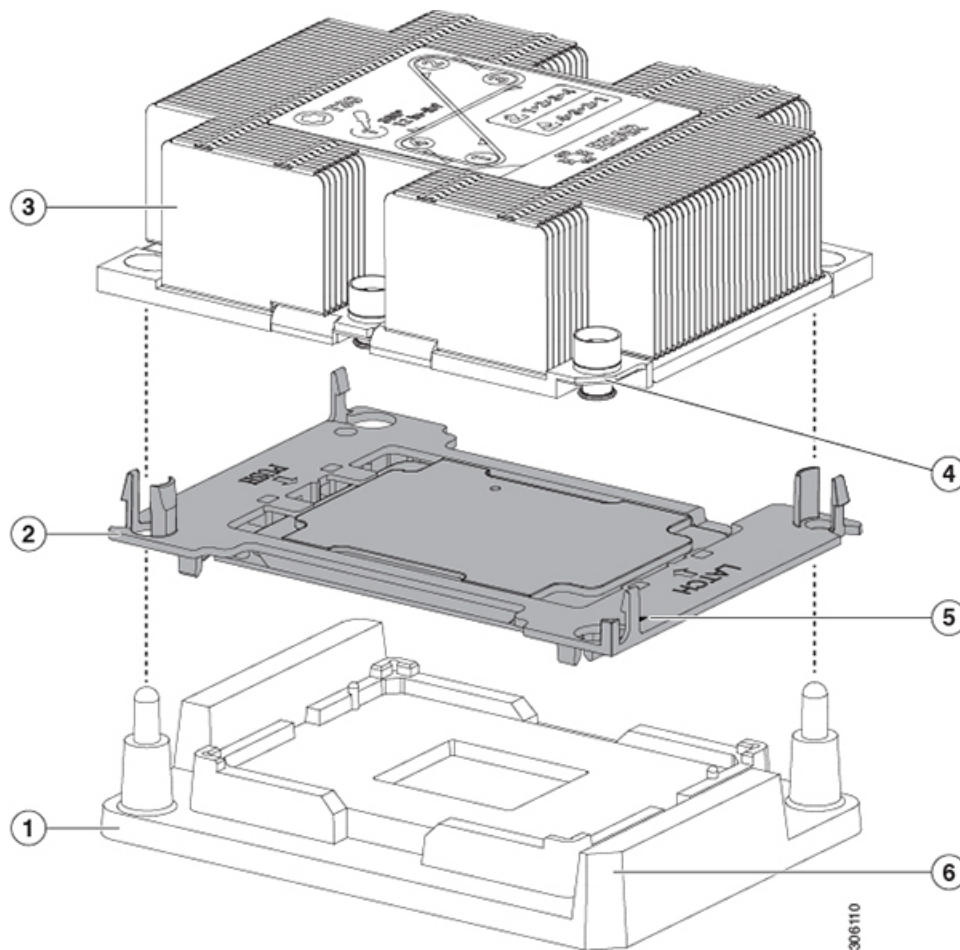
Note Handle the CPU-assembly by the plastic carrier only. Do not touch the CPU surface. Do not separate the CPU from the plastic carrier.

Step 3 The new CPU assembly is shipped on a CPU assembly tool. Take the new CPU assembly and CPU assembly tool out of the carton.

If the CPU assembly and CPU assembly tool become separated, note the alignment features for correct orientation. The pin 1 triangle on the CPU carrier must be aligned with the angled corner on the CPU assembly tool.

Caution CPUs and their sockets are fragile and must be handled with extreme care to avoid damaging pins.

Figure 18: CPU Assembly Tool, CPU Assembly, and Heatsink Alignment Features



1 CPU assembly tool	4 Angled corner on heatsink (pin 1 alignment feature)
2 CPU assembly (CPU in plastic carrier frame)	5 Triangle cut into plastic carrier (pin 1 alignment feature)
3 Heatsink	6 Angled corner on CPU assembly tool (pin 1 alignment feature)

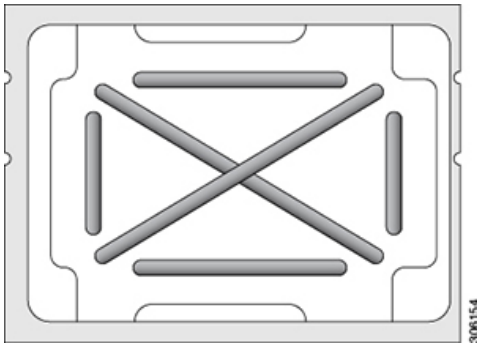
Step 4 Apply new TIM to the heatsink:

Note The heatsink must have new TIM on the heatsink-to-CPU surface to ensure proper cooling and performance.

- If you are installing a new heatsink, it is shipped with a pre-applied pad of TIM. Go to step 5.

- If you are reusing a heatsink, you must remove the old TIM from the heatsink and then apply new TIM to the CPU surface from the supplied syringe. Continue with step **a** below.
- a) Apply the cleaning solution that is included with the heatsink cleaning kit (UCSX-HSCK=) to the old TIM on the heatsink and let it soak for a least 15 seconds.
- b) Wipe all of the TIM off the heatsink using the soft cloth that is included with the heatsink cleaning kit. Be careful to avoid scratching the heatsink surface.
- c) Using the syringe of TIM provided with the new CPU (UCS-CPU-TIM=), apply 4 cubic centimeters of thermal interface material to the top of the CPU. Use the pattern shown below to ensure even coverage.

Figure 19: Thermal Interface Material Application Pattern



- Step 5** **Note** Use only the correct heatsink for your CPUs to ensure proper cooling. There are two different heatsinks: UCSC-HS-C240M5 for standard-performance CPUs 150 W and less; UCSC-HS2-C240M5 for high-performance CPUs above 150 W. Note the wattage described on the heatsink label.

With the CPU assembly on the CPU assembly tool, set the heatsink onto the CPU assembly. Note the Pin 1 alignment features for correct orientation. Push down gently until you hear the corner clips of the CPU carrier click onto the heatsink corners.

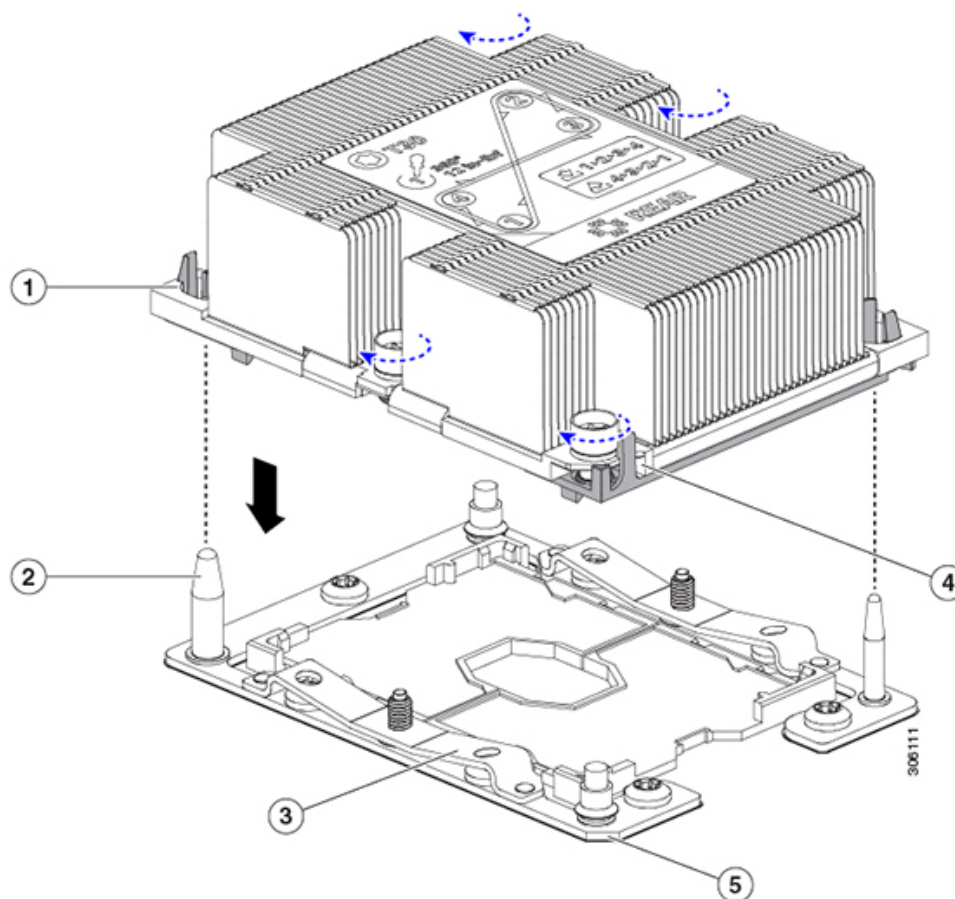
- Caution** In the following step, use extreme care to avoid touching or damaging the CPU contacts or the CPU socket pins.

- Step 6** Install the CPU/heatsink assembly to the server:

- a) Lift the heatsink with attached CPU assembly from the CPU assembly tool.
- b) Align the assembly over the CPU socket on the motherboard.

Note the alignment features. The pin 1 angled corner on the heatsink must align with the pin 1 angled corner on the CPU socket. The CPU-socket posts must align with the guide-holes in the assembly.

Figure 20: Installing the Heatsink/CPU Assembly to the CPU Socket



1 Guide hole in assembly (two)	4 Angled corner on heatsink (pin 1 alignment feature)
2 CPU socket alignment post (two)	5 Angled corner on socket (pin 1 alignment feature)
3 CPU socket leaf spring	-

- c) Set the heatsink with CPU assembly down onto the CPU socket.
- d) Use the T-30 Torx driver that is supplied with the replacement CPU to tighten the four captive nuts that secure the heatsink to the motherboard standoffs.

Note Alternate tightening the heatsink nuts evenly so that the heatsink remains level while it is lowered. Tighten the heatsink nuts in the order shown on the heatsink label: 1, 2, 3, 4. The captive nuts must be fully tightened so that the leaf springs on the CPU socket lie flat.

- e) Replace the top cover to the server.
- f) Replace the server in the rack, replace cables, and then fully power on the server by pressing the Power button.

Additional CPU-Related Parts to Order with RMA Replacement CPUs

When a return material authorization (RMA) of the CPU is done on a Cisco UCS C-Series server, additional parts might not be included with the CPU spare. The TAC engineer might need to add the additional parts to the RMA to help ensure a successful replacement.



Note The following items apply to CPU *replacement* scenarios. If you are replacing a system chassis and *moving* existing CPUs to the new chassis, you do not have to separate the heatsink from the CPU. See [Additional CPU-Related Parts to Order with RMA Replacement System Chassis, on page 56](#).

- Scenario 1—You are reusing the existing heatsinks:
 - Heat sink cleaning kit (UCSX-HSCK=)
One cleaning kit can clean up to four CPUs.
 - Thermal interface material (TIM) kit for M5 servers (UCS-CPU-TIM=)
One TIM kit covers one CPU.
- Scenario 2—You are replacing the existing heatsinks:



Caution Use only the correct heatsink for your CPUs to ensure proper cooling. There are two different heatsinks: UCSC-HS-C240M5= for CPUs 150 W and less; UCSC-HS2-C240M5= for CPUs above 150 W.

- Heat sink: UCSC-HS-C240M5= for CPUs 150 W and less; UCSC-HS2-C240M5= for CPUs above 150 W
New heatsinks have a pre-applied pad of TIM.
- Heat sink cleaning kit (UCSX-HSCK=)
One cleaning kit can clean up to four CPUs.
- Scenario 3—You have a damaged CPU carrier (the plastic frame around the CPU):
 - CPU Carrier: UCS-M5-CPU-CAR=
 - #1 flat-head screwdriver (for separating the CPU from the heatsink)
 - Heatsink cleaning kit (UCSX-HSCK=)
One cleaning kit can clean up to four CPUs.
 - Thermal interface material (TIM) kit for M5 servers (UCS-CPU-TIM=)
One TIM kit covers one CPU.

A CPU heat sink cleaning kit is good for up to four CPU and heat sink cleanings. The cleaning kit contains two bottles of solution, one to clean the CPU and heat sink of old TIM and the other to prepare the surface of the heat sink.

New heat sink spares come with a pre-applied pad of TIM. It is important to clean any old TIM off of the CPU surface prior to installing the heat sinks. Therefore, even when you are ordering new heat sinks, you must order the heat sink cleaning kit.

Additional CPU-Related Parts to Order with RMA Replacement System Chassis

When a return material authorization (RMA) of the system chassis is done on a Cisco UCS C-Series server, you move existing CPUs to the new chassis.



Note Unlike previous generation CPUs, the M5 server CPUs do not require you to separate the heatsink from the CPU when you *move* the CPU-heatsink assembly. Therefore, no additional heatsink cleaning kit or thermal-interface material items are required.

- The only tool required for moving a CPU/heatsink assembly is a T-30 Torx driver.

To move a CPU to a new chassis, use the procedure in [Moving an M5 Generation CPU, on page 56](#).

Moving an M5 Generation CPU

Tool required for this procedure: T-30 Torx driver



Caution When you receive a replacement server for an RMA, it includes dust covers on all CPU sockets. These covers protect the socket pins from damage during shipping. You must transfer these covers to the system that you are returning, as described in this procedure.

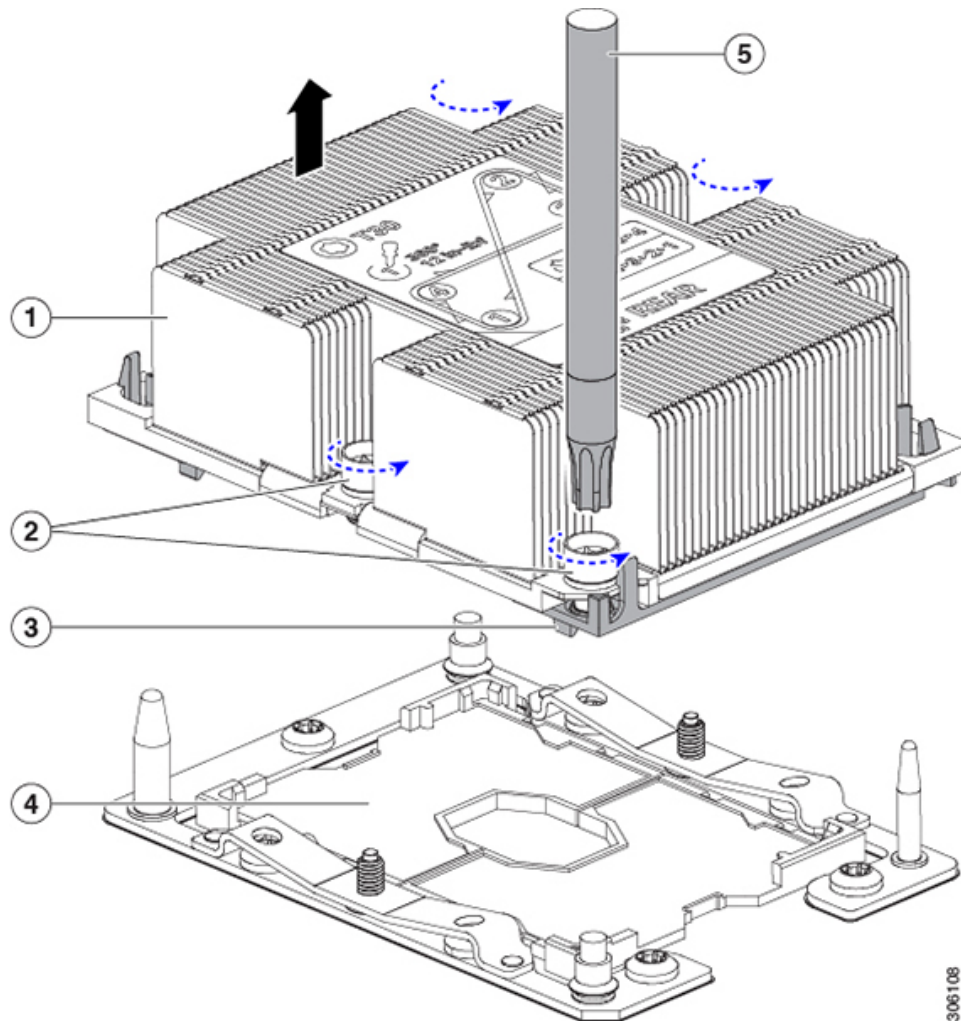
Step 1 When moving an M5 CPU to a new server, you do not have to separate the heatsink from the CPU. Perform the following steps:

- Use a T-30 Torx driver to loosen the four captive nuts that secure the assembly to the board standoffs.

Note Alternate loosening the heatsink nuts evenly so that the heatsink remains level as it is raised. Loosen the heatsink nuts in the order shown on the heatsink label: 4, 3, 2, 1.

- Lift straight up on the CPU/heatsink assembly to remove it from the board.
- Set the CPUs with heatsinks aside on an anti-static surface.

Figure 21: Removing the CPU/Heatsink Assembly



Heatsink	4 CPU socket on motherboard
Heatsink captive nuts (two on each side)	5-30 Torx driver
CPU carrier (below heatsink in this view)	-

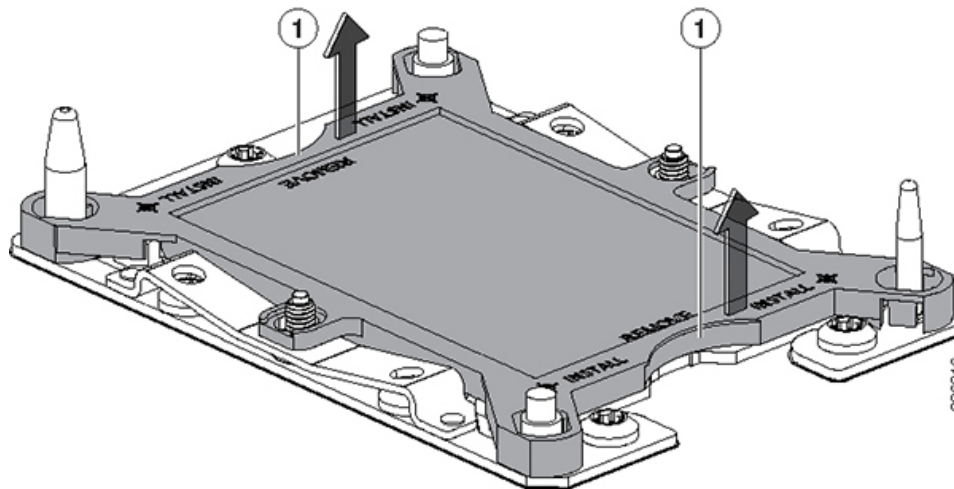
Step 2

Transfer the CPU socket covers from the new system to the system that you are returning:

- a) Remove the socket covers from the replacement system. Grasp the two recessed finger-grip areas marked "REMOVE" and lift straight up.

Note Keep a firm grasp on the finger-grip areas at both ends of the cover. Do not make contact with the CPU socket pins.

Figure 22: Removing a CPU Socket Dust Cover



Finger-grip areas marked "REMOVE"	-
-----------------------------------	---

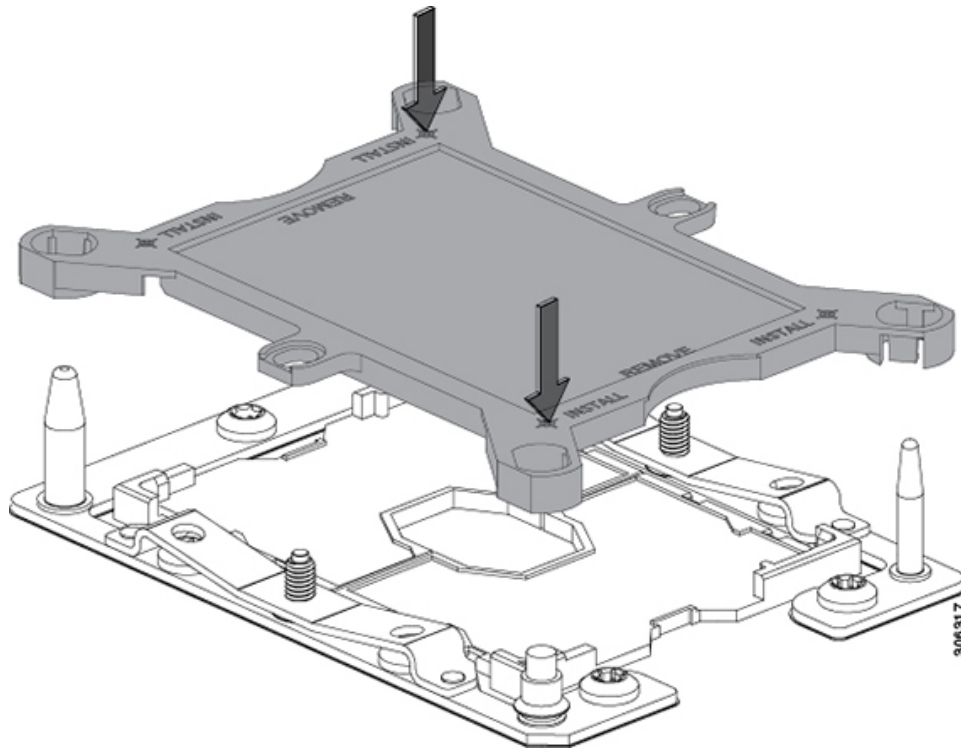
- b) With the wording on the dust cover facing up, set it in place over the CPU socket. Make sure that all alignment posts on the socket plate align with the cutouts on the cover.

Caution In the next step, do not press down anywhere on the cover except the two points described. Pressing elsewhere might damage the socket pins.

- c) Press down on the two circular markings next to the word "INSTALL" that are closest to the two threaded posts (see the following figure). Press until you feel and hear a click.

Note You must press until you feel and hear a click to ensure that the dust covers do not come loose during shipping.

Figure 23: Installing a CPU Socket Dust Cover



Press down on the two circular marks next to the word INSTALL.	-
--	---

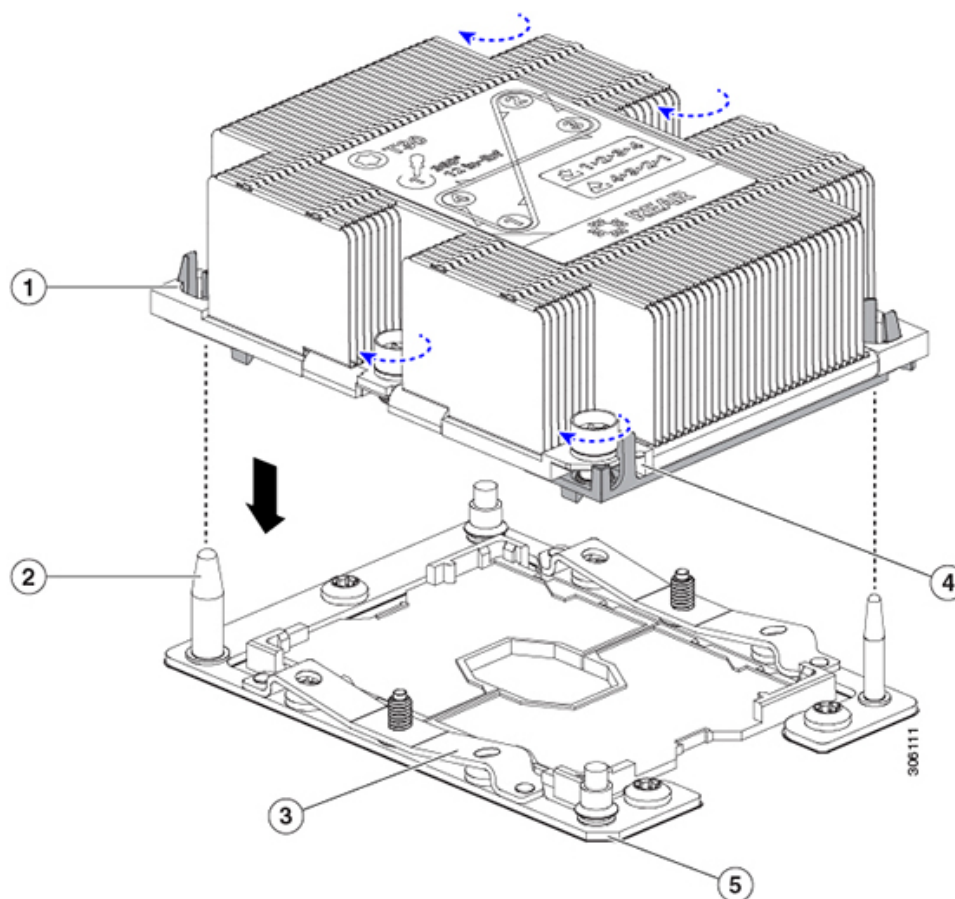
Step 3

Install the CPUs to the new system:

- a) On the new board, align the assembly over the CPU socket, as shown below.

Note the alignment features. The pin 1 angled corner on the heatsink must align with the pin 1 angled corner on the CPU socket. The CPU-socket posts must align with the guide-holes in the assembly.

Figure 24: Installing the Heatsink/CPU Assembly to the CPU Socket



1 Guide hole in assembly (two)	4 Angled corner on heatsink (pin 1 alignment feature)
2 CPU socket alignment post (two)	5 Angled corner on socket (pin 1 alignment feature)
3 CPU socket leaf spring	-

- b) On the new board, set the heatsink with CPU assembly down onto the CPU socket.
- c) Use a T-30 Torx driver to tighten the four captive nuts that secure the heatsink to the board standoffs.

Note Alternate tightening the heatsink nuts evenly so that the heatsink remains level while it is lowered. Tighten the heatsink nuts in the order shown on the heatsink label: 1, 2, 3, 4. The captive nuts must be fully tightened so that the leaf springs on the CPU socket lie flat.

Replacing Memory DIMMs


Caution

DIMMs and their sockets are fragile and must be handled with care to avoid damage during installation.


Caution

Cisco does not support third-party DIMMs. Using non-Cisco DIMMs in the server might result in system problems or damage to the motherboard.


Note

To ensure the best server performance, it is important that you are familiar with memory performance guidelines and population rules before you install or replace DIMMs.

