Cisco UCS C220 M5 Server Installation and Service Guide

First Published: 2017-07-14

Last Modified: 2022-04-20

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

Preface

This preface contains the following topics:

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.

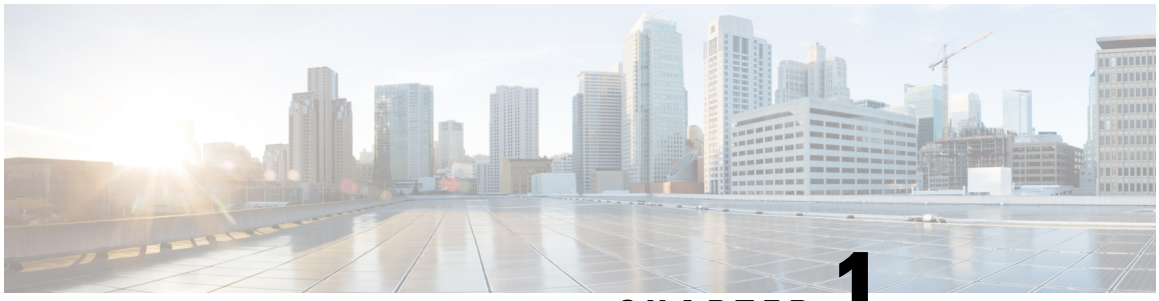
Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective 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

The server is orderable in different versions, each with a different front panel/drive-backplane configuration.

- Cisco UCS C220 M5 (UCSC-220-M5SX)—Small form-factor (SFF) drives, with 10-drive backplane. Supports up to 10 2.5-inch SAS/SATA drives. Drive bays 1 and 2 support NVMe SSDs.
- Cisco UCS C220 M5 (UCSC-220-M5SN)—SFF drives, with 10-drive backplane. Supports up to 10 2.5-inch NVMe-only SSDs.
- Cisco UCS C220 M5 (UCSC-220-M5L)—Large form-factor (LFF) drives, with four-drive backplane. Supports up to four 3.5-inch SAS/SATA drives. Drive bays 1 and 2 support NVMe SSDs. A size-converter drive sled is required to hold 2.5-inch SSDs.

External Features

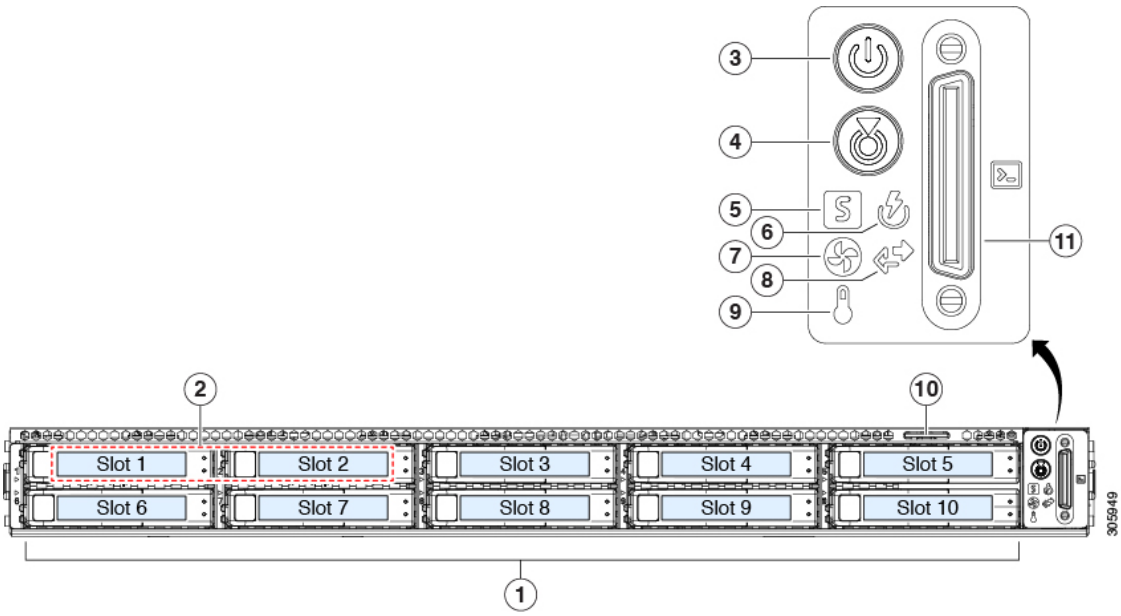
This topic shows the external features of the server versions.

Cisco UCS C220 M5 Server (SFF Drives) Front Panel Features

The following figure shows the front panel features of the small form-factor drive versions of the server.

For definitions of LED states, see Front-Panel LEDs, on page 27.

Figure 1: Cisco UCS C220 M5 Server (SFF Drives) Front Panel



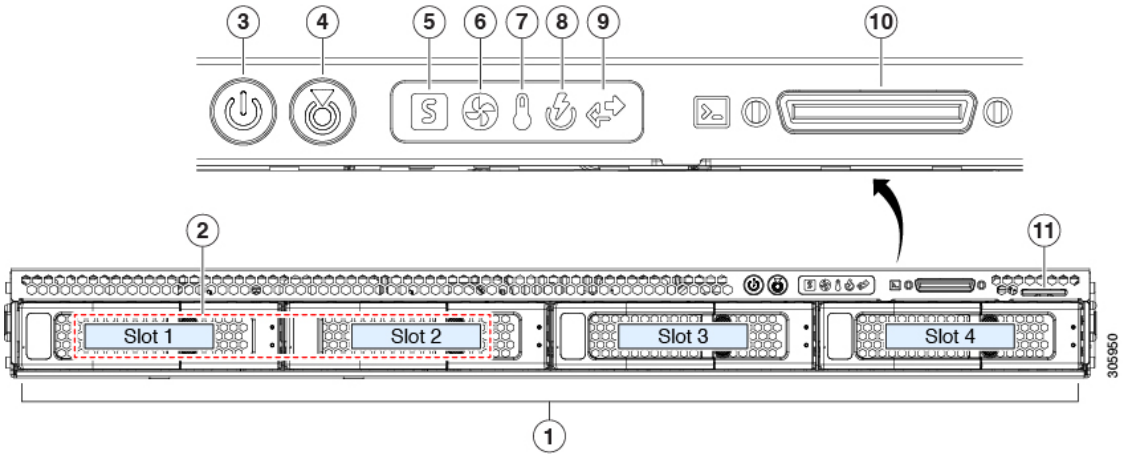
1	Drive bays 1 – 10 support SAS/SATA hard disk drives (HDDs) and solid state drives (SSDs)	**7**	Fan status LED
2	• UCSC-220-M5SX: Drive bays 1 and 2 support NVMe PCIe SSDs. • UCSC-220-M5SN: Drive bays 1 – 10 support *only* NVMe PCIe SSDs.	**8**	Network link activity LED
3	Power button/power status LED	**9**	Temperature status LED
4	Unit identification button/LED	**10**	Pull-out asset tag
5	System status LED	**11**	KVM connector (used with KVM cable that provides one DB-15 VGA, one DB-9 serial, and two USB connectors)
6	Power supply status LED	-	

Cisco UCS C220 M5 Server (LFF Drives) Front Panel Features

The following figure shows the front panel features of the large form-factor drive version of the server.

For definitions of LED states, see Front-Panel LEDs, on page 27.

Figure 2: Cisco UCS C220 M5 Server (LFF Drives) Front Panel



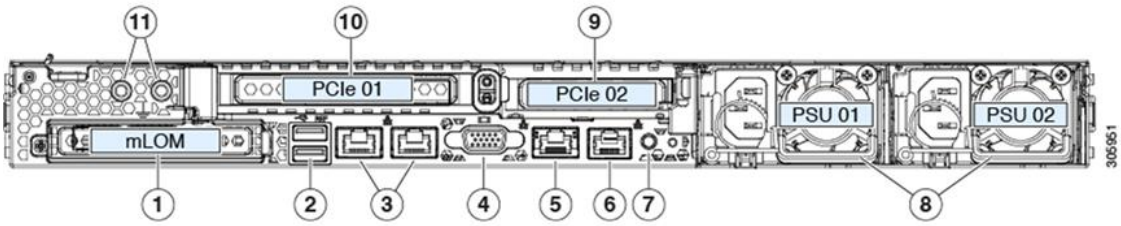
1	Drive bays 1 – 4 support SAS/SATA HDDs and SSDs	**7**	Temperature status LED
2	Drive bays 1 and 2 support NVMe PCIe SSDs. A size-converter drive sled is required if 2.5-inch SSDs are used.	**8**	Power supply status LED
3	Power button/power status LED	**9**	Network link activity LED
4	Unit identification button/LED	**10**	KVM connector (used with KVM cable that provides one DB-15 VGA, one DB-9 serial, and two USB connectors)
5	System health LED	**11**	Pull-out asset tag
6	Fan status LED	-	

Cisco UCS C220 M5 Server Rear Panel Features

The rear panel features are the same for all versions of the server.

For definitions of LED states, see Rear-Panel LEDs, on page 30.

Figure 3: Cisco UCS C220 M5 Server Rear Panel

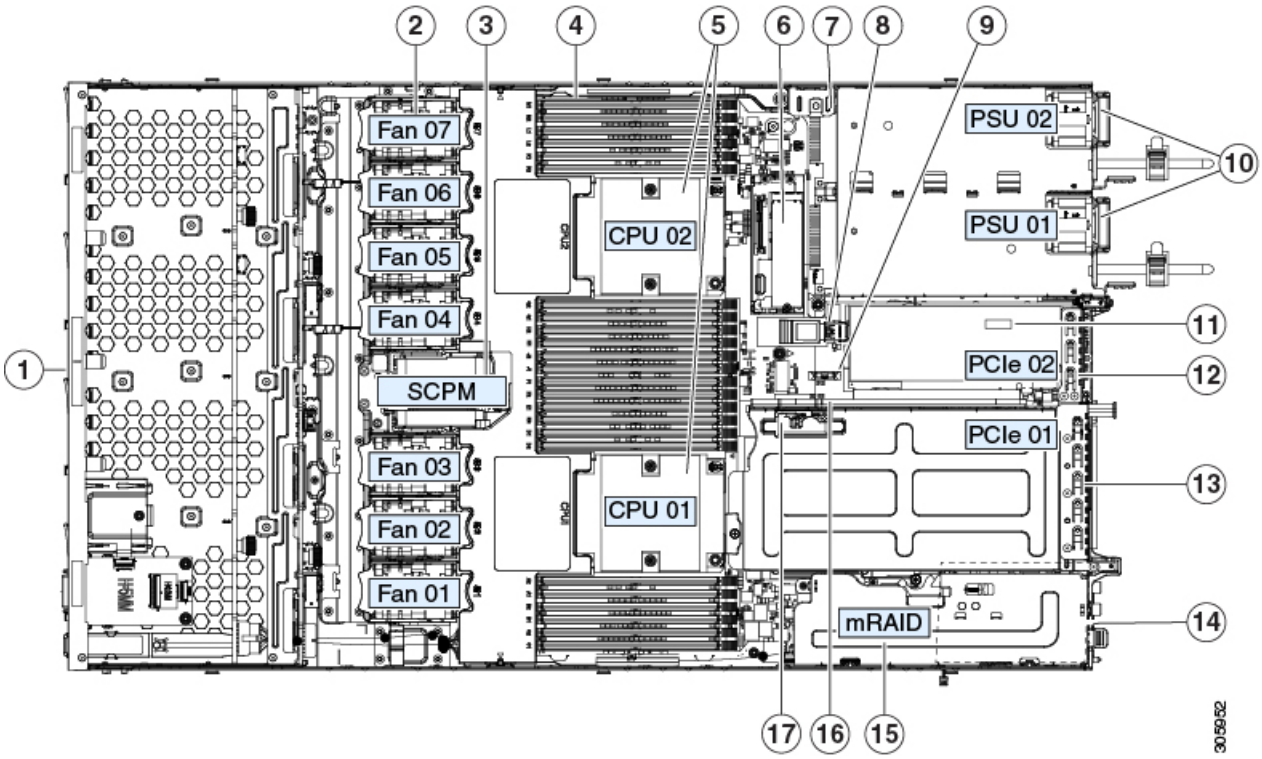


1	Modular LAN-on-motherboard (mLOM) card bay (x16 PCIe lane)	**7**	Rear unit identification button/LED
2	USB 3.0 ports (two)	**8**	Power supplies (two, redundant as 1+1)
3	Dual 1-Gb/10-Gb Ethernet ports (LAN1 and LAN2) The dual LAN ports can support 1 Gbps and 10 Gbps, depending on the link partner capability.	**9**	PCIe riser 2/slot 2 (x16 lane) Includes PCIe cable connectors for front-loading NVMe SSDs (x8 lane)
4	VGA video port (DB-15 connector)	**10**	PCIe riser 1/slot 1 (x16 lane)
5	1-Gb Ethernet dedicated management port	**11**	Threaded holes for dual-hole grounding lug
6	Serial port (RJ-45 connector)	-	

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 4: Cisco UCS C220 M5 Server, Serviceable Component Locations



1	Front-loading drive bays 1–10 support SAS/SATA drives. • UCSC-220-M5SX: Drive bays 1 and 2 support NVMe PCIe SSDs. • UCSC-220-M5SN: Drive bays 1 – 10 support *only* NVMe PCIe SSDs. • UCSC-220-M5L: Drive bays 1 and 2 support NVMe PCIe SSDs.	**10**	Power supplies (hot-swappable when redundant as 1+1)
2	Cooling fan modules (seven, hot-swappable)	**11**	Trusted platform module (TPM) socket on motherboard (not visible in this view)
3	Supercap unit mounting bracket (RAID backup)	**12**	PCIe riser 2/slot 2 (half-height, x16 lane) Includes PCIe cable connectors for front-loading NVMe SSDs (x8 lane)
4	DIMM sockets on motherboard (12 per CPU)	**13**	PCIe riser 1/slot 1 (full-height, x16 lane) Includes socket for Micro-SD card
5	CPUs and heatsinks (up to two)	**14**	Modular LOM (mLOM) card bay on chassis floor (x16 PCIe lane), not visible in this view

6	Mini-storage module socket. Options: • SD card module with two SD card slots • M.2 module with slots for either two SATA M.2 drives or two NVMe M.2 drives • 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 M.2 drives in a RAID 1 array)	**15**	Modular RAID (mRAID) riser, can optionally be a riser that supports either: • Hardware RAID controller card • Interposer card for embedded SATA RAID
7	Chassis intrusion switch (optional)	**16**	PCIe cable connectors for front-loading NVMe SSDs on PCIe riser 2
8	Internal USB 3.0 port on motherboard	**17**	Micro-SD card socket on PCIe riser 1
9	RTC battery, vertical socket	**-**	

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.

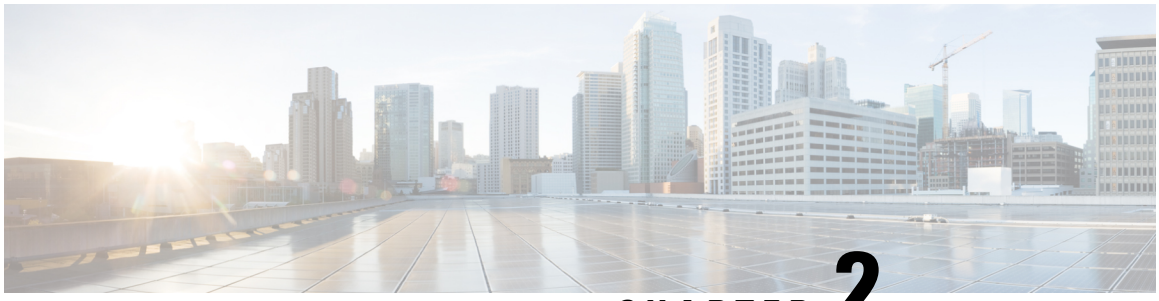
Feature	Description
Chassis	One rack-unit (1RU) chassis
Central Processor	Up to two CPUs from the Intel Xeon Processor Scalable Family. This includes CPUs from the following series: • Intel Xeon Bronze 3XXX Processors • Intel Xeon Silver 4XXX Processors • Intel Xeon Gold 5XXX Processors • Intel Xeon 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
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.

Feature	Description
Network and management I/O	Rear panel: • One 1-Gb Ethernet dedicated management port (RJ-45 connector) • Two 1-Gb/10-Gb BASE-T Ethernet LAN ports (RJ-45 connectors) The dual LAN ports can support 1 Gbps and 10 Gbps, depending on the link partner capability. • One RS-232 serial port (RJ-45 connector) • One VGA video connector port (DB-15 connector) • Two USB 3.0 ports Front panel: • One front-panel keyboard/video/mouse (KVM) connector that is used with the KVM cable, which provides two USB 2.0, one VGA, and one DB-9 serial connector.
Modular LOM	One dedicated socket (x16 PCIe lane) that can be used to add an mLOM card for additional rear-panel connectivity.
Power	Two power supplies, redundant as 1+1: • AC power supplies 770 W AC each • AC power supplies 1050 W AC each • AC power supplies 1600 W AC each • DC power supplies 1050 W DC each Do not mix power supply types or wattages in the server.
ACPI	The advanced configuration and power interface (ACPI) 4.0 standard is supported.
Cooling	Seven hot-swappable fan modules for front-to-rear cooling.
PCIe I/O	Two horizontal PCIe expansion slots on a PCIe riser assembly. See PCIe Slot Specifications, on page 82 for specifications of the slots.
InfiniBand	The PCIe bus slots in this server support the InfiniBand architecture.

Feature	Description
Storage, front-panel	The server is orderable in three different versions, each with a different front panel/drive-backplane configuration. • Cisco UCS C220 M5 (UCSC-220-M5SX)—Small form-factor (SFF) drives, with 10-drive backplane. Supports up to 10 2.5-inch SAS/SATA drives. Drive bays 1 and 2 support NVMe SSDs. • Cisco UCS C220 M5 (UCSC-220-M5SN)—SFF drives, with 10-drive backplane. Supports up to 10 2.5-inch NVMe-only SSDs in drive bays 1-10. • Cisco UCS C220 M5 (UCSC-220-M5L)—Large form-factor (LFF) drives, with four-drive backplane. Supports up to four 3.5-inch SAS/SATA drives. Drive bays 1 and 2 support NVMe SSDs. A size-converter drive sled is required to hold 2.5-inch SSDs.

Storage, internal	The server has these internal storage options:
	• One USB port on the motherboard.
	• One micro-SD card socket on PCIe riser 1.
	• Mini-storage module socket, optionally with either:
	  • SD card module. Supports up to two SD cards.
	  • M.2 SSD module. Supports either two SATA M.2 SSDs or two NVMe 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	The server has a dedicated internal mRAID riser that supports one of the following storage-controller options: • A PCIe-style Cisco modular RAID controller card (SAS/SATA). • A PCIe-style interposer card for the server's embedded SATA RAID controller. For a detailed list of storage controller options, see Supported Storage Controllers and Cables, on page 121.
RAID backup	The server has a mounting bracket near the cooling fans for the supercap unit that is used with the Cisco modular RAID controller card.
Integrated video	Integrated VGA video.



CHAPTER 2

Installing the Server

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.

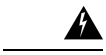
Statement 1071

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

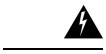
Warning **The plug-socket combination must be accessible at all times, because it serves as the main disconnecting device.**

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

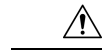


Warning **Installation of the equipment must comply with local and national electrical codes.**

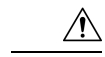
Statement 1074

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 113.
- 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 114. 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.
- 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 one rack unit (RU), equal to 1.75 in. (44.45 mm).

Supported Cisco Slide Rail Kits

The server supports the following rail kit options:

- Cisco part UCSC-RAILB-M4= (ball-bearing slide rail kit)
- Cisco part UCSC-RAILF-M4= (friction slide rail kit)
- Cisco part UCSC-CMAF-M4= (cable management arm)

Rack Installation Tools Required

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

Slide Rail and Cable Management Arm Dimensions

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

The optional cable management arm (CMA) adds additional length requirements:

- The additional distance from the rear of the server to the rear of the CMA is 5.4 inches (137.4 mm).
- The total length of the server including the CMA is 35.2 inches (894 mm).

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

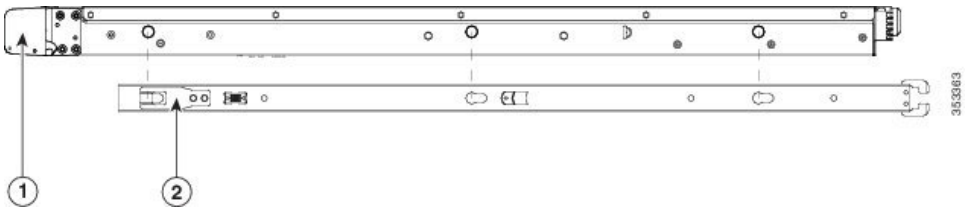
Step 1 Attach the inner rails to the sides of the server:

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

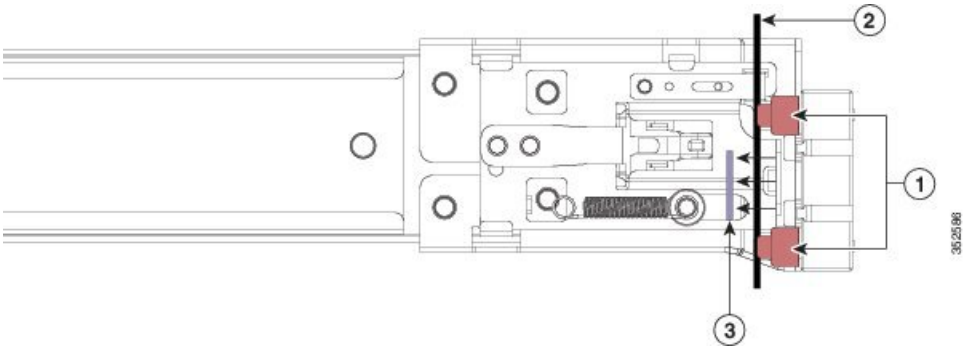


1	Front of server	**2**	Locking clip on front of inner rail

Step 2 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



1	Front mounting pegs	**3**	Securing plate shown pulled back to the open position
2	Rack post between mounting pegs and opened securing plate	-	

Step 3 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.

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 then push the rear mounting pegs into 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) 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.

f) Pull the inner slide rails on each assembly out toward the rack front until they hit the internal stops and lock in place.

Step 4 Insert the server into the slide rails:

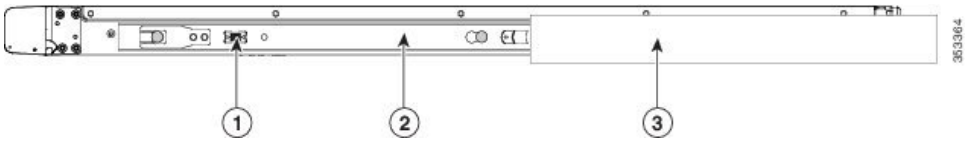
Caution This server can weigh up to 60 pounds (27 kilograms) when fully loaded with components. We recommend that you use a minimum of two people or a mechanical lift when lifting the server. Attempting this procedure alone could result in personal injury or equipment damage.

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 its front slam-latches engage with the rack posts.

Figure 7: Inner-Rail Release Clip



1	Inner-rail release clip	**3**	Outer slide rail attached to rack post
2	Inner rail attached to server and inserted into outer slide rail	-	

Step 5 (Optional) Secure the server in the rack more permanently by using the two screws that are provided with the slide rails. Perform this step if you plan to move the rack with servers installed.

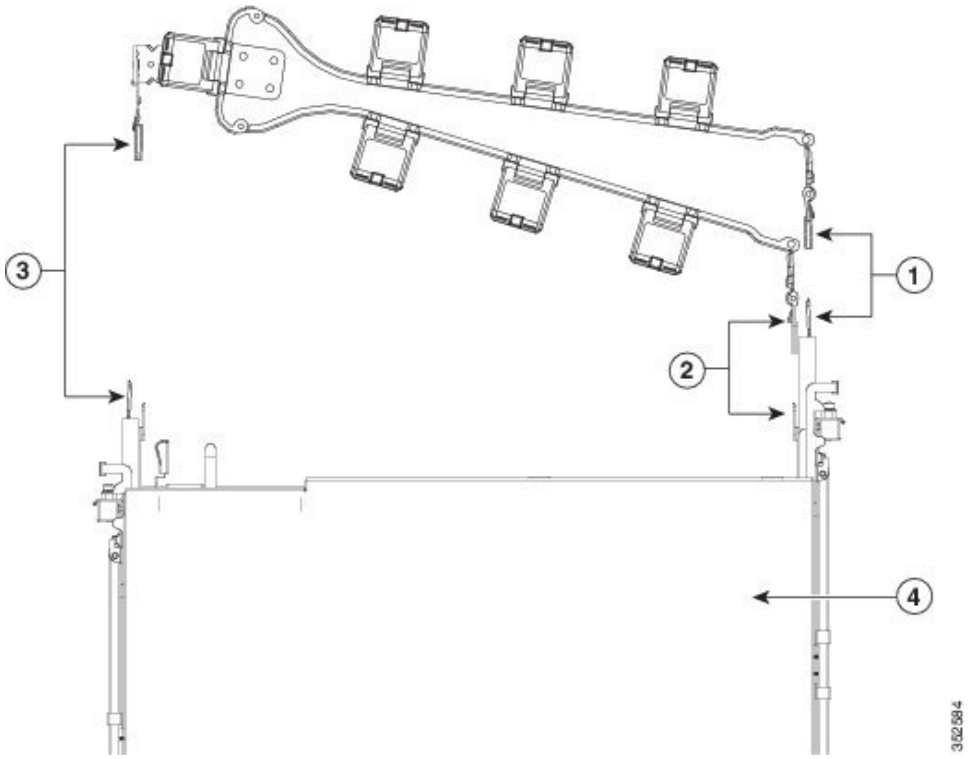
With the server fully pushed into the slide rails, open a hinged slam latch lever on the front of the server and insert a screw through the hole that is under the lever. The screw threads into the static part of the rail on the rack post and prevents the server from being pulled out. Repeat for the opposite slam latch.

Installing the Cable Management Arm (Optional)

Note The cable management arm (CMA) is reversible left-to-right. To reverse the CMA, see Reversing the Cable Management Arm (Optional), on page 15 before installation.

Step 1 With the server pushed fully into the rack, slide the CMA tab of the CMA arm that is farthest from the server onto the end of the stationary slide rail that is attached to the rack post. Slide the tab over the end of the rail until it clicks and locks.

Figure 8: Attaching the CMA to the Rear Ends of the Slide Rails



1	CMA tab on arm farthest from server attaches to end of stationary outer slide rail.	**3**	CMA tab on width-adjustment slider attaches to end of stationary outer slide rail.
2	CMA tab on arm closest to the server attaches to end of inner slide rail attached to server.	**4**	Rear of server

Step 2 Slide the CMA tab that is closest to the server over the end of the inner rail that is attached to the server. Slide the tab over the end of the rail until it clicks and locks

Step 3 Pull out the width-adjustment slider that is at the opposite end of the CMA assembly until it matches the width of your rack.

Step 4 Slide the CMA tab that is at the end of the width-adjustment slider onto the end of the stationary slide rail that is attached to the rack post. Slide the tab over the end of the rail until it clicks and locks.

Step 5 Open the hinged flap at the top of each plastic cable guide and route your cables through the cable guides as desired.

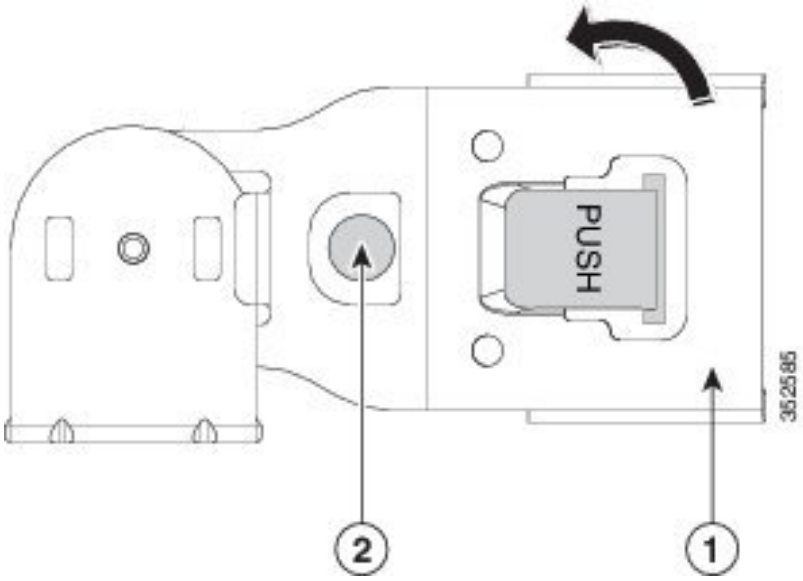
Reversing the Cable Management Arm (Optional)

Step 1 Rotate the entire CMA assembly 180 degrees, left-to-right. The plastic cable guides must remain pointing upward.

Step 2 Flip the tabs at the ends of the CMA arms so that they point toward the rear of the server.

Step 3 Pivot the tab that is at the end of the width-adjustment slider. Depress and hold the metal button on the outside of the tab and pivot the tab 180 degrees so that it points toward the rear of the server.

Figure 9: Reversing the CMA



1	CMA tab on end of width-adjustment slider	**2**	Metal button on outside of tab

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 151.

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 19.

- 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 a KVM cable (Cisco PID N20-BKVM) or the ports on the rear 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.

This section contains the following topics:

Connecting to the Server Locally For Setup

This procedure requires the following equipment:

- VGA monitor
- USB keyboard
- Either the supported Cisco KVM cable (Cisco PID N20-BKVM); or a 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 power outlet.

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 VGA monitor to the server using one of the following methods:

- Connect an optional KVM cable (Cisco PID N20-BKVM) to the KVM connector on the front panel. Connect your USB keyboard and VGA monitor to the KVM cable.
- Connect a USB keyboard and VGA monitor to the corresponding connectors on the rear 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*. The Strong Password feature is enabled.

The 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 4 Continue with Setting Up the System With the Cisco IMC Configuration Utility, on page 19.

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 power outlet.

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 rear 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*. The Strong Password feature is enabled.

The 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 19.

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).
  - 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.

You can use this option to reset user credentials in future. For detailed steps, refer *Cisco UCS C-Series Integrated Management Controller GUI Configuration Guide* for your Cisco IMC release at Configuration Guides.

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 Integrated Management Controller GUI Configuration Guide* or the *Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide* for instructions on using those interfaces for your Cisco IMC release. The links to the configuration guides are in the Cisco Integrated Management Controller.

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).
  - 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.

Older NAND Flash Not Detectable By Latest Cisco IMC

Caution If your system is running Cisco IMC 4.0(1b) or later, and you have the latest NAND flash chip MT29F4G08ABAFAWP-IT:F (M70A), do not downgrade the Cisco IMC to an earlier version. Earlier versions of the BMC cannot detect this latest NAND Flash chip.

Cisco IMC 4.0(1a) supports only the original Micron BMC (MT29F4G08ABADAWP-IT:D).

Cisco IMC 4.0(1b) supports the original Micron BMC (MT29F4G08ABADAWP-IT:D) and the new Micron BMC (MT29F4G08ABAFAWP-IT:F (M70A)).

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 either the RJ-45 serial connector on the server rear panel, or a DB-9 connection when using the KVM cable (Cisco PID N20-BKVM) on the front-panel KVM console connector.
  - 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

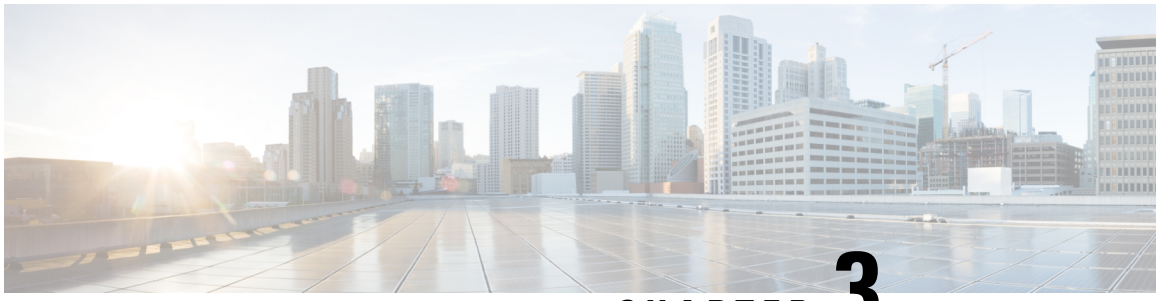
This server supports the Smart Access USB feature. The board management controller (BMC) in this server can accept a USB mass storage device and access the data on it. This feature allows you to use the front-panel USB device as a medium to transfer data between the BMC and the user without need for 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:
  - The KVM cable (Cisco PID N20-BKVM) connected to the front panel KVM console connector.
  - A USB storage device connected to one of the USB 2.0 connectors on the KVM cable. The USB device must draw less than 500 mA to avoid disconnect by the current-protection circuit.

    Note Any mouse or keyboard that is connected to the KVM cable is disconnected when you enable Smart Access USB.
  - 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.

- The front-panel KVM connector has been designed to switch the USB port between Host OS and BMC.
- 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

Status LEDs and Buttons

This section contains information for interpreting front, rear, and internal LED states.

Front-Panel LEDs

Figure 10: Front Panel LEDs

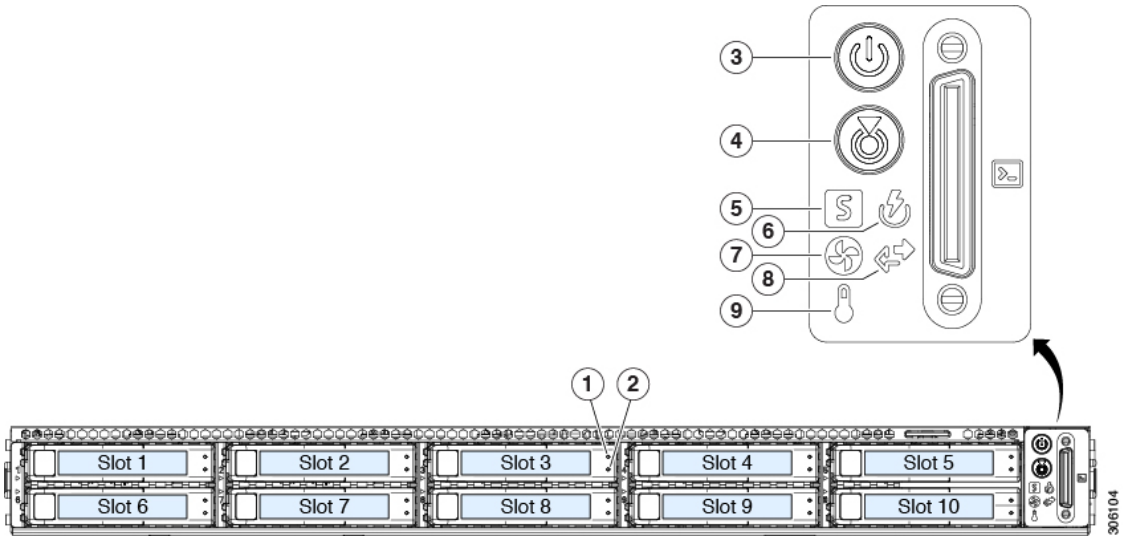


Table 2: Front Panel LEDs, Definition of States

	LED Name	States

1 **SAS**	SAS/SATA drive fault **Note** NVMe solid state drive (SSD) drive tray LEDs have different behavior than SAS/SATA drive trays.	• 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.
2 **SAS**	SAS/SATA drive activity LED	• 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.
1 **NVMe**	NVMe SSD drive fault **Note** NVMe solid state drive (SSD) drive tray LEDs have different behavior than SAS/SATA drive trays.	• 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.
2 **NVMe**	NVMe SSD activity	• Off—No drive activity. • Green, blinking—There is drive activity.
3	Power button/LED	• 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.
4	Unit identification	• Off—The unit identification function is not in use. • Blue, blinking—The unit identification function is activated.

5	System health	• 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:
		  • 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.

6	Power supply status	• 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.
7	Fan status	• Green—All fan modules are operating properly. • Amber, blinking—One or more fan modules breached the non-recoverable threshold.
8	Network link activity	• 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.
9	Temperature status	• 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.

Rear-Panel LEDs

Figure 11: Rear Panel LEDs

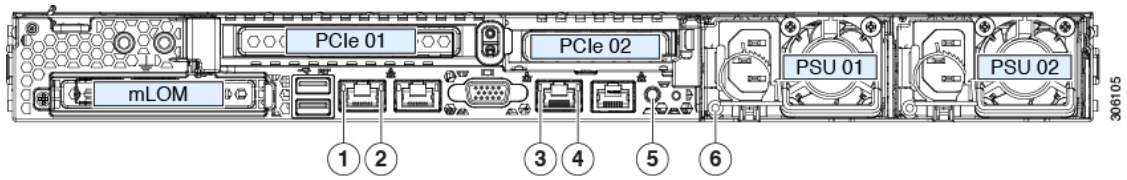


Table 3: Rear Panel LEDs, Definition of States

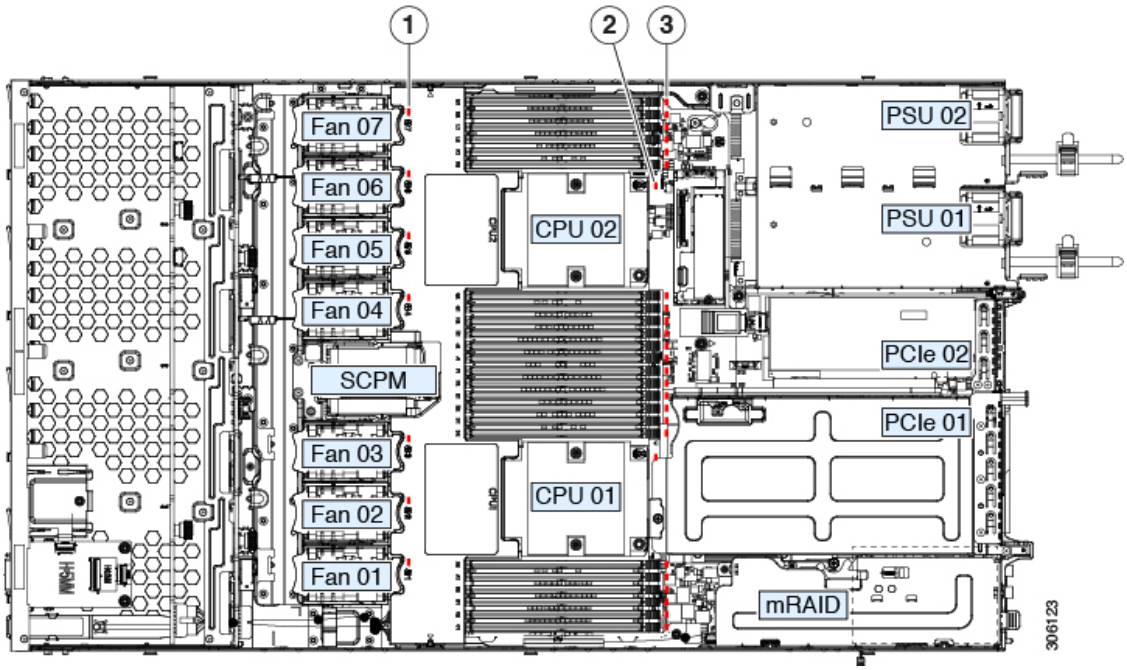
	LED Name	States
1	1-Gb/10-Gb Ethernet link speed (on both LAN1 and LAN2)	• Amber—Link speed is 100 Mbps. • Amber—Link speed is 1 Gbps. • Green—Link speed is 10 Gbps.
2	1-Gb/10-Gb Ethernet link status (on both LAN1 and LAN2)	• Off—No link is present. • Green—Link is active. • Green, blinking—Traffic is present on the active link.
3	1-Gb Ethernet dedicated management link speed	• Off—Link speed is 10 Mbps. • Amber—Link speed is 100 Mbps. • Green—Link speed is 1 Gbps.
4	1-Gb Ethernet dedicated management link status	• Off—No link is present. • Green—Link is active. • Green, blinking—Traffic is present on the active link.
5	Rear unit identification	• Off—The unit identification function is not in use. • Blue, blinking—The unit identification function is activated.

6	Power supply status (one LED each power supply unit)	**AC power supplies:** • 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). **DC power supplies:** • 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).

Internal Diagnostic LEDs

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

Figure 12: Internal Diagnostic LED Locations



1	Fan module fault LEDs (one behind each fan connector on the motherboard) • Amber—Fan has a fault or is not fully seated. • Green—Fan is OK.	**3**	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.
2	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.	-	

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 (supplied with replacement CPUs for heatsink removal)
- #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 as directed in some service procedures, you must disconnect all power cords from all power supplies in the server.

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

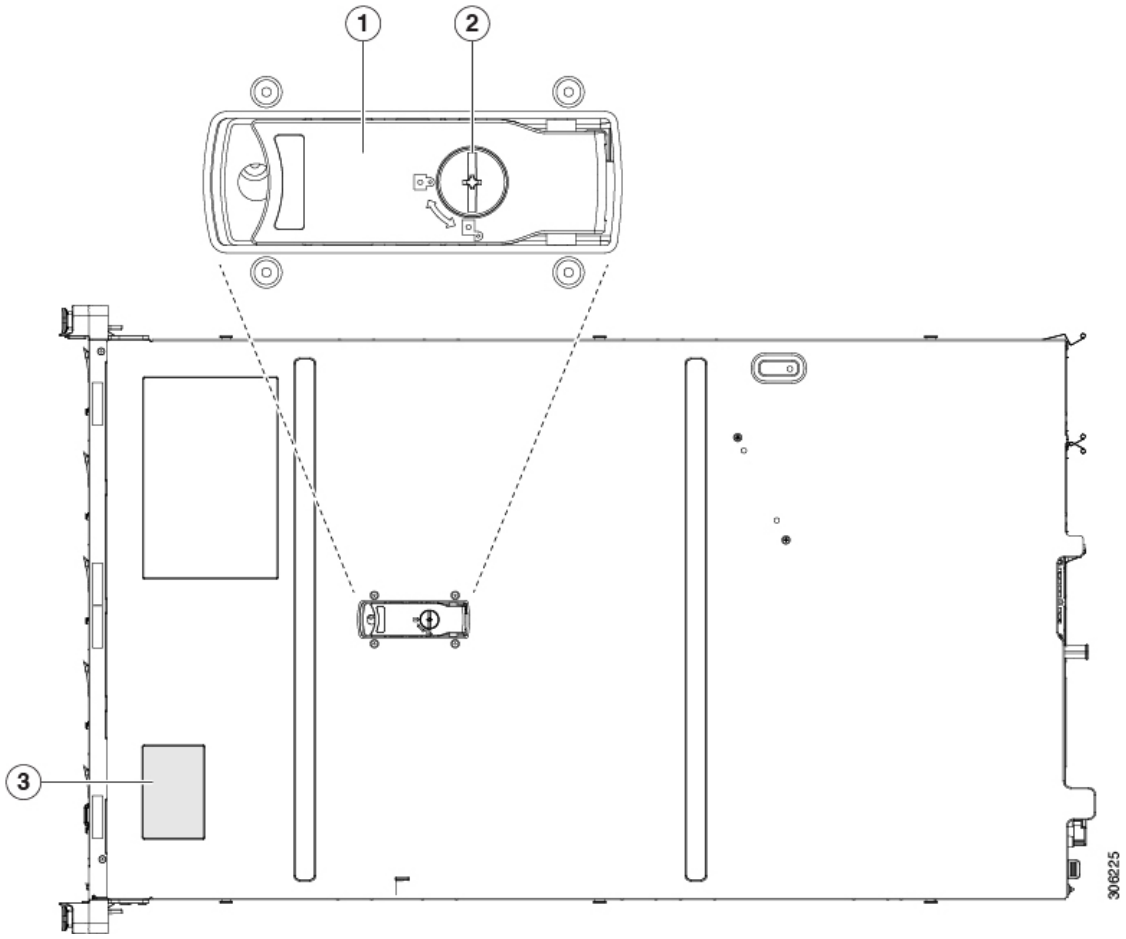
Step 1 Remove the top cover:

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:

a) 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.
b) Press the cover latch down to the closed position. The cover is pushed forward to the closed position as you push down the latch.
c) If desired, lock the latch by using a screwdriver to turn the lock 90-degrees clockwise.