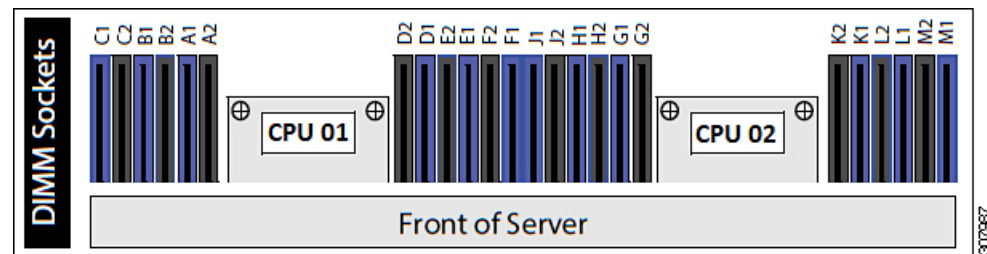
DIMM Population Rules and Memory Performance Guidelines

This topic describes the rules and guidelines for maximum memory performance.

DIMM Slot Numbering

The following figure shows the numbering of the DIMM slots on the motherboard.

Figure 25: DIMM Slot Numbering



DIMM Population Rules

Observe the following guidelines when installing or replacing DIMMs for maximum performance:

- Each CPU supports six memory channels.
 - CPU 1 supports channels A, B, C, D, E, F.
 - CPU 2 supports channels G, H, J, K, L, M.
- Each channel has two DIMM sockets (for example, channel A = slots A1, A2).
- In a single-CPU configuration, populate the channels for CPU1 only (A, B, C, D, E, F).

- For optimal performance, populate DIMMs in the order shown in the following table, depending on the number of CPUs and the number of DIMMs per CPU. If your server has two CPUs, balance DIMMs evenly across the two CPUs as shown in the table.



Note The table below lists recommended configurations. Using 5, 7, 9, 10, or 11 DIMMs per CPU is not recommended.

Table 4: DIMM Population Order

Number of DIMMs per CPU (Recommended Configurations)	Populate CPU 2 Slot		Populate CPU 1 Slots	
	Blue #1 Slots	Black #2 Slots	Blue #1 Slots	Black #2 Slots
1	(K1)	-	(D1)	-
2	(K1, L1)	-	(D1, E1)	-
3	(K1, L1, M1)	-	(D1, E1, F1)	-
4	(K1, L1); (G1, H1)	-	(D1, E1); (A1, B1)	-
6	(K1, L1); (M1, G1); (H1, J1)	-	(D1, E1); (F1, A1); (B1, C1)	-
8	(K1, L1); (G1, H1)	(K2, L2); (G2, H2)	(D1, E1); (A1, B1)	(D2, E2); (A2, B2)
12	(K1, L1); (M1, G1); (H1, J1)	(K2, L2); (M2, G2); (H2, J2)	(D1, E1); (F1, A1); (B1, C1)	(D2, E2); (F2, A2); (B2, C2)

- The maximum combined memory allowed in the 12 DIMM slots controlled by any one CPU is 768 GB. To populate the 12 DIMM slots with more than 768 GB of combined memory, you must use a high-memory CPU that has a PID that ends with an "M", for example, UCS-CPU-6134M.
- Memory mirroring reduces the amount of memory available by 50 percent because only one of the two populated channels provides data. When memory mirroring is enabled, you must install DIMMs in even numbers of channels.
- NVIDIA M-Series GPUs can support only less-than 1 TB memory in the server.
- NVIDIA P-Series GPUs can support 1 TB or more memory in the server.
- AMD FirePro S7150 X2 GPUs can support only less-than 1 TB memory in the server.
- Observe the DIMM mixing rules shown in the following table.

Table 5: DIMM Mixing Rules

DIMM Parameter	DIMMs in the Same Channel	DIMMs in the Same Bank
----------------	---------------------------	------------------------

DIMM Capacity For example, 8GB, 16GB, 32GB, 64GB, 128GB	You can mix different capacity DIMMs in the same channel (for example, A1, A2).	You cannot mix DIMM capacities in a bank (for example A1, B1). Pairs of DIMMs must be identical (same PID and revision).
DIMM speed For example, 2666 GHz	You can mix speeds, but DIMMs will run at the speed of the slowest DIMMs/CPUs installed in the channel.	You cannot mix DIMM speeds in a bank (for example A1, B1). Pairs of DIMMs must be identical (same PID and revision).
DIMM type RDIMMs or LRDIMMs	You cannot mix DIMM types in a channel.	You cannot mix DIMM types in a bank.

Memory Mirroring

The CPUs in the server support memory mirroring only when an even number of channels are populated with DIMMs. If one or three channels are populated with DIMMs, memory mirroring is automatically disabled.

Memory mirroring reduces the amount of memory available by 50 percent because only one of the two populated channels provides data. The second, duplicate channel provides redundancy.

Replacing DIMMs

Identifying a Faulty DIMM

Each DIMM socket has a corresponding DIMM fault LED, directly in front of the DIMM socket. See [Internal Diagnostic LEDs, on page 29](#) for the locations of these LEDs. When the server is in standby power mode, these LEDs light amber to indicate a faulty DIMM.

Step 1

Remove an existing DIMM:

- Shut down and remove power from the server as described in [Shutting Down and Removing Power From the Server, on page 31](#).
- Slide the server out the front of the rack far enough so that you can remove the top cover. You might have to detach cables from the rear panel to provide clearance.

Caution If you cannot safely view and access the component, remove the server from the rack.

- Remove the top cover from the server as described in [Removing the Server Top Cover, on page 33](#).
- Remove the air baffle that covers the front ends of the DIMM slots to provide clearance.
- Locate the DIMM that you are removing, and then open the ejector levers at each end of its DIMM slot.

Step 2

Install a new DIMM:

Note Before installing DIMMs, see the memory population rules for this server: [DIMM Population Rules and Memory Performance Guidelines, on page 61](#).

- Align the new DIMM with the empty slot on the motherboard. Use the alignment feature in the DIMM slot to correctly orient the DIMM.
- Push down evenly on the top corners of the DIMM until it is fully seated and the ejector levers on both ends lock into place.
- Replace the top cover to the server.

- d) Replace the server in the rack, replace cables, and then fully power on the server by pressing the Power button.

Replacing Intel Optane DC Persistent Memory Modules

This topic contains information for replacing Intel Optane Data Center Persistent memory modules (DCPMMs), including population rules and methods for verifying functionality. DCPMMs have the same form-factor as DDR4 DIMMs and they install to DIMM slots.



Caution

DCPMMs and their sockets are fragile and must be handled with care to avoid damage during installation.



Note

To ensure the best server performance, it is important that you are familiar with memory performance guidelines and population rules before you install or replace DCPMMs.



Note

Intel Optane DC persistent memory modules require Second Generation Intel Xeon Scalable processors. You must upgrade the server firmware and BIOS to version 4.0(4) or later and install the supported Second Generation Intel Xeon Scalable processors before installing DCPMMs.

DCPMMs can be configured to operate in one of three modes:

- **Memory Mode:** The module operates as 100% memory module. Data is volatile and DRAM acts as a cache for DCPMMs.
- **App Direct Mode:** The module operates as a solid-state disk storage device. Data is saved and is non-volatile.
- **Mixed Mode (25% Memory Mode + 75% App Direct):** The module operates with 25% capacity used as volatile memory and 75% capacity used as non-volatile storage.

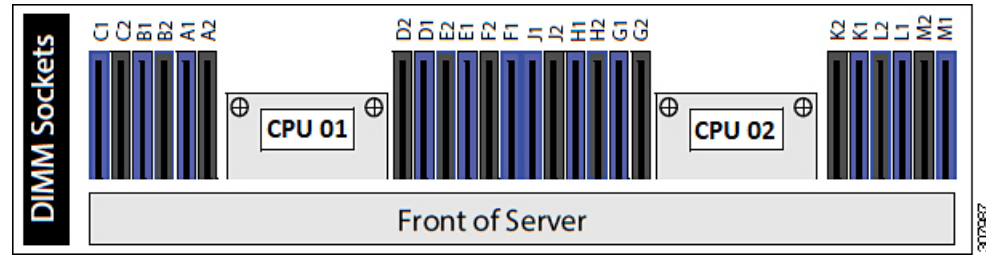
Intel Optane DC Persistent Memory Module Population Rules and Performance Guidelines

This topic describes the rules and guidelines for maximum memory performance when using Intel Optane DC persistent memory modules (DCPMMs) with DDR4 DRAM DIMMs.

DIMM Slot Numbering

The following figure shows the numbering of the DIMM slots on the server motherboard.

Figure 26: DIMM Slot Numbering



Configuration Rules

Observe the following rules and guidelines:

- To use DCPMMs in this server, two CPUs must be installed.
- Intel Optane DC persistent memory modules require Second Generation Intel Xeon Scalable processors. You must upgrade the server firmware and BIOS to version 4.0(4) or later and then install the supported Second Generation Intel Xeon Scalable processors before installing DCPMMs.
- The DCPMMs run at 2666 MHz. If you have 2933 MHz RDIMMs or LRDIMMs in the server and you add DCPMMs, the main memory speed clocks down to 2666 MHz to match the speed of the DCPMMs.
- Each DCPMM draws 18 W sustained, with a 20 W peak.
- When using DCPMMs in a server:
 - The DDR4 DIMMs installed in the server must all be the same size.
 - The DCPMMs installed in the server must all be the same size and must have the same SKU.
- The following table shows supported DCPMM configurations for this server. Fill the DIMM slots for CPU 1 and CPU2 as shown, depending on which DCPMM:DRAM ratio you want to populate.

Figure 27: Supported DCPMM Configurations for Dual-CPU Configurations

DIMM to DCPMM Count	CPU 1											
	IMC1						IMC0					
	Channel 2		Channel 1		Channel 0		Channel 2		Channel 1		Channel 0	
	F2	F1	E2	E1	D2	D1	C2	C1	B2	B1	A2	A1
6 to 2		DIMM		DIMM	DCPMM	DIMM		DIMM		DIMM	DCPMM	DIMM
6 to 4		DIMM	DCPMM	DIMM	DCPMM	DIMM		DIMM	DCPMM	DIMM	DCPMM	DIMM
6 to 6	DCPMM	DIMM	DCPMM	DIMM	DCPMM	DIMM	DCPMM	DIMM	DCPMM	DIMM	DCPMM	DIMM

DIMM to DCPMM Count	CPU 2											
	IMC1						IMC0					
	Channel 2		Channel 1		Channel 0		Channel 2		Channel 1		Channel 0	
	M2	M1	L2	L1	K2	K1	J2	J1	H2	H1	G2	G1
6 to 2		DIMM		DIMM	DCPMM	DIMM		DIMM		DIMM	DCPMM	DIMM
6 to 4		DIMM	DCPMM	DIMM	DCPMM	DIMM		DIMM	DCPMM	DIMM	DCPMM	DIMM
6 to 6	DCPMM	DIMM	DCPMM	DIMM	DCPMM	DIMM	DCPMM	DIMM	DCPMM	DIMM	DCPMM	DIMM

Installing Intel Optane DC Persistent Memory Modules



Note DCPMM configuration is always applied to all DCPMMs in a region, including a replacement DCPMM. You cannot provision a specific replacement DCPMM on a preconfigured server.

Understand which mode your DCPMM is operating in. App Direct mode has some additional considerations in this procedure.



Caution Replacing a DCPMM in App-Direct mode requires all data to be wiped from the DCPMM. Make sure to backup or offload data before attempting this procedure.

Step 1 For App Direct mode, backup the existing data stored in all Optane DIMMs to some other storage.

Step 2 For App Direct mode, remove the Persistent Memory policy which will remove goals and namespaces automatically from all Optane DIMMs.

Step 3 Remove an existing DCPMM:

- a) Shut down and remove power from the server as described in [Shutting Down and Removing Power From the Server, on page 31](#).
- b) Slide the server out the front of the rack far enough so that you can remove the top cover. You might have to detach cables from the rear panel to provide clearance.

Caution If you cannot safely view and access the component, remove the server from the rack.

- c) Remove the top cover from the server as described in [Removing the Server Top Cover, on page 33](#).
- d) Remove the air baffle that covers the front ends of the DIMM slots to provide clearance.

Caution If you are moving DCPMMs with active data (persistent memory) from one server to another as in an RMA situation, each DCPMM must be installed to the identical position in the new server. Note the positions of each DCPMM or temporarily label them when removing them from the old server.

- e) Locate the DCPMM that you are removing, and then open the ejector levers at each end of its DIMM slot.

Step 4 Install a new DCPMM:

Note Before installing DCPMMs, see the population rules for this server: [Intel Optane DC Persistent Memory Module Population Rules and Performance Guidelines, on page 64](#).

- a) Align the new DCPMM with the empty slot on the motherboard. Use the alignment feature in the DIMM slot to correctly orient the DCPMM.
- b) Push down evenly on the top corners of the DCPMM until it is fully seated and the ejector levers on both ends lock into place.
- c) Reinstall the air baffle.
- d) Replace the top cover to the server.
- e) Replace the server in the rack, replace cables, and then fully power on the server by pressing the Power button.

Step 5 Perform post-installation actions:

Note If your Persistent Memory policy is Host Controlled, you must perform the following actions from the OS side.

- If the existing configuration is in 100% Memory mode, and the new DCPMM is also in 100% Memory mode (the factory default), the only action is to ensure that all DCPMMs are at the latest, matching firmware level.
- If the existing configuration is fully or partly in App-Direct mode and new DCPMM is also in App-Direct mode, then ensure that all DCPMMs are at the latest matching firmware level and also re-provision the DCPMMs by creating a new goal.
 - For App Direct mode, reapply the Persistent Memory policy.
 - For App Direct mode, restore all the offloaded data to the DCPMMs.
- If the existing configuration and the new DCPMM are in different modes, then ensure that all DCPMMs are at the latest matching firmware level and also re-provision the DCPMMs by creating a new goal.

There a number of tools for configuring goals, regions, and namespaces.

- To use the server's BIOS Setup Utility, see [Server BIOS Setup Utility Menu for DCPMM, on page 67](#).
- To use Cisco IMC or Cisco UCS Manager, see the [Cisco UCS: Configuring and Managing Intel Optane DC Persistent Memory Modules](#) guide.

Server BIOS Setup Utility Menu for DCPMM



Caution Potential data loss: If you change the mode of a currently installed DCPMM from App Direct or Mixed Mode to Memory Mode, any data in persistent memory is deleted.

DCPMMs can be configured by using the server's BIOS Setup Utility, Cisco IMC, Cisco UCS Manager, or OS-related utilities.

- To use the BIOS Setup Utility, see the section below.
- To use Cisco IMC, see the configuration guides for Cisco IMC 4.0(4) or later: [Cisco IMC CLI and GUI Configuration Guides](#)
- To use Cisco UCS Manager, see the configuration guides for Cisco UCS Manager 4.0(4) or later: [Cisco UCS Manager CLI and GUI Configuration Guides](#)

The server BIOS Setup Utility includes menus for DCPMMs. They can be used to view or configure DCPMM regions, goals, and namespaces, and to update DCPMM firmware.

To open the BIOS Setup Utility, press **F2** when prompted onscreen during a system boot.

The DCPMM menu is on the Advanced tab of the utility:

Advanced > Intel Optane DC Persistent Memory Configuration

From this tab, you can access other menus:

- **DIMMs:** Displays the installed DCPMMs. From this page, you can update DCPMM firmware and configure other DCPMM parameters.

- Monitor health
- Update firmware
- Configure security

You can enable security mode and set a password so that the DCPMM configuration is locked. When you set a password, it applies to all installed DCPMMs. Security mode is disabled by default.

- Configure data policy

- **Regions:** Displays regions and their persistent memory types. When using App Direct mode with interleaving, the number of regions is equal to the number of CPU sockets in the server. When using App Direct mode without interleaving, the number of regions is equal to the number of DCPMMs in the server.

From the Regions page, you can configure memory goals that tell the DCPMM how to allocate resources.

- Create goal config

- **Namespaces:** Displays namespaces and allows you to create or delete them when persistent memory is used. Namespaces can also be created when creating goals. A namespace provisioning of persistent memory applies only to the selected region.

Existing namespace attributes such as the size cannot be modified. You can only add or delete namespaces.

- **Total capacity:** Displays the total DCPMM resource allocation across the server.

Updating the DCPMM Firmware Using the BIOS Setup Utility

You can update the DCPMM firmware from the BIOS Setup Utility if you know the path to the .bin files. The firmware update is applied to all installed DCPMMs.

1. Navigate to **Advanced > Intel Optane DC Persistent Memory Configuration > DIMMs > Update firmware**
2. Under **File:** , provide the file path to the .bin file.
3. Select **Update** .

Replacing a Micro SD Card

There is one socket for a Micro SD card on the top of PCIe riser 1.



Caution

To avoid data loss, we do not recommend that you hot-swap the Micro SD card while it is operating, as indicated by its activity LED turning amber. The activity LED turns amber when the Micro SD card is updating or deleting.

-
- Step 1** Remove an existing Micro SD card:

- a) Shut down and remove power from the server as described in [Shutting Down and Removing Power From the Server, on page 31](#).
- b) Slide the server out the front of the rack far enough so that you can remove the top cover. You might have to detach cables from the rear panel to provide clearance.

Caution If you cannot safely view and access the component, remove the server from the rack.

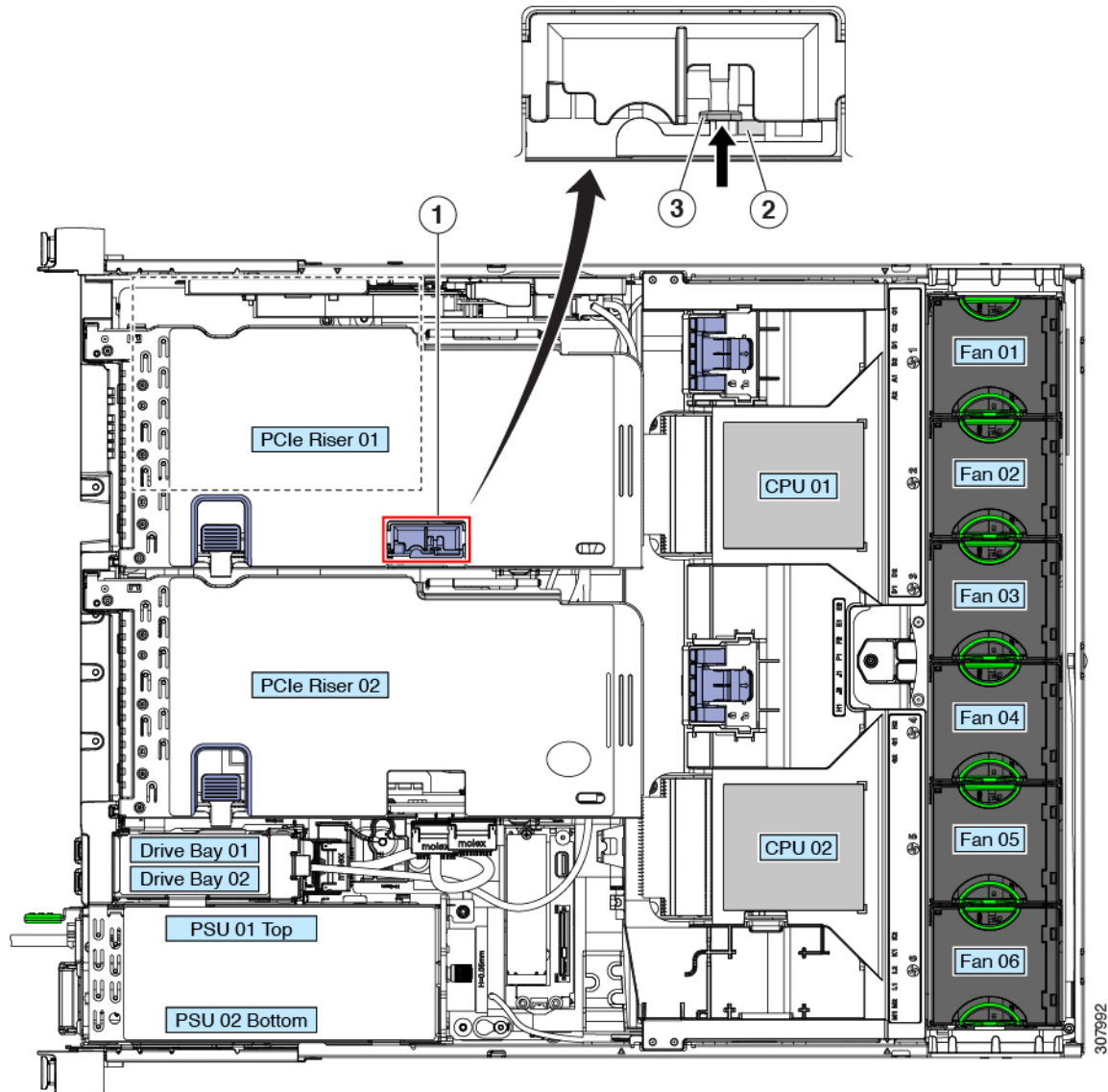
- c) Remove the top cover from the server as described in [Removing the Server Top Cover, on page 33](#).
- d) Locate the Micro SD card. The socket is on the top of PCIe riser 1, under a plastic cover.
- e) Use your fingertip to push the retainer on the plastic socket cover open far enough to provide access to the Micro SD card, then push down and release the Micro SD card to make it spring up.
- f) Grasp the Micro SD card and lift it from the socket.

Step 2

Install a new Micro SD card:

- a) While holding the retainer on the plastic cover open with your fingertip, align the new Micro SD card with the socket.
- b) Gently push down on the card until it clicks and locks in place in the socket.
- c) Replace the top cover to the server.
- d) Replace the server in the rack, replace cables, and then fully power on the server by pressing the Power button.

Figure 28: Location of Internal Micro SD Card Socket



Location of Micro SD card socket on the top of PCIe riser 1	Plastic retainer (push aside to access socket)
Micro SD card socket under plastic retainer	

Replacing a USB Drive

**Caution**

We do not recommend that you hot-swap the internal USB drive while the server is powered on because of the potential for data loss.

Step 1

Remove an existing internal USB drive:

- a) Shut down and remove power from the server as described in [Shutting Down and Removing Power From the Server, on page 31](#).
- b) Slide the server out the front of the rack far enough so that you can remove the top cover. You might have to detach cables from the rear panel to provide clearance.

Caution

If you cannot safely view and access the component, remove the server from the rack.

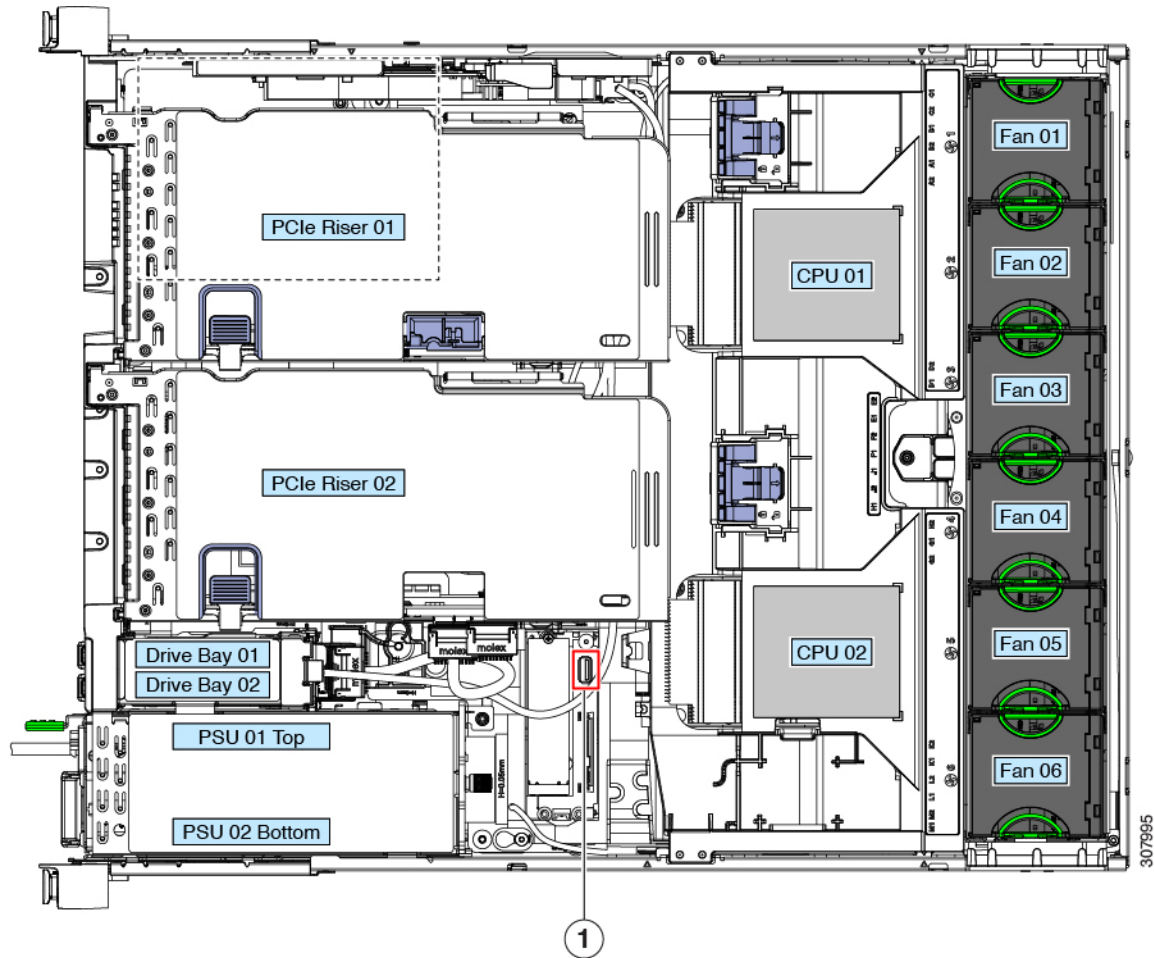
- c) Remove the top cover from the server as described in [Removing the Server Top Cover, on page 33](#).
- d) Locate the USB socket on the motherboard, in front of the power supplies.
- e) Grasp the USB drive and pull it vertically to free it from the socket.

Step 2

Install a new internal USB drive:

- a) Align the USB drive with the socket.
- b) Push the USB drive vertically to fully engage it with the socket.
- c) Replace the top cover to the server.
- d) Replace the server in the rack, replace cables, and then fully power on the server by pressing the Power button.