Figure 13: Removing the Top Cover



1	Top cover	**2**	Locking cover latch
		3	Serial number label location

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 35.

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.

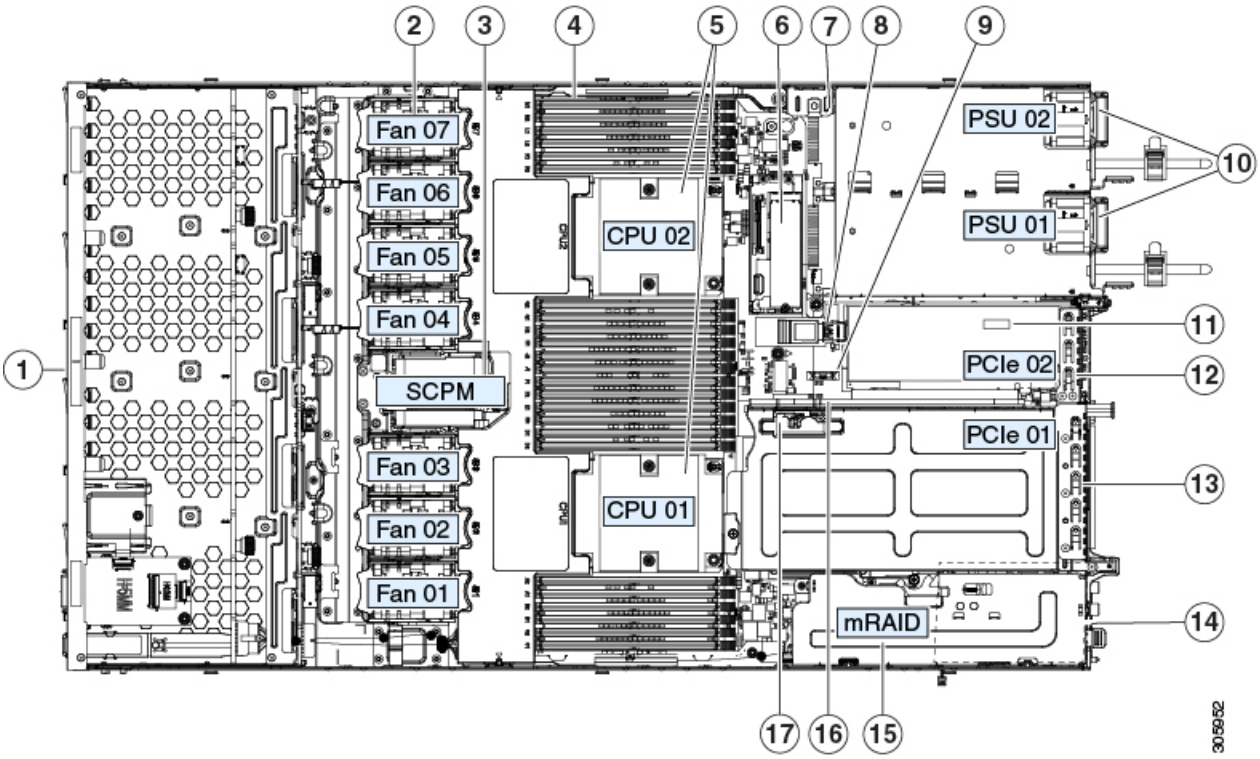
Tip You can press the unit identification button on the front panel or rear panel to turn on a flashing, blue unit identification LED on both the front and rear panels of the server. This button allows you to locate the specific server that you are servicing when you go to the opposite side of the rack. 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 14: Cisco UCS C220 M5 Server, Serviceable Component Locations



1	Front-loading drive bays 1–10 support SAS/SATA drives. • UCSC-220-M5SX: Drive bays 1 and 2 support NVMe PCIe SSDs. • UCSC-220-M5SN: Drive bays 1 – 10 support *only* NVMe PCIe SSDs. • UCSC-220-M5L: Drive bays 1 and 2 support NVMe PCIe SSDs.	**10**	Power supplies (hot-swappable when redundant as 1+1)
2	Cooling fan modules (seven, hot-swappable)	**11**	Trusted platform module (TPM) socket on motherboard (not visible in this view)
3	Supercap unit mounting bracket (RAID backup)	**12**	PCIe riser 2/slot 2 (half-height, x16 lane) Includes PCIe cable connectors for front-loading NVMe SSDs (x8 lane)
4	DIMM sockets on motherboard (12 per CPU)	**13**	PCIe riser 1/slot 1 (full-height, x16 lane) Includes socket for Micro-SD card
5	CPUs and heatsinks (up to two)	**14**	Modular LOM (mLOM) card bay on chassis floor (x16 PCIe lane), not visible in this view

6	Mini-storage module socket. Options: • SD card module with two SD card slots • M.2 module with slots for either two SATA M.2 drives or two NVMe M.2 drives • 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 M.2 drives in a RAID 1 array)	**15**	Modular RAID (mRAID) riser, can optionally be a riser that supports either: • Hardware RAID controller card • Interposer card for embedded SATA RAID
7	Chassis intrusion switch (optional)	**16**	PCIe cable connectors for front-loading NVMe SSDs on PCIe riser 2
8	Internal USB 3.0 port on motherboard	**17**	Micro-SD card socket on PCIe riser 1
9	RTC battery, vertical socket	-	

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 Hard Drives or Solid State Drives

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. To replace an NVMe PCIe SSD drive, which must be shut down before removal, see Replacing a Front-Loading NVMe SSD, on page 42.

SAS/SATA Drive Population Guidelines

The server is orderable in three different versions, each with a different front panel/drive-backplane configuration.

- Cisco UCS C220 M5 (UCSC-220-M5SX)—Small form-factor (SFF) drives, with 10-drive backplane. Supports up to 10 2.5-inch SAS/SATA drives. Drive bays 1 and 2 support NVMe SSDs.
- Cisco UCS C220 M5 (UCSC-220-M5SN)—SFF drives, with 10-drive backplane. Supports up to 10 2.5-inch NVMe-only SSDs.
- Cisco UCS C220 M5 (UCSC-220-M5L)—Large form-factor (LFF) drives, with four-drive backplane. Supports up to four 3.5-inch SAS/SATA drives. Drive bays 1 and 2 support NVMe SSDs. A size-converter drive sled is required to hold 2.5-inch SSDs.

Drive bay numbering is shown in the following figures.

Figure 15: Small Form-Factor Drive Versions, Drive Bay Numbering

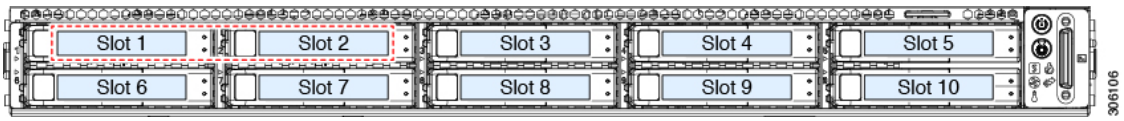
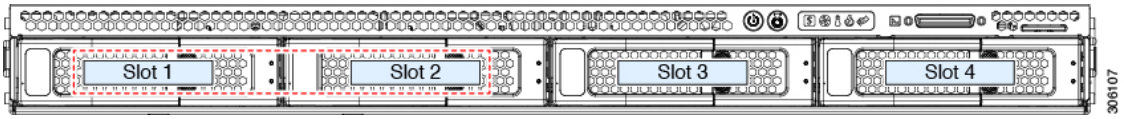


Figure 16: Large Form-Factor Drive Version, Drive Bay Numbering



Observe these drive population guidelines for optimum performance:

- When populating drives, add drives to the lowest-numbered bays first.
- Keep an empty drive blanking tray in any unused bays to ensure proper airflow.
- 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. UEFI mode is the system default. Only if the mode has been changed and must be changed back to UEFI mode, see the following procedure.
- 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

UEFI mode is the system default. Use this procedure if the mode has been changed and must be set back to UEFI mode.

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 **Boot Mode** to **UEFI Mode**.

Step 4 Under **Boot Option Priorities**, set your OS installation media (such as a virtual DVD) as your **Boot Option #1**.

Step 5 Press **F10** to save changes and exit the BIOS setup utility. Allow the server to reboot.

Step 6 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**.

Replacing a SAS/SATA Drive

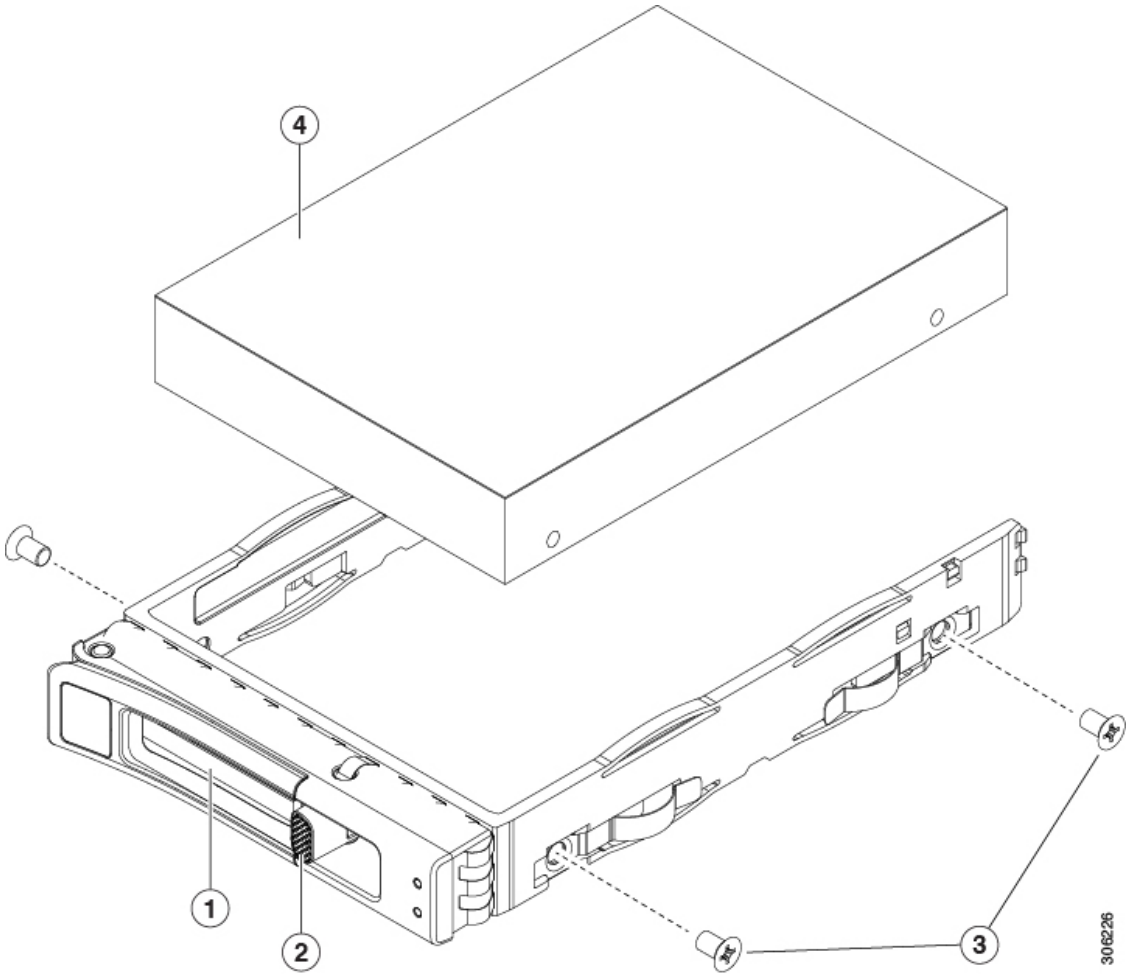
Step 1 Remove the drive that you are replacing or remove a blank drive tray from the bay:

a) Press the release button on the face of the drive tray.
b) Grasp and open the ejector lever and then pull the drive tray out of the slot.
c) 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:

a) Place a new drive 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.

Figure 17: Replacing a Drive in a Drive Tray



1	Ejector lever	**3**	Drive tray screws (two on each side)
2	Release button	**4**	Drive removed from drive tray

Replacing a Front-Loading NVMe SSD

This section is for replacing 2.5-inch or 3.5-inch form-factor NVMe solid-state drives (SSDs) in front-panel drive bays. To replace HHHL form-factor NVMe SSDs in the PCIe slots, see Replacing HHHL Form-Factor NVMe Solid State Drives, on page 46.

Front-Loading NVMe SSD Population Guidelines

The front drive bay support for 2.5- or 3.5-inch NVMe SSDs differs by server PID:

- UCSC-220-M5SX—Small form-factor (SFF) drives, with 10-drive backplane. Drive bays 1 and 2 support 2.5-inch NVMe SSDs.
- UCSC-220-M5SN—SFF drives, with 10-drive backplane. Drive bay 1 - 10 support 2.5-inch NVMe-only SSDs.
- UCSC-220-M5L—Large form-factor (LFF) drives, with four-drive backplane. Drive bays 1 and 2 support 2.5-inch and 3.5-inch NVMe SSDs. If you use 2.5-inch NVMe SSDs, a size-converter drive tray (UCS-LFF-SFF-SLED2) is required for this version of the server.

Front-Loading NVME SSD Requirements and Restrictions

Observe these requirements:

- The server must have two CPUs. PCIe riser 2 is not available in a single-CPU system. PCIe riser 2 has connectors for the cable that connects to the front-panel drive backplane.
- PCIe cable CBL-NVME-C220FF. This is the cable that carries the PCIe signal from the front-panel drive backplane to PCIe riser 2. This cable is for all versions of this server.
- 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.
- The NVMe-optimized, SFF 10-drive version, UCSC-C220-M5SN, supports NVMe drives only. This version of the server comes with an NVMe-switch card factory-installed in the internal mRAID riser for support of NVMe drives in slots 3 - 10. The NVMe drives in slots 1 and 2 are supported by PCIe riser 2. The NVMe switch card is not orderable separately.

Observe these restrictions:

- NVMe SFF 2.5- and 3.5-inch SSDs support booting only in UEFI mode. Legacy boot is not supported. For instructions on setting up UEFI boot, see 4K Sector Format SAS/SATA Drives Considerations, on page 40.
- 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- 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.
- 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 Front-Loading NVMe SSD

This topic describes how to replace 2.5- or 3.5-inch form-factor NVMe SSDs in the front-panel 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 43.

Step 1 Remove an existing front-loading 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 front-loading NVMe SSDs are being installed in the server, you must install PCIe cable CBL-NVME-C220FF before installing the drive. See Installing a PCIe Cable For Front-Loading NVMe SSDs, on page 45.

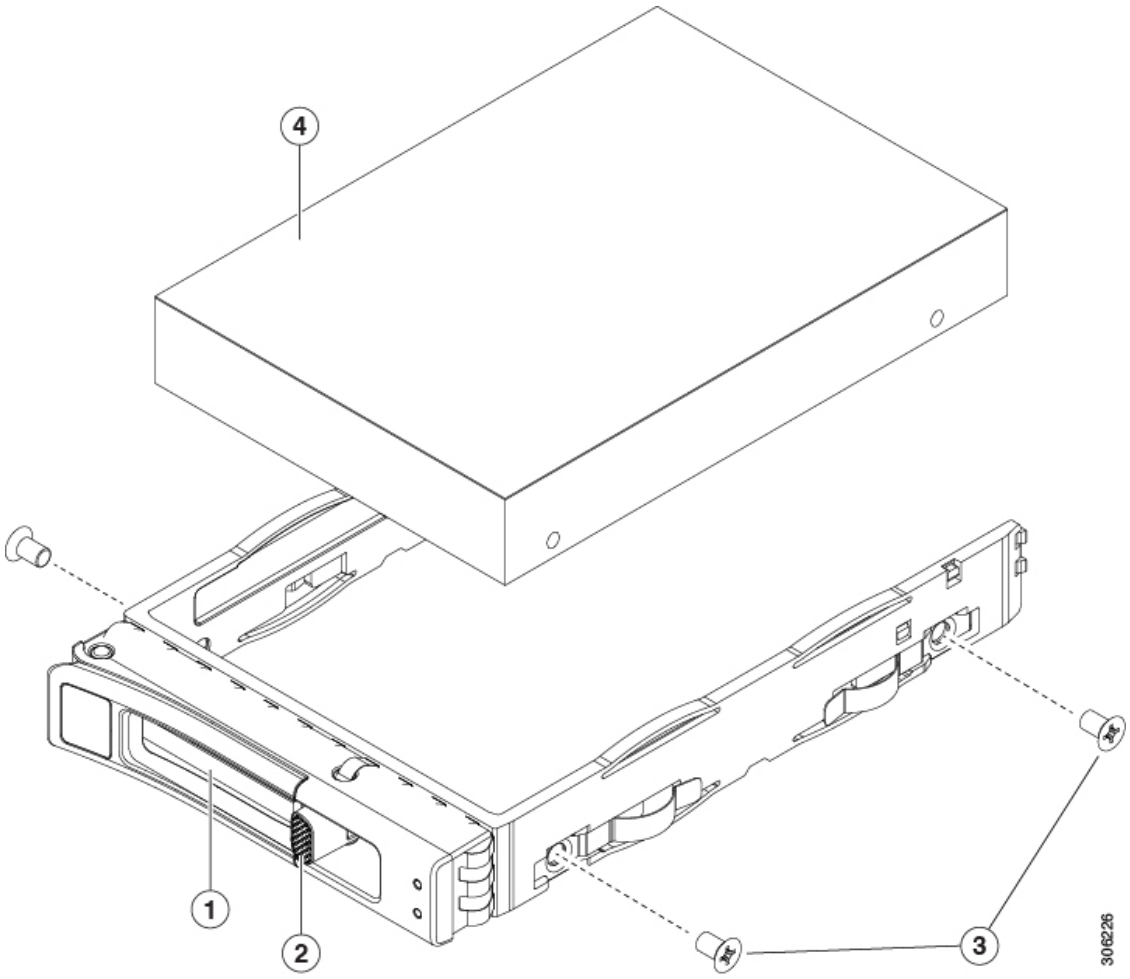
Step 2 Install a new front-loading NVMe SSD:

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 18: Replacing a Drive in a Drive Tray



1	Ejector lever	**3**	Drive tray screws (two on each side)
2	Release button	**4**	Drive removed from drive tray

Installing a PCIe Cable For Front-Loading NVMe SSDs

The front-loading NVMe SSDs interface with the server via the PCIe bus. Cable CBL-NVME-C220FF connects the front-panel drive backplane to the PCIe riser 2 board on the PCIe riser assembly.

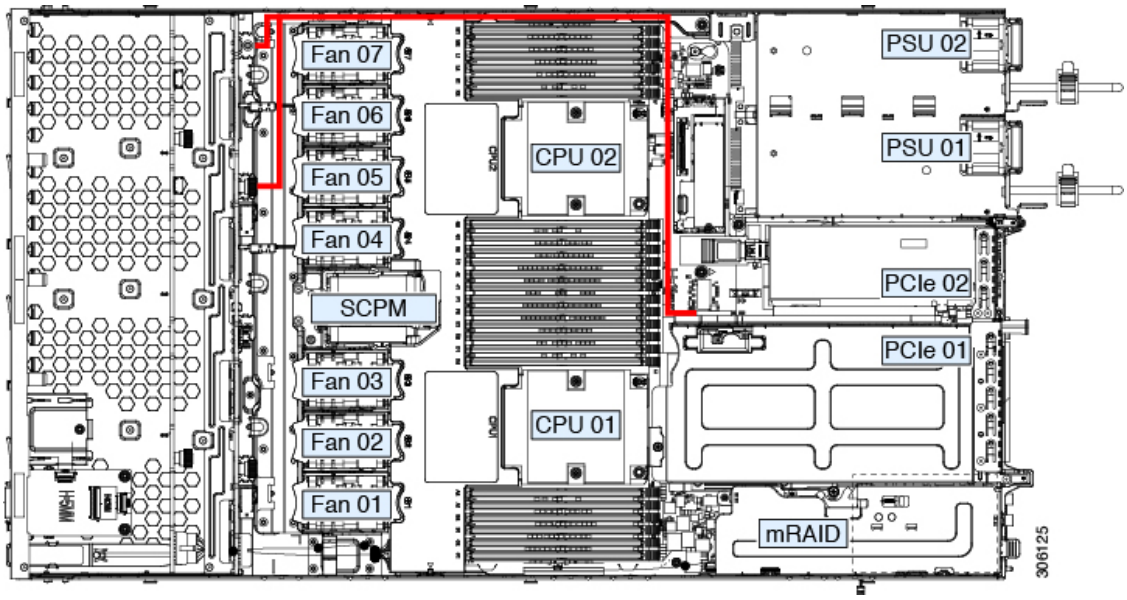
- If the server was ordered with 2.5- or 3.5-inch form-factor NVMe SSDs, this cable was preinstalled at the factory. No action is required.
- If you are adding 2.5- or 3.5-inch form-factor NVMe SSDs for the first time, you must order and install the cable as described in the following procedure.

Step 1 Connect the two connectors on one end of the cable to the PCIE-A1 and PCIE-A2 connectors on the drive backplane.

Step 2 Route the cables through the chassis cable guides to the rear of the server as shown below.

Step 3 Connect the single connector on the other end of the cable to the PCIE-FRONT connector on PCIe riser 2.

Figure 19: PCIe Cabling to Drive Backplane



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 slots. To replace 2.5- or 3.5-inch NVMe SSDs in the front-panel drive bays, see Replacing a Front-Loading NVMe SSD, on page 42.

HHHL SSD Population Guidelines

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

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

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:

a) Shut down and remove power from the server as described in Shutting Down and Removing Power From the Server, on page 33.

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 35.

d) Use two hands to grasp the external riser handle and the blue area at the front of the riser.

e) Open the hinged, plastic card retainer that secures the rear-panel tab of the card.

f) 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 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 retainer over the card's rear-panel tab.

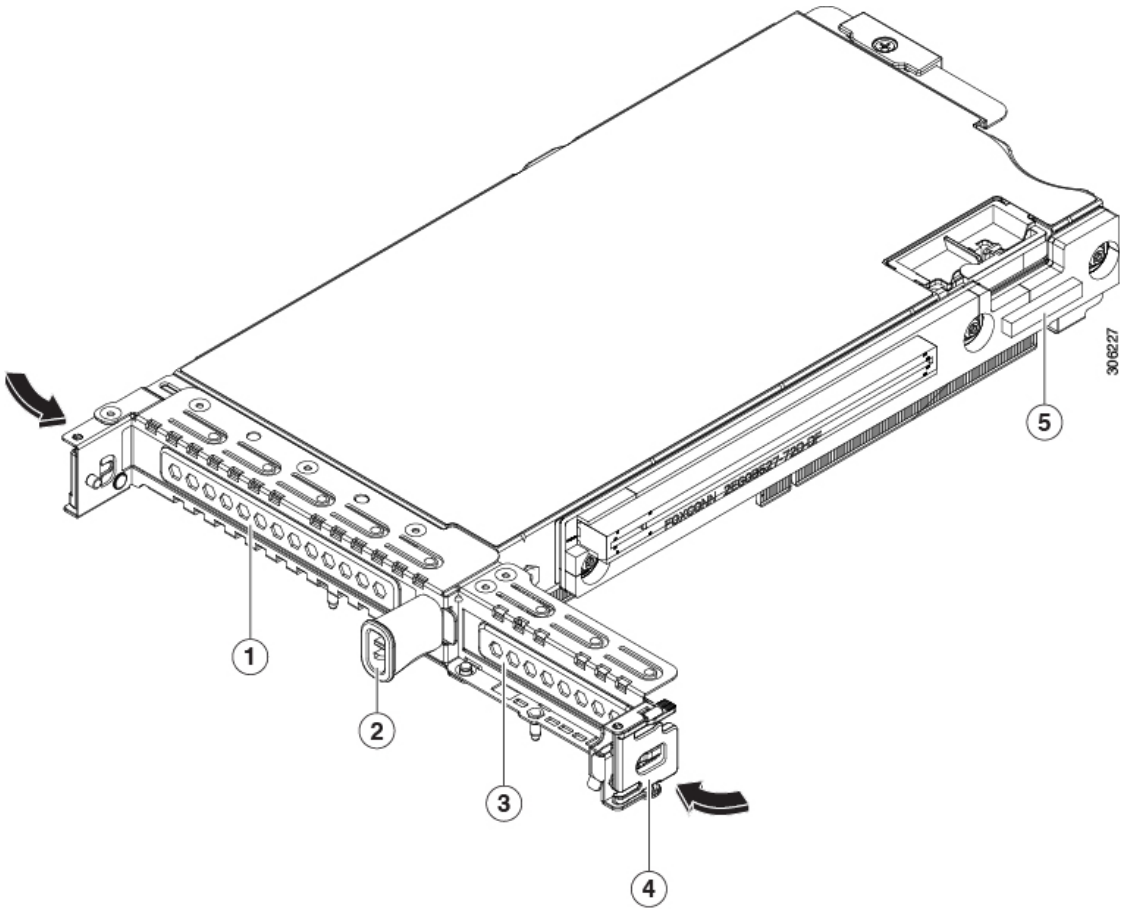
e) Position the PCIe riser over its two sockets on the motherboard and over the chassis alignment channels.

f) Carefully push down on both ends of the PCIe riser to fully engage its two connectors with the two sockets on the motherboard.

g) Replace the top cover to the server.

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

Figure 20: PCIe Riser Assembly



1	PCIe slot 1 rear-panel opening	**4**	Hinged card retainer (one each slot)
2	External riser handle	**5**	PCIe connector for cable that supports front-panel NVMe SSDs
3	PCIe slot 2 rear-panel opening		

Replacing Fan Modules

The seven fan modules in the server are numbered as shown in Figure 4: Cisco UCS C220 M5 Server, Serviceable Component Locations, on page 5.

Tip Each fan module has a fault LED next to the fan connector on the motherboard. 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 35.

c) Grasp the fan module at its front and rear finger-grips. 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.

Replacing CPUs and Heatsinks

This section contains CPU configuration rules and the procedure for replacing CPUs and heatsinks:

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 4: 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 DIM channels (12 DIMM slots). See DIMM Slot Numbering, on page 63.

- 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 protective 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 (slot 2) is unavailable.
  - Front-loading NVME drives are unavailable (they require PCIe riser 2).
- The NVIDIA Tesla P4 GPU is not supported with Second Generation Intel Xeon Scalable processors.

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 57.

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.

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 33.

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.

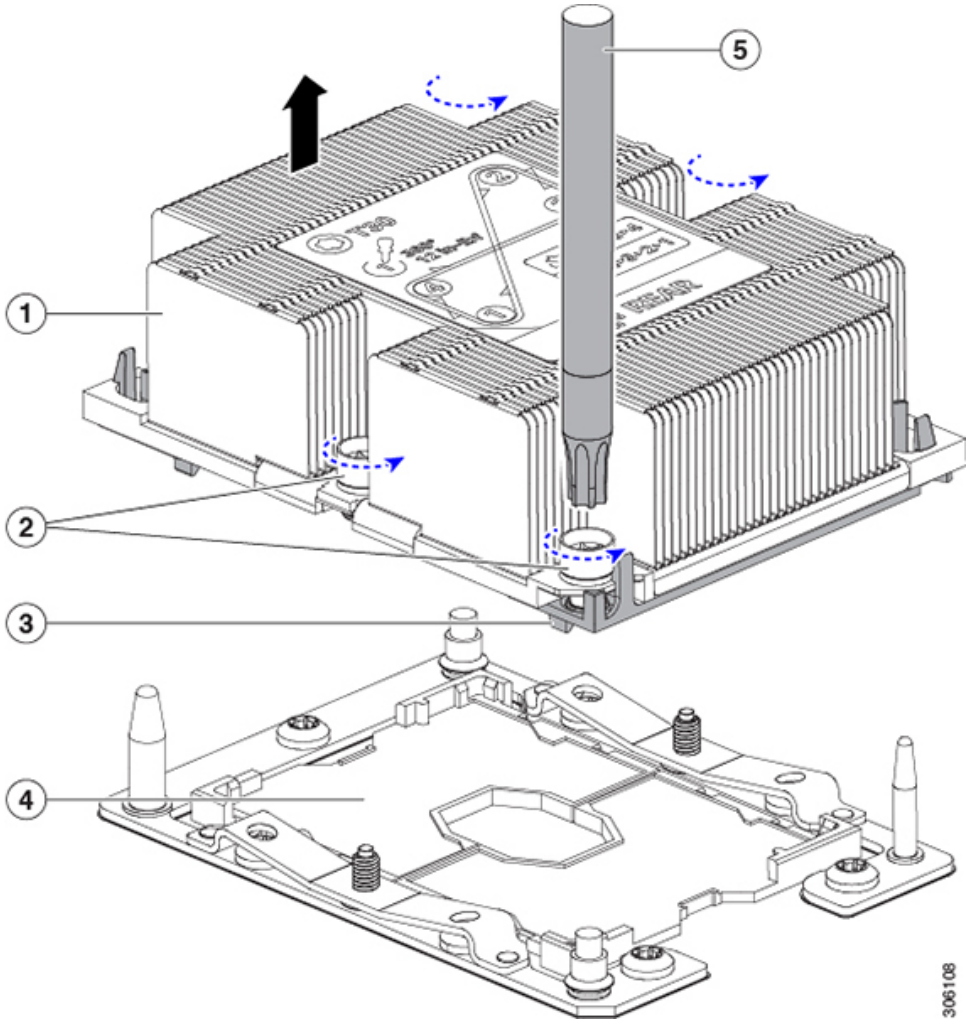
c) Remove the top cover from the server as described in Removing the Server Top Cover, on page 35.

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 21: Removing the CPU/Heatsink Assembly



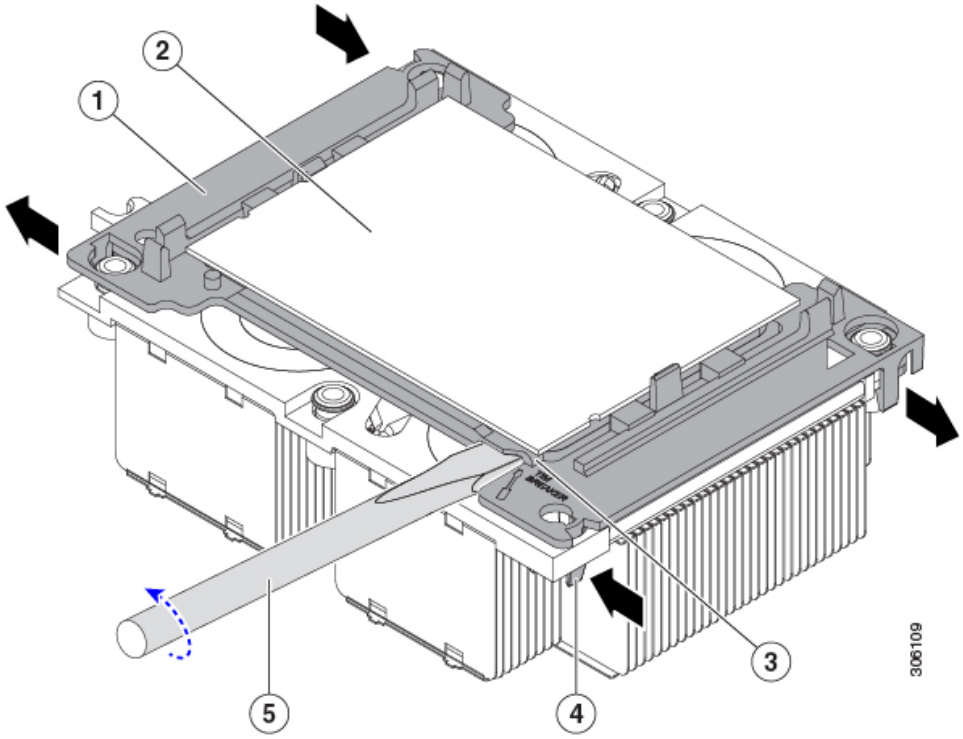
1	Heatsink	**4**	CPU socket on motherboard
2	Heatsink captive nuts (two on each side)	**5**	T-30 Torx driver
3	CPU carrier (below heatsink in this view)	-	

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

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

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

Figure 22: 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 inner-latch 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.

Caution 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 inner-latch 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.

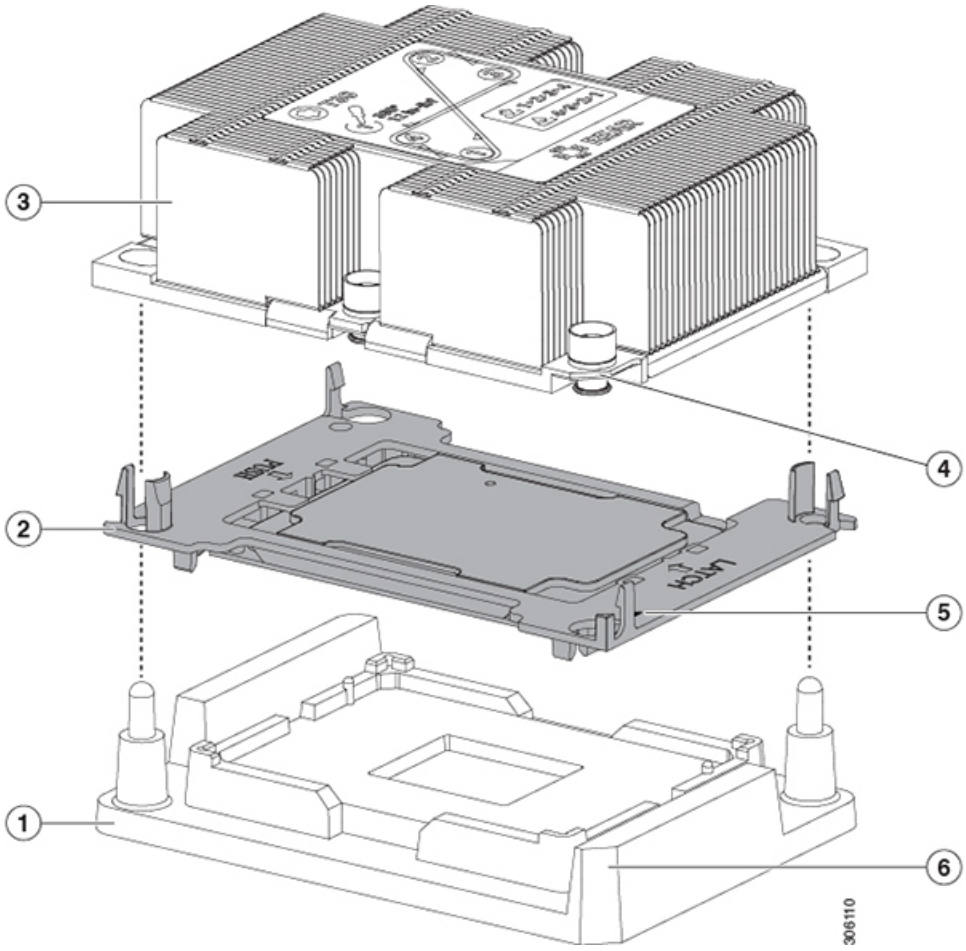
Note Handle the CPU-assembly by the plastic carrier only. Do not touch the CPU surface. Do not separate the CPU from the carrier.

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 shown below 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 23: 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)	**5**	Triangle cut into carrier (pin 1 alignment feature)
3	Heatsink	**6**	Angled corner on CPU assembly tool (pin 1 alignment feature)

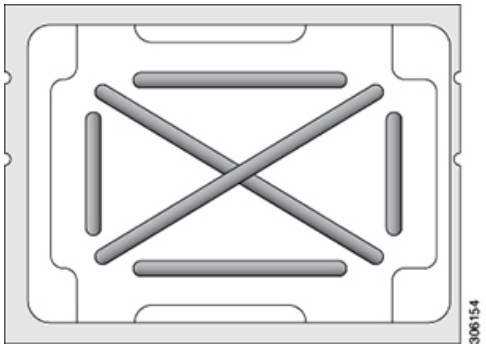
Step 4 Apply new TIM to the heatsink:

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 1.5 cubic centimeters (1.5 ml) of thermal interface material to the top of the CPU. Use the pattern shown below to ensure even coverage.

Figure 24: Thermal Interface Material Application Pattern



Caution Use only the correct heatsink for your CPUs to ensure proper cooling. There are two different heatsinks: UCSC-HS-C220M5= for standard-performance CPUs 150 W and less; UCSC-HS2-C220M5= for high-performance CPUs above 150 W. Note the wattage described on the heatsink label.

Step 5 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.

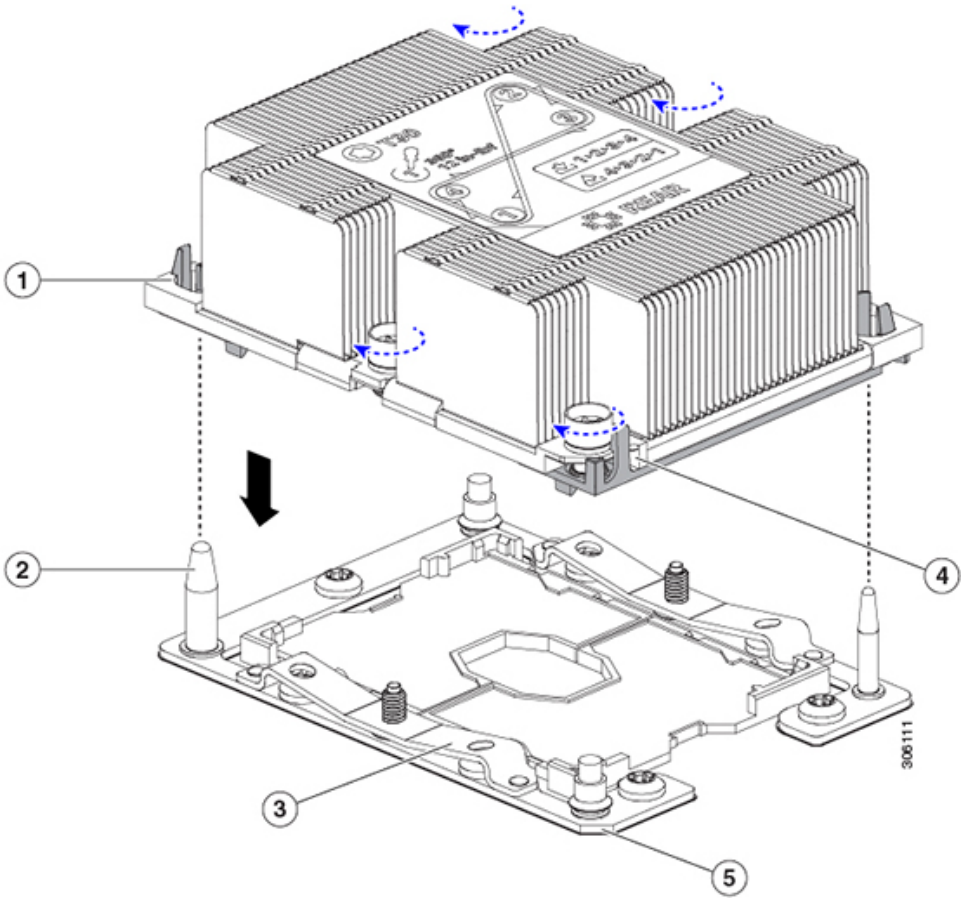
Caution In the following step, use extreme care to avoid touching or damaging the CPU contacts or the CPU socket pins.

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 CPU with heatsink over the CPU socket on the motherboard, 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 25: 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.

Caution 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 motherboard, 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 58.

- Scenario 1—You are reusing the existing heatsinks:
  - 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.
- 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-C220M5= for CPUs 150 W and less; UCSC-HS2-C220M5= for CPUs above 150 W.
  - Heatsink: UCSC-HS-C220M5= for CPUs 150 W and less; UCSC-HS2-C220M5= for CPUs above 150 W

    New heatsinks have a pre-applied pad of TIM.
  - Heatsink 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 heatsink cleaning kit is good for up to four CPU and heatsink cleanings. The cleaning kit contains two bottles of solution, one to clean the CPU and heatsink of old TIM and the other to prepare the surface of the heatsink.

New heatsink 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 heatsinks. Therefore, even when you are ordering new heatsinks, you must order the heatsink 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 58.

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:

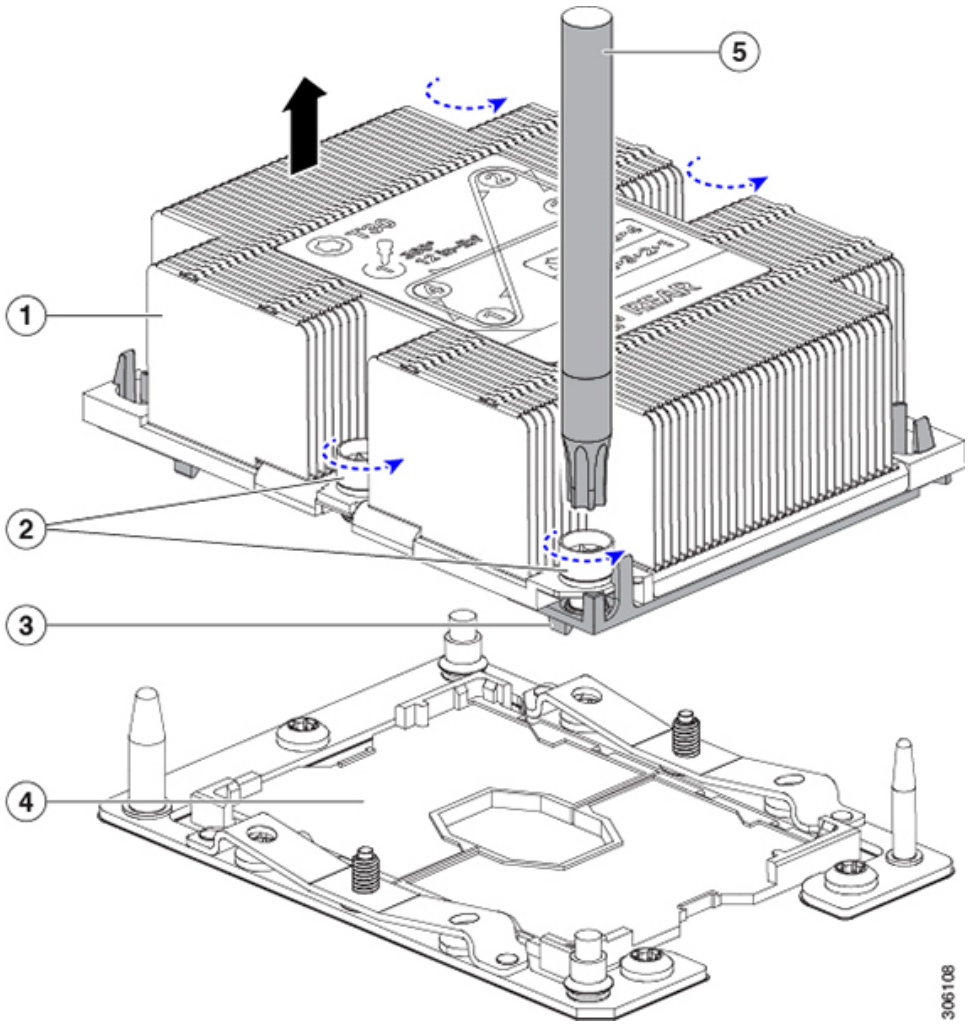
a) Use a T-30 Torx driver to loosen the four captive nuts that secure the assembly to the board standoffs.