Figure 29: Location of Internal USB Port



Location of vertical USB socket on motherboard	-
--	---

Enabling or Disabling the Internal USB Port

The factory default is that all USB ports on the server are enabled. However, the internal USB port can be enabled or disabled in the server BIOS.

- Step 1** Enter the BIOS Setup Utility by pressing the **F2** key when prompted during bootup.
- Step 2** Navigate to the **Advanced** tab.
- Step 3** On the Advanced tab, select **USB Configuration**.
- Step 4** On the USB Configuration page, select **USB Ports Configuration**.
- Step 5** Scroll to **USB Port: Internal**, press **Enter**, and then choose either **Enabled** or **Disabled** from the dialog box.

Step 6 Press **F10** to save and exit the utility.

Replacing the RTC Battery

**Warning**

There is danger of explosion if the battery is replaced incorrectly. Replace the battery only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.

[Statement 1015]

**Warning**

Recyclers: Do not shred the battery! Make sure you dispose of the battery according to appropriate regulations for your country or locale.

The real-time clock (RTC) battery retains system settings when the server is disconnected from power. The battery type is CR2032. Cisco supports the industry-standard CR2032 battery, which can be ordered from Cisco (PID N20-MBLIBATT) or purchased from most electronic stores.

Removing the RTC battery impacts the following:

- Real clock time gets reset to default value.
- CMOS setting of the server is lost. You should reset the system setting after replacing the RTC battery.

Step 1 Remove the RTC battery:

- a) Shut down and remove power from the server as described in [Shutting Down and Removing Power From the Server, on page 31](#).
- b) Slide the server out the front of the rack far enough so that you can remove the top cover. You might have to detach cables from the front panel to provide clearance.

Caution If you cannot safely view and access the component, remove the server from the rack.

- c) Remove the top cover from the server as described in [Removing the Server Top Cover, on page 33](#).
- d) Remove PCIe riser 1 from the server to provide clearance to the RTC battery socket that is on the motherboard. See [Replacing a PCIe Riser, on page 79](#).
- e) Locate the horizontal RTC battery socket.
- f) Remove the battery from the socket on the motherboard. Gently pry the securing clip to the side to provide clearance, then lift up on the battery.

Step 2 Install a new RTC battery:

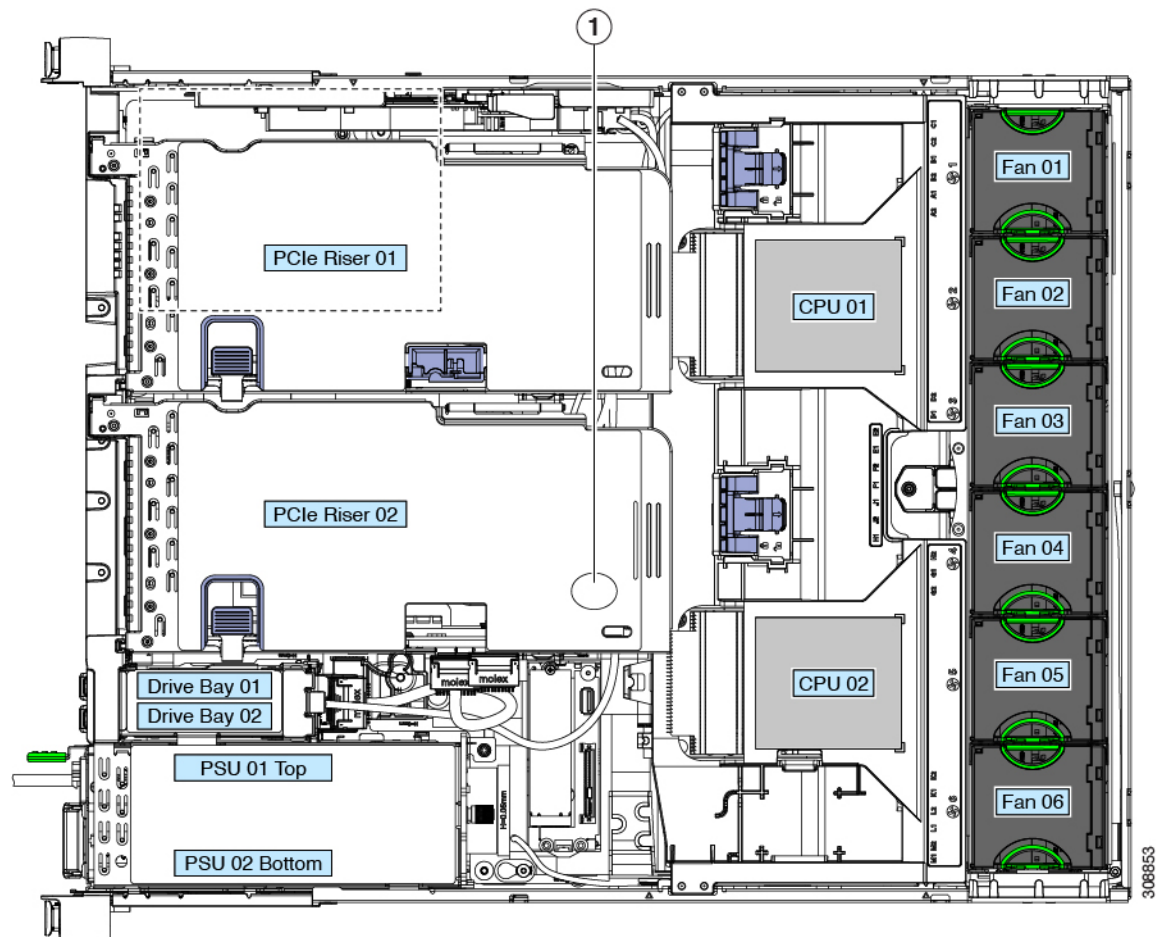
- a) Insert the battery into its socket and press down until it clicks in place under the clip.

Note The positive side of the battery marked “3V+” should face up.

- b) Replace PCIe riser 1 to the server. See [Replacing a PCIe Riser, on page 79](#).
- c) Replace the top cover to the server.

d) Replace the server in the rack, replace cables, and then fully power on the server by pressing the Power button.

Figure 30: RTC Battery Location on Motherboard



RTC battery in horizontal socket on motherboard	-
---	---

Replacing Power Supplies

The server can have one or two power supplies. When two power supplies are installed they are redundant as 1+1.

- See also [Power Specifications, on page 116](#) for more information about the supported power supplies.
- See also [Front-Panel LEDs, on page 26](#) for information about the power supply LEDs.

This section includes procedures for replacing AC and DC power supply units.

Replacing AC Power Supplies



Note If you have ordered a server with power supply redundancy (two power supplies), you do not have to power off the server to replace a power supply because they are redundant as 1+1.



Note Do not mix power supply types or wattages in the server. Both power supplies must be identical.



Caution DO NOT interchange power supplies of Cisco UCS C240 M5 servers and Cisco UCS C240 SD M5 servers.

Step 1 Remove the power supply that you are replacing or a blank panel from an empty bay:

a) Perform one of the following actions:

- If your server has only one power supply, shut down and remove power from the server as described in [Shutting Down and Removing Power From the Server, on page 31](#).
- If your server has two power supplies, you do not have to shut down the server.

b) Remove the power cord from the power supply that you are replacing.

c) Grasp the power supply handle while pinching the release lever toward the handle.

d) Pull the power supply out of the bay.

Step 2 Install a new power supply:

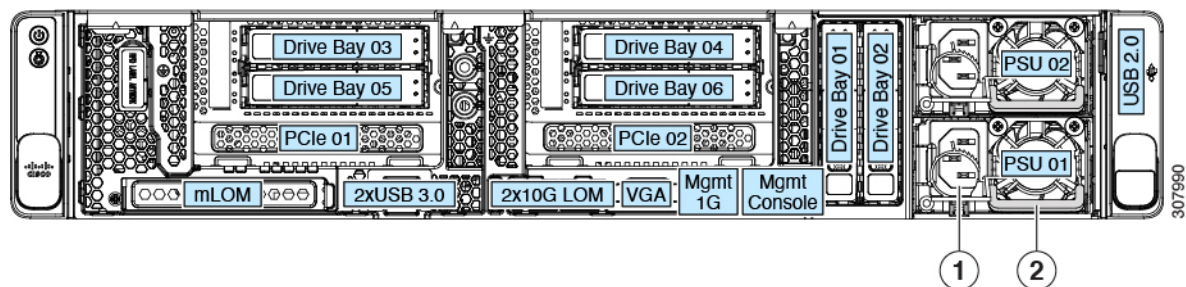
a) Grasp the power supply handle and insert the new power supply into the empty bay.

b) Push the power supply into the bay until the release lever locks.

c) Connect the power cord to the new power supply.

d) Only if you shut down the server, press the Power button to boot the server to main power mode.

Figure 31: Replacing AC Power Supplies



Power supply release lever

Power supply handle

Replacing DC Power Supplies



Note This procedure is for replacing DC power supplies in a server that already has DC power supplies installed. If you are installing DC power supplies to the server for the first time, see [Installing DC Power Supplies \(First Time Installation\)](#), on page 77.



Warning A readily accessible two-poled disconnect device must be incorporated in the fixed wiring.

Statement 1022



Warning This product requires short-circuit (overcurrent) protection, to be provided as part of the building installation. Install only in accordance with national and local wiring regulations.

Statement 1045



Warning Installation of the equipment must comply with local and national electrical codes.

Statement 1074



Note If you are replacing DC power supplies in a server with power supply redundancy (two power supplies), you do not have to power off the server to replace a power supply because they are redundant as 1+1.



Note Do not mix power supply types or wattages in the server. Both power supplies must be identical.

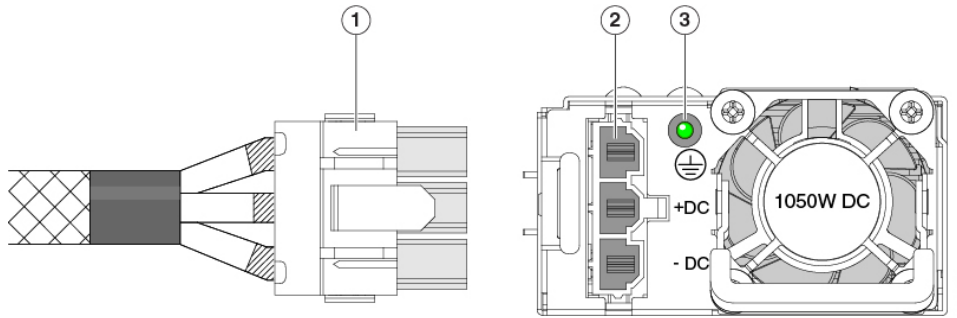
Step 1 Remove the DC power supply that you are replacing or a blank panel from an empty bay:

- a) Perform one of the following actions:
 - If you are replacing a power supply in a server that has only one DC power supply, shut down and remove power from the server as described in [Shutting Down and Removing Power From the Server](#), on page 31.
 - If you are replacing a power supply in a server that has two DC power supplies, you do not have to shut down the server.
- b) Remove the power cord from the power supply that you are replacing. Lift the connector securing clip slightly and then pull the connector from the socket on the power supply.
- c) Grasp the power supply handle while pinching the release lever toward the handle.
- d) Pull the power supply out of the bay.

Step 2 Install a new DC power supply:

- a) Grasp the power supply handle and insert the new power supply into the empty bay.
- b) Push the power supply into the bay until the release lever locks.
- c) Connect the power cord to the new power supply. Press the connector into the socket until the securing clip clicks into place.
- d) Only if you shut down the server, press the Power button to boot the server to main power mode.

Figure 32: Replacing DC Power Supplies



Keyed cable connector (CAB-48DC-40A-8AWG)	PSU status LED
Keyed DC input socket	-

Installing DC Power Supplies (First Time Installation)



Note

This procedure is for installing DC power supplies to the server for the first time. If you are replacing DC power supplies in a server that already has DC power supplies installed, see [Replacing DC Power Supplies, on page 76](#).



Warning

A readily accessible two-poled disconnect device must be incorporated in the fixed wiring.

Statement 1022



Warning

This product requires short-circuit (overcurrent) protection, to be provided as part of the building installation. Install only in accordance with national and local wiring regulations.

Statement 1045



Warning

Installation of the equipment must comply with local and national electrical codes.

Statement 1074



Note Do not mix power supply types or wattages in the server. Both power supplies must be identical.



Caution As instructed in the first step of this wiring procedure, turn off the DC power source from your facility's circuit breaker to avoid electric shock hazard.

Step 1 Turn off the DC power source from your facility's circuit breaker to avoid electric shock hazard.

Note The required DC input cable is Cisco part CAB-48DC-40A-8AWG. This 3-meter cable has a 3-pin connector on one end that is keyed to the DC input socket on the power supply. The other end of the cable has no connector so that you can wire it to your facility's DC power.

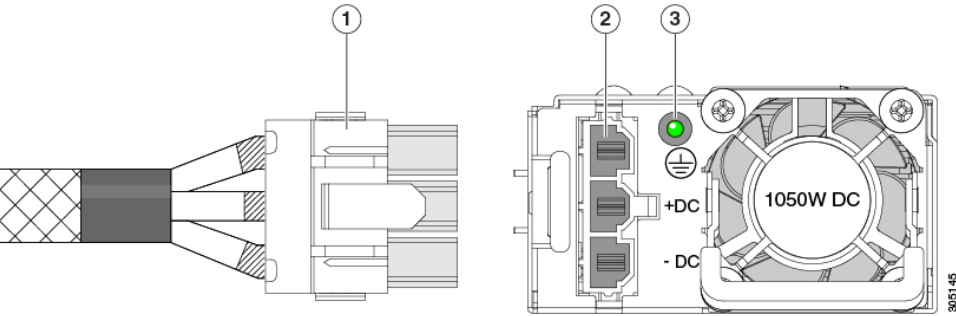
Step 2 Wire the non-terminated end of the cable to your facility's DC power input source.

Step 3 Connect the terminated end of the cable to the socket on the power supply. The connector is keyed so that the wires align for correct polarity and ground.

Step 4 Return DC power from your facility's circuit breaker.

Step 5 Press the Power button to boot the server to main power mode.

Figure 33: Replacing DC Power Supplies



Keyed cable connector (CAB-48DC-40A-8AWG)	PSU status LED
Keyed DC input socket	-

Step 6 See [Grounding for DC Power Supplies, on page 78](#) for information about additional chassis grounding.

Grounding for DC Power Supplies

AC power supplies have internal grounding and so no additional grounding is required when the supported AC power cords are used.

When using a DC power supply, additional grounding of the server chassis to the earth ground of the rack is available. Two screw holes for use with your dual-hole grounding lug and grounding wire are supplied on the chassis rear panel.



Note The grounding points on the chassis are sized for M5 screws. You must provide your own screws, grounding lug, and grounding wire. The grounding lug must be dual-hole lug that fits M5 screws. The grounding cable that you provide must be 14 AWG (2 mm), minimum 60° C wire, or as permitted by the local code.

Replacing a PCIe Riser

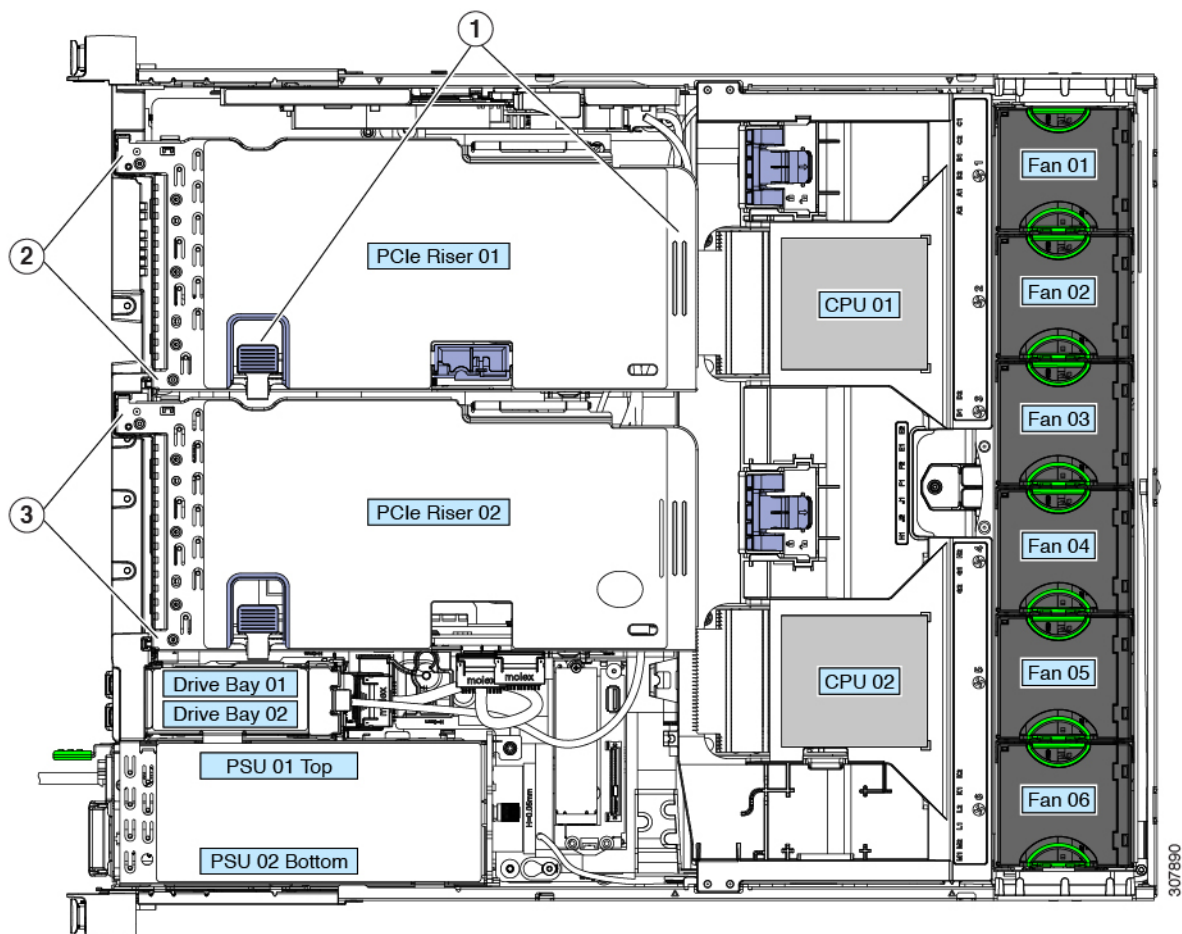
This server has two toolless PCIe risers for horizontal installation of PCIe cards and SAS/SATA/NVMe SSDs. Each riser is available in two versions. See [PCIe Slot Specifications, on page 83](#) for detailed descriptions of the slots and features in each riser version.

Before you begin

Ensure that you disconnect any cable from the riser, which you wish to remove, to avoid damaging the cables.

- Step 1** Shut down and remove power from the server as described in [Shutting Down and Removing Power From the Server, on page 31](#).
- Step 2** Slide the server out the front of the rack far enough so that you can remove the top cover. You might have to detach cables from the rear panel to provide clearance.
- Caution** If you cannot safely view and access the component, remove the server from the rack.
- Step 3** Remove the top cover from the server as described in [Removing the Server Top Cover, on page 33](#).
- Step 4** Remove the PCIe riser that you are replacing:
- a) Grasp the flip-up handle on the riser and the blue forward edge, and then lift up evenly to disengage its circuit board from the socket on the motherboard. Set the riser on an antistatic surface.
 - b) If the riser has a card installed, remove the card from the riser. See [Replacing a PCIe Card, on page 86](#).
- Step 5** Install a new PCIe riser:
- Note** The PCIe risers are not interchangeable. If you plug a PCIe riser into the wrong socket, the server will not boot. Riser 1 must plug into the motherboard socket labeled “RISER1.” Riser 2 must plug into the motherboard socket labeled “RISER2.”
- a) If you removed a card from the old PCIe riser, install the card to the new riser. See [Replacing a PCIe Card, on page 86](#).
 - b) Position the PCIe riser over its socket on the motherboard and over its alignment slots in the chassis.
 - c) Carefully push down on both ends of the PCIe riser to fully engage its circuit board connector with the socket on the motherboard.
- Step 6** Replace the top cover to the server.
- Step 7** Replace the server in the rack, replace cables, and then fully power on the server by pressing the Power button.

Figure 34: PCIe Riser Alignment Features



Riser handling points (flip-up handle and blue forward edge)	Riser 2 alignment features in chassis
Riser 1 alignment features in chassis	

Installing PCIe Risers 1C and 2E

Each riser is available in two versions. See [PCIe Slot Specifications, on page 83](#) for detailed descriptions of the slots and features in each riser version.

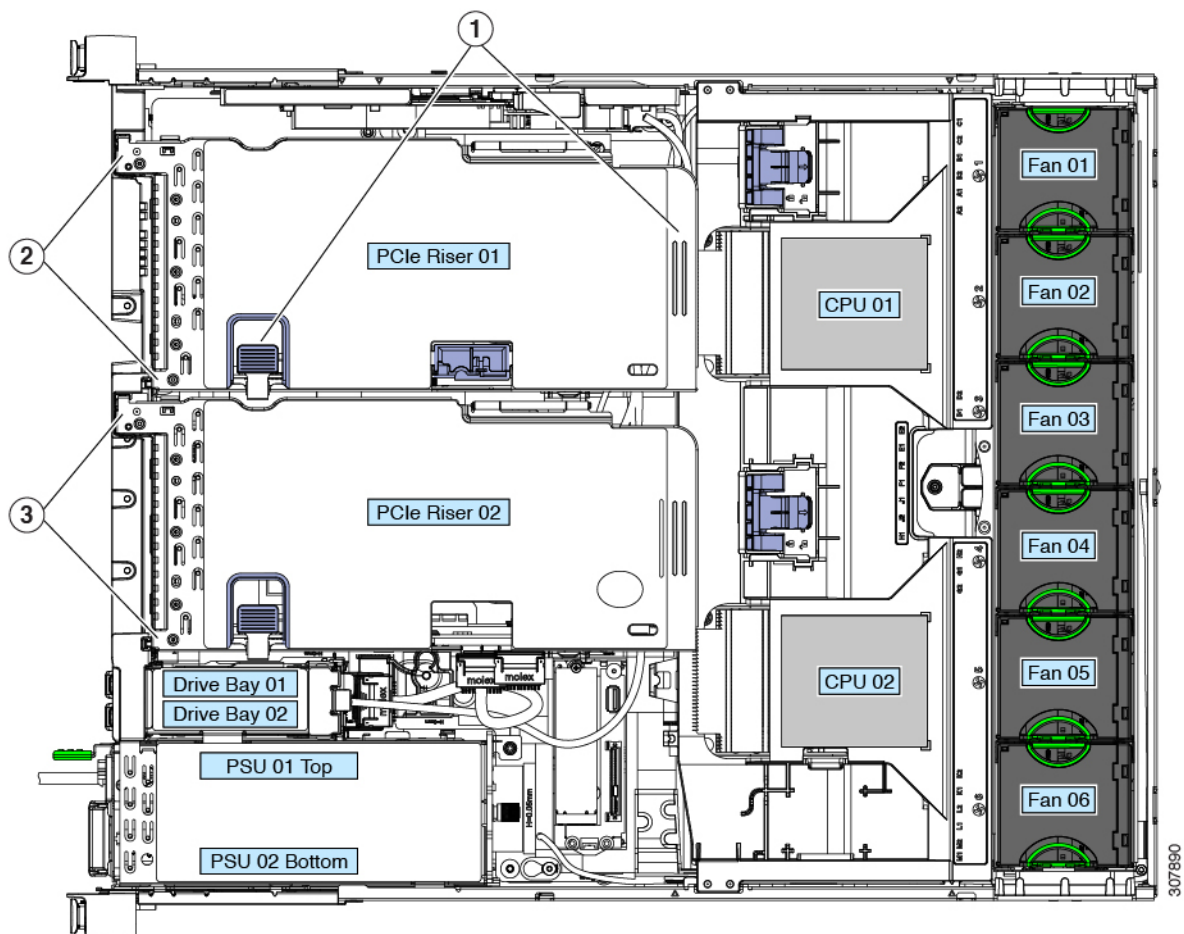
This procedure explains how to install risers 1C and 2E, which support NVMe SSDs, after removing risers 1 and 2B, which do not support NVMe SSDs.

Before you begin

Ensure that you disconnect any cable from the riser, which you wish to remove, to avoid damaging the cables.

-
- Step 1** Shut down and remove power from the server as described in [Shutting Down and Removing Power From the Server, on page 31](#).
- Step 2** Slide the server out the front of the rack far enough so that you can remove the top cover. You might have to detach cables from the rear panel to provide clearance.
- Caution** If you cannot safely view and access the component, remove the server from the rack.
- Step 3** Remove the top cover from the server as described in [Removing the Server Top Cover, on page 33](#).
- Step 4** Remove the PCIe risers 1 and 2B:
- Grasp the flip-up handle on the riser and the blue forward edge, and then lift up evenly to disengage its circuit board from the socket on the motherboard. Set the riser on an antistatic surface.
 - If the riser has a card installed, remove the card from the riser. See [Replacing a PCIe Card, on page 86](#).
- Step 5** Install new PCIe risers:
- Note** The PCIe risers are not interchangeable. If you plug a PCIe riser into the wrong socket, the server will not boot. Riser 1 must plug into the motherboard socket labeled “RISER1.” Riser 2 must plug into the motherboard socket labeled “RISER2.”
- If you removed a card from the old PCIe riser, install the card to the new riser. See [Replacing a PCIe Card, on page 86](#).
 - Position the PCIe riser over its socket on the motherboard and over its alignment slots in the chassis.
 - Carefully push down on both ends of the PCIe riser to fully engage its circuit board connector with the socket on the motherboard.
 - Connect the cable from the mother board to riser 2E (connector CN6).
 - Connect the cable from riser 1C (connector CFG1) to 2E (connector CN9).
 - (Optional) If you have HBA (UCSC-SAS-M5), connect the cable from vertical backplane to the HBA connector labeled as B1.
 - (Optional) If SAS is required for horizontal drives (UCSC-RSAS-C240M5) in riser 1, connect the cable from horizontal drive backplane to the HBA connector labeled as A1.
 - (Optional) If SAS is required for horizontal drives (UCSC-RSAS-C240M5) in riser 2, connect the cable from horizontal drive backplane to the HBA connector labeled as A2.
- Step 6** Replace the top cover to the server.
- Step 7** Replace the server in the rack, replace cables, and then fully power on the server by pressing the Power button.