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.

b) Lift straight up on the CPU/heatsink assembly to remove it from the board.

c) Set the CPUs with heatsinks aside on an anti-static surface.

Figure 26: Removing the CPU/Heatsink Assembly



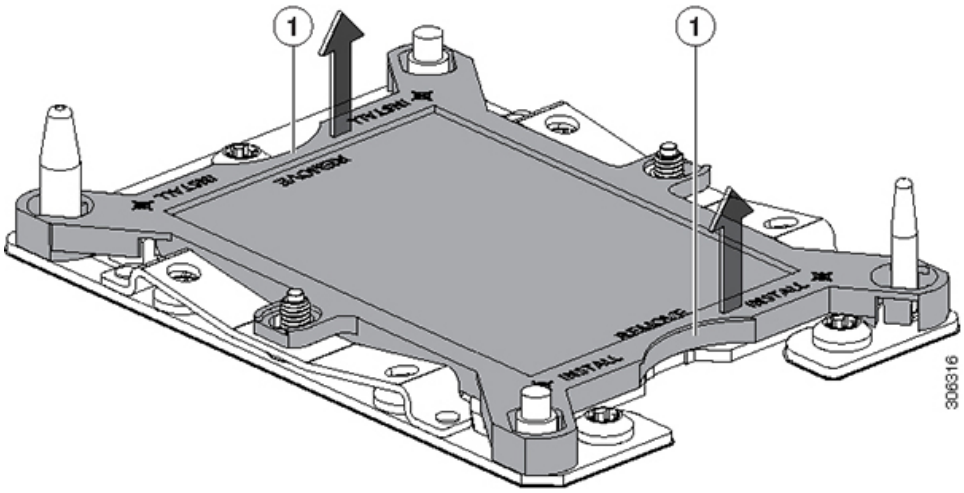
1	Heatsink	**4**	CPU socket on motherboard
2	Heatsink captive nuts (two on each side)	**5**	T-30 Torx driver
3	CPU carrier (below heatsink in this view)	-	

Step 2 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 27: Removing a CPU Socket Dust Cover



1	Finger-grip areas marked "REMOVE"	-	

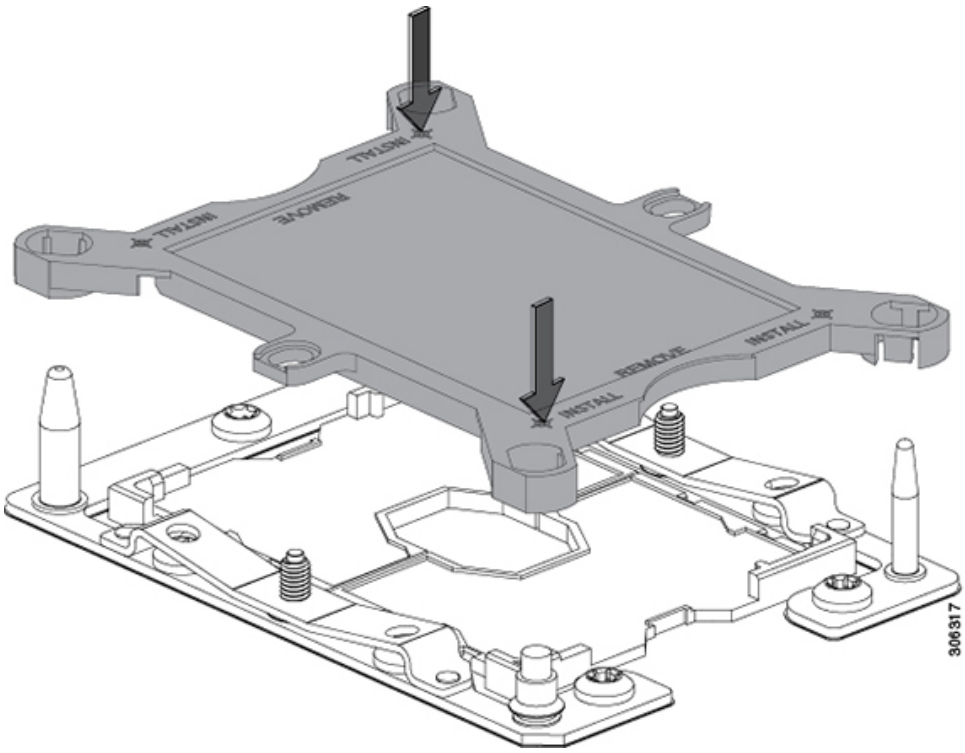
b) With the wording on the dust cover facing up, set it in place over the CPU socket. Make sure that all alignment posts on the socket plate align with the cutouts on the cover.

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 28: Installing a CPU Socket Dust Cover



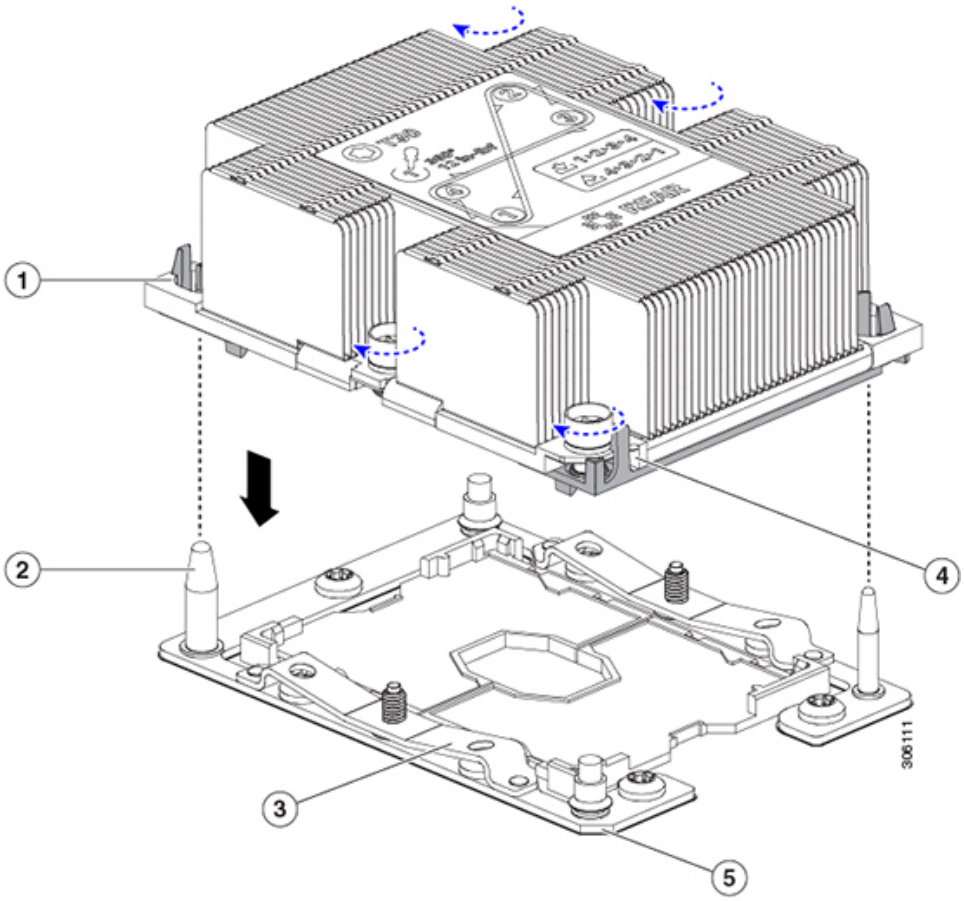
-	Press down on the two circular marks next to the word INSTALL.	-	

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 29: 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.

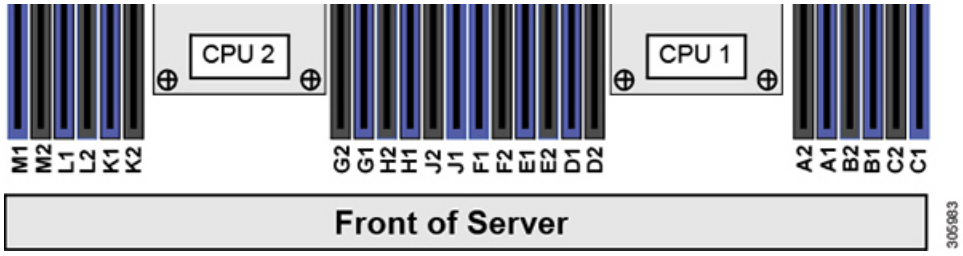
DIMM Population Rules and Memory Performance Guidelines

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 30: 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 5: DIMM Population Order

Number of DIMMs per CPU (Recommended Configurations)	Populate CPU 1 Slot		Populate CPU2 Slots	
	Blue #1 Slots	Black #2 Slots	Blue #1 Slots	Black #2 Slots
1	(A1)	-	(G1)	-
2	(A1, B1)	-	(G1, H1)	-
3	(A1, B1, C1)	-	(G1, H1, J1)	-
4	(A1, B1); (D1, E1)	-	(G1, H1); (K1, L1)	-
6	(A1, B1); (C1, D1); (E1, F1)	-	(G1, H1); (J1, K1); (L1, M1)	-
8	(A1, B1); (D1, E1)	(A2, B2); (D2, E2)	(G1, H1); (K1, L1)	(G2, H2); (K2, L2)
12	(A1, B1); (C1, D1); (E1, F1)	(A2, B2); (C2, D2); (E2, F2)	(G1, H1); (J1, K1); (L1, M1)	(G2, H2); (J2, K2); (L2, M2)

- 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.
- The NVIDIA Tesla P-Series GPU can support more than 1 TB of memory in the server. All other NVIDIA GPUs (M-Series) can support only 1 TB or less of memory in the server.
- Observe the DIMM mixing rules shown in the following table.

Table 6: 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 DIMMs with different capacities and Revisions in the same bank (for example A1, B1). The Revision value depends on the manufactures. Two DIMMs with the same PID can have different Revisions.

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 DIMMs with different speeds and Revisions in the same bank (for example A1, B1). The Revision value depends on the manufactures. Two DIMMs with the same PID can have different Revisions.
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 31 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:

a) Shut down and remove power from the server as described in Shutting Down and Removing Power From the Server, on page 33.

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 35.

d) Remove the air baffle that covers the front ends of the DIMM slots to provide clearance.

e) 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 63.

a) Align the new DIMM with the empty slot on the motherboard. Use the alignment feature in the DIMM slot to correctly orient the DIMM.

b) 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.

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.

Replacing Intel Optane DC Persistent Memory Modules

This topic contains information for replacing Intel Optane Data Center Persistent Memory modules (DCPMMs), including population rules. 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 (default): The module operates as 100% memory module. Data is volatile and DRAM acts as a cache for DCPMMs. This is the factory default setting.
- 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.

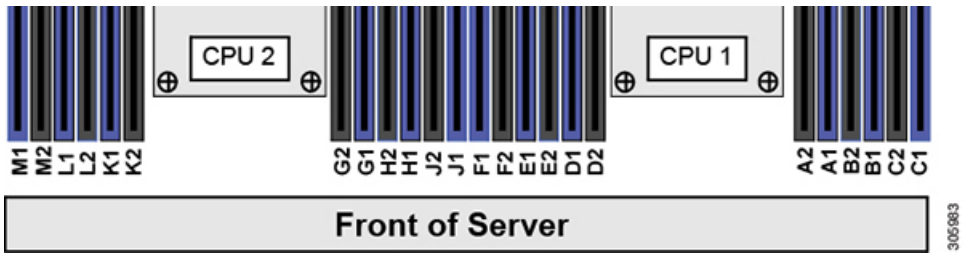
Intel Optane DC Persistent Memory Module Population Rules and Performance Guidelines

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 31: DIMM Slot Numbering



Configuration Rules

Observe the following rules and guidelines:

- To use DCPMMs in this server, two CPUs must be installed.
- DCPMMs 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.
- 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 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.
- 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 32: 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

310788

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 attemping 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 33.

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 35.

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 66.

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 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 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 69.
- 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 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 menu items:

- `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 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 Mini-Storage Module

The mini-storage module plugs into a motherboard socket to provide additional internal storage. The module is available in two different versions:

- SD card carrier—provides two SD card sockets.
- M.2 SSD Carrier—provides two M.2 form-factor SSD sockets.

Note The Cisco IMC firmware does not include an out-of-band management interface for the M.2 drives installed in the M.2 version of this mini-storage module (UCS-MSTOR-M2). The M.2 drives are not listed in Cisco IMC inventory, nor can they be managed by Cisco IMC. This is expected behavior.

Replacing a Mini-Storage Module Carrier

This topic describes how to remove and replace a mini-storage module carrier. The carrier has one media socket on its top and one socket on its underside. Use the following procedure for any type of mini-storage module carrier (SD card or M.2 SSD).

Step 1 Shut down and remove power from the server as described in Shutting Down and Removing Power From the Server, on page 33.

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 35.

Step 4 Remove a carrier from its socket:

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

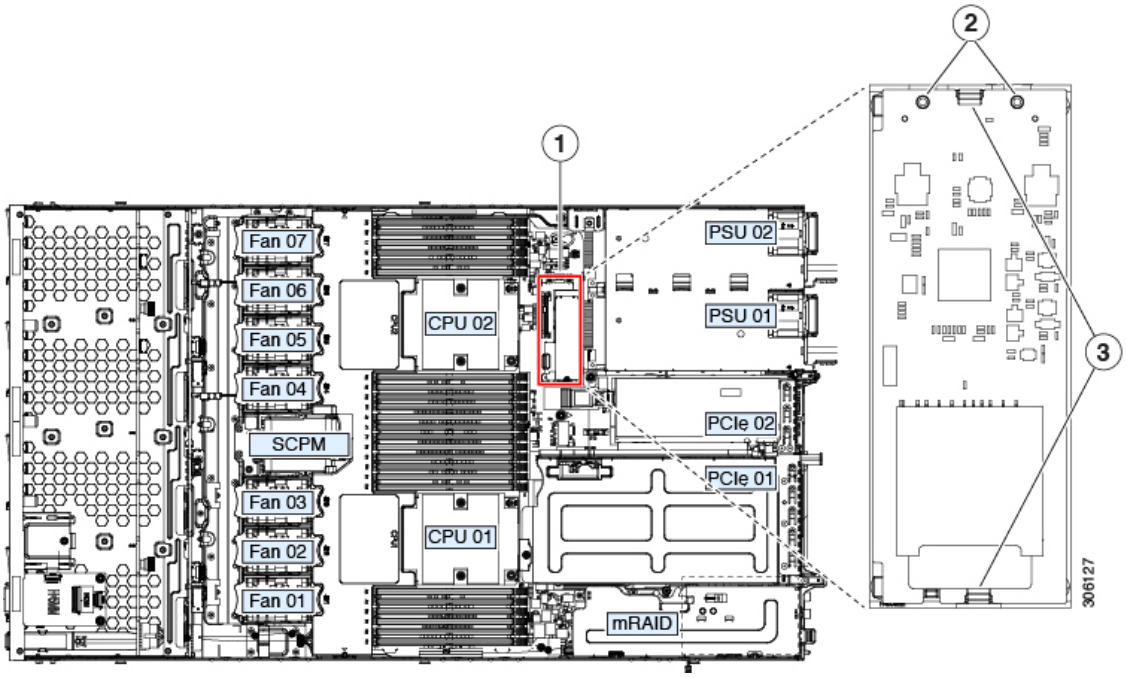
Step 5 Install a carrier to its socket:

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

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 33: Mini-Storage Module Carrier



1	Location of socket on motherboard	**3**	Securing clips
2	Alignment pegs	-	

Replacing an SD Card in a Mini-Storage Carrier For SD

This topic describes how to remove and replace an SD card in a mini-storage carrier for SD (PID UCS-MSTOR-SD). The carrier has one SD card slot on its top and one slot on its underside.

Population Rules For Mini-Storage SD Cards

- You can use one or two SD cards in the carrier.
- Dual SD cards can be configured in a RAID 1 array through the Cisco IMC interface.
- SD slot 1 is on the top side of the carrier; SD slot 2 is on the underside of the carrier (the same side as the carrier's motherboard connector).

Step 1 Power off the server and then remove the mini-storage module carrier from the server as described in Replacing a Mini-Storage Module Carrier, on page 70.

Step 2 Remove an SD card:

a) Push on the top of the SD card, and then release it to allow it to spring out from the socket.
b) Grasp and remove the SD card from the socket.

Step 3 Install a new SD card:

a) Insert the new SD card into the socket with its label side facing up.
b) Press on the top of the SD card until it clicks in the socket and stays in place.

Step 4 Install the mini-storage module carrier back into the server and then power it on as described in Replacing a Mini-Storage Module Carrier, on page 70.

Replacing an M.2 SSD in a Mini-Storage Carrier For M.2

This topic describes how to remove and replace an M.2 SATA or M.2 NVMe SSD in a mini-storage carrier for M.2 (UCS-MSTOR-M2). The carrier has one M.2 SSD socket on its top and one socket on its underside.

Population Rules For Mini-Storage M.2 SSDs

- Both M.2 SSDs must be either SATA or NVMe; do not mix types in the carrier.
- You can use one or two M.2 SSDs in the carrier.
- M.2 socket 1 is on the top side of the carrier; M.2 socket 2 is on the underside of the carrier (the same side as the carrier's motherboard connector).
- Dual SATA M.2 SSDs can be configured in a RAID 1 array with the BIOS Setup Utility's built in embedded SATA RAID utility. See Embedded SATA RAID Controller, on page 127.

  If M.2 *NVMe* SSDs are installed in the M.2 module, the embedded SATA controller is automatically disabled.

Note You cannot control M.2 SATA SSDs in the server with a HW RAID controller.

Step 1 Power off the server and then remove the mini-storage module carrier from the server as described in Replacing a Mini-Storage Module Carrier, on page 70.

Step 2 Remove an M.2 SSD:

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

b) Remove the M.2 SSD from its socket on the carrier.

Step 3 Install a new M.2 SSD:

a) Angle the M.2 SSD downward and insert the connector-end into the socket on the carrier. The M.2 SSD's label must face up.

b) Press the M.2 SSD flat against the carrier.

c) Install the single screw that secures the end of the M.2 SSD to the carrier.

Step 4 Install the mini-storage module carrier back into the server and then power it on as described in Replacing a Mini-Storage Module Carrier, on page 70.

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 33.

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 35.

d) Locate the Micro SD card. The socket is on the top of PCIe riser 1, under a flexible plastic cover.

e) Use your fingertip to push open the retainer on the socket cover 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:

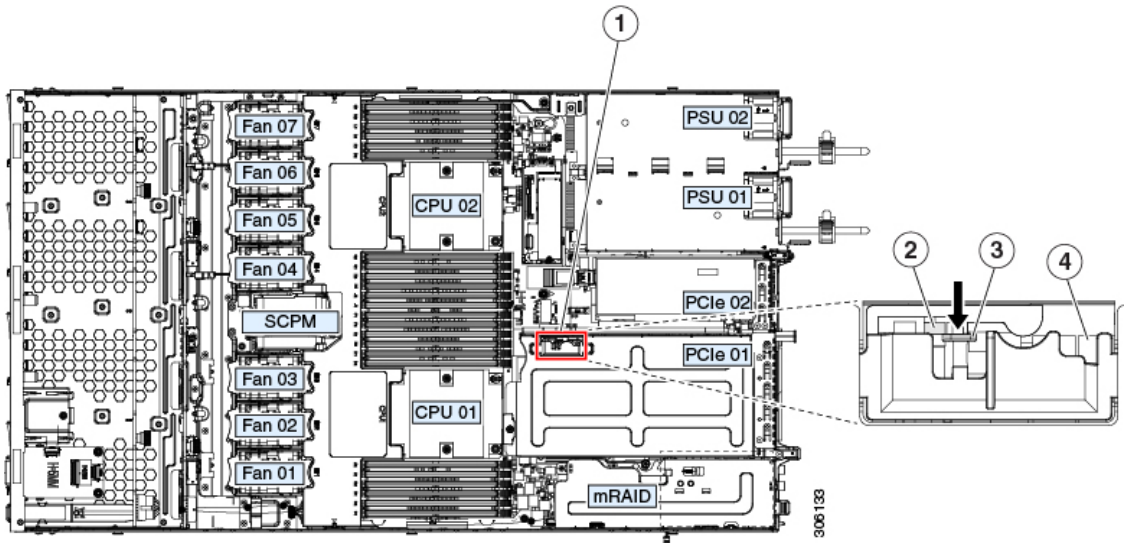
a) While holding the retainer on the plastic cover open with your fingertip, align the new Micro SD card with the socket.

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 34: Internal Micro SD Card Socket



1	Location of Micro SD card socket on the top of PCIe riser 1	**3**	Plastic retainer (push aside to access socket)
2	Micro SD card socket under plastic retainer	**4**	Micro SD activity LED

Replacing an Internal USB Drive

This section includes procedures for installing a USB drive and for enabling or disabling the internal USB port.

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 33.

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 35.

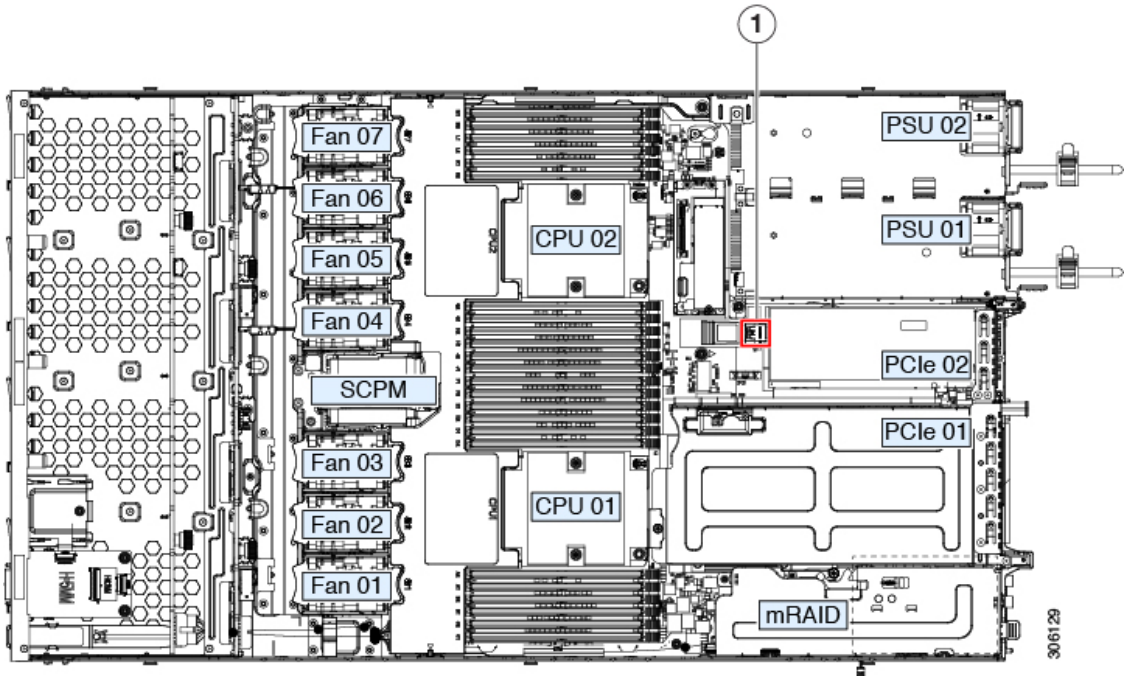
d) Locate the USB socket on the motherboard, directly in front of PCIe riser 2.

e) Grasp the USB drive and pull it horizontally 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 horizontally 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 35: Location of Internal USB Port



1	Location of horizontal 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.

Caution 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.

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 purchased from most electronic stores.

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 33.

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 35.

d) Locate the RTC battery. The vertical socket is directly in front of PCIe riser 2.

e) Remove the battery from the socket on the motherboard. Gently pry the securing clip on one side open to provide clearance, then lift straight up on the battery.

Step 2 Install a new RTC battery:

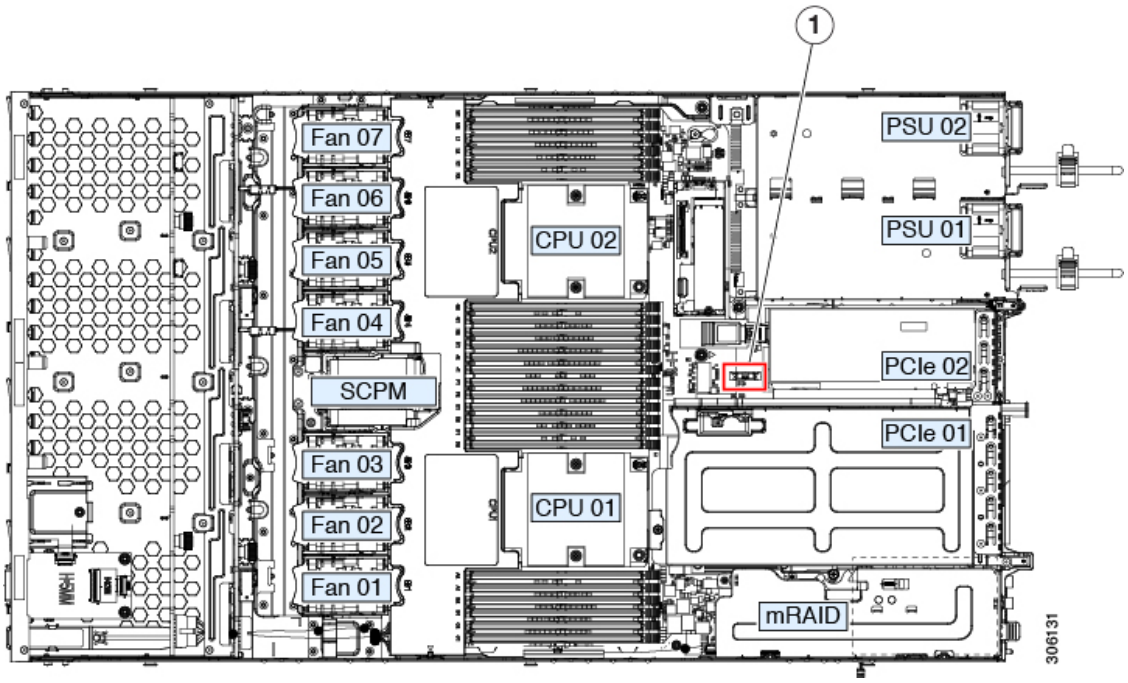
a) Insert the battery into its holder and press down until it clicks in place under the clip.

Note The flat, positive side of the battery marked "3V+" should face left as you face the server front.

b) Replace the top cover to the server.

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

Figure 36: RTC Battery Location on Motherboard



1	RTC battery in vertical socket	-	

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 114 for more information about the power supplies.
- See also Rear-Panel LEDs, on page 30 for information about the power supply LEDs.

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

- Replacing AC Power Supplies, on page 78
- Replacing DC Power Supplies, on page 78
- Installing DC Power Supplies (First Time Installation), on page 80
- Grounding for DC Power Supplies, on page 81

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.

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 33.
- 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:

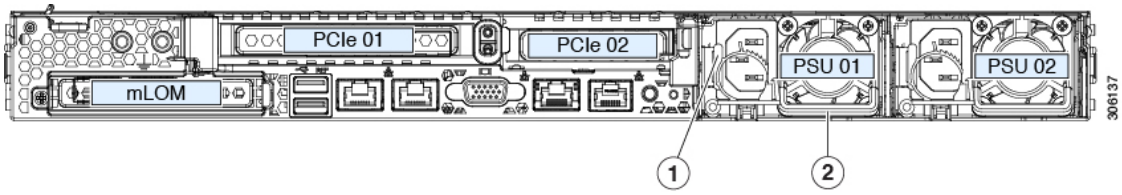
a) Grasp the power supply handle and insert the new power supply into the empty bay.

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 37: Replacing AC Power Supplies



1	Power supply release lever	**2**	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 80.

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 33.
- 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:

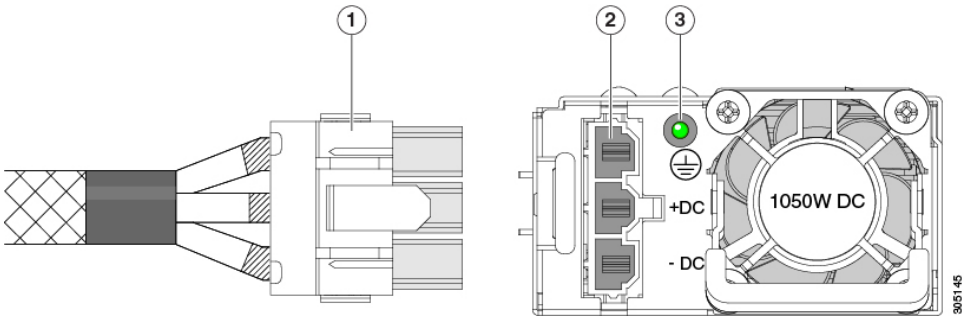
a) Grasp the power supply handle and insert the new power supply into the empty bay.

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 38: Replacing DC Power Supplies



1	Keyed cable connector (CAB-48DC-40A-8AWG)	**3**	PSU status LED
2	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 78.

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.

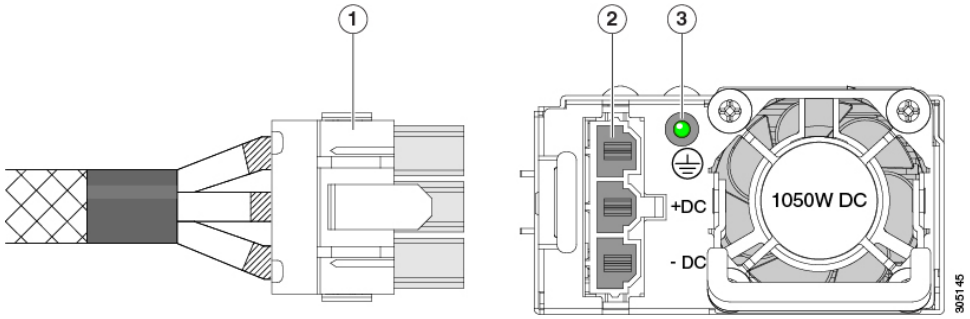
Step 2 Wire the non-terminated end of the cable to your facility's DC power input source.

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 39: Installing DC Power Supplies



1	Keyed cable connector (CAB-48DC-40A-8AWG)	**3**	PSU status LED
2	Keyed DC input socket	**-**	

Step 6 See Installation Grounding, page 3-66 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 10-32 screws. You must provide your own screws, grounding lug, and grounding wire. The grounding lug must be dual-hole lug that fits 10-32 screws. The grounding cable that you provide must be 14 AWG (2 mm), minimum 60° C wire, or as permitted by the local code.

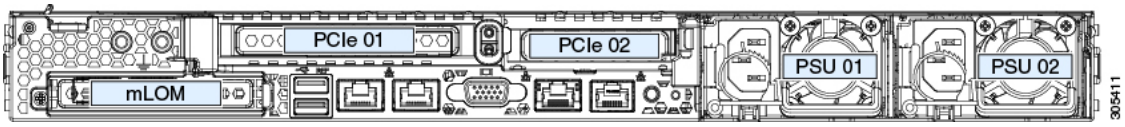
Replacing a PCIe Card

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 PCIe slots on one riser assembly for horizontal installation of PCIe cards. Both slots support the NCSI protocol and 12V standby power.

Figure 40: Rear Panel, Showing PCIe Slot Numbering



The following tables describe the specifications for the slots.

Table 7: PCIe Riser 1/Slot 1

Slot Number	Electrical Lane Width	Connector Length	Maximum Card Length	Card Height (Rear Panel Opening)	NCSI Support
1	Gen-3 x16	x24 connector	¾ length	Full-height	Yes
Micro SD card slot	One socket for Micro SD card				

Table 8: PCIe Riser 2/Slot 2

Slot Number	Electrical Lane Width	Connector Length	Maximum Card Length	Card Height (Rear Panel Opening)	NCSI Support
2	Gen-3 x16	x24 connector	½ length	½ height	Yes
PCIe cable connector for front-panel NVMe SSDs	Gen-3 x8	Other end of cable connects to front drive backplane to support front-panel NVMe SSDs.			

Note Riser 2/Slot 2 is not available in single-CPU configurations.

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 85.

Note RAID controller cards install into a separate mRAID riser. See Replacing a SAS Storage Controller Card (RAID or HBA) in Riser 3, on page 89.

Step 1 Remove an existing PCIe card (or a blank filler panel) from the PCIe riser:

a) Shut down and remove power from the server as described in Shutting Down and Removing Power From the Server, on page 33.

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 35.

d) Remove any cables from the ports of the PCIe card that you are replacing.

e) Use two hands to grasp the external riser handle and the blue area at the front of the riser.

f) Lift straight up to disengage the riser's connectors from the two sockets on the motherboard. Set the riser upside-down on an antistatic surface.

g) Open the hinged plastic retainer that secures the rear-panel tab of the card.

h) 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 2 Install a new PCIe card:

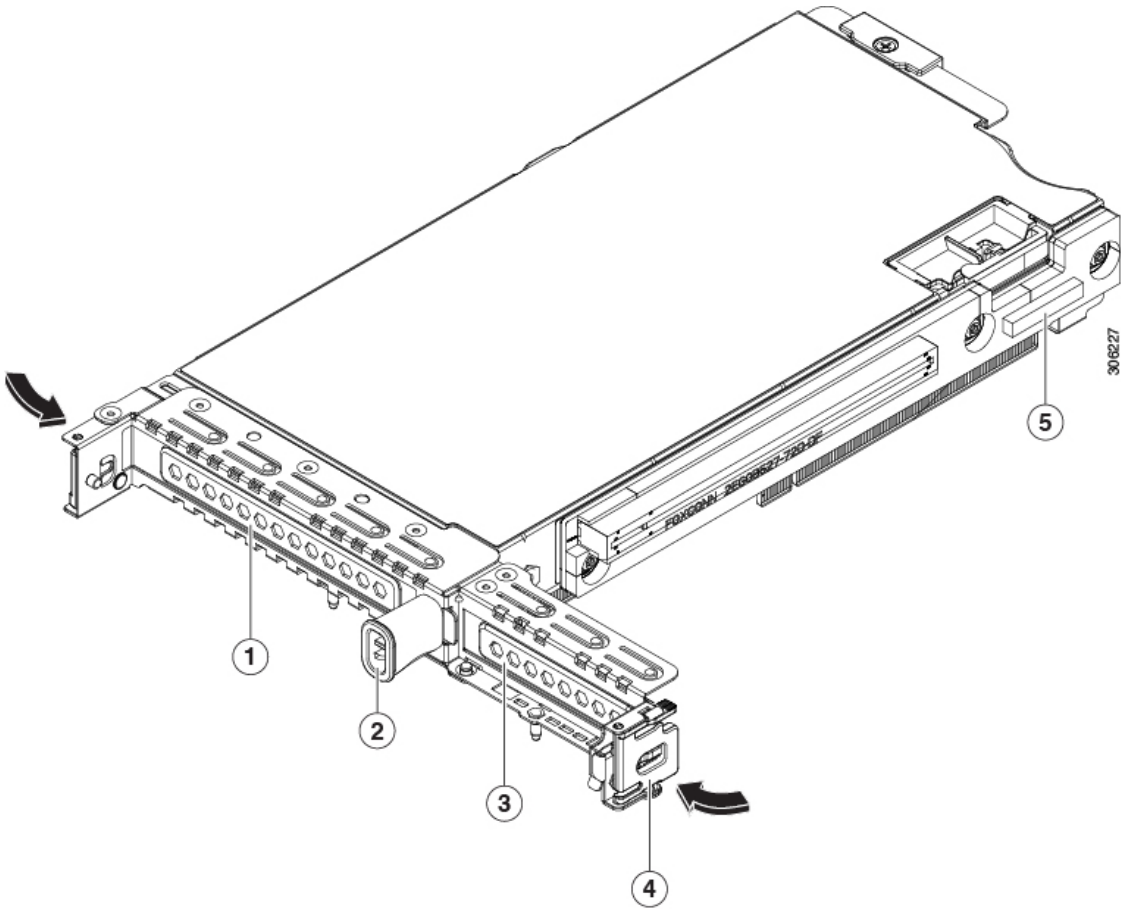
a) With the hinged tab retainer open, align the new PCIe card with the empty socket on the PCIe riser.

PCIe riser 1/slot 1 has a long-card guide at the front end of the riser. Use the slot in the long-card guide to help support a full-length card.

b) Push down evenly on both ends of the card until it is fully seated in the socket.

c) Ensure that the card’s rear panel tab sits flat against the riser rear-panel opening and then close the hinged tab retainer over the card’s rear-panel tab.

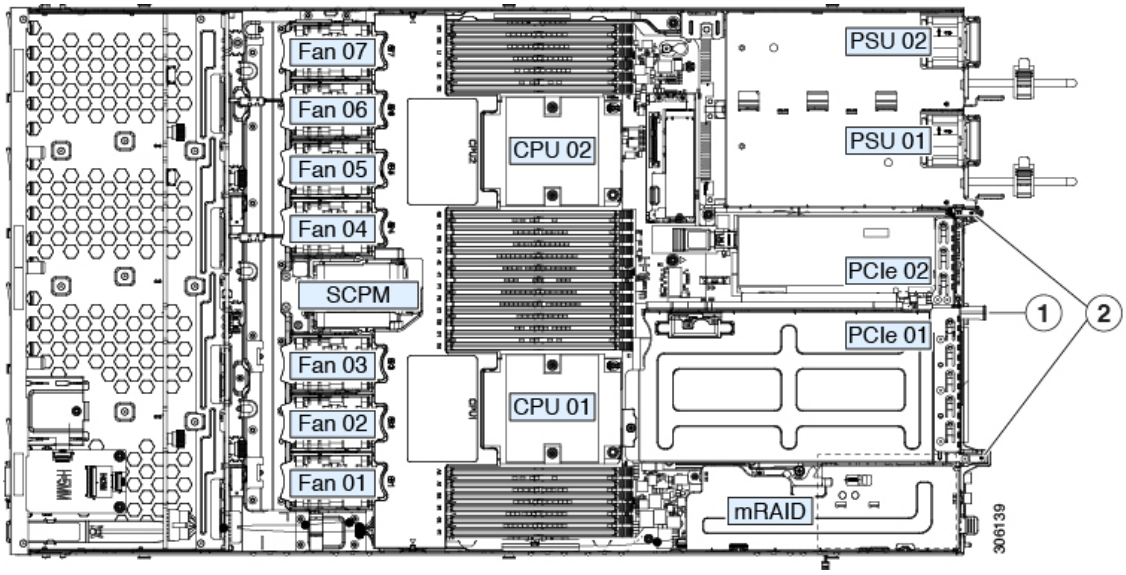
Figure 41: PCIe Riser Assembly



1	PCIe slot 1 rear-panel opening	**4**	Hinged card retainer (one each slot)
2	External riser handle	**5**	PCIe connector for cable that supports front-panel NVMe SSDs
3	PCIe slot 2 rear-panel opening		

d) Position the PCIe riser over its two sockets on the motherboard and over the two chassis alignment channels.

Figure 42: PCIe Riser Alignment Features



1	Blue riser handle	**2**	Riser alignment features in chassis

e) Carefully push down on both ends of the PCIe riser to fully engage its two connectors with the two sockets on the motherboard.
f) Replace the top cover to the server.
g) Replace the server in the rack, replace cables, and then fully power on the server by pressing the Power button.

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 9: 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 1385 UCSC-PCIE-C40Q-03	2 PCIe	PCIe 1 PCIe 2	PCIe 1	PCIe 1	3.1(1)

Cisco UCS VIC 1455 UCSC-PCIE-C25Q-04	2 PCIe	PCIe 1 PCIe 2	PCIe 1	PCIe 1	4.0(1)
Cisco UCS VIC 1495 UCSC-PCIE-C100-04	2 PCIe	PCIe 1 PCIe 2	PCIe 1	PCIe 1	4.0(2)
Cisco UCS VIC 1387 UCSC-MLOM-C40Q-03	1 mLOM	mLOM	mLOM	mLOM	3.1(1)
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)

Replacing an mLOM Card

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

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.

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 33.

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 35.

d) Remove the mRAID riser to provide access to the mLOM socket below the riser.

To remove the mRAID riser, use both hands to grasp the external blue handle on the rear and the blue finger-grip on the front. Lift straight up.

You do not have to disconnect cables from any RAID card or interposer card that is installed in the riser. Carefully move the riser aside only far enough to provide clearance.

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.

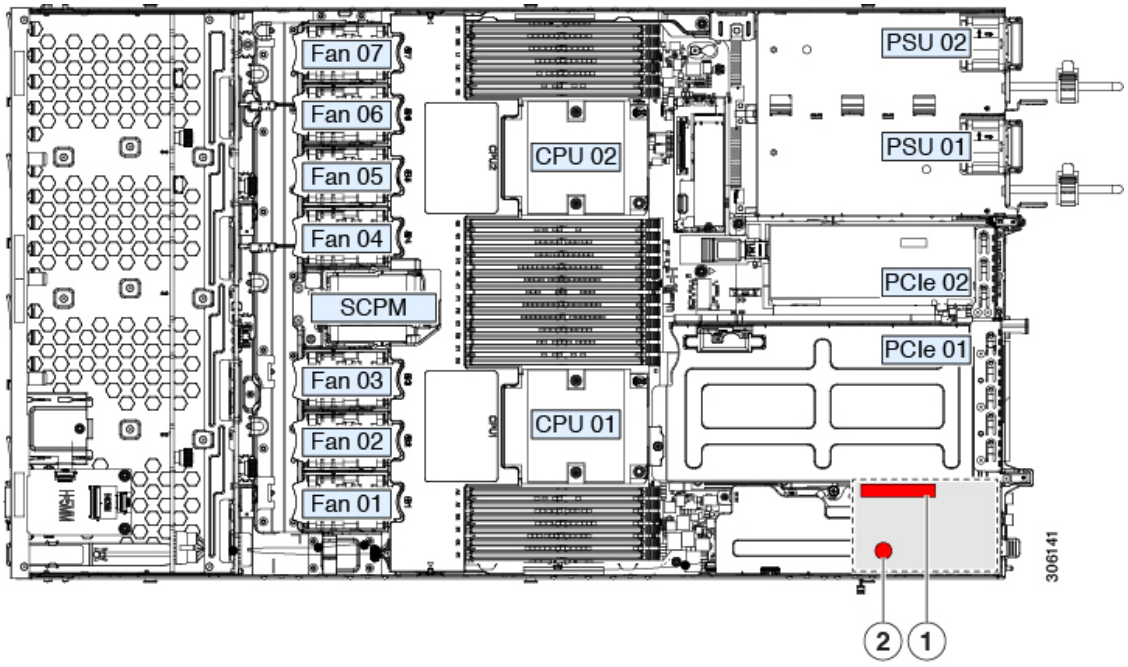
c) Tighten the captive thumbscrew to secure the card to the standoff on the chassis floor.

d) Return the mRAID riser to its socket.

Carefully align the riser's edge connector with the motherboard socket at the same time you align the two channels on the riser with the two pegs on the inner chassis wall. Press down evenly on both ends of the riser to fully engage its connector with the motherboard socket.