Figure 35: PCIe Riser Alignment Features

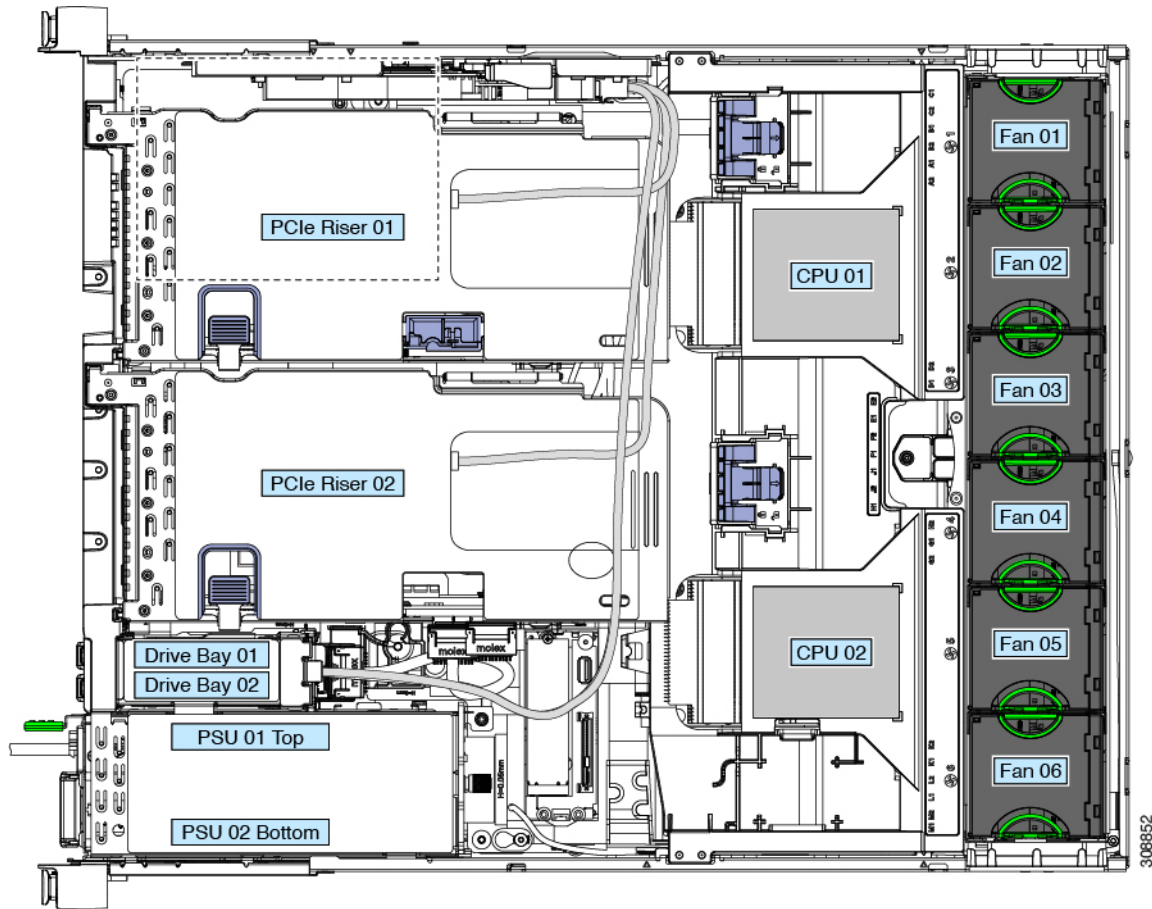


Riser handling points (flip-up handle and blue forward edge)

Riser 2 alignment features in chassis

Riser 1 alignment features in chassis

Figure 36: PCIe Riser Cabling



Replacing a PCIe Card



Note

Cisco supports all PCIe cards qualified and sold by Cisco. PCIe cards not qualified or sold by Cisco are the responsibility of the customer. Although Cisco will always stand behind and support the C-Series rack-mount servers, customers using standard, off-the-shelf, third-party cards must go to the third-party card vendor for support if any issue with that particular card occurs.

PCIe Slot Specifications

The server contains two toolless PCIe risers for horizontal installation of PCIe cards. Each riser is orderable in two versions.

- Riser 1 is available in two different options:

- Option 1 (UCSC-RIS-1-240M5)—Slots 1 (x8), 2 (x16), and 3 (x8). Slots 1 and 2 are controlled by CPU 1; slot 3 is controlled by CPU 2 and is unavailable in a single-CPU configuration.
- Option 1C (UCSC-RS1C-240M5SD)—With Drive Bay 3 (x4), Drive Bay 5 (x4), and PCIe Slot 1 (x16). All slots are controlled by CPU 1.
- In addition, Riser 1 has Micro-SD card slot.
- Riser 2 is available in two different options:
 - Option 2B (UCSC-RIS-2B-240M5)—With slots 4 (x8), 5 (x16), and 6 (x8); includes one PCIe cable connector for front-loading NVMe SSDs.
 - Option 2E (UCSC-RS2E-240M5SD)—With Drive Bay 4 (x4), Drive Bay 6 (x4), and PCIe Slot 2 (x16); includes one PCIe cable connector for front-loading NVMe SSDs.

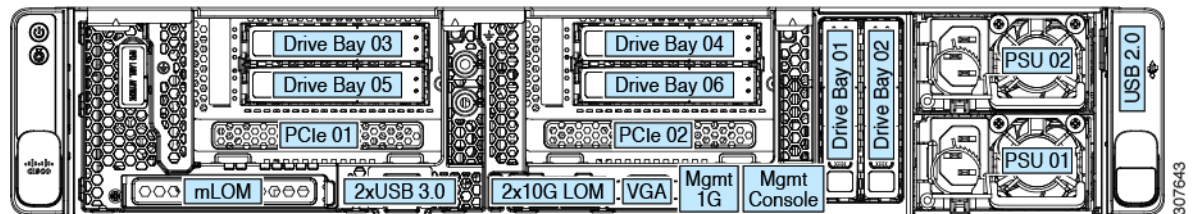
The server is orderable with two possible PCIe riser combinations:

- PCIe Riser 1 and PCIe Riser 2B
- PCIe Riser 1C and PCIe Riser 2E



Note Any other combination is not supported.

Figure 37: Front Panel, Showing PCIe Slot Numbering



The following tables describe the specifications for the slots.

Table 6: PCIe Riser 1 (UCSC-RIS-1-240M5) PCIe Expansion Slots

Slot Number	Electrical Lane Width	Connector Length	Maximum Card Length	Card Height (Rear Panel Opening)	NCSI Support	Double-Wide GPU Card Support
1	Gen-3 x8	x24 connector	¾ length	Full height	Yes	No
2	Gen-3 x16	x24 connector	Full length	Full height	Yes	Yes
3 ¹	Gen-3 x8	x16 connector	Full length	Full height	No	No
Micro SD card slot	One socket for Micro SD card on the top of the riser.					

¹ Slot 3 is not available in a single-CPU system.

Table 7: PCIe Riser 2B (UCSC-RIS-2B-240M5) PCIe Expansion Slots

Slot Number	Electrical Lane Width	Connector Length	Maximum Card Length	Card Height (Rear Panel Opening)	NCSI Support	Double-Wide GPU Card Support
4	Gen-3 x8	x24 connector	¾ length	Full height	Yes	No
5	Gen-3 x16	x24 connector	Full length	Full height	Yes	No
6	Gen-3 x8	x16 connector	Full length	Full height	No	No
Vertical NVMe Connector	Gen-3 x8	To front drive backplane; supports front-loading NVMe SSDs.				

Table 8: PCIe Riser 1C (UCSC-RS1C-C240M5SD) PCIe Expansion Slots

Slot Number	Electrical Lane Width	Connector Length	Maximum Card Length	Card Height (Rear Panel Opening)	NCSI Support	Double-Wide GPU Card Support
Drive Bay 3	Gen-3 x4	Drive Bay Connector	NA	2.5"	NA	No
Drive Bay 5	Gen-3 x4	Drive Bay Connector	NA	2.5"	NA	No
PCIe 1	Gen-3 x16	x24	¾ length	Full height	Yes	No
Micro SD card slot	One socket for Micro SD card on the top of the riser.					

Table 9: PCIe Riser 2E (UCSC-RS2E-240M5SD) PCIe Expansion Slots

Slot Number	Electrical Lane Width	Connector Length	Maximum Card Length	Card Height (Rear Panel Opening)	NCSI Support	Double-Wide GPU Card Support
Drive Bay 4	Gen-3 x4	Drive Bay Connector	NA	2.5"	NA	No
Drive Bay 6	Gen-3 x4	Drive Bay Connector	NA	2.5"	NA	No
PCIe 2	Gen-3 x16	x24	¾ length	Full height	Yes	No
Vertical NVMe Connector	Gen-3 x8	To front vertical drive backplane; supports two PCIe NVMe drives.				

Replacing a PCIe Card



Note If you are installing a Cisco UCS Virtual Interface Card, there are prerequisite considerations. See [Cisco Virtual Interface Card \(VIC\) Considerations, on page 87](#).



Note RAID controller cards install into a dedicated motherboard socket. See [Replacing a SAS Storage Controller Card \(RAID or HBA\), on page 90](#).



Note For instructions on installing or replacing double-wide GPU cards, see [GPU Card Installation, on page 123](#).

Step 1 Shut down and remove power from the server as described in [Shutting Down and Removing Power From the Server, on page 31](#).

Step 2 Slide the server out the front of the rack far enough so that you can remove the top cover. You might have to detach cables from the rear panel to provide clearance.

Caution If you cannot safely view and access the component, remove the server from the rack.

Step 3 Remove the top cover from the server as described in [Removing the Server Top Cover, on page 33](#).

Step 4 Remove the PCIe card that you are replacing:

- Remove any cables from the ports of the PCIe card that you are replacing.
- Use two hands to flip up and grasp the blue riser handle and the blue fingergrip area on the front edge of the riser, and then lift straight up.
- On the bottom of the riser, push the release latch that holds the securing plate, and then swing the hinged securing plate open.
- Open the hinged card-tab retainer that secures the rear-panel tab of the card.
- Pull evenly on both ends of the PCIe card to remove it from the socket on the PCIe riser.

If the riser has no card, remove the blanking panel from the rear opening of the riser.

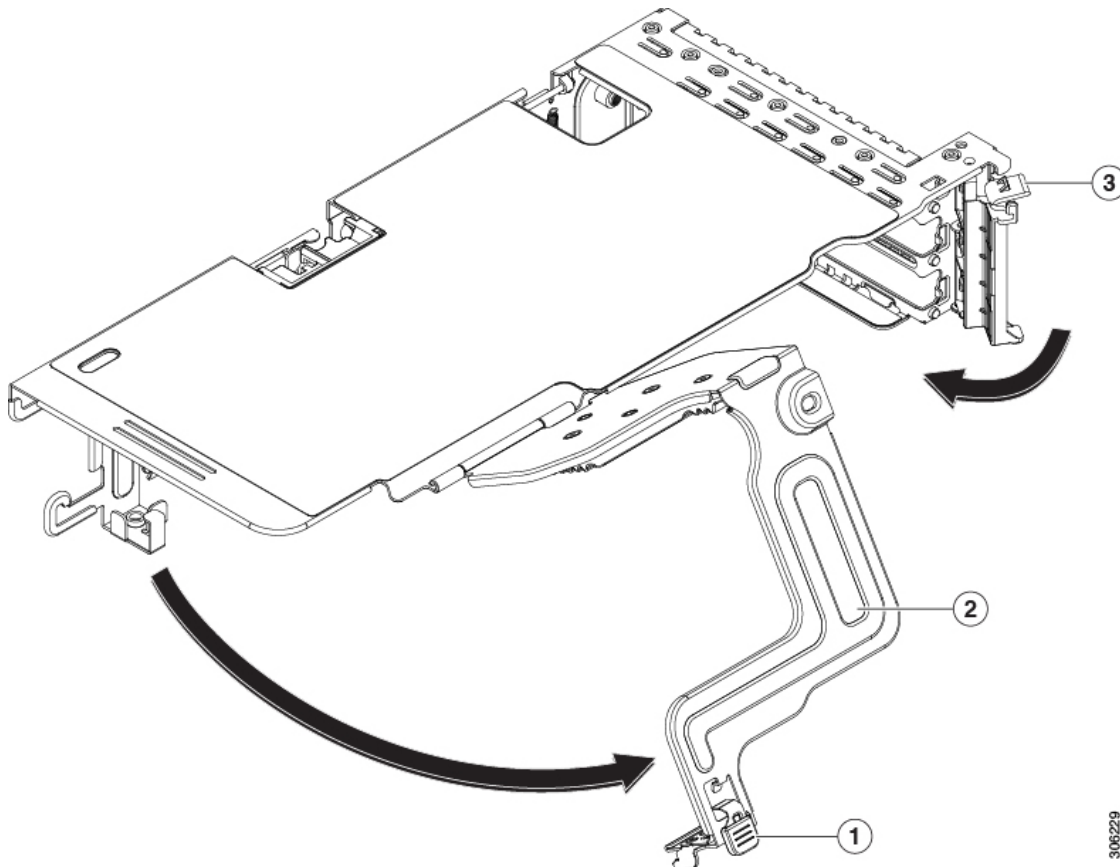
Step 5 Install a new PCIe card:

- With the hinged card-tab retainer open, align the new PCIe card with the empty socket on the PCIe riser.
- Push down evenly on both ends of the card until it is fully seated in the socket.
- Ensure that the card's rear panel tab sits flat against the riser rear-panel opening and then close the hinged card-tab retainer over the card's rear-panel tab.
- Swing the hinged securing plate closed on the bottom of the riser. Ensure that the clip on the plate clicks into the locked position.
- Position the PCIe riser over its socket on the motherboard and over the chassis alignment channels.
- Carefully push down on both ends of the PCIe riser to fully engage its connector with the sockets on the motherboard.

Step 6 Replace the top cover to the server.

Step 7 Replace the server in the rack, replace cables, and then fully power on the server by pressing the Power button.

Figure 38: PCIe Riser Card Securing Mechanisms



306229

Release latch on hinged securing plate	Hinged card-tab retainer
Hinged securing plate	-

Cisco Virtual Interface Card (VIC) Considerations

This section describes VIC card support and special considerations for this server.



Note If you use the *Cisco Card* NIC mode, you must also make a *VIC Slot* setting that matches where your VIC is installed. The options are Riser1, Riser2, and Flex-LOM. See [NIC Mode and NIC Redundancy Settings, on page 21](#) for more information about NIC modes.

If you want to use the Cisco UCS VIC card for Cisco UCS Manager integration, see also the [Cisco UCS C-Series Server Integration with Cisco UCS Manager Guides](#) for details about supported configurations, cabling, and other requirements.

Table 10: VIC Support and Considerations in This Server

VIC	How Many Supported in Server	Slots That Support VICs	Primary Slot For Cisco UCS Manager Integration	Primary Slot For Cisco Card NIC Mode	Minimum Cisco IMC Firmware
Cisco UCS VIC 1455 UCSC-PCIE-C25Q-04	2 PCIe	PCIe 2 PCIe 5	PCIe 2	PCIe 2	4.0(1)
Cisco UCS VIC 1495 UCSC-PCIE-C100-04	2 PCIe	PCIe 2 PCIe 5	PCIe 2	PCIe 2	4.0(2)
Cisco UCS VIC 1457 UCSC-MLOM-C25Q-04	1 mLOM	mLOM	mLOM	mLOM	4.0(1)
Cisco UCS VIC 1497 UCSC-MLOM-C100-04	1 mLOM	mLOM	mLOM	mLOM	4.0(2)

- A total of 3 VICs are supported in Riser 1 and Riser 2B combination server: 2 PCIe style, and 1 mLOM style.



Note Single wire management is supported on only one VIC at a time. If multiple VICs are installed on a server, only one slot has NCSI enabled at a time. For single wire management, priority goes to the MLOM slot, then slot 2, then slot 5 for NCSI management traffic. When multiple cards are installed, connect the single-wire management cables in the priority order mentioned above.

- The primary slot for a VIC card in PCIe riser 1 is slot 2. The secondary slot for a VIC card in PCIe riser 1 is slot 1.



Note The NCSI protocol is supported in only one slot at a time in each riser. If a GPU card is present in slot 2, NCSI automatically shifts from slot 2 to slot 1.

- The primary slot for a VIC card in PCIe riser 2 is slot 5. The secondary slot for a VIC card in PCIe riser 2 is slot 4.



Note The NCSI protocol is supported in only one slot at a time in each riser. If a GPU card is present in slot 5, NCSI automatically shifts from slot 5 to slot 4.



Note PCIe riser 2 is not available in a single-CPU system.

Replacing an mLOM Card

The server supports a modular LOM (mLOM) card to provide additional rear-panel connectivity. The mLOM socket is on the motherboard, under the storage controller card.

The mLOM socket provides a Gen-3 x16 PCIe lane. The socket remains powered when the server is in 12 V standby power mode and it supports the network communications services interface (NCSI) protocol.



Note If your mLOM card is a Cisco UCS Virtual Interface Card (VIC), see [Cisco Virtual Interface Card \(VIC\) Considerations, on page 87](#) for more information and support details.

Step 1 Remove any existing mLOM card (or a blanking panel):

- a) Shut down and remove power from the server as described in [Shutting Down and Removing Power From the Server, on page 31](#).
- b) Slide the server out the front of the rack far enough so that you can remove the top cover. You might have to detach cables from the rear panel to provide clearance.

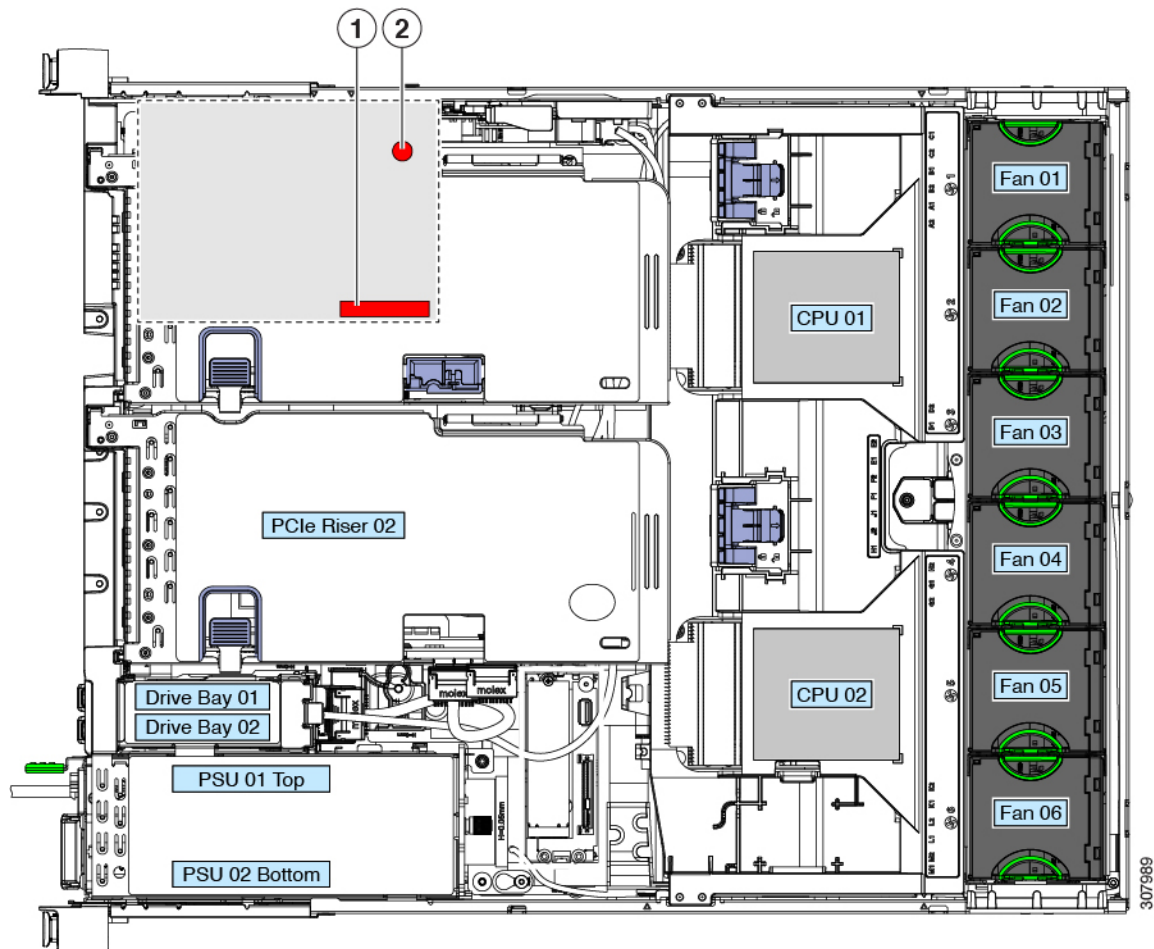
Caution If you cannot safely view and access the component, remove the server from the rack.

- c) Remove the top cover from the server as described in [Removing the Server Top Cover, on page 33](#).
- d) Remove any storage controller (RAID or HBA card) to provide clearance to the mLOM socket on the motherboard. See [Replacing a SAS Storage Controller Card \(RAID or HBA\), on page 90](#).
- e) Loosen the single captive thumbscrew that secures the mLOM card to the threaded standoff on the chassis floor.
- f) Slide the mLOM card horizontally to free it from the socket, then lift it out of the server.

Step 2 Install a new mLOM card:

- a) Set the mLOM card on the chassis floor so that its connector is aligned with the motherboard socket.
- b) Push the card horizontally to fully engage the card's edge connector with the socket.
- c) Tighten the captive thumbscrew to secure the card to the chassis floor.
- d) Return the storage controller card to the server. See [Replacing a SAS Storage Controller Card \(RAID or HBA\), on page 90](#).
- e) Replace the top cover to the server.
- f) Replace the server in the rack, replace cables, and then fully power on the server by pressing the Power button.

Figure 39: Location of the mLOM Card Socket Below the Storage Controller Card



Position of horizontal mLOM card socket

Position of mLOM card thumbscrew

Replacing a SAS Storage Controller Card (RAID or HBA)

For hardware-based storage control, the server can use a Cisco modular SAS RAID controller or SAS HBA that plugs into a dedicated, vertical socket on the motherboard.

Storage Controller Card Firmware Compatibility

Firmware on the storage controller (RAID or HBA) must be verified for compatibility with the current Cisco IMC and BIOS versions that are installed on the server. If not compatible, upgrade or downgrade the storage controller firmware using the Host Upgrade Utility (HUU) for your firmware release to bring it to a compatible level.



Note For servers running in standalone mode only: After you replace controller hardware (UCSC-SAS-M5) you must run the Cisco UCS Host Upgrade Utility (HUU) to update the controller firmware, even if the firmware Current Version is the same as the Update Version. This is necessary to program the controller's suboem-id to the correct value for the server SKU. If you do not do this, drive enumeration might not display correctly in the software. This issue does not affect servers controlled in UCSM mode.

See the HUU guide for your Cisco IMC release for instructions on downloading and using the utility to bring server components to compatible levels: [HUU Guides](#).

Replacing a SAS Storage Controller Card (RAID or HBA)

For detailed information about storage controllers in this server, see [Supported Storage Controllers and Cables, on page 121](#).

The chassis includes a plastic mounting bracket that the card must be attached to before installation.

Step 1 Prepare the server for component installation:

- Shut down and remove power from the server as described in [Shutting Down and Removing Power From the Server, on page 31](#).
- Slide the server out the front of the rack far enough so that you can remove the top cover. You might have to detach cables from the rear panel to provide clearance.

Caution If you cannot safely view and access the component, remove the server from the rack.

- Remove the top cover from the server as described in [Removing the Server Top Cover, on page 33](#).

Step 2 Remove any existing storage controller card from the server:

Note The chassis includes a plastic mounting bracket that the card must be attached to before installation. During replacement, you must remove the old card from the bracket and then install the new card to the bracket before installing this assembly to the server.

- Disconnect SAS/SATA cables and any supercap cable from the existing card.
- Lift up on the card's blue ejector lever to unseat it from the motherboard socket.
- Lift straight up on the card's carrier frame to disengage the card from the motherboard socket and to disengage the frame from two pegs on the chassis wall.
- Remove the existing card from its plastic carrier bracket. Carefully push the retainer tabs aside and then lift the card from the bracket.

Step 3 Install a new storage controller card:

- Install the new card to the plastic carrier bracket. Make sure that the retainer tabs close over the edges of the card.
- Position the assembly over the chassis and align the card edge with the motherboard socket. At the same time, align the two slots on the back of the carrier bracket with the pegs on the chassis inner wall.
- Push on both corners of the card to seat its connector in the riser socket. At the same time, ensure that the slots on the carrier frame engage with the pegs on the inner chassis wall.
- Fully close the blue ejector lever on the card to lock the card into the socket.
- Connect SAS/SATA cables and any supercap cable to the new card.

Step 4 Replace the top cover to the server.