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 43: Location of the mLOM Card Socket Below the mRAID Riser



1	Position of horizontal mLOM card socket	**2**	Position of mLOM card thumbscrew

Replacing an mRAID Riser (Riser 3)

The server has a dedicated internal riser that is used for either a Cisco modular storage controller card (RAID or HBA) or the SATA interposer card for embedded software RAID. This riser plugs into a dedicated motherboard socket and provides a horizontal socket for the installed card.

This riser can be ordered as the following options:

- UCSC-XRAIDR-220M5—Replacement unit for this mRAID riser.
- UCSC-MRAID1GB-KIT—Kit for first-time addition of this riser (includes RAID controller, supercap, and supercap cable).

  See also Replacing a SAS Storage Controller Card (RAID or HBA) in Riser 3, on page 89.

  See also Replacing the Supercap (RAID Backup), on page 95.

- UCSC-SATA-KIT-M5—Kit for first-time addition of this riser (includes SATA interposer for embedded software RAID and SATA cables).

See also Replacing a SATA Interposer Card , on page 96.

- The NVMe-optimized, SFF 10-drive version, UCSC-220-M5SN, supports NVMe drives only and so does not use SAS or SATA RAID. This version of the server comes with an NVMe-switch card factory-installed in the internal mRAID riser to support NVMe drives in front-loading bays 3 - 10. The NVMe switch card is not orderable separately.

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 33.

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 35.

Step 2 Remove the existing mRAID riser:

a) Using both hands, grasp the external blue handle on the rear of the riser and the blue finger-grip on the front end of the riser.

b) Lift the riser straight up to disengage it from the motherboard socket.

c) Set the riser upside down on an antistatic surface.

d) Remove any card from the riser. Open the blue card-ejector lever that is on the edge of the card and then pull the card straight out from its socket on the riser.

Step 3 Install a new mRAID riser:

a) Install your card into the new riser. Close the card-ejector lever on the card to lock it into the riser.

b) Connect cables to the installed card.

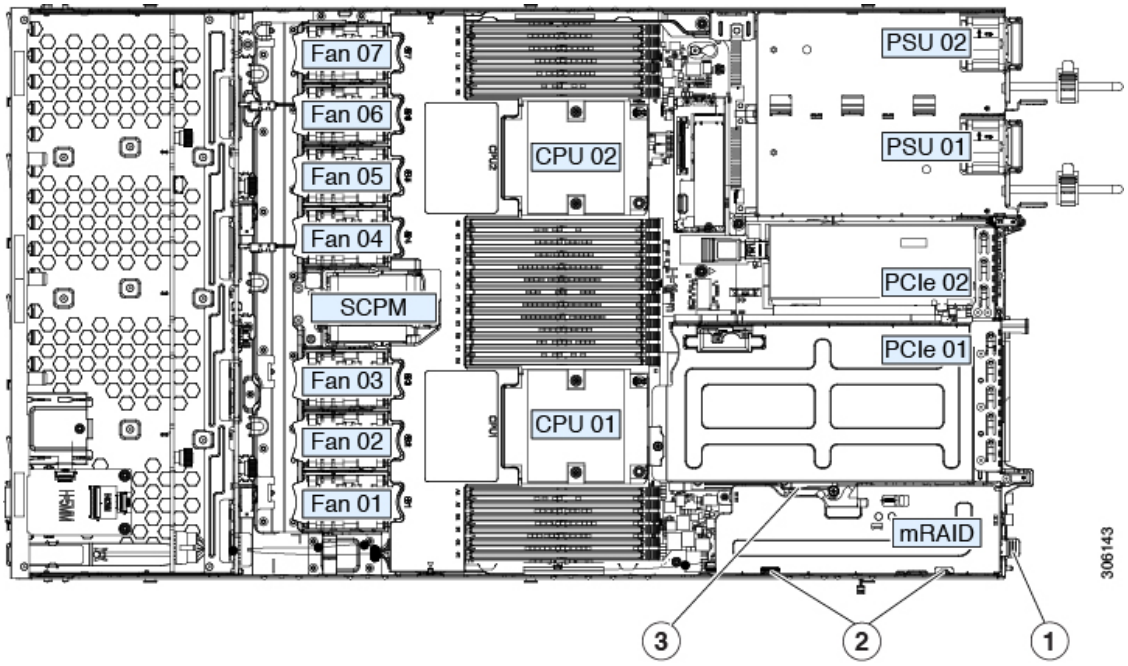
c) Align the riser with the socket on the motherboard. At the same time, align the two slots on the back side of the bracket with the two pegs on the inner chassis wall.

d) Push down gently to engage the riser with the motherboard socket. The metal riser bracket must also engage the two pegs that secure it to the chassis wall.

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.

Figure 44: mRAID Riser (Internal Riser 3) Location



1	External blue handle	**3**	Card-ejector lever
2	Two pegs on inner chassis wall	-	

Replacing a SAS Storage Controller Card (RAID or HBA) in Riser 3

For hardware-based storage control, the server can use a Cisco modular SAS RAID controller or SAS HBA that plugs into a horizontal socket on a dedicated mRAID riser (internal riser 3).

Note You cannot use a hardware RAID controller card and the embedded software RAID controller to control front-panel drives at the same time. See Embedded SATA RAID Controller, on page 127 for details.

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 Cisco Host Upgrade Utility (HUU) for your firmware release to bring it to a compatible level.

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.

Note **For servers running in standalone mode only:** After you replace controller hardware, you must run the Cisco 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.

Replacing a SAS Storage Controller Card (RAID or HBA)

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 33.

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 35.

Step 2 Remove the mRAID riser (riser 3) from the server:

a) Using both hands, grasp the external blue handle on the rear of the riser and the blue finger-grip on the front end of the riser.

b) Lift the riser straight up to disengage it from the motherboard socket.

c) Set the riser upside down on an antistatic surface.

Step 3 Remove any existing card from the riser:

a) Disconnect cables from the existing card.

b) Open the blue card-ejector lever on the back side of the card to eject it from the socket on the riser.

c) Pull the card from the riser and set it aside.

Step 4 Install a new storage controller card to the riser:

a) With the riser upside down, set the card on the riser.

b) Push on both corners of the card to seat its connector in the riser socket.

c) Close the card-ejector lever on the card to lock it into the riser.

d) Connect cables to the installed card.

Step 5 Return the riser to the server:

a) Align the connector on the riser with the socket on the motherboard. At the same time, align the two slots on the back side of the bracket with the two pegs on the inner chassis wall.

b) Push down gently to engage the riser connector with the motherboard socket. The metal riser bracket must also engage the two pegs that secure it to the chassis wall.

Step 6 Replace the top cover to the server.

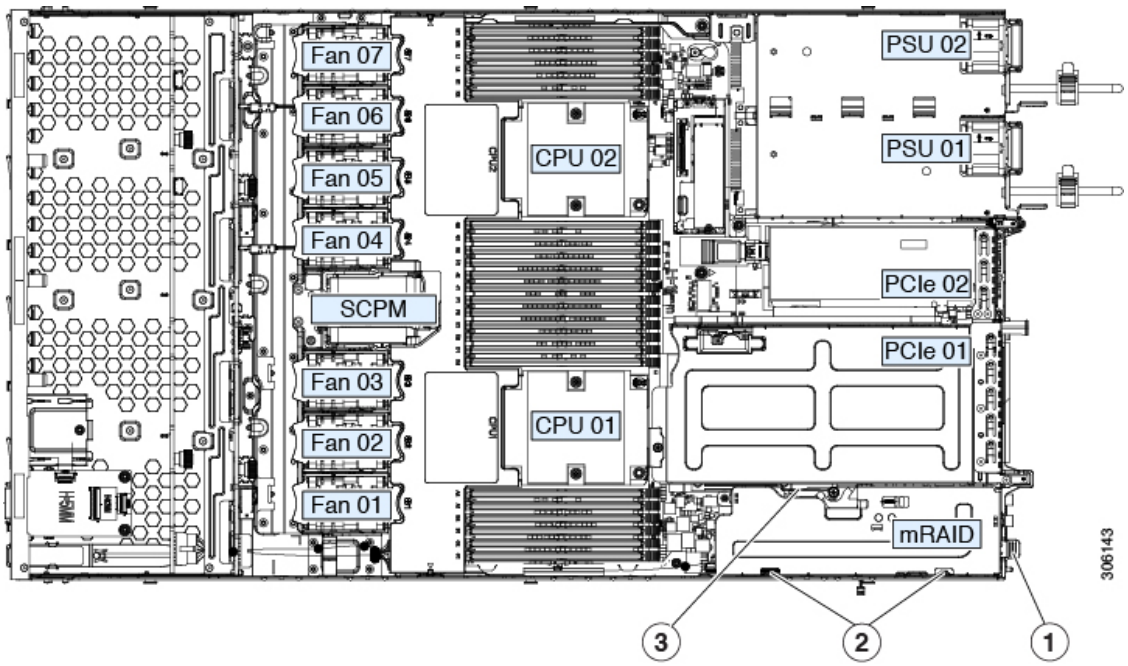
Step 7 Replace the server in the rack, replace cables, and then fully power on the server by pressing the Power button.

Step 8 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-RAID-M5 or 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 45: mRAID Riser (Internal Riser 3) Location



1	External blue handle	**3**	Card-ejector lever
2	Two pegs on inner chassis wall	-	

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:

Note The Cisco Boot-Optimized M.2 RAID Controller is not supported when the server is used as a compute-only node in Cisco HyperFlex configurations.

- 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 33.

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.

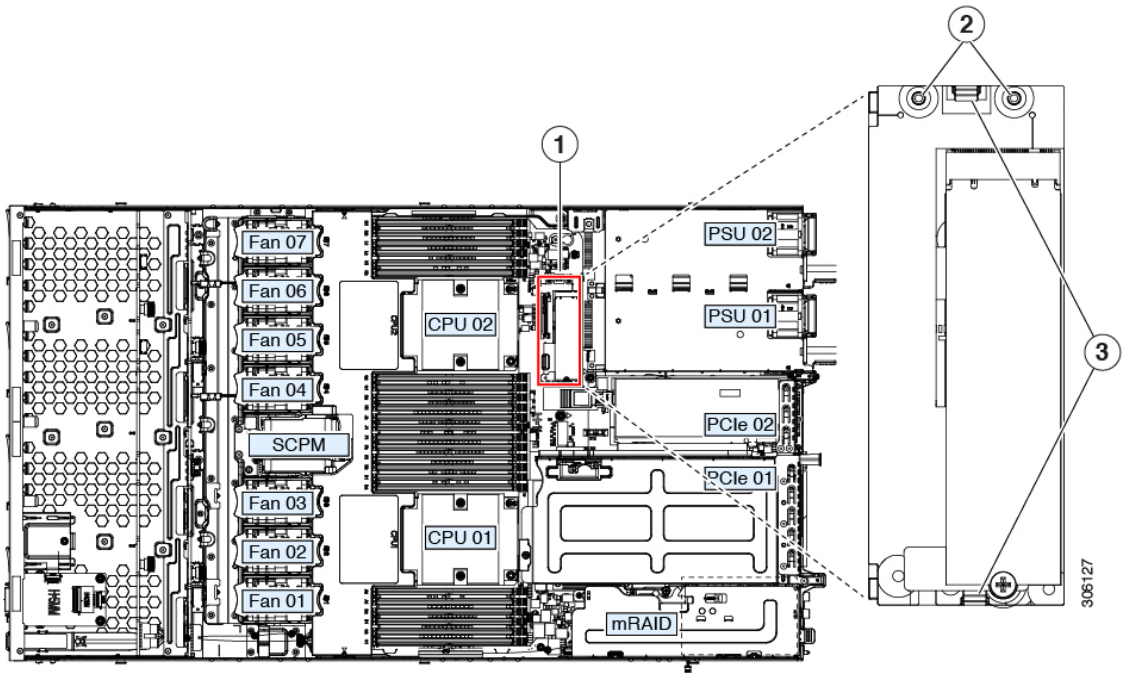
Caution If you cannot safely view and access the component, remove the server from the rack.

Step 3 Remove the top cover from the server as described in Removing the Server Top Cover, on page 35.

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



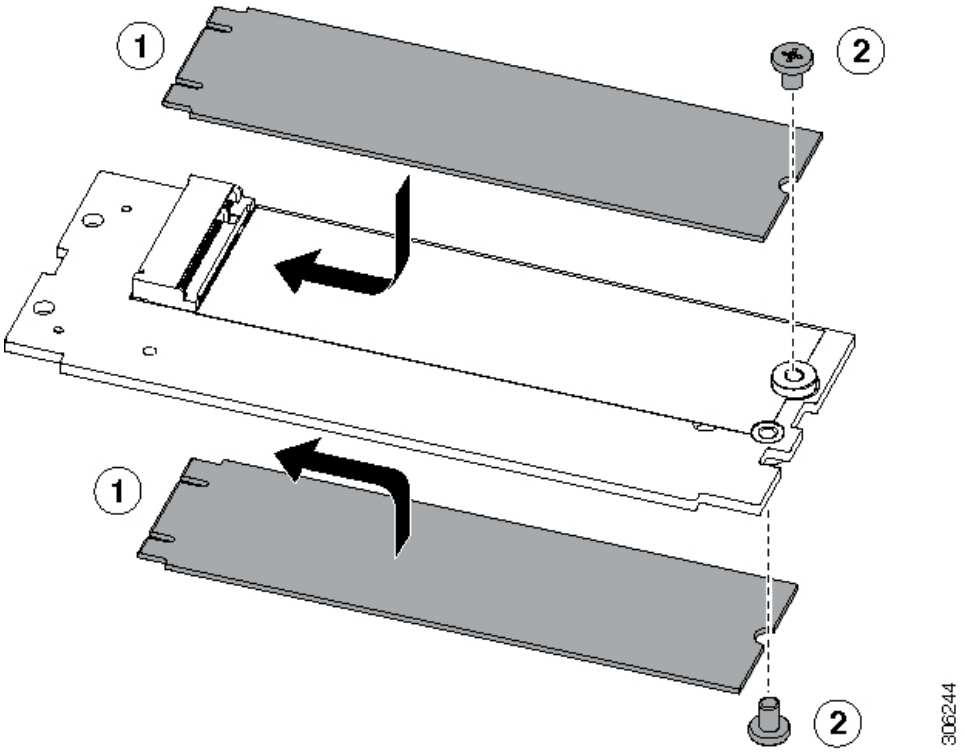
1	Location of socket on motherboard	**3**	Securing clips
2	Alignment pegs	-	

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 47: 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 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 the Supercap (RAID Backup)

This server supports installation of one supercap unit. The unit mounts to a bracket that is in the middle of the row of cooling fan modules.

The supercap provides approximately three years of backup for the disk write-back cache DRAM in the case of a sudden power loss by offloading the cache to the NAND flash.

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 33.

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 35.

Step 2 Remove an existing supercap:

a) Disconnect the supercap cable from the existing supercap.

b) Push aside the securing tab to open the hinged latch that secures the supercap to its bracket on the removable air baffle.

c) Lift the supercap free of the bracket and set it aside.

Step 3 Install a new supercap:

a) Set the new supercap into the mounting bracket.

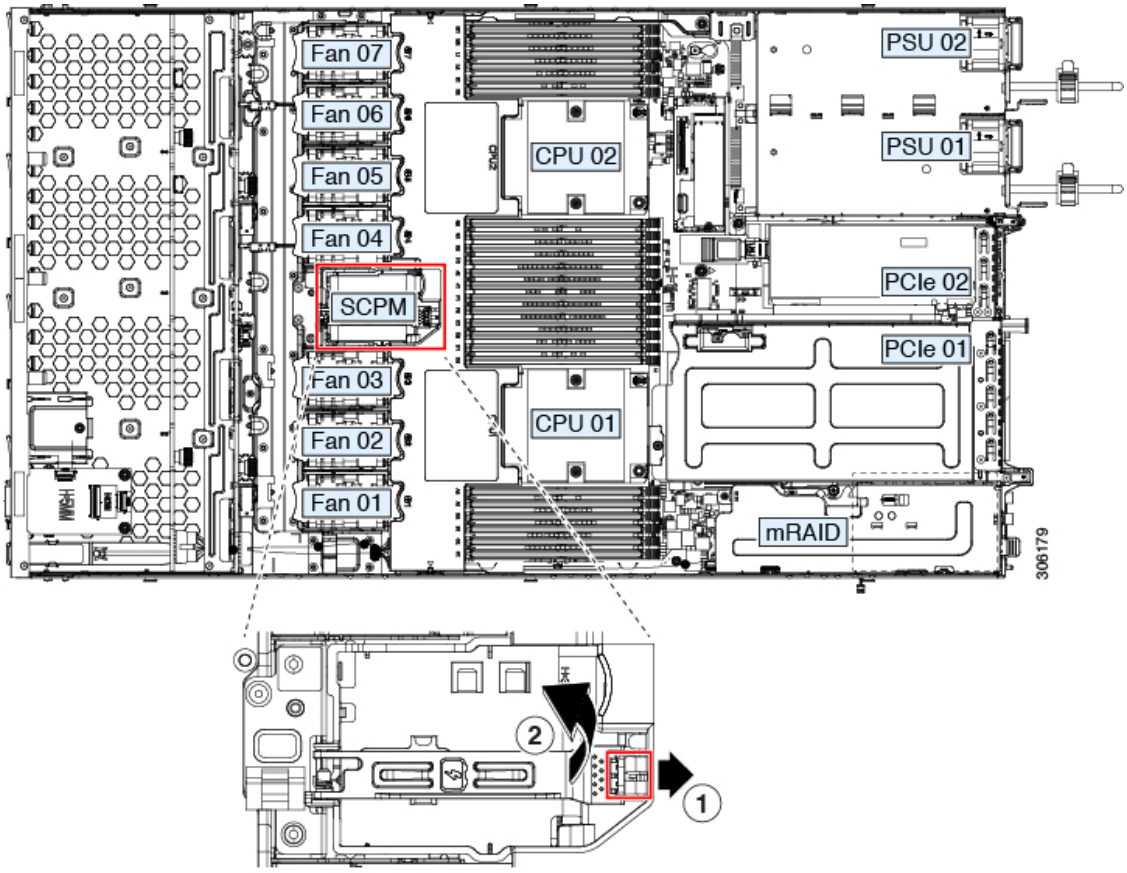
b) Close the hinged plastic clip over the supercap. Push down until the securing tab clicks.

c) Connect the supercap cable from the RAID controller card to the connector on the new supercap cable.

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.

Figure 48: Replacing Supercap



1	Securing tab	**2**	Hinged latch

Replacing a SATA Interposer Card

For software-based storage control that uses the server's embedded SATA controller, the server requires a SATA interposer card that plugs into a horizontal socket on a dedicated mRAID riser (internal riser 3).

Note You cannot use a hardware RAID controller card and the embedded software RAID controller at the same time. See Embedded SATA RAID Controller, on page 127 for details about RAID support.

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 33.
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 35.

Step 2 Remove the mRAID riser (riser 3) from the server:

a) Using both hands, grasp the external blue handle on the rear of the riser and the blue finger-grip on the front end of the riser.
b) Lift the riser straight up to disengage it from the motherboard socket.
c) Set the riser upside down on an antistatic surface.

Step 3 Remove any existing card from the riser:

a) Disconnect cables from the existing card.
b) Open the blue card-ejector lever on the back side of the card to eject it from the socket on the riser.
c) Pull the card from the riser and set it aside.

Step 4 Install a new card to the riser:

a) With the riser upside down, set the card on the riser.
b) Push on both corners of the card to seat its connector in the riser socket.
c) Close the card-ejector lever on the card to lock it into the riser.

Step 5 Return the riser to the server:

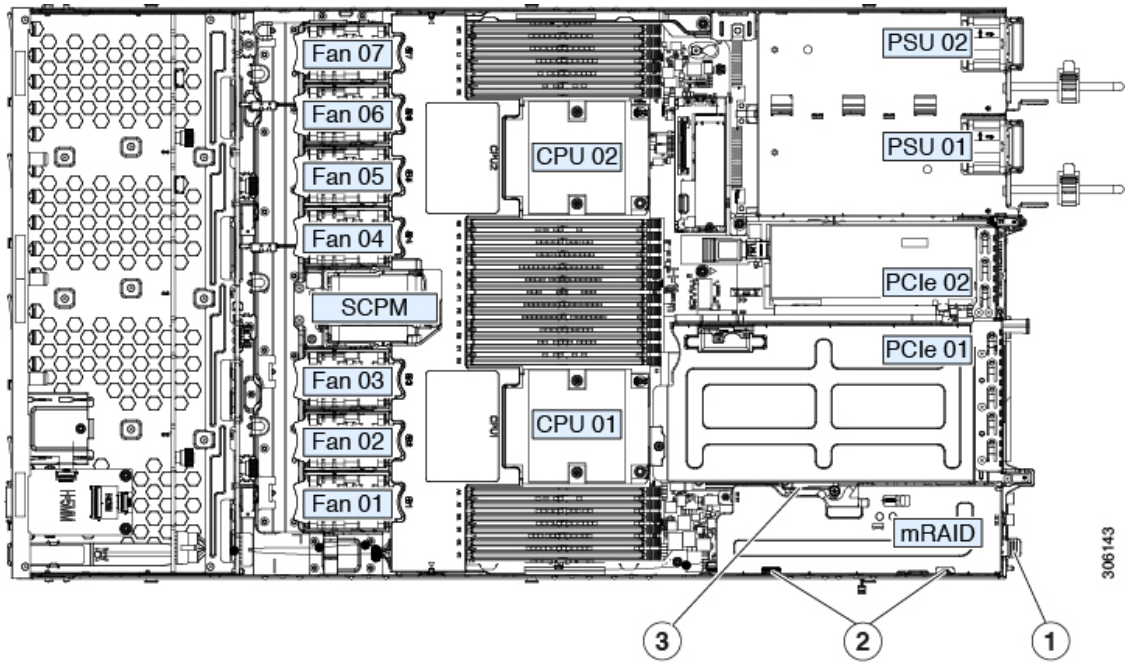
a) Align the connector on the riser with the socket on the motherboard. At the same time, align the two slots on the back side of the bracket with the two pegs on the inner chassis wall.
b) Push down gently to engage the riser connector with the motherboard socket. The metal riser bracket must also engage the two pegs that secure it to the chassis wall.