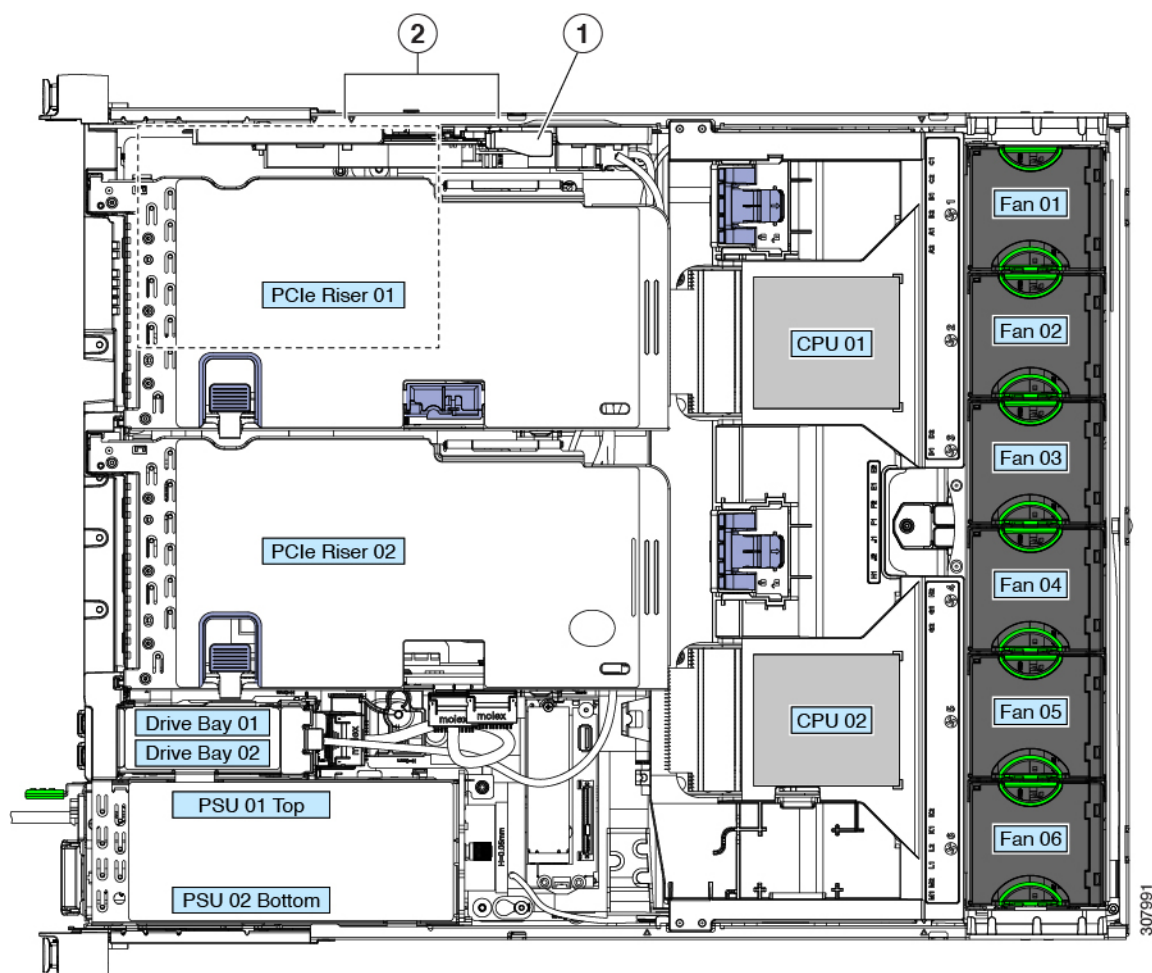
Step 5 Replace the server in the rack, replace cables, and then fully power on the server by pressing the Power button.

Step 6 If your server is running in standalone mode, use the Cisco UCS Host Upgrade Utility to update the controller firmware and program the correct suboem-id for the controller.

Note **For servers running in standalone mode only:** After you replace controller hardware (UCSC-SAS-M5), you must run the Cisco UCS Host Upgrade Utility (HUU) to update the controller firmware, even if the firmware Current Version is the same as the Update Version. This is necessary to program the controller's suboem-id to the correct value for the server SKU. If you do not do this, drive enumeration might not display correctly in the software. This issue does not affect servers controlled in UCSM mode.

See the HUU guide for your Cisco IMC release for instructions on downloading and using the utility to bring server components to compatible levels: [HUU Guides](#).

Figure 40: Replacing a Storage Controller Card



Blue ejector lever on card top edge

Pegs on inner chassis wall (two)

Replacing a Boot-Optimized M.2 RAID Controller Module

The Cisco Boot-Optimized M.2 RAID Controller module connects to the mini-storage module socket on the motherboard. It includes slots for two SATA M.2 drives, plus an integrated 6-Gbps SATA RAID controller that can control the SATA M.2 drives in a RAID 1 array.

Cisco Boot-Optimized M.2 RAID Controller Considerations

Review the following considerations:

- The minimum version of Cisco IMC and Cisco UCS Manager that support this controller is 4.0(4) and later.
- This controller supports RAID 1 (single volume) and JBOD mode.



Note Do not use the server's embedded SW MegaRAID controller to configure RAID settings when using this controller module. Instead, you can use the following interfaces:

- Cisco IMC 4.0(4a) and later
 - BIOS HII utility, BIOS 4.0(4a) and later
 - Cisco UCS Manager 4.0(4a) and later (UCS Manager-integrated servers)
-
- A SATA M.2 drive in slot 1 (the top) is the first SATA device; a SATA M.2 drive in slot 2 (the underside) is the second SATA device.
 - The name of the controller in the software is MSTOR-RAID.
 - A drive in Slot 1 is mapped as drive 253; a drive in slot 2 is mapped as drive 254.
 - When using RAID, we recommend that both SATA M.2 drives are the same capacity. If different capacities are used, the smaller capacity of the two drives is used to create a volume and the rest of the drive space is unusable.

JBOD mode supports mixed capacity SATA M.2 drives.
 - Hot-plug replacement is *not* supported. The server must be powered off.
 - Monitoring of the controller and installed SATA M.2 drives can be done using Cisco IMC and Cisco UCS Manager. They can also be monitored using other utilities such as UEFI HII, PMCLI, XMLAPI, and Redfish.
 - Updating firmware of the controller and the individual drives:
 - For standalone servers, use the Cisco Host Upgrade Utility (HUU). Refer to the [HUU Documentation](#).
 - For servers integrated with Cisco UCS Manager, refer to the [Cisco UCS Manager Firmware Management Guide](#).
 - The SATA M.2 drives can boot in UEFI mode only. Legacy boot mode is not supported.

- If you replace a single SATA M.2 drive that was part of a RAID volume, rebuild of the volume is auto-initiated after the user accepts the prompt to import the configuration. If you replace both drives of a volume, you must create a RAID volume and manually reinstall any OS.
- We recommend that you erase drive contents before creating volumes on used drives from another server. The configuration utility in the server BIOS includes a SATA secure-erase function.
- The server BIOS includes a configuration utility specific to this controller that you can use to create and delete RAID volumes, view controller properties, and erase the physical drive contents. Access the utility by pressing **F2** when prompted during server boot. Then navigate to **Advanced > Cisco Boot Optimized M.2 RAID Controller**.

Replacing a Cisco Boot-Optimized M.2 RAID Controller

This topic describes how to remove and replace a Cisco Boot-Optimized M.2 RAID Controller. The controller board has one M.2 socket on its top (Slot 1) and one M.2 socket on its underside (Slot 2).

Step 1 Shut down and remove power from the server as described in [Shutting Down and Removing Power From the Server, on page 31](#).

Step 2 Slide the server out the front of the rack far enough so that you can remove the top cover. You might have to detach cables from the rear panel to provide clearance.

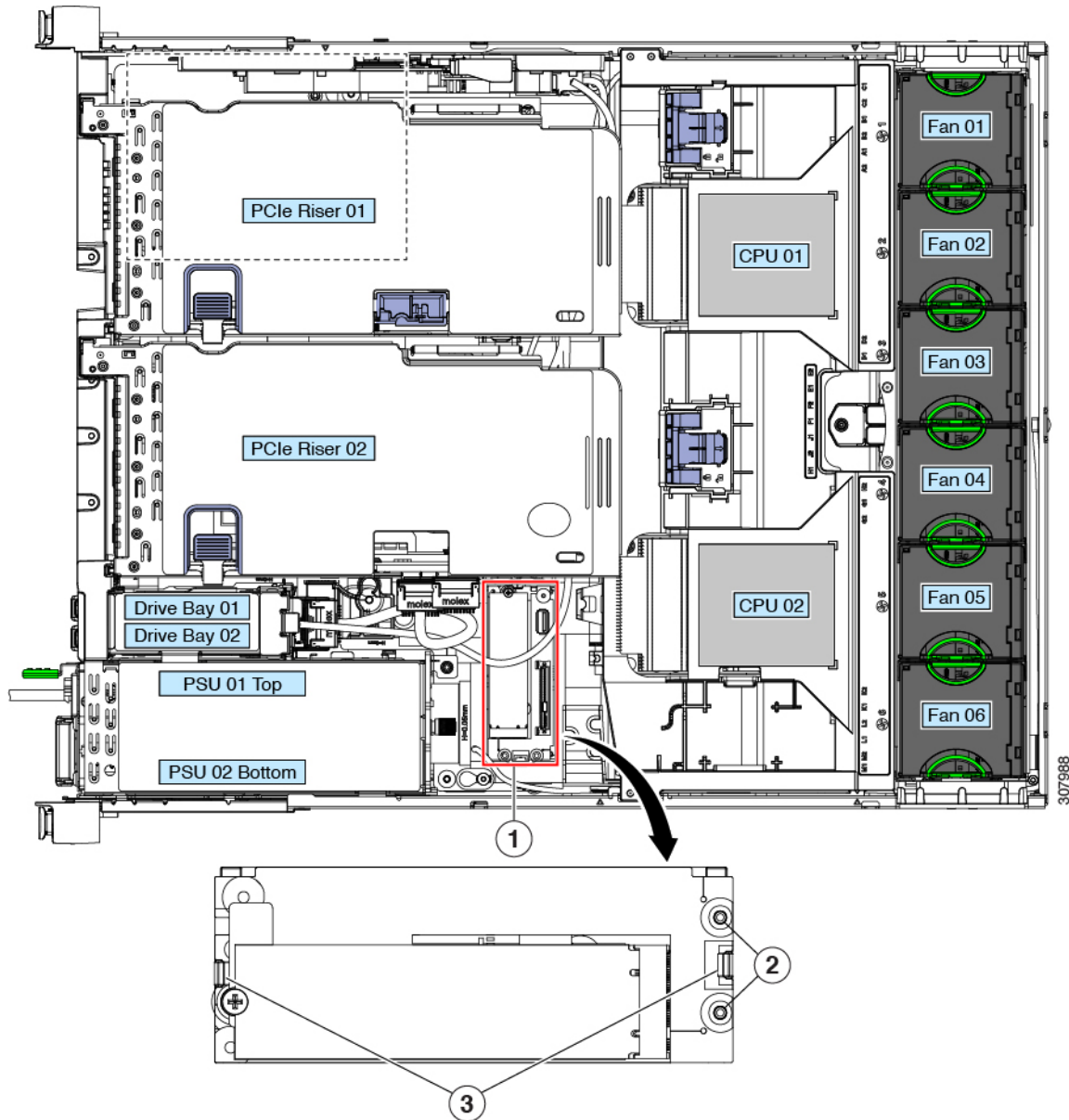
Caution If you cannot safely view and access the component, remove the server from the rack.

Step 3 Remove the top cover from the server as described in [Removing the Server Top Cover, on page 33](#).

Step 4 Remove a controller from its motherboard socket:

- a) Locate the controller in its socket just in front of power supply 1.
- b) At each end of the controller board, push outward on the clip that secures the carrier.
- c) Lift both ends of the controller to disengage it from the socket on the motherboard.
- d) Set the carrier on an anti-static surface.

Figure 41: Cisco Boot-Optimized M.2 RAID Controller on Motherboard



Location of socket on motherboard	Securing clips
Alignment pegs	-

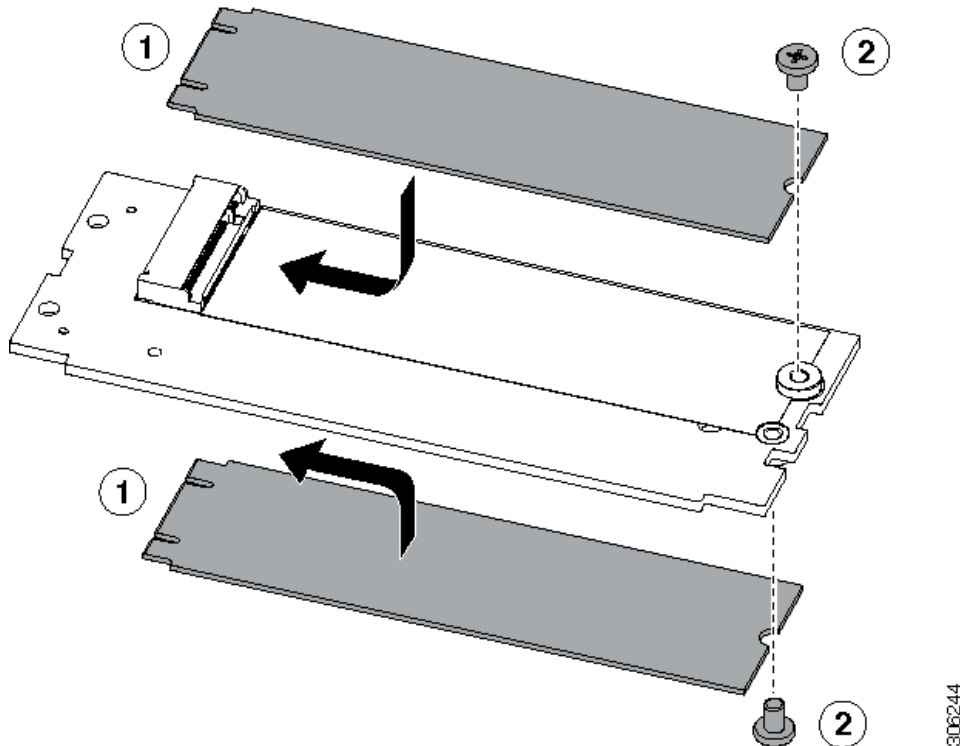
Step 5 If you are transferring SATA M.2 drives from the old controller to the replacement controller, do that before installing the replacement controller:

Note Any previously configured volume and data on the drives are preserved when the M.2 drives are transferred to the new controller. The system will boot the existing OS that is installed on the drives.

- a) Use a #1 Phillips-head screwdriver to remove the single screw that secures the M.2 drive to the carrier.

- b) Lift the M.2 drive from its socket on the carrier.
- c) Position the replacement M.2 drive over the socket on the controller board.
- d) Angle the M.2 drive downward and insert the connector-end into the socket on the carrier. The M.2 drive's label must face up.
- e) Press the M.2 drive flat against the carrier.
- f) Install the single screw that secures the end of the M.2 SSD to the carrier.
- g) Turn the controller over and install the second M.2 drive.

Figure 42: Cisco Boot-Optimized M.2 RAID Controller, Showing M.2 Drive Installation



Step 6 Install the controller to its socket on the motherboard:

- a) Position the controller over the socket, with the controller's connector facing down and at the same end as the motherboard socket. Two alignment pegs must match with two holes on the controller.
- b) Gently push down the socket end of the controller so that the two pegs go through the two holes on the controller.
- c) Push down on the controller so that the securing clips click over it at both ends.

Step 7 Replace the top cover to the server.

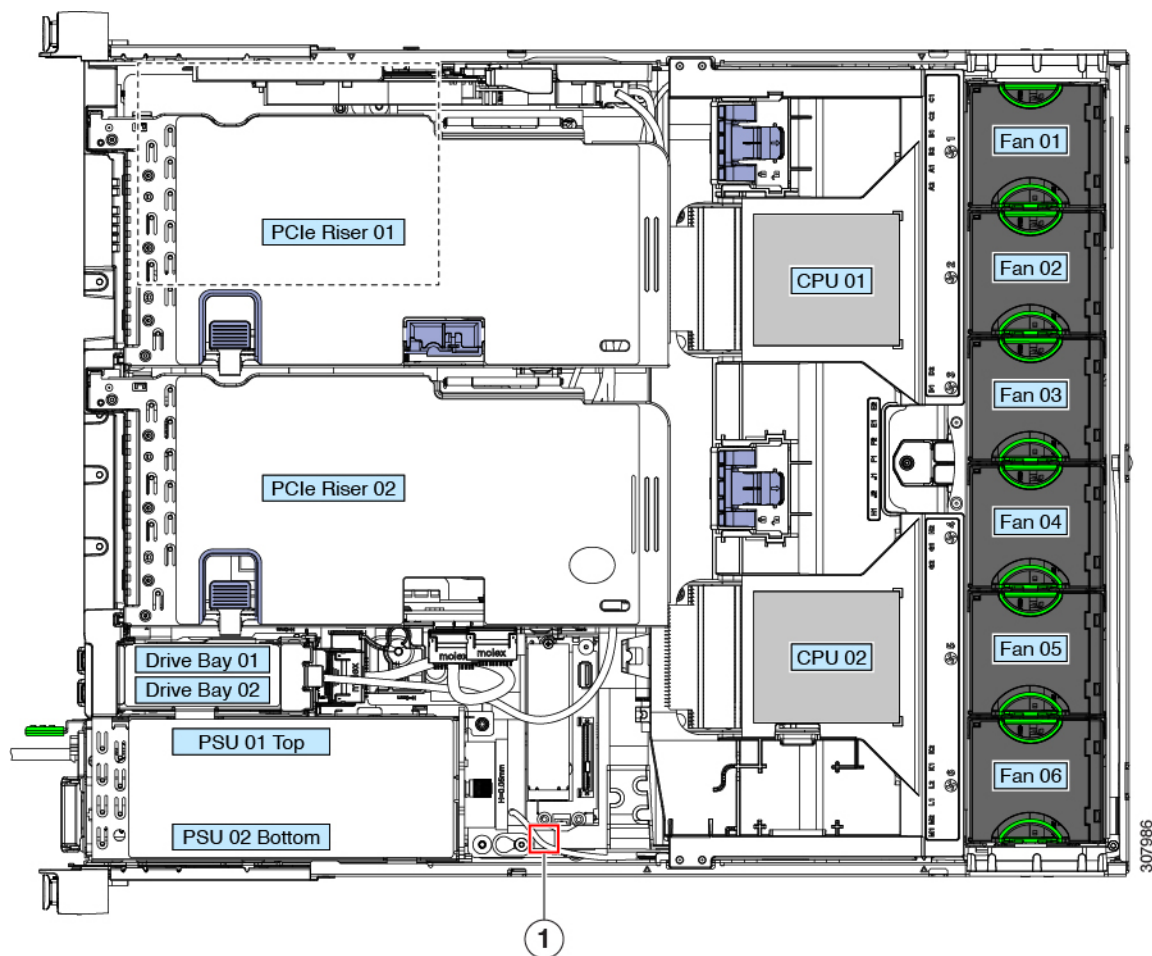
Step 8 Replace the server in the rack, replace cables, and then fully power on the server by pressing the Power button.

Replacing a Chassis Intrusion Switch

The chassis intrusion switch is an optional security feature that logs an event in the system event log (SEL) whenever the cover is removed from the chassis.

-
- Step 1** Prepare the server for component installation:
- Shut down and remove power from the server as described in [Shutting Down and Removing Power From the Server, on page 31](#).
 - Slide the server out the front of the rack far enough so that you can remove the top cover. You might have to detach cables from the rear panel to provide clearance.
- Caution** If you cannot safely view and access the component, remove the server from the rack.
- Remove the top cover from the server as described in [Removing the Server Top Cover, on page 33](#).
- Step 2** Remove an existing intrusion switch:
- Disconnect the intrusion switch cable from the socket on the motherboard.
 - Use a #1 Phillips-head screwdriver to loosen and remove the single screw that holds the switch mechanism to the chassis wall.
 - Slide the switch mechanism straight up to disengage it from the clips on the chassis.
- Step 3** Install a new intrusion switch:
- Slide the switch mechanism down into the clips on the chassis wall so that the screwholes line up.
 - Use a #1 Phillips-head screwdriver to install the single screw that secures the switch mechanism to the chassis wall.
 - Connect the switch cable to the socket on the motherboard.
- Step 4** Replace the cover to the server.
- Step 5** Replace the server in the rack, replace cables, and then fully power on the server by pressing the Power button.

Figure 43: Replacing a Chassis Intrusion Switch



Intrusion switch location	-
---------------------------	---

Installing a Trusted Platform Module (TPM)

The trusted platform module (TPM) is a small circuit board that plugs into a motherboard socket and is then permanently secured with a one-way screw. The socket location is on the motherboard below PCIe riser 2.

TPM Considerations

- This server supports either TPM version 1.2 or TPM version 2.0. The TPM 2.0, UCSX-TPM2-002B(=), is compliant with Federal Information Processing (FIPS) Standard 140-2. FIPS support has existed, but FIPS 140-2 is now supported.
- Field replacement of a TPM is not supported; you can install a TPM after-factory only if the server does not already have a TPM installed.

- If there is an existing TPM 1.2 installed in the server, you cannot upgrade to TPM 2.0. If there is no existing TPM in the server, you can install TPM 2.0.
- If the TPM 2.0 becomes unresponsive, reboot the server.

Installing and Enabling a TPM



Note Field replacement of a TPM is not supported; you can install a TPM after-factory only if the server does not already have a TPM installed.

This topic contains the following procedures, which must be followed in this order when installing and enabling a TPM:

1. Installing the TPM Hardware
2. Enabling the TPM in the BIOS
3. Enabling the Intel TXT Feature in the BIOS

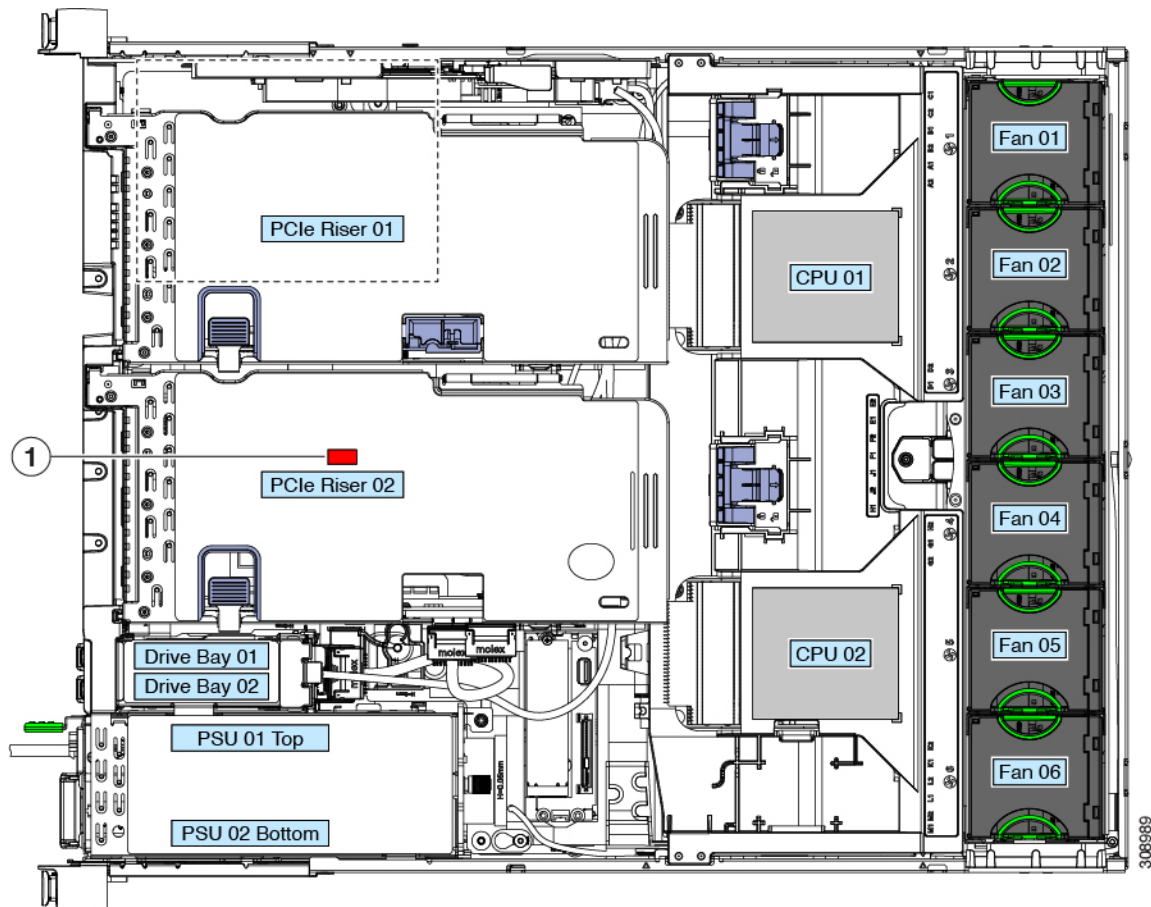
Installing TPM Hardware



Note For security purposes, the TPM is installed with a one-way screw. It cannot be removed with a standard screwdriver.

- Step 1** Prepare the server for component installation:
- a) Shut down and remove power from the server as described in [Shutting Down and Removing Power From the Server, on page 31](#).
 - b) Slide the server out the front of the rack far enough so that you can remove the top cover. You might have to detach cables from the rear panel to provide clearance.
- Caution** If you cannot safely view and access the component, remove the server from the rack.
- c) Remove the top cover from the server as described in [Removing the Server Top Cover, on page 33](#).
- Step 2** Remove PCIe riser 2 from the server to provide clearance to the TPM socket on the motherboard.
- Step 3** Install a TPM:
- a) Locate the TPM socket on the motherboard.
 - b) Align the connector that is on the bottom of the TPM circuit board with the motherboard TPM socket. Align the screw hole on the TPM board with the screw hole that is adjacent to the TPM socket.
 - c) Push down evenly on the TPM to seat it in the motherboard socket.
 - d) Install the single one-way screw that secures the TPM to the motherboard.
- Step 4** Replace PCIe riser 2 to the server. See [Replacing a PCIe Riser, on page 79](#).
- Step 5** Replace the cover to the server.
- Step 6** Replace the server in the rack, replace cables, and then fully power on the server by pressing the Power button.

Step 7 Continue with [Enabling the TPM in the BIOS](#), on page 100.



TPM socket location on motherboard, below PCIe riser 2 -

Enabling the TPM in the BIOS

After hardware installation, you must enable TPM support in the BIOS.



Note You must set a BIOS Administrator password before performing this procedure. To set this password, press the **F2** key when prompted during system boot to enter the BIOS Setup utility. Then navigate to **Security > Set Administrator Password** and enter the new password twice as prompted.

Step 1 Enable TPM Support:

- Watch during bootup for the F2 prompt, and then press **F2** to enter BIOS setup.
- Log in to the BIOS Setup Utility with your BIOS Administrator password.
- On the BIOS Setup Utility window, choose the **Advanced** tab.

- d) Choose **Trusted Computing** to open the TPM Security Device Configuration window.
- e) Change TPM SUPPORT to **Enabled**.
- f) Press **F10** to save your settings and reboot the server.

Step 2 Verify that TPM support is now enabled:

- a) Watch during bootup for the F2 prompt, and then press **F2** to enter BIOS setup.
- b) Log into the BIOS Setup utility with your BIOS Administrator password.
- c) Choose the **Advanced** tab.
- d) Choose **Trusted Computing** to open the TPM Security Device Configuration window.
- e) Verify that TPM SUPPORT and TPM State are Enabled.

Step 3 Continue with [Enabling the Intel TXT Feature in the BIOS, on page 101](#).

Enabling the Intel TXT Feature in the BIOS

Intel Trusted Execution Technology (TXT) provides greater protection for information that is used and stored on the business server. A key aspect of that protection is the provision of an isolated execution environment and associated sections of memory where operations can be conducted on sensitive data, invisibly to the rest of the system. Intel TXT provides for a sealed portion of storage where sensitive data such as encryption keys can be kept, helping to shield them from being compromised during an attack by malicious code.

Step 1 Reboot the server and watch for the prompt to press F2.

Step 2 When prompted, press **F2** to enter the BIOS Setup utility.

Step 3 Verify that the prerequisite BIOS values are enabled:

- a) Choose the **Advanced** tab.
- b) Choose **Intel TXT(LT-SX) Configuration** to open the Intel TXT(LT-SX) Hardware Support window.
- c) Verify that the following items are listed as Enabled:
 - VT-d Support (default is Enabled)
 - VT Support (default is Enabled)
 - TPM Support
 - TPM State
- d) Do one of the following:
 - If VT-d Support and VT Support are already enabled, skip to step 4.
 - If VT-d Support and VT Support are not enabled, continue with the next steps to enable them.
- e) Press **Escape** to return to the BIOS Setup utility **Advanced** tab.
- f) On the Advanced tab, choose **Processor Configuration** to open the Processor Configuration window.
- g) Set Intel (R) VT and Intel (R) VT-d to **Enabled**.

Step 4 Enable the Intel Trusted Execution Technology (TXT) feature:

- a) Return to the Intel TXT(LT-SX) Hardware Support window if you are not already there.
- b) Set TXT Support to **Enabled**.

Step 5 Press **F10** to save your changes and exit the BIOS Setup utility.

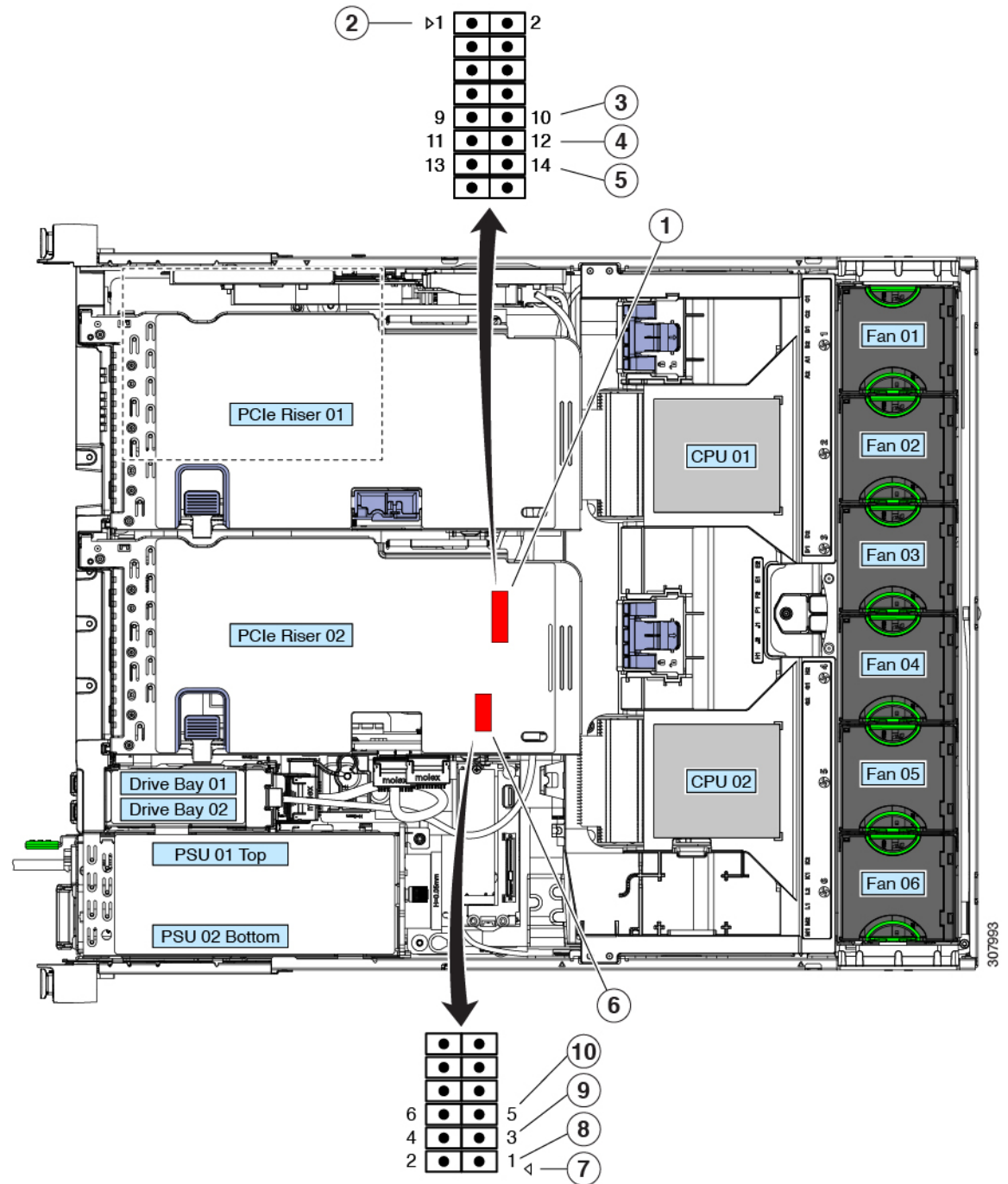
Service Headers and Jumpers

This server includes two blocks of headers (J38, J39) that you can jumper for certain service and debug functions.

This section contains the following topics:

- [Using the Clear CMOS Header \(J38, Pins 9 - 10\), on page 104](#)
- [Using the BIOS Recovery Header \(J38, Pins 11 - 12\), on page 104](#)
- [Using the Clear Password Header \(J38, Pins 13 - 14\), on page 106](#)
- [Using the Boot Alternate Cisco IMC Image Header \(J39, Pins 1 - 2\), on page 107](#)
- [Using the Reset Cisco IMC Password to Default Header \(J39, Pins 3 - 4\), on page 108](#)
- [Using the Reset Cisco IMC to Defaults Header \(J39, Pins 5 - 6\), on page 108](#)

Figure 44: Location of Service Header Blocks J38 and J39



Location of header block J38	Location of header block J39
J38 pin 1 arrow printed on motherboard	J39 pin 1 arrow printed on motherboard
Clear CMOS: J38 pins 9 - 10	Boot Cisco IMC from alternate image: J39 pins 1 - 2

Recover BIOS: J38 pins 11 - 12	Reset Cisco IMC password to default: J39 pins 3 - 4
Clear password: J38 pins 13 - 14	Reset Cisco IMC to defaults: J39 pins 5 - 6

Using the Clear CMOS Header (J38, Pins 9 - 10)

You can use this switch to clear the server's CMOS settings in the case of a system hang. For example, if the server hangs because of incorrect settings and does not boot, use this jumper to invalidate the settings and reboot with defaults.



Caution Clearing the CMOS removes any customized settings and might result in data loss. Make a note of any necessary customized settings in the BIOS before you use this clear CMOS procedure.

-
- Step 1** Shut down and remove power from the server as described in [Shutting Down and Removing Power From the Server, on page 31](#).
- Step 2** Slide the server out the front of the rack far enough so that you can remove the top cover. You might have to detach cables from the rear panel to provide clearance.
- Caution** If you cannot safely view and access the component, remove the server from the rack.
- Step 3** Remove the top cover from the server as described in [Removing the Server Top Cover, on page 33](#).
- Step 4** Install a two-pin jumper across J38 pins 9 and 10.
- Step 5** Reinstall the top cover and reconnect AC power cords to the server. The server powers up to standby power mode, indicated when the Power LED on the front panel is amber.
- Step 6** Return the server to main power mode by pressing the Power button on the front panel. The server is in main power mode when the Power LED is green.
- Note** You must allow the entire server to reboot to main power mode to complete the reset. The state of the jumper cannot be determined without the host CPU running.
- Step 7** Press the Power button to shut down the server to standby power mode, and then remove AC power cords from the server to remove all power.
- Step 8** Remove the top cover from the server.
- Step 9** Remove the jumper that you installed.
- Note** If you do not remove the jumper, the CMOS settings are reset to the defaults every time you power-cycle the server.
- Step 10** Replace the top cover, replace the server in the rack, replace power cords and any other cables, and then power on the server by pressing the Power button.
-

Using the BIOS Recovery Header (J38, Pins 11 - 12)

Depending on which stage the BIOS becomes corrupted, you might see different behavior.

- If the BIOS BootBlock is corrupted, you might see the system get stuck on the following message:

Initializing and configuring memory/hardware

- If it is a non-BootBlock corruption, a message similar to the following is displayed:

```
****BIOS FLASH IMAGE CORRUPTED****
Flash a valid BIOS capsule file using Cisco IMC WebGUI or CLI interface.
IF Cisco IMC INTERFACE IS NOT AVAILABLE, FOLLOW THE STEPS MENTIONED BELOW.
1. Connect the USB stick with bios.cap file in root folder.
2. Reset the host.
IF THESE STEPS DO NOT RECOVER THE BIOS
1. Power off the system.
2. Mount recovery jumper.
3. Connect the USB stick with bios.cap file in root folder.
4. Power on the system.
Wait for a few seconds if already plugged in the USB stick.
REFER TO SYSTEM MANUAL FOR ANY ISSUES.
```



Note

As indicated by the message shown above, there are two procedures for recovering the BIOS. Try procedure 1 first. If that procedure does not recover the BIOS, use procedure 2.

Procedure 1: Reboot With bios.cap Recovery File

-
- Step 1** Download the BIOS update package and extract it to a temporary location.
- Step 2** Copy the contents of the extracted recovery folder to the root directory of a USB drive. The recovery folder contains the bios.cap file that is required in this procedure.
- Note** The bios.cap file must be in the root directory of the USB drive. Do not rename this file. The USB drive must be formatted with either the FAT16 or FAT32 file system.
- Step 3** Insert the USB drive into a USB port on the server.
- Step 4** Reboot the server.
- Step 5** Return the server to main power mode by pressing the Power button on the front panel.
- The server boots with the updated BIOS boot block. When the BIOS detects a valid bios.cap file on the USB drive, it displays this message:
- ```
Found a valid recovery file...Transferring to Cisco IMC
System would flash the BIOS image now...
System would restart with recovered image after a few seconds...
```
- Step 6** Wait for server to complete the BIOS update, and then remove the USB drive from the server.
- Note** During the BIOS update, Cisco IMC shuts down the server and the screen goes blank for about 10 minutes. Do not unplug the power cords during this update. Cisco IMC powers on the server after the update is complete.
- 

## Procedure 2: Use BIOS Recovery Header and bios.cap File

- 
- Step 1** Download the BIOS update package and extract it to a temporary location.

**Step 2** Copy the contents of the extracted recovery folder to the root directory of a USB drive. The recovery folder contains the bios.cap file that is required in this procedure.

**Note** The bios.cap file must be in the root directory of the USB drive. Do not rename this file. The USB drive must be formatted with either the FAT16 or FAT32 file system.

**Step 3** Shut down and remove power from the server as described in [Shutting Down and Removing Power From the Server, on page 31](#). Disconnect power cords from all power supplies.

**Step 4** Slide the server out the front of the rack far enough so that you can remove the top cover. You might have to detach cables from the rear panel to provide clearance.

**Caution** If you cannot safely view and access the component, remove the server from the rack.

**Step 5** Remove the top cover from the server as described in [Removing the Server Top Cover, on page 33](#).

**Step 6** Install a two-pin jumper across J38 pins 11 and 12.

**Step 7** Reconnect AC power cords to the server. The server powers up to standby power mode.

**Step 8** Insert the USB thumb drive that you prepared in Step 2 into a USB port on the server.

**Step 9** Return the server to main power mode by pressing the Power button on the front panel.

The server boots with the updated BIOS boot block. When the BIOS detects a valid bios.cap file on the USB drive, it displays this message:

```
Found a valid recovery file...Transferring to Cisco IMC
System would flash the BIOS image now...
System would restart with recovered image after a few seconds...
```

**Step 10** Wait for server to complete the BIOS update, and then remove the USB drive from the server.

**Note** During the BIOS update, Cisco IMC shuts down the server and the screen goes blank for about 10 minutes. Do not unplug the power cords during this update. Cisco IMC powers on the server after the update is complete.

**Step 11** After the server has fully booted, power off the server again and disconnect all power cords.

**Step 12** Remove the jumper that you installed.

**Note** If you do not remove the jumper, after recovery completion you see the prompt, "Please remove the recovery jumper."

**Step 13** Replace the top cover, replace the server in the rack, replace power cords and any other cables, and then power on the server by pressing the Power button.

## Using the Clear Password Header (J38, Pins 13 - 14)

You can use this switch to clear the administrator password.

**Step 1** Shut down and remove power from the server as described in [Shutting Down and Removing Power From the Server, on page 31](#). Disconnect power cords from all power supplies.

**Step 2** Slide the server out the front of the rack far enough so that you can remove the top cover. You might have to detach cables from the rear panel to provide clearance.

**Caution** If you cannot safely view and access the component, remove the server from the rack.

- Step 3** Remove the top cover from the server as described in [Removing the Server Top Cover, on page 33](#).
- Step 4** Install a two-pin jumper across J38 pins 13 and 14.
- Step 5** Reinstall the top cover and reconnect AC power cords to the server. The server powers up to standby power mode, indicated when the Power LED on the front panel is amber.
- Step 6** Return the server to main power mode by pressing the Power button on the front panel. The server is in main power mode when the Power LED is green.
- Note** You must allow the entire server to reboot to main power mode to complete the reset. The state of the jumper cannot be determined without the host CPU running.
- Step 7** Press the Power button to shut down the server to standby power mode, and then remove AC power cords from the server to remove all power.
- Step 8** Remove the top cover from the server.
- Step 9** Remove the jumper that you installed.
- Note** If you do not remove the jumper, the password is cleared every time you power-cycle the server.
- Step 10** Replace the top cover, replace the server in the rack, replace power cords and any other cables, and then power on the server by pressing the Power button.

## Using the Boot Alternate Cisco IMC Image Header (J39, Pins 1 - 2)

You can use this Cisco IMC debug header to force the system to boot from an alternate Cisco IMC image.

- Step 1** Shut down and remove power from the server as described in [Shutting Down and Removing Power From the Server, on page 31](#). Disconnect power cords from all power supplies.
- Step 2** Slide the server out the front of the rack far enough so that you can remove the top cover. You might have to detach cables from the rear panel to provide clearance.
- Caution** If you cannot safely view and access the component, remove the server from the rack.
- Step 3** Remove the top cover from the server as described in [Removing the Server Top Cover, on page 33](#).
- Step 4** Install a two-pin jumper across J39 pins 1 and 2.
- Step 5** Reinstall the top cover and reconnect AC power cords to the server. The server powers up to standby power mode, indicated when the Power LED on the front panel is amber.
- Step 6** Return the server to main power mode by pressing the Power button on the front panel. The server is in main power mode when the Power LED is green.
- Note** When you next log in to Cisco IMC, you see a message similar to the following:
- ```
'Boot from alternate image' debug functionality is enabled.
CIMC will boot from alternate image on next reboot or input power cycle.
```
- Note** If you do not remove the jumper, the server will boot from an alternate Cisco IMC image every time that you power cycle the server or reboot Cisco IMC.
- Step 7** To remove the jumper, press the Power button to shut down the server to standby power mode, and then remove AC power cords from the server to remove all power.
- Step 8** Remove the top cover from the server.

- Step 9** Remove the jumper that you installed.
- Step 10** Replace the top cover, replace the server in the rack, replace power cords and any other cables, and then power on the server by pressing the Power button.

Using the Reset Cisco IMC Password to Default Header (J39, Pins 3 - 4)

You can use this Cisco IMC debug header to force the Cisco IMC password back to the default.

- Step 1** Shut down and remove power from the server as described in [Shutting Down and Removing Power From the Server, on page 31](#). Disconnect power cords from all power supplies.
- Step 2** Slide the server out the front of the rack far enough so that you can remove the top cover. You might have to detach cables from the rear panel to provide clearance.
- Caution** If you cannot safely view and access the component, remove the server from the rack.
- Step 3** Remove the top cover from the server as described in [Removing the Server Top Cover, on page 33](#).
- Step 4** Install a two-pin jumper across J39 pins 3 and 4.
- Step 5** Reinstall the top cover and reconnect AC power cords to the server. The server powers up to standby power mode, indicated when the Power LED on the front panel is amber.
- Step 6** Return the server to main power mode by pressing the Power button on the front panel. The server is in main power mode when the Power LED is green.
- Note** When you next log in to Cisco IMC, you see a message similar to the following:
- ```
'Reset to default CIMC password' debug functionality is enabled.
On input power cycle, CIMC password will be reset to defaults.
```
- Note** If you do not remove the jumper, the server will reset the Cisco IMC password to the default every time that you power cycle the server. The jumper has no effect if you reboot Cisco IMC.
- Step 7** To remove the jumper, press the Power button to shut down the server to standby power mode, and then remove AC power cords from the server to remove all power.
- Step 8** Remove the top cover from the server.
- Step 9** Remove the jumper that you installed.
- Step 10** Replace the top cover, replace the server in the rack, replace power cords and any other cables, and then power on the server by pressing the Power button.

## Using the Reset Cisco IMC to Defaults Header (J39, Pins 5 - 6)

You can use this Cisco IMC debug header to force the Cisco IMC settings back to the defaults.

- Step 1** Shut down and remove power from the server as described in [Shutting Down and Removing Power From the Server, on page 31](#). Disconnect power cords from all power supplies.
- Step 2** Slide the server out the front of the rack far enough so that you can remove the top cover. You might have to detach cables from the rear panel to provide clearance.

**Caution** If you cannot safely view and access the component, remove the server from the rack.

- Step 3** Remove the top cover from the server as described in [Removing the Server Top Cover, on page 33](#).
- Step 4** Install a two-pin jumper across J39 pins 5 and 6.
- Step 5** Reinstall the top cover and reconnect AC power cords to the server. The server powers up to standby power mode, indicated when the Power LED on the front panel is amber.
- Step 6** Return the server to main power mode by pressing the Power button on the front panel. The server is in main power mode when the Power LED is green.
- Note** When you next log in to Cisco IMC, you see a message similar to the following:
- ```
'CIMC reset to factory defaults' debug functionality is enabled.
On input power cycle, CIMC will be reset to factory defaults.
```
- Note** If you do not remove the jumper, the server will reset the Cisco IMC to the default settings every time that you power cycle the server. The jumper has no effect if you reboot Cisco IMC.
- Step 7** To remove the jumper, press the Power button to shut down the server to standby power mode, and then remove AC power cords from the server to remove all power.
- Step 8** Remove the top cover from the server.
- Step 9** Remove the jumper that you installed.
- Step 10** Replace the top cover, replace the server in the rack, replace power cords and any other cables, and then power on the server by pressing the Power button.

Recycling the PCB Assembly (PCBA)

The PCBA is secured to the server by external and internal screws. Additional parts must be removed to expose the mounting screws that connect the PCBA to its sheet metal tray. You must disconnect the PCBA from the tray before recycling the PCBA. The PCBA is secured by M3.5x0.6mm screws.

Before you begin

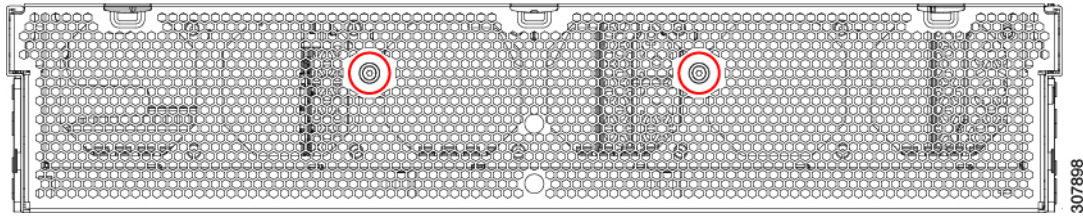


Note **For Recyclers Only!** This procedure is not a standard field-service option. This procedure is for recyclers who will be reclaiming the electronics for proper disposal to comply with local eco design and e-waste regulations.

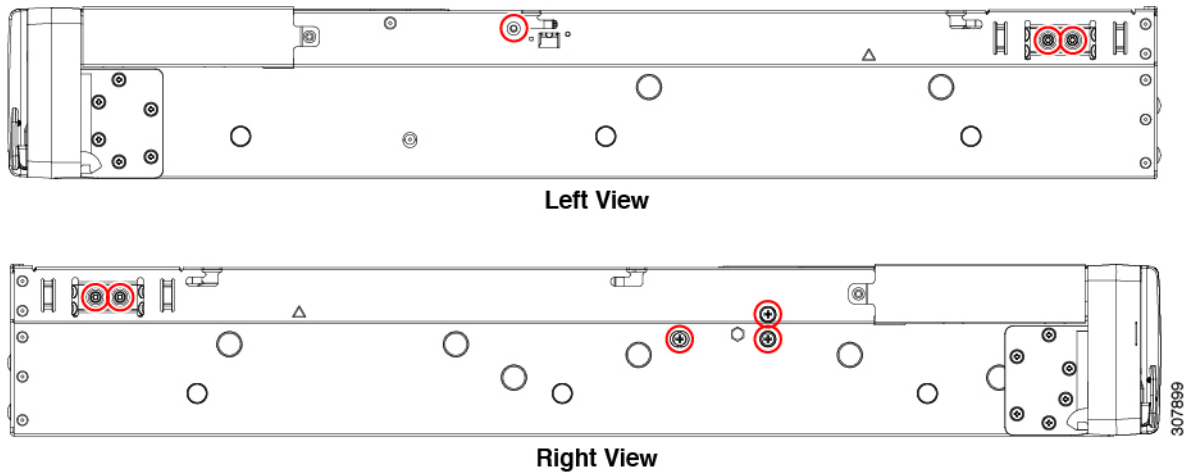
To remove the printed circuit board assembly (PCBA), the following requirements must be met:

- The server must be disconnected from facility power.
- The server must be removed from the equipment rack.
- The server's top cover must be removed. See [Removing the Server Top Cover, on page 33](#).

- Step 1** Remove the external screws.
- a) Using a screwdriver, remove the face plate screws.

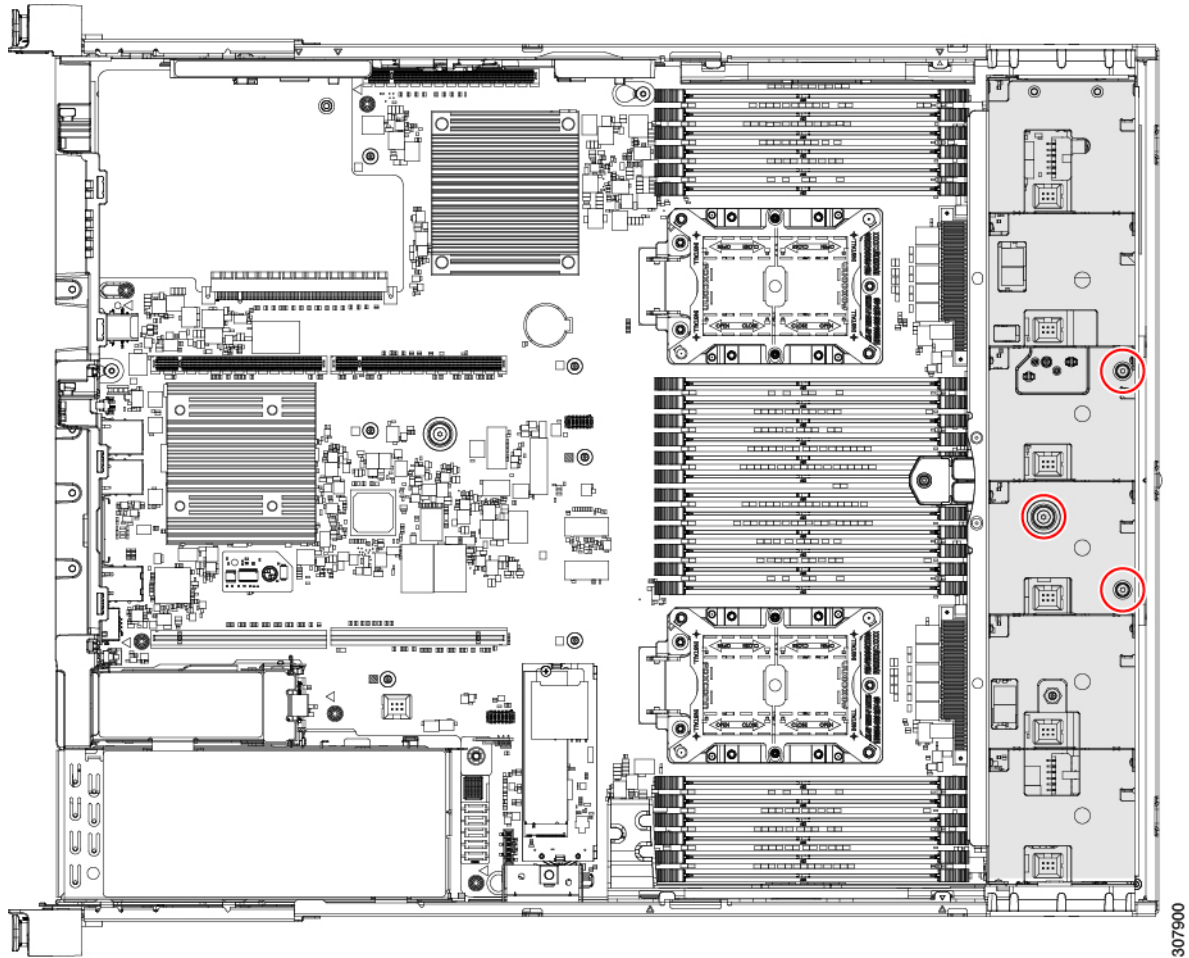
Figure 45: Location of PCBA Faceplate Screws

- b) Using a screwdriver, remove the screws from each side of the chassis.

Figure 46: Location of PCBA Chassis Screws

Step 2 Remove the fan cage screws.

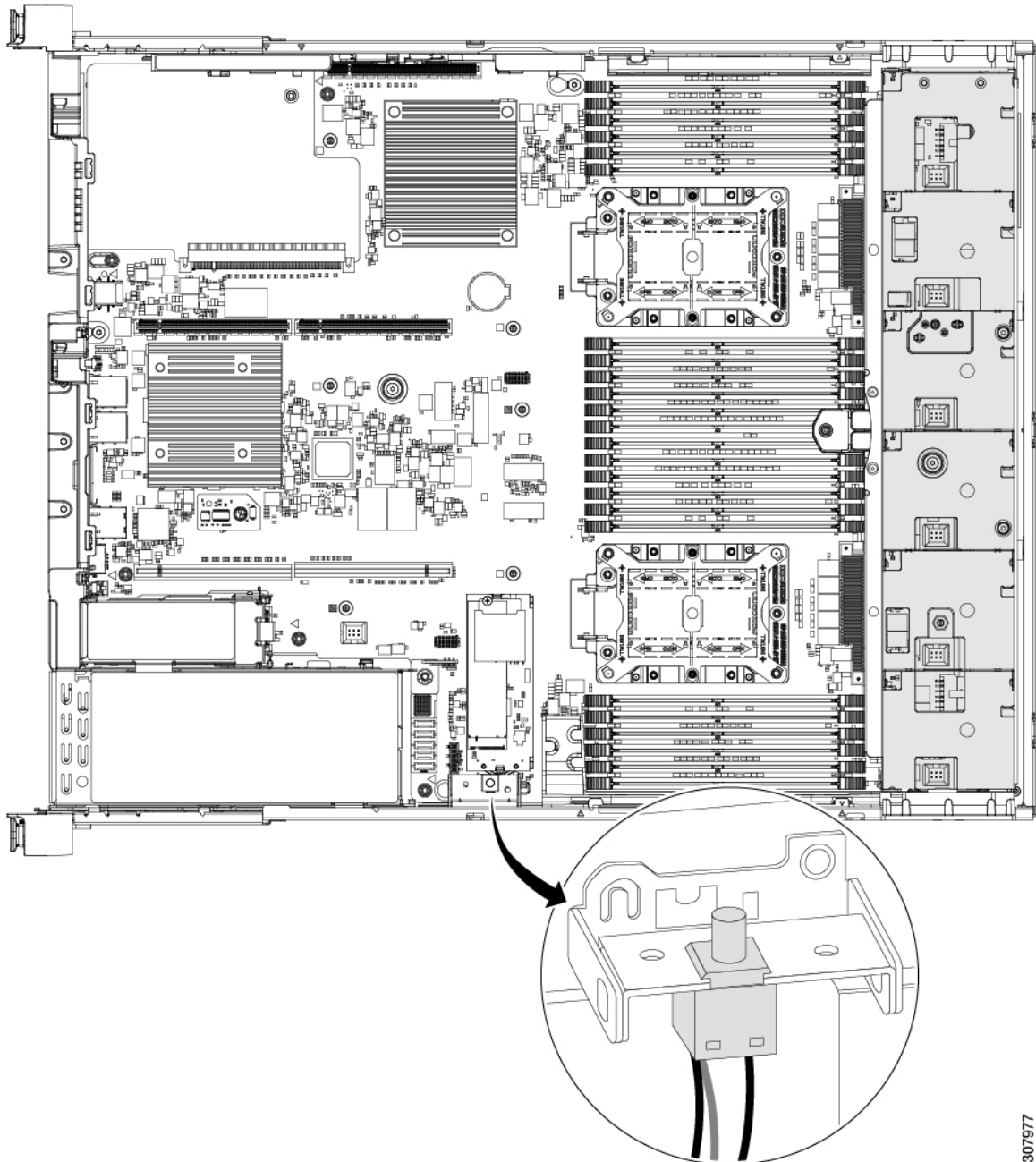
Figure 47: Location of Fan Cage Screws



Step 3 Grasp the Fan cage and remove it.

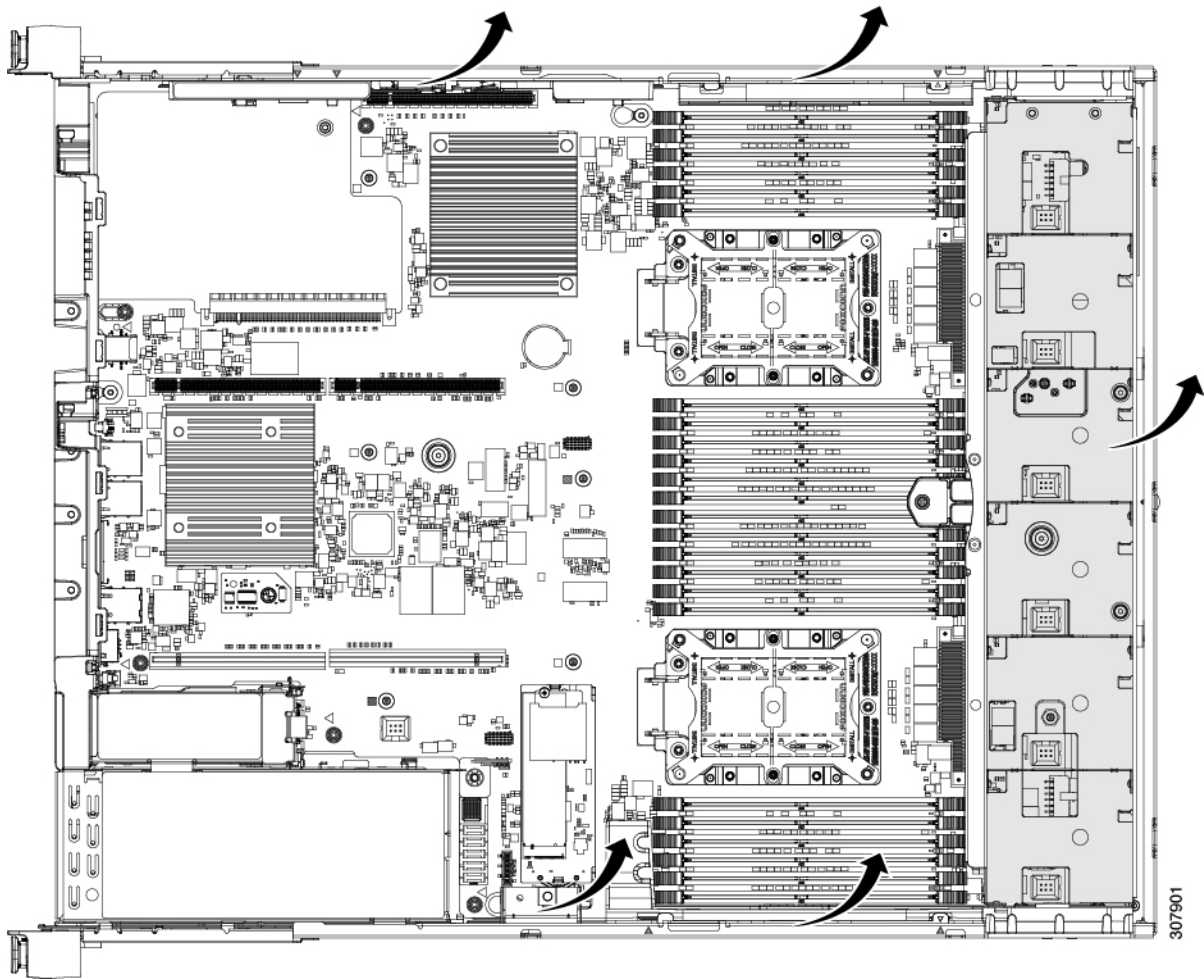
Step 4 Disconnect the intrusion protection switch (IPS), which is shown in the following figure.

- a) On the motherboard, break the IPS locking tab off the connector.
- b) Grasp the IPS cables and disconnect them from the motherboard.

Figure 48: Location of Intrusion Protection Switch

307977

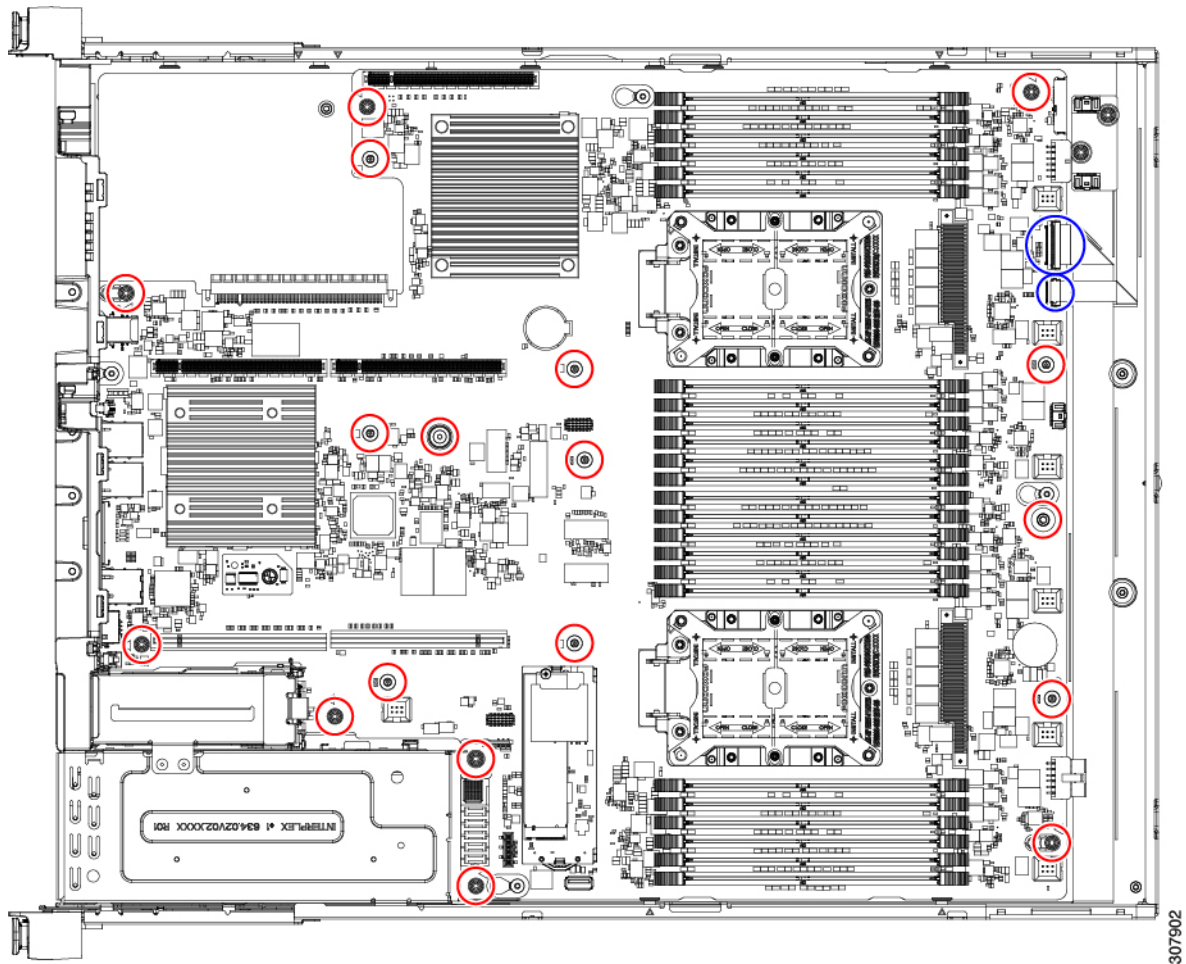
- Step 5** Continue removing the internal components.
- Grasp the cable holders and remove them.
 - Grasp the RAID card bracket and remove it.

Figure 49: Locations of Internal Components**Step 6**

Remove the PCBA.

- Grasp each of the ribbon cables and disconnect it.
- Using a screwdriver, remove all the PCBA mounting screws.
- Disconnect the PCBA from the sheet metal tray and dispose of the PCBA properly.

Figure 50: Locations of PCBA Cables and Mounting Screws





APPENDIX **A**

Server Specifications

- [Server Specifications, on page 115](#)
- [Power Cord Specifications, on page 118](#)

Server Specifications

This appendix lists the physical, environmental, and power specifications for the server.

- [Physical Specifications, on page 115](#)
- [Environmental Specifications, on page 115](#)
- [Power Specifications, on page 116](#)

Physical Specifications

The following table lists the physical specifications for the server versions.

Table 11: Physical Specifications

Description	Specification
Height	3.4 in. (86.4 mm)
Width	17.48 in. (443.9 mm)
Depth (length)	Server only: 21.16 in. (537.5 mm) Server with slide rail: 22.66 in (575.5 mm)
Maximum weight (fully loaded chassis)	40 lb. (18.0 Kg)

Environmental Specifications

The following table lists the environmental requirements and specifications for the server.

Table 12: Physical Specifications

Description	Specification
Temperature, Operating	<p>50 to 95°F (10 to 35°C)</p> <p>Extended environment 41 to 104°F (5 to 40°C)</p> <p>Derate the maximum temperature by 1°C per every 305 meters of altitude above sea level.</p> <p>Note Although the ASHRAE guidelines define multiple classes with different operating ranges, the <i>recommended</i> temperature and humidity operating range is the same for each class. The <i>recommended</i> temperature and humidity ranges are:</p> <ul style="list-style-type: none"> • Operating Temperature: 64.4°F to 80.6°F (18°C to 27°C) <p>For general information, see the Cisco Unified Computing System Site Planning Guide: Data Center Power and Cooling.</p>
Temperature, non-operating (when the server is stored or transported)	–40 to 149°F (–40 to 65°C)
Humidity (RH), operating	8 to 90%
Humidity (RH), non-operating (when the server is stored or transported)	5 to 93%
Altitude, operating	0 to 10,000 feet
Altitude, non-operating (when the server is stored or transported)	0 to 40,000 feet
Sound power level Measure A-weighted per ISO7779 LwAd (Bels) Operation at 73°F (23°C)	5.5
Sound pressure level Measure A-weighted per ISO7779 LpAm (dBA) Operation at 73°F (23°C)	40

Power Specifications



Note Do not mix power supply types or wattages in the server. Both power supplies must be identical.

You can get more specific power information for your exact server configuration by using the Cisco UCS Power Calculator:

<http://ucspowercalc.cisco.com>

The power specifications for the supported power supply options are listed in the following sections.

1050 W AC Power Supply

This section lists the specifications for each 1050 W AC power supply (Cisco part number UCSC-PSUF-1050W).

Table 13: 1050 W AC Specifications

Description	Specification
AC Input Voltage	Nominal range: 100–120 VAC, 200–240 VAC (Range: 90–132 VAC, 180–264 VAC)
AC Input Frequency	Nominal range: 50 to 60Hz (Range: 47–63 Hz)
Maximum AC Input current	12.5 A at 100 VAC 6.0 A at 208 VAC
Maximum input volt-amperes	1250 VA at 100 VAC
Maximum inrush current	15 A (sub-cycle duration)
Maximum hold-up time	12 ms at 1050 W
Maximum output power per PSU	800 W at 100–120 VAC 1050 W at 200–240 VAC
Power supply output voltage	12 VDC
Power supply standby voltage	12 VDC
Efficiency rating	Climate Savers Platinum Efficiency (80Plus Platinum certified)
Form factor	RSP2
Input connector	IEC320 C14

1050 W DC Power Supply

This section lists the specifications for each 1050 W DC power supply (Cisco part number UCSC-PSUF-1050WDC).

Table 14: 1050 W DC Specifications

Description	Specification
-------------	---------------

DC Input Voltage	Nominal range: -48 to -60 VDC (Range: -40 to -72 VDC)
Maximum DC input current	N32 A at -40 VDC
Maximum input wattage	1234 W
Maximum inrush current	35 A (sub-cycle duration)
Maximum hold-up time	5 ms at 100% load (1050 W main and 36 W standby)
Maximum output power per PSU	1050 W on 12 VDC main power 36 W on 12 VDC standby power
Power supply output voltage	12 VDC
Power supply standby voltage	12 VDC
Efficiency rating	≥ 92% at 50% load
Form factor	RSP2
Input connector	Fixed 3-wire block

Power Cord Specifications

Each power supply in the server has a power cord. Standard power cords or jumper power cords are available for connection to the server. The shorter jumper power cords, for use in racks, are available as an optional alternative to the standard power cords.



Note Only the approved power cords or jumper power cords listed below are supported.

Table 15: Supported Power Cords

Description	Length (Feet)	Length (Meters)
CAB-48DC-40A-8AWG DC power cord, -48 VDC, 40 A, 8 AWG Three-socket Mini-Fit connector to three-wire	11.7	3.5
CAB-C13-C14-AC AC power cord, 10 A; C13 to C14, recessed receptacle	9.8	3.0
CAB-250V-10A-AR AC power cord, 250 V, 10 A Argentina	8.2	2.5

CAB-C13-C14-2M-JP AC Power Cord, C13 to C14 Japan PSE Mark	6.6	2.0
CAB-9K10A-EU AC Power Cord, 250 V, 10 A; CEE 7/7 Plug Europe	8.2	2.5
CAB-250V-10A-IS AC Power Cord, 250 V, 10 A Israel	8.2	2.5
CAB-250V-10A-CN AC power cord, 250 V, 10 A PR China	8.2	2.5
CAB-ACTW AC power cord, 250 V, 10 A Taiwan	7.5	2.3
CAB-C13-CBN AC cabinet jumper power cord, 250, 10 A, C13 to C14	2.2	0.68
CAB-C13-C14-2M AC cabinet jumper power cord, 250 V, 10 A, C13 to C14	6.6	2.0
CAB-9K10A-AU AC power cord, 250 V, 10 A, 3112 plug, Australia	8.2	2.5
CAB-N5K6A-NA AC power cord, 200/240 V, 6 A, North America	8.2	2.5
CAB-250V-10A-ID AC power Cord, 250 V, 10 A, India	8.2	2.5

CAB-9K10A-SW AC power cord, 250 V, 10 A, MP232 plug Switzerland	8.2	2.5
CAB-250V-10A-BR AC power Cord, 250 V, 10 A Brazil	8.2	2.5
CAB-9K10A-UK AC power cord, 250 V, 10 A (13 A fuse), BS1363 plug United Kingdom	8.2	2.5
CAB-9K12A-NA AC power cord, 125 V, 13 A, NEMA 5-15 plug North America	8.2	2.5
CAB-AC-L620-C13 AC power cord, NEMA L6-20 to C13 connectors	6.6	2.0
CAB-9K10A-IT AC power cord, 250 V, 10 A, CEI 23-16/VII plug Italy	8.2	2.5
R2XX-DMYMPWRCORD No power cord; PID option for ordering server with no power cord	NA	NA



APPENDIX **B**

Storage Controller Considerations

This appendix provides storage controller (RAID and HBA) information.

- [Supported Storage Controllers and Cables, on page 121](#)
- [Storage Controller Card Firmware Compatibility, on page 121](#)
- [Write-Cache Policy for Cisco 12G SAS Modular RAID Controllers, on page 122](#)
- [For More RAID Utility Information, on page 122](#)

Supported Storage Controllers and Cables

Cisco UCS C240 SD M5 server supports a single Cisco 12G SAS HBA (JBOD/Pass-through Mode) controller that plugs into a dedicated internal socket.



Note NVMe PCIe SSDs cannot be controlled by this RAID controller.

This server supports the RAID and HBA controller options and cable requirements shown in the following table.

Controller	Maximum Drives Controlled	RAID Levels	Optional Supercap Backup?	Required Cables
Cisco 12G Modular SAS HBA UCSC-SAS-M5	Includes 2-GB cache; controls up to 16 drives.	Non-RAID JBOD mode is also supported.	No	Factory-installed in the dedicated internal slot

Storage Controller Card Firmware Compatibility

Firmware on the storage controller (RAID or HBA) must be verified for compatibility with the current Cisco IMC and BIOS versions that are installed on the server. If not compatible, upgrade or downgrade the storage controller firmware using the Host Upgrade Utility (HUU) for your firmware release to bring it to a compatible level.



Note For servers running in standalone mode only: After you replace controller hardware (UCSC-SAS-M5) you must run the Cisco UCS Host Upgrade Utility (HUU) to update the controller firmware, even if the firmware Current Version is the same as the Update Version. This is necessary to program the controller's suboem-id to the correct value for the server SKU. If you do not do this, drive enumeration might not display correctly in the software. This issue does not affect servers controlled in UCSM mode.

See the HUU guide for your Cisco IMC release for instructions on downloading and using the utility to bring server components to compatible levels: [HUU Guides](#).

Write-Cache Policy for Cisco 12G SAS Modular RAID Controllers

For this server and other Cisco Generation M5 servers, the default write-cache policy for the Cisco Modular RAID controllers is *Write Through* (irrespective of the presence of a charged supercap or “good BBU”). This utilizes the optimal performance characteristics of the controller.

The write policy can be set to *Write Back*, if preferred. You can set the write policy using the following methods:

- For standalone servers, use the Cisco IMC interface to set Virtual Drive Properties > Write Policy. See the “Managing Storage Adapters” section in your Cisco IMC Configuration Guide.

[Cisco IMC GUI and CLI Configuration Guides](#)

- For Cisco UCS-integrated servers, use the Cisco UCS Manager interface to set the write-cache policy as part of virtual drive configuration in your storage profile.

[Cisco UCS Manager Configuration Guides](#)

- Use the LSI Option ROM Configuration Utility.

For More RAID Utility Information

The Broadcom utilities have help documentation for more information about using the utilities.

- For basic information about RAID and for using the utilities for the RAID controller cards that are supported in Cisco servers, see the [Cisco UCS Servers RAID Guide](#).
- For hardware SAS MegaRAID configuration—[Broadcom 12Gb/s MegaRAID SAS Software User Guide, Version 2.8](#)
- For embedded software MegaRAID and the utility that is accessed via the server BIOS (refer to Chapter 4)—[Broadcom Embedded MegaRAID Software User Guide, March 2018](#).



APPENDIX C

GPU Card Installation

This appendix contains configuration rules and installation procedures for the supported GPU cards.

- [Server Firmware Requirements, on page 123](#)
- [GPU Card Configuration Rules, on page 123](#)
- [Requirement For All GPUs: Memory-Mapped I/O Greater Than 4 GB, on page 124](#)
- [Installing a GPU Card, on page 125](#)
- [Using NVIDIA GRID License Server For T-Series GPUs, on page 128](#)
- [Installing Drivers to Support the GPU Cards, on page 135](#)

Server Firmware Requirements

The following table lists the minimum server firmware versions for the supported GPU cards.

GPU Card	Cisco IMC/BIOS Minimum Version Required
Nvidia T4 PCIe 16GB 70W	4.1(2a)

GPU Card Configuration Rules

Note the following rules when populating a server with GPU cards.

- Use the UCS power calculator at the following link to determine the power needed based on your server configuration: <http://ucspowercalc.cisco.com>
- Up to two double-wide GPU cards are supported in PCIe riser 1, slot 2 and in PCIe riser 2, slot 5.



Note Double-wide GPU cards are not supported in all PCIe riser options. Double-wide GPU cards are supported only in the following riser options:

- PCIe riser 1 (UCSC-RIS-1-240M5)
- PCIe riser 2B (UCSC-RIS-2B-240M5)

- A double-wide GPU card installed in slot 2 also covers slot 4; a double wide GPU card installed in slot 5 also covers slot 6.
- NVIDIA T4:

Observe the following PCIe slot usage in Riser 1/2B and Riser 1C/2E combinations:

Riser Combinations	Riser Slots Available for GPUs	
	Single CPU	Two CPUs
Riser 1 and 2B	Slot 2	Slot 2 and 5
Riser 1C and 2E	Slot 1	Slots 1 and 2

- You can install a GPU card and a Cisco UCS VIC in the same riser. When you install a GPU card in slot 2, NCSI support in riser 1 automatically moves to slot 1. When you install a GPU card in slot 5, NCSI support in riser 2 automatically moves to slot 4.
- NVIDIA T-Seires GPUs can support 1 TB or more memory in the server.

Requirement For All GPUs: Memory-Mapped I/O Greater Than 4 GB

All supported GPU cards require enablement of the BIOS setting that allows greater than 4 GB of memory-mapped I/O (MMIO).

- Standalone Server: If the server is used in standalone mode, this BIOS setting is enabled by default:

Advanced > PCI Configuration > Memory Mapped I/O Above 4 GB [Enabled]

If you need to change this setting, enter the BIOS Setup Utility by pressing **F2** when prompted during bootup.

- If the server is integrated with Cisco UCS Manager and is controlled by a service profile, this setting is enabled by default in the service profile when a GPU is present.

To change this setting manually, use the following procedure.

Step 1 Refer to the Cisco UCS Manager configuration guide (GUI or CLI) for your release for instructions on configuring service profiles:

[Cisco UCS Manager Configuration Guides](#)

Step 2 Refer to the chapter on Configuring Server-Related Policies > Configuring BIOS Settings.

Step 3 In the section of your profile for PCI Configuration BIOS Settings, set `Memory Mapped IO Above 4GB Config` to one of the following:

- **Disabled**—Does not map 64-bit PCI devices to 64 GB or greater address space.
- **Enabled**—Maps I/O of 64-bit PCI devices to 64 GB or greater address space.

- **Platform Default**—The policy uses the value for this attribute contained in the BIOS defaults for the server. Use this only if you know that the server BIOS is set to use the default enabled setting for this item.

Step 4 Reboot the server.

Note Cisco UCS Manager pushes BIOS configuration changes through a BIOS policy or default BIOS settings to the Cisco Integrated Management Controller (CIMC) buffer. These changes remain in the buffer and do not take effect until the server is rebooted.

Installing a GPU Card

Use the following procedure to install or replace the following supported GPU card:

- Nvidia T4 PCIe 16GB 70W

Table 16: Cisco UCS C240 SD M5 Operating Temperature Requirements For GPU Card

GPU Card	Maximum Server Operating Temperature (Air Inlet Temperature)
Nvidia T4 PCIe 16GB 70W	35° C (95.0° F)



Note **For NVIDIA GPUs:** The NVIDIA GPU card might be shipped with two power cables: a straight cable and a Y-cable. The straight cable is used for connecting power to the GPU card in this server; do not use the Y-cable, which is used for connecting the GPU card in external devices only (such as the Magma chassis).

In the table below, the cable that is used with the GPU is listed. It is also indicated whether the cable is included in the GPU BOM or must be ordered separately.

- Separate = Cable must be ordered separately when the ordering tool prompts you.
- Included = Cable is included with the GPU; no additional action is needed.

Step 1 Shut down and remove power from the server as described in [Shutting Down and Removing Power From the Server, on page 31](#).

Step 2 Slide the server out the front of the rack far enough so that you can remove the top cover. You might have to detach cables from the rear panel to provide clearance.

Caution If you cannot safely view and access the component, remove the server from the rack.

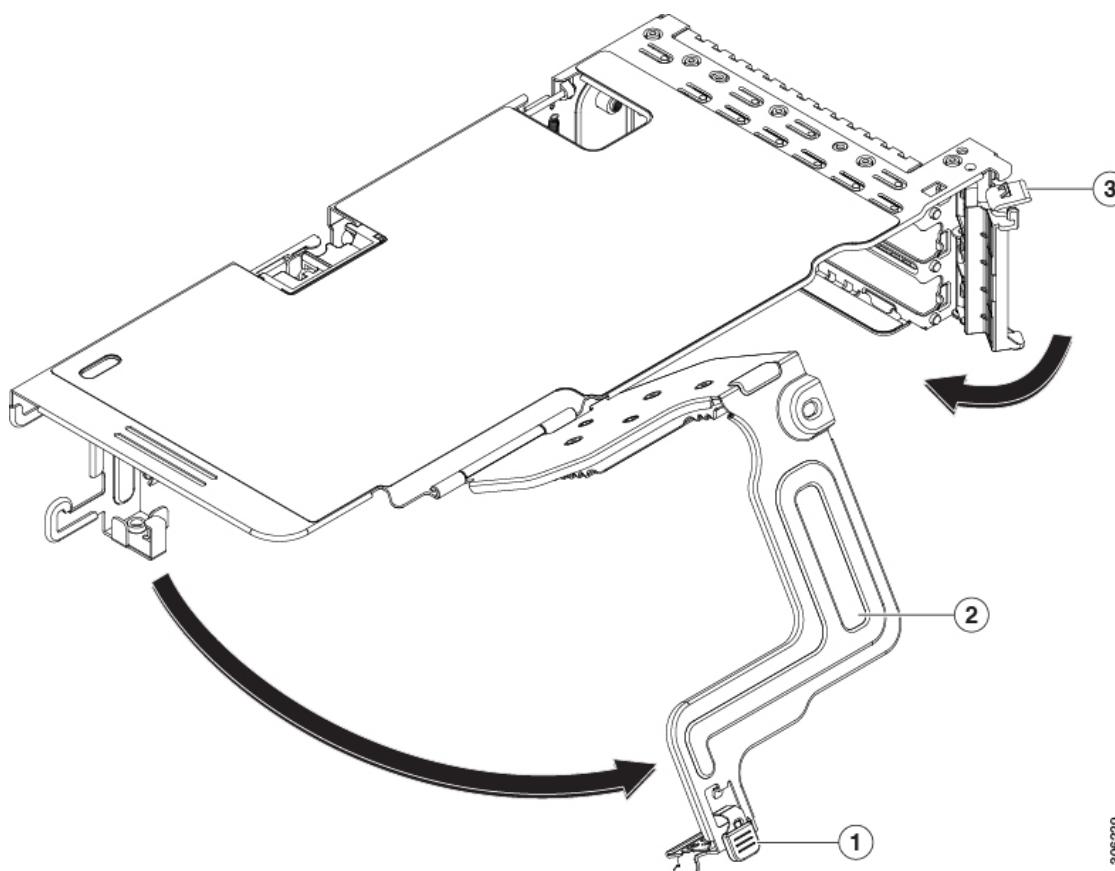
Step 3 Remove the top cover from the server as described in [Removing the Server Top Cover, on page 33](#).

Step 4 Remove an existing GPU card:

- Use two hands to grasp the metal bracket of the PCIe riser and lift straight up to disengage its connector from the socket on the motherboard. Set the riser on an antistatic surface.
- On the bottom of the riser, press down on the clip that holds the securing plate.

- c) Swing open the hinged securing plate to provide access.
- d) Open the hinged plastic retainer that secures the rear-panel tab of the card.
- e) Disconnect the GPU card's power cable from the power connector on the PCIe riser.
- f) Pull evenly on both ends of the GPU card to remove it from the socket on the PCIe riser.

Figure 51: PCIe Riser Card Securing Mechanisms



Release latch on hinged securing plate	Hinged card-tab retainer
Hinged securing plate	-

Step 5 Install a new GPU card:

Note Observe the configuration rules for this server, as described in [GPU Card Configuration Rules](#), on page 123.

- a) Align the GPU card with the socket on the riser, and then gently push the card's edge connector into the socket. Press evenly on both corners of the card to avoid damaging the connector.
- b) Connect the GPU power cable. The straight power cable connectors are color-coded. Connect the cable's black connector into the black connector on the GPU card and the cable's white connector into the white GPU POWER connector on the PCIe riser.

Caution Do not reverse the straight power cable. Connect the *black* connector on the cable to the *black* connector on the GPU card. Connect the *white* connector on the cable to the *white* connector on the PCIe riser.

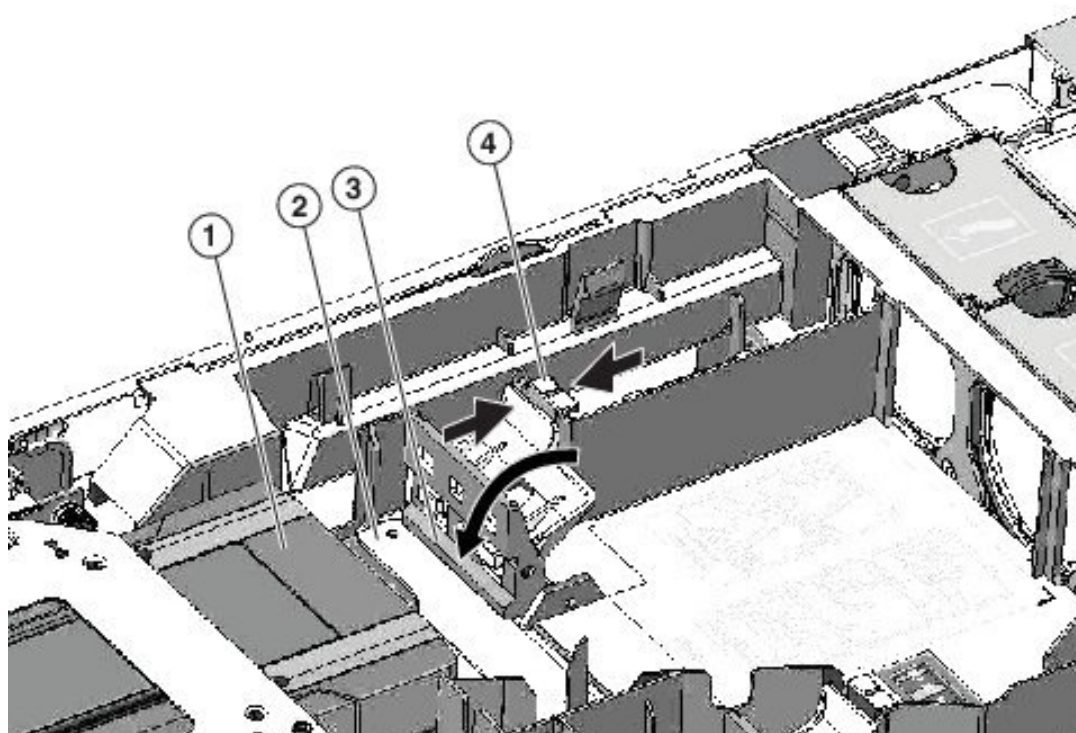
- c) Close the card-tab retainer over the end of the card.
- d) Swing the hinged securing plate closed on the bottom of the riser. Ensure that the clip on the plate clicks into the locked position.
- e) Position the PCIe riser over its socket on the motherboard and over the chassis alignment channels.
- f) Carefully push down on both ends of the PCIe riser to fully engage its connector with the sockets on the motherboard.

At the same time, align the GPU front support bracket (on the front end of the GPU card) with the securing latch that is on the server's air baffle.

Step 6 Insert the GPU front support bracket into the latch that is on the air baffle:

- a) Pinch the latch release tab and hinge the latch toward the front of the server.
- b) Hinge the latch back down so that its lip closes over the edge of the GPU front support bracket.
- c) Ensure that the latch release tab clicks and locks the latch in place.

Figure 52: GPU Front Support Bracket Inserted to Securing latch on Air Baffle



Front end of GPU card	Lip on securing latch
GPU front support bracket	Securing latch release tab

Step 7 Replace the top cover to the server.

Step 8 Replace the server in the rack, replace cables, and then fully power on the server by pressing the Power button.

Step 9 Optional: Continue with [Installing Drivers to Support the GPU Cards](#), on page 135.

Note NVIDIA offers GRID features for few cards. You must install the GRID licenses to use the GRID features. See [Using NVIDIA GRID License Server For T-Series GPUs, on page 128](#).

Using NVIDIA GRID License Server For T-Series GPUs

This section applies to NVIDIA Tesla T-Series GPUs.

Use the topics in this section in the following order when obtaining and using NVIDIA GRID licenses.

1. Familiarize yourself with the NVIDIA GRID License Server.

[NVIDIA GRID License Server Overview, on page 128](#)

2. Register your product activation keys with NVIDIA.

[Registering Your Product Activation Keys With NVIDIA, on page 129](#)

3. Download the GRID software suite.

[Downloading the GRID Software Suite, on page 130](#)

4. Install the GRID License Server software to a host.

[Installing NVIDIA GRID License Server Software, on page 130](#)

5. Generate licenses on the NVIDIA Licensing Portal and download them.

[Installing GRID Licenses From the NVIDIA Licensing Portal to the License Server, on page 132](#)

6. Manage your GRID licenses.

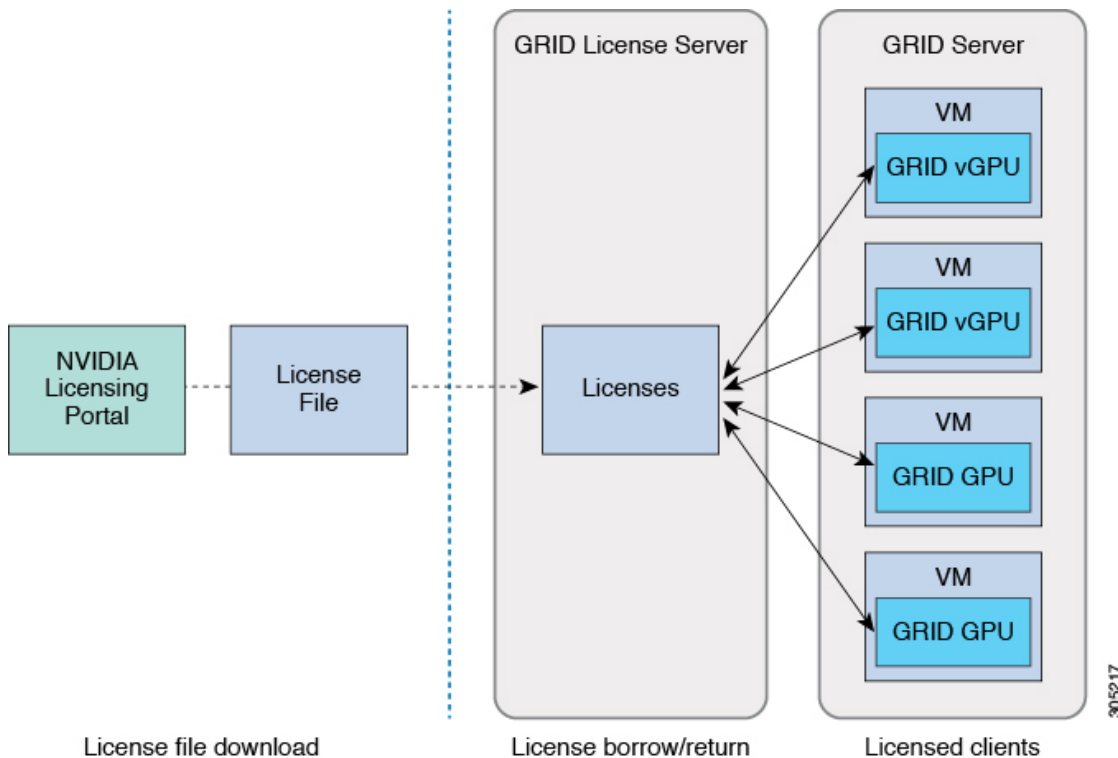
[Managing GRID Licenses , on page 133](#)

NVIDIA GRID License Server Overview

The NVIDIA M-Series GPUs combine Tesla and GRID functionality when the licensed GRID features such as GRID vGPU and GRID Virtual Workstation are enabled. These features are enabled during OS boot by borrowing a software license that is served over the network from the NVIDIA GRID License Server virtual appliance. The license is returned to the license server when the OS shuts down.

You obtain the licenses that are served by the GRID License Server from NVIDIA's Licensing Portal as downloadable license files, which you install into the GRID License Server via its management interface.

Figure 53: NVIDIA GRID Licensing Architecture



There are three editions of GRID licenses, which enable three different classes of GRID features. The GRID software automatically selects the license edition based on the features that you are using.

GRID License Edition	GRID Feature
GRID Virtual GPU (vGPU)	Virtual GPUs for business desktop computing
GRID Virtual Workstation	Virtual GPUs for midrange workstation computing
GRID Virtual Workstation – Extended	Virtual GPUs for high-end workstation computing Workstation graphics on GPU pass-through

Registering Your Product Activation Keys With NVIDIA

After your order is processed, NVIDIA sends you a Welcome email that contains your product activation keys (PAKs) and a list of the types and quantities of licenses that you purchased.

-
- Step 1** Select the **Log In** link, or the **Register** link if you do not already have an account.
The NVIDIA Software Licensing Center > License Key Registration dialog opens.
- Step 2** Complete the License Key Registration form and then click **Submit My Registration Information**.
The NVIDIA Software Licensing Center > Product Information Software dialog opens.

- Step 3** If you have additional PAKs, click **Register Additional Keys**. For each additional key, complete the form on the License Key Registration dialog and then click **Submit My Registration Information**.
- Step 4** Agree to the terms and conditions and set a password when prompted.
-

Downloading the GRID Software Suite

- Step 1** Return to the NVIDIA Software Licensing Center > Product Information Software dialog.
- Step 2** Click the **Current Releases** tab.
- Step 3** Click the **NVIDIA GRID** link to access the Product Download dialog. This dialog includes download links for:
- NVIDIA License Manager software
 - The gpumodeswitch utility
 - The host driver software
- Step 4** Use the links to download the software.
-

Installing NVIDIA GRID License Server Software

For full installation instructions and troubleshooting, refer to the *NVIDIA GRID License Server User Guide*. Also refer to the *NVIDIA GRID License Server Release Notes* for the latest information about your release.

<http://www.nvidia.com>

Platform Requirements for NVIDIA GRID License Server

- The hosting platform can be a physical or a virtual machine. NVIDIA recommends using a host that is dedicated only to running the License Server.
- The hosting platform must run a supported Windows OS.
- The hosting platform must have a constant IP address.
- The hosting platform must have at least one constant Ethernet MAC address.
- The hosting platform's date and time must be set accurately.

Installing GRID License Server on Windows

The License Server requires a Java runtime environment and an Apache Tomcat installation. Apache Tomcat is installed when you use the NVIDIA installation wizard for Windows.

- Step 1** Download and install the latest Java 32-bit runtime environment from <https://www.oracle.com/downloads/index.html>.
- Note** Install the 32-bit Java Runtime Environment, regardless of whether your platform is Windows 32-bit or 64-bit.

- Step 2** Create a server interface:
- On the NVIDIA Software Licensing Center dialog, click **Grid Licensing > Create License Server**.
 - On the Create Server dialog, fill in your desired server details.
 - Save the .bin file that is generated onto your license server for installation.
- Step 3** Unzip the NVIDIA License Server installer Zip file that you downloaded previously and run setup.exe.
- Step 4** Accept the EULA for the NVIDIA License Server software and the Apache Tomcat software. Tomcat is installed automatically during the License Server installation.
- Step 5** Use the installer wizard to step through the installation.
- Note** On the Choose Firewall Options dialog, select the ports to be opened in the firewall. NVIDIA recommends that you use the default setting, which opens port 7070 but leaves port 8080 closed.
- Step 6** Verify the installation. Open a web browser on the License Server host and connect to the URL <http://localhost:8080/licserver>. If the installation was successful, you see the NVIDIA License Client Manager interface.
-

Installing GRID License Server on Linux

The License Server requires a Java runtime environment and an Apache Tomcat installation. You must install both separately before installing the License Server on Linux.

- Step 1** Verify that Java was installed with your Linux installation. Use the following command:
- ```
java -version
```
- If no Java version is displayed, use your Linux package manager to install with the following command:
- ```
sudo yum install java
```
- Step 2** Use your Linux package manager to install the tomcat and tomcat-webapps packages:
- Use the following command to install Tomcat:

```
sudo yum install tomcat
```
 - Enable the Tomcat service for automatic startup on boot:

```
sudo systemctl enable tomcat.service
```
 - Start the Tomcat service:

```
sudo systemctl start tomcat.service
```
 - Verify that the Tomcat service is operational. Open a web browser on the License Server host and connect to the URL <http://localhost:8080>. If the installation was successful, you see the Tomcat webapp.
- Step 3** Install the License Server:
- Unpack the License Server tar file using the following command:

```
tar xzf NVIDIA-linux-2015.09-0001.tgz
```
 - Run the unpacked setup binary as root:

```
sudo ./setup.bin
```
 - Accept the EULA and then continue with the installation wizard to finish the installation.

Note On the Choose Firewall Options dialog, select the ports to be opened in the firewall. NVIDIA recommends that you use the default setting, which opens port 7070 but leaves port 8080 closed.

Step 4 Verify the installation. Open a web browser on the License Server host and connect to the URL <http://localhost:8080/licserver>. If the installation was successful, you see the NVIDIA License Client Manager interface.

Installing GRID Licenses From the NVIDIA Licensing Portal to the License Server

Accessing the GRID License Server Management Interface

Open a web browser on the License Server host and access the URL <http://localhost:8080/licserver>.

If you configured the License Server host's firewall to permit remote access to the License Server, the management interface is accessible from remote machines at the URL <http://hostname:8080/licserver>

Reading Your License Server's MAC Address

Your License Server's Ethernet MAC address is used as an identifier when registering the License Server with NVIDIA's Licensing Portal.

Step 1 Access the GRID License Server Management Interface in a browser.

Step 2 In the left-side License Server panel, select **Configuration**.

The License Server Configuration panel opens. Next to **Server host ID**, a pull-down menu lists the possible Ethernet MAC addresses.

Step 3 Select your License Server's MAC address from the **Server host ID** pull-down.

Note It is important to use the same Ethernet ID consistently to identify the server when generating licenses on NVIDIA's Licensing Portal. NVIDIA recommends that you select one entry for a primary, non-removable Ethernet interface on the platform.

Installing Licenses From the Licensing Portal

Step 1 Access the GRID License Server Management Interface in a browser.

Step 2 In the left-side License Server panel, select **Configuration**.

The License Server Configuration panel opens.

Step 3 Use the License Server Configuration menu to install the .bin file that you generated earlier.

- Click **Choose File**.
- Browse to the license .bin file that you want to install and click **Open**.
- Click **Upload**.

The license file is installed on your License Server. When installation is complete, you see the confirmation message, “Successfully applied license file to license server.”

Viewing Available GRID Licenses

Use the following procedure to view which licenses are installed and available, along with their properties.

-
- Step 1** Access the GRID License Server Management Interface in a browser.
 - Step 2** In the left-side License Server panel, select **Licensed Feature Usage**.
 - Step 3** Click on a feature in the **Feature** column to see detailed information about the current usage of that feature.
-

Viewing Current License Usage

Use the following procedure to view information about which licenses are currently in-use and borrowed from the server.

-
- Step 1** Access the GRID License Server Management Interface in a browser.
 - Step 2** In the left-side License Server panel, select **Licensed Clients**.
 - Step 3** To view detailed information about a single licensed client, click on its **Client ID** in the list.
-

Managing GRID Licenses

Features that require GRID licensing run at reduced capability until a GRID license is acquired.

Acquiring a GRID License on Windows

-
- Step 1** Open the NVIDIA Control Panel using one of the following methods:
 - Right-click on the Windows desktop and select **NVIDIA Control Panel** from the menu.
 - Open Windows Control Panel and double-click the **NVIDIA Control Panel** icon.
 - Step 2** In the NVIDIA Control Panel left-pane under Licensing, select **Manage License**.

The Manage License task pane opens and shows the current license edition being used. The GRID software automatically selects the license edition based on the features that you are using. The default is Tesla (unlicensed).
 - Step 3** If you want to acquire a license for GRID Virtual Workstation, under License Edition, select **GRID Virtual Workstation**.
 - Step 4** In the **License Server** field, enter the address of your local GRID License Server. The address can be a domain name or an IP address.
 - Step 5** In the **Port Number** field, enter your port number or leave it set to the default used by the server, which is 7070.
 - Step 6** Select **Apply**.

The system requests the appropriate license edition from your configured License Server. After a license is successfully acquired, the features of that license edition are enabled.

Note After you configure licensing settings in the NVIDIA Control Panel, the settings persist across reboots.

Acquiring a GRID License on Linux

Step 1 Edit the configuration file `/etc/nvidia/gridd.conf`:

```
sudo vi /etc/nvidia/gridd.conf
```

Step 2 Edit the `ServerUrl` line with the address of your local GRID License Server.

The address can be a domain name or an IP address. See the example file below.

Step 3 Append the port number (default 7070) to the end of the address with a colon. See the example file below.

Step 4 Edit the `FeatureType` line with the integer for the license type. See the example file below.

- GRID vGPU = 1
- GRID Virtual Workstation = 2

Step 5 Restart the `nvidia-gridd` service.

```
sudo service nvidia-gridd restart
```

The service automatically acquires the license edition that you specified in the `FeatureType` line. You can confirm this in `/var/log/messages`.

Note After you configure licensing settings in the NVIDIA Control Panel, the settings persist across reboots.

Sample configuration file:

```
# /etc/nvidia/gridd.conf - Configuration file for NVIDIA Grid Daemon
# Description: Set License Server URL
# Data type: string
# Format: "<address>:<port>"
ServerUrl=10.31.20.45:7070

# Description: Set Feature to be enabled
# Data type: integer
# Possible values:
# 1 => for GRID vGPU
# 2 => for GRID Virtual Workstation
FeatureType=2
```

Using gpumodeswitch

The command line utility `gpumodeswitch` can be run in the following environments:

- Windows 64-bit command prompt (requires administrator permissions)

- Linux 32/64-bit shell (including Citrix XenServer dom0) (requires root permissions)



Note Consult NVIDIA product release notes for the latest information on compatibility with compute and graphic modes.

The `gpumodeswitch` utility supports the following commands:

- `--listgpumodes`

Writes information to a log file named `listgpumodes.txt` in the current working directory.

- `--gpumode graphics`

Switches to graphics mode. Switches mode of all supported GPUs in the server unless you specify otherwise when prompted.

- `--gpumode compute`

Switches to compute mode. Switches mode of all supported GPUs in the server unless you specify otherwise when prompted.



Note After you switch GPU mode, reboot the server to ensure that the modified resources of the GPU are correctly accounted for by any OS or hypervisor running on the server.

Installing Drivers to Support the GPU Cards

After you install the hardware, you must update to the correct level of server BIOS and then install GPU drivers and other software in this order:

1. Update the server BIOS.
2. Update the GPU drivers.

1. Updating the Server BIOS

Install the latest Cisco UCS C240 M4 server BIOS by using the Host Upgrade Utility for the Cisco UCS C240 M4 server.



Note You must do this procedure before you update the NVIDIA drivers.

Step 1 Navigate to the following URL: <http://www.cisco.com/cisco/software/navigator.html>.

Step 2 Click **Servers–Unified Computing** in the middle column.

Step 3 Click **Cisco UCS C-Series Rack-Mount Standalone Server Software** in the right-hand column.

- Step 4** Click the name of your model of server in the right-hand column.
- Step 5** Click **Unified Computing System (UCS) Server Firmware**.
- Step 6** Click the release number.
- Step 7** Click **Download Now** to download the `ucs-server platform-huu-version_number.iso` file.
- Step 8** Verify the information on the next page, and then click **Proceed With Download**.
- Step 9** Continue through the subsequent screens to accept the license agreement and browse to a location where you want to save the file.
- Step 10** Use the Host Upgrade Utility to update the server BIOS.
- The user guides for the Host Upgrade Utility are at [Utility User Guides](#).
-

2. Updating the GPU Card Drivers

After you update the server BIOS, you can install GPU drivers to your hypervisor virtual machine.

- Step 1** Install your hypervisor software on a computer. Refer to your hypervisor documentation for the installation instructions.
- Step 2** Create a virtual machine in your hypervisor. Refer to your hypervisor documentation for instructions.
- Step 3** Install the GPU drivers to the virtual machine. Download the drivers from either:
- NVIDIA Enterprise Portal for GRID hypervisor downloads (requires NVIDIA login): <https://nvidia.flexnetoperations.com/>
 - NVIDIA public driver area: <http://www.nvidia.com/Download/index.aspx>
 - AMD: <http://support.amd.com/en-us/download>
- Step 4** Restart the server.
- Step 5** Check that the virtual machine is able to recognize the GPU card. In Windows, use the Device Manager and look under Display Adapters.
-



APPENDIX **D**

Installation For Cisco UCS Manager Integration

- [Installation For Cisco UCS Manager Integration, on page 137](#)

Installation For Cisco UCS Manager Integration

The Cisco UCS Manager integration instructions are in the integration guides found here:

[Cisco UCS C-Series Server Integration with UCS Manager Configuration Guides](#)

Refer to the guide that is for the version of Cisco UCS Manager that you are using.

Also refer to the release notes for Cisco UCS Manager software and C-Series Cisco IMC software for any special considerations regarding integration in your release.

- [Cisco UCS Manager Release Notes](#)
- [Cisco C-Series Software Release Notes](#)