Step 6 Reconnect the cables to their connectors on the new card.

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.

Figure 49: mRAID Riser (Internal Riser 3) Location



1	External blue handle	**3**	Card-ejector lever
2	Two pegs on inner chassis wall	-	

Replacing a Chassis Intrusion Switch

The chassis intrusion switch in 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:

a) Shut down and remove power from the server as described in Shutting Down and Removing Power From the Server, on page 33.

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 35.

Step 2 Remove an existing intrusion switch:

a) Disconnect the intrusion switch cable from the socket on the motherboard.

b) Use a #1 Phillips-head screwdriver to loosen and remove the single screw that holds the switch mechanism to the chassis wall.

c) Slide the switch mechanism straight up to disengage it from the clips on the chassis.

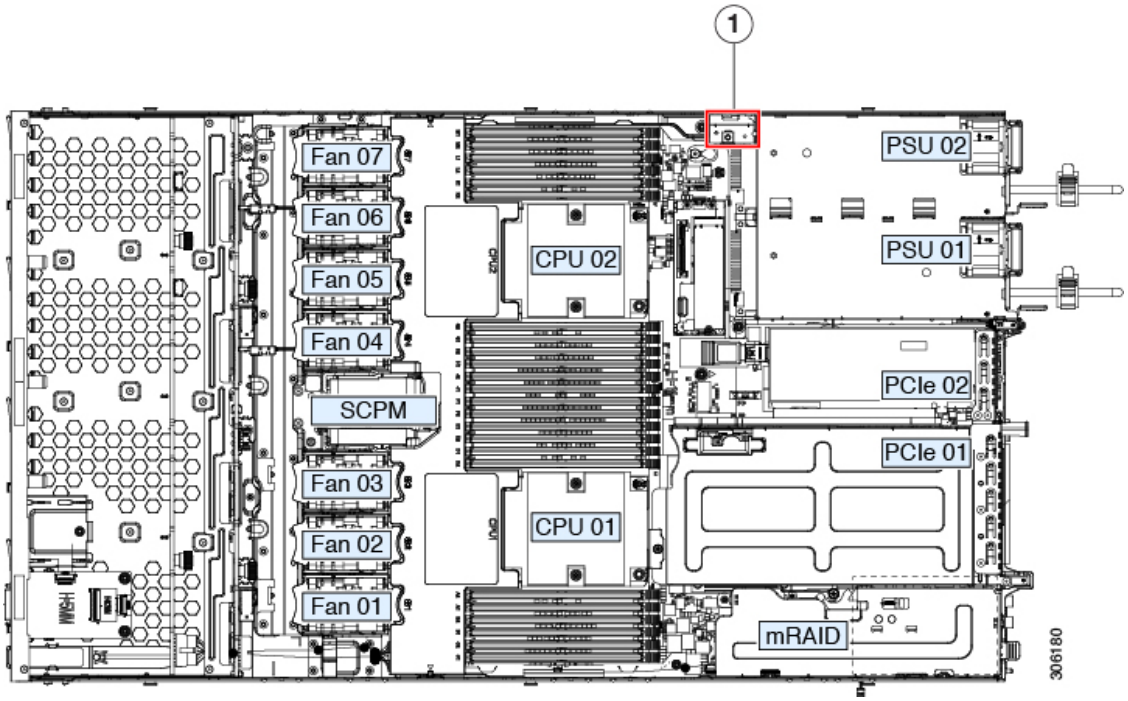
Step 3 Install a new intrusion switch:

a) Slide the switch mechanism down into the clips on the chassis wall so that the screwhole lines up.
b) Use a #1 Phillips-head screwdriver to install the single screw that secures the switch mechanism to the chassis wall.
c) 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 50: Replacing a Chassis Intrusion Switch



1	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 33.

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 35.

Step 2 Check if there is a card installed in PCIe riser 2:

- If no card is installed in PCIe riser 2, you can access the TPM socket. Go to the next step.
- If a card is installed in PCIe riser 2, remove the PCIe riser assembly from the chassis to provide clearance before continuing with the next step. See Replacing a PCIe Card, on page 83 for instructions on removing the PCIe riser.

Step 3 Install a TPM:

a) Locate the TPM socket on the motherboard, as shown below.

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.

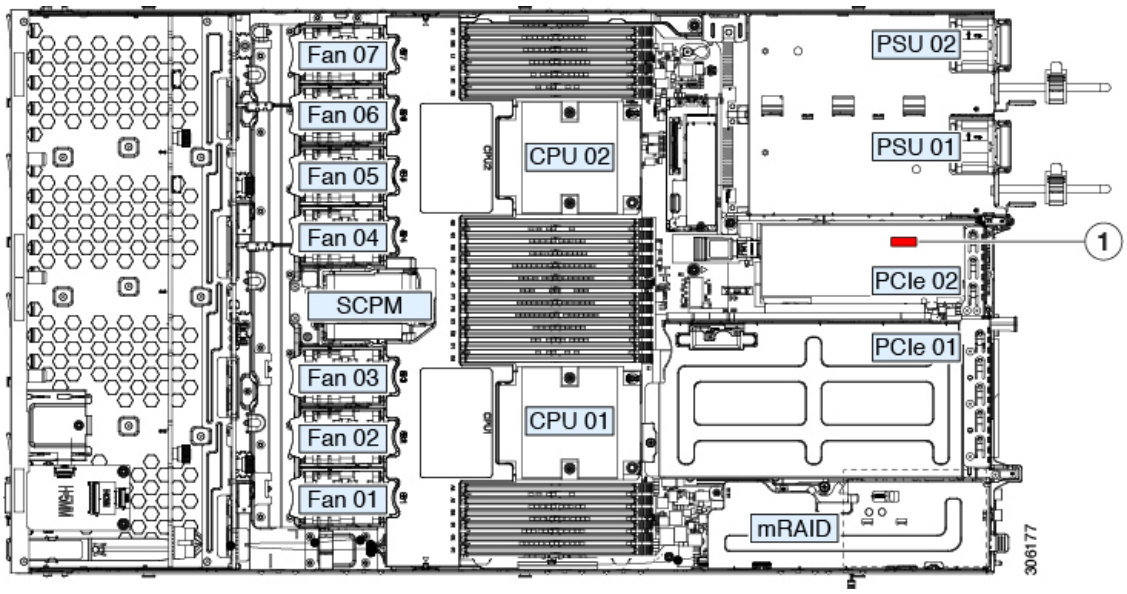
d) Install the single one-way screw that secures the TPM to the motherboard.

e) If you removed the PCIe riser assembly to provide clearance, return it to the server now.

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 51: Location of the TPM Socket



1	TPM socket location on motherboard below any card in PCIe riser 2	-	

Step 6 Continue with Enabling the TPM in the BIOS, on page 101.

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:

a) Watch during bootup for the F2 prompt, and then press **F2** to enter BIOS setup.
b) Log in to the BIOS Setup Utility with your BIOS Administrator password.
c) 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 102.

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.

Removing the Trusted Platform Module (TPM)

The TPM module is attached to the printed circuit board assembly (PCBA). You must disconnect the TPM module from the PCBA before recycling the PCBA. The TPM module is secured to a threaded standoff by a tamper resistant screw. If you do not have the correct tool for the screw, you can use a pair of pliers to remove the screw.

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.

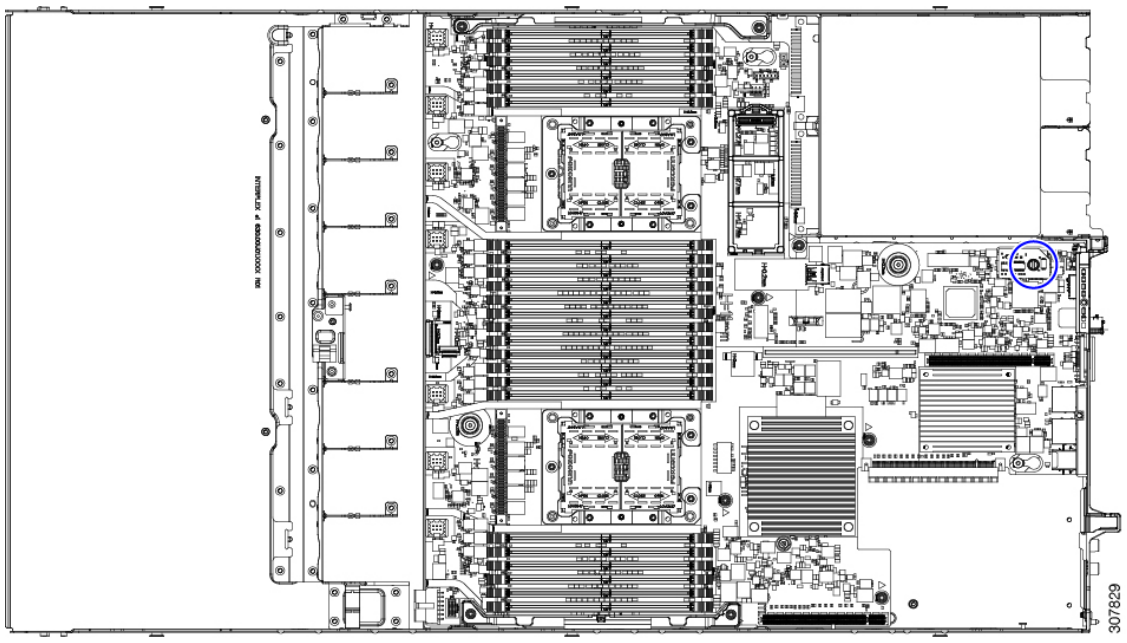
To remove the TPM, the following requirements must be met for the server:

- It must be disconnected from facility power.
- It must removed from the equipment rack.
- The top cover must be removed. If the top cover is not removed, see Removing the Server Top Cover, on page 35.

Step 1 Locate the TPM module.

The following illustration shows the location of the TPM module's screw.

Figure 52: Screw Location for Removing the TPM Module



Step 2 Using the pliers, grip the head of the screw and turn it counter clockwise until the screw releases.

Step 3 Remove the TPM module and dispose of it properly.

What to do next

Remove the PCBA. See Removing the PCB Assembly (PCBA), on page 104.

Removing the PCB Assembly (PCBA)

The PCBA is secured to the server's sheet metal. You must disconnect the PCBA from the tray before recycling the PCBA. The PCBA is secured by twelve 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 35.

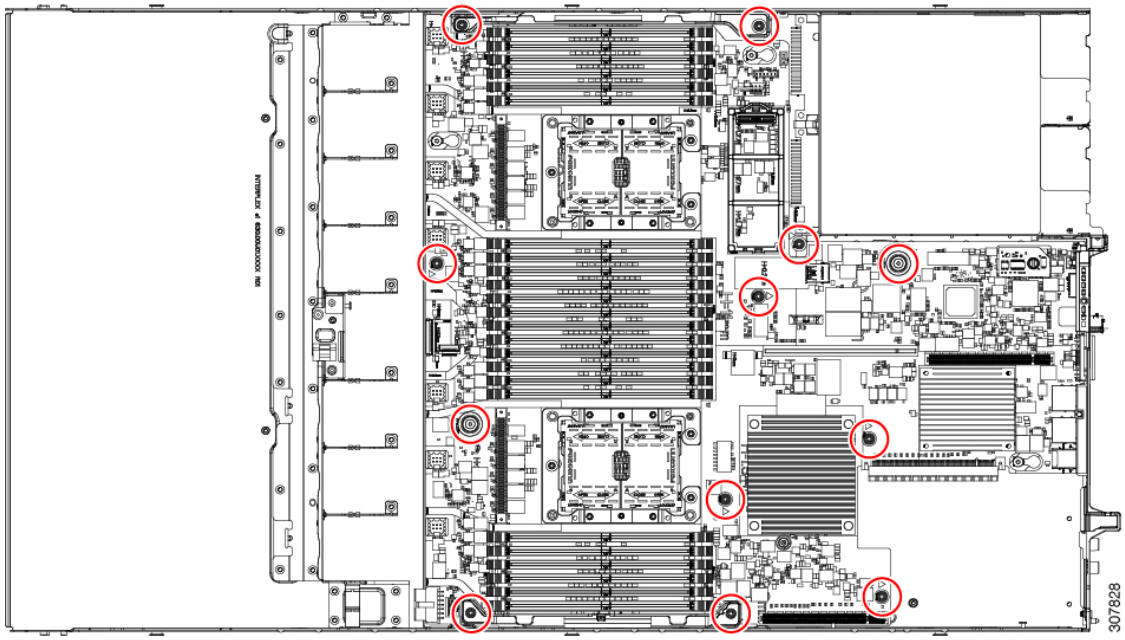
Step 1 If you have not removed the TPM module, do so now.

See Removing the Trusted Platform Module (TPM), on page 103.

Step 2 When the TPM module is detached, locate the PCBA's mounting screws.

The following figure shows the location of the mounting screws.

Figure 53: Screw Locations for Removing the PCBA



Step 3 Using a screwdriver, remove the screws.

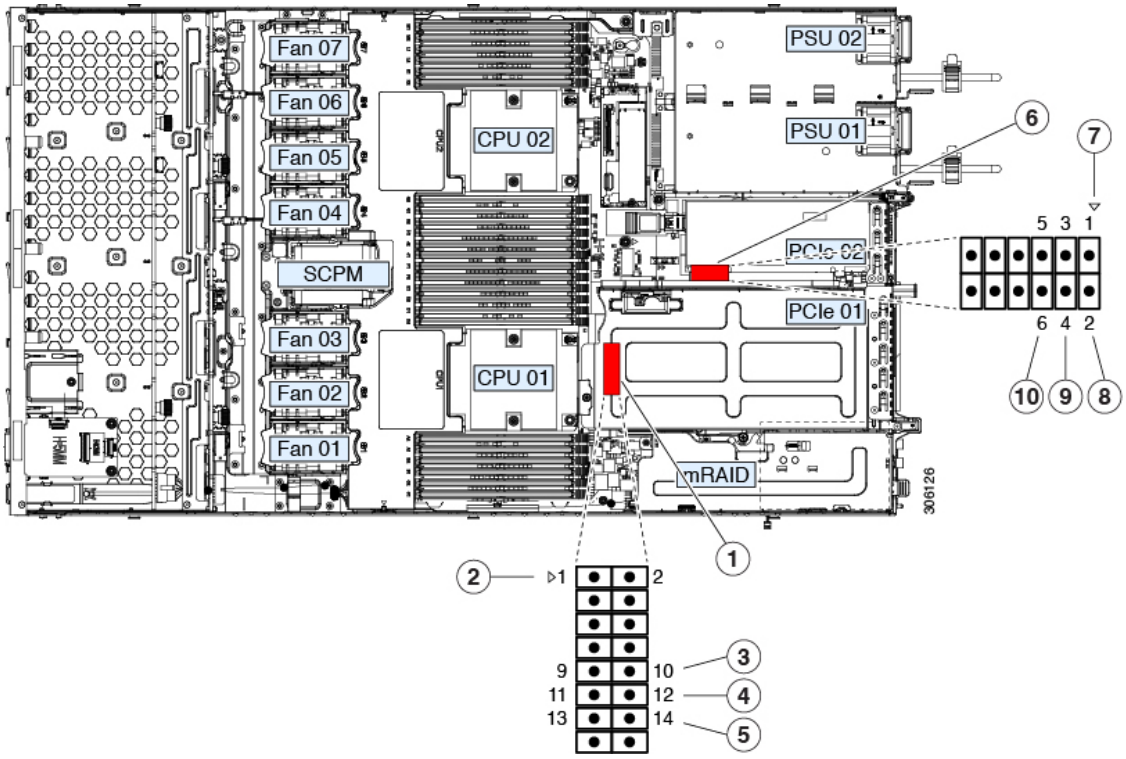
Step 4 Remove the PCBA and dispose of it properly.

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:

Figure 54: Location of Service Header Blocks J38 and J39



1	Location of header block J38	**6**	Location of header block J39
2	J38 pin 1 arrow printed on motherboard	**7**	J39 pin 1 arrow printed on motherboard
3	Clear CMOS: J38 pins 9 - 10	**8**	Boot Cisco IMC from alternate image: J39 pins 1 - 2
4	Recover BIOS: J38 pins 11 - 12	**9**	Reset Cisco IMC password to default: J39 pins 3 - 4
5	Clear password: J38 pins 13 - 14	**10**	Reset Cisco IMC to defaults: J39 pins 5 - 6

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

You can use this header 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 33. 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 35.

Step 4 Locate header block J38 and pins 9-10, as shown in Service Headers and Jumpers, on page 105.

Step 5 Install a two-pin jumper across pins 9 and 10.

Step 6 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 7 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 8 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 9 Remove the top cover from the server.

Step 10 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 11 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 recovery.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 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 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 Shut down and remove power from the server as described in Shutting Down and Removing Power From the Server, on page 33. 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 35.

Step 6 Locate header block J38 and pins 11-12, as shown in Service Headers and Jumpers, on page 105.

Step 7 Install a two-pin jumper across pins 11 and 12.

Step 8 Reconnect AC power cords to the server. The server powers up to standby power mode.

Step 9 Insert the USB thumb drive that you prepared in Step 2 into a USB port on the server.

Step 10 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 11 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 12 After the server has fully booted, power off the server again and disconnect all power cords.

Step 13 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 14 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 header 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 33. 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 35.

Step 4 Locate header block J38 and pins 13-14, as shown in Service Headers and Jumpers, on page 105.

Step 5 Install a two-pin jumper across pins 13 and 14.

Step 6 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 7 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 8 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 9 Remove the top cover from the server.

Step 10 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 11 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 33. 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 35.

Step 4 Locate header block J39, pins 1-2, as shown in Service Headers and Jumpers, on page 105.

Step 5 Install a two-pin jumper across J39 pins 1 and 2.

Step 6 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 7 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.
```

Step 8 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 9 Remove the top cover from the server.

Step 10 Remove the jumper that you installed.

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 11 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 33. 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 35.

Step 4 Locate header block J39, pins 3-4, as shown in Service Headers and Jumpers, on page 105.

Step 5 Install a two-pin jumper across J39 pins 3 and 4.

Step 6 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 7 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.
```

Step 8 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 9 Remove the top cover from the server.

Step 10 Remove the jumper that you installed.

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 11 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 33. 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 35.

Step 4 Locate header block J39, pins 5-6, as shown in Service Headers and Jumpers, on page 105.

Step 5 Install a two-pin jumper across J39 pins 5 and 6.

Step 6 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 7 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.
```

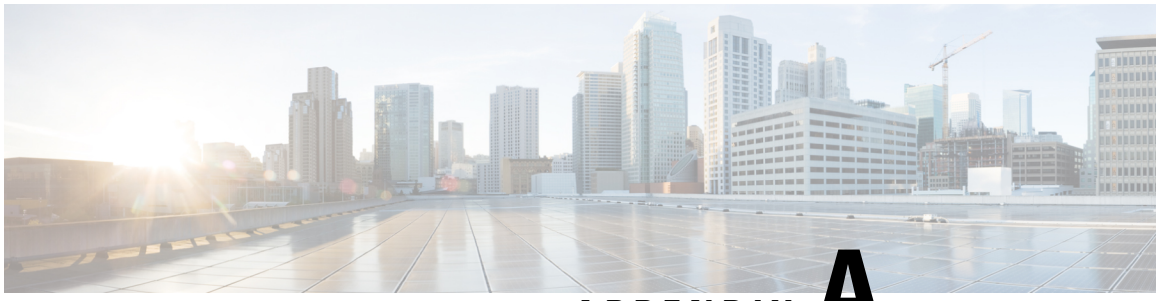
Step 8 To remove the jumper, press the Power button to shut down the server to standby power mode, and then remove AC power cords from the server to remove all power.

Step 9 Remove the top cover from the server.

Step 10 Remove the jumper that you installed.

Note If you do not remove the jumper, the server will reset the Cisco IMC to the default settiings every time that you power cycle the server. The jumper has no effect if you reboot Cisco IMC.

Step 11 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.



APPENDIX A

Server Specifications

Server Specifications

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

Physical Specifications

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

Table 10: Physical Specifications

Description	Specification
Height	1.7 in. (43.2 mm)
Width	16.9 in. (429.0 mm)
Depth (length)	Server only: 29.5 in. (740.3 mm) Server with slide rail: 31.0 in (787.4 mm)
Weight	Maximum: 37.5 lb. (17.0 Kg) Minimum: 29.0 lb. (13.2 Kg)

Environmental Specifications

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

As a Class A2 product, the server has the following environmental specifications.

Table 11: Environmental Specifications

Description	Specification

Temperature, Operating	Dry bulb temperature of 50 to 95°F (10 to 35°C) Maximum rate of change of 41°F per hour (5°C) Extended environment 41 to 104°F (5 to 40°C) with no direct sunlight Derate the maximum temperature by 1°C per every 305 meters of altitude above sea level. **Note** Although the ASHRAE guidelines define multiple classes with different operating ranges, the *recommended* temperature and humidity operating range is the same for each class. The *recommended* temperature and humidity ranges are: • Operating Temperature: 64.4°F to 80.6°F (18°C to 27°C) For general information, see the Cisco Unified Computing System Site Planning Guide: Data Center Power and Cooling.
Temperature, non-operating (when the server is stored or transported)	Dry bulb temperature of 40 °C to 65 °C (-40°F to 149 °F)
Humidity (RH), operating	10% to 90% and 28°C (82.4°F) maximum dew-point temperature, non-condensing environment
Humidity (RH), non-operating (when the server is stored or transported)	5% to 93% relative humidity, non-condensing, with a maximum wet bulb temperature of 28 °C across the 20 °C to 40 °C dry bulb range.
Altitude, operating	A maximum elevation of 3050 meters (10,006 feet)
Altitude, non-operating (when the server is stored or transported)	An elevation of 0 to 12,000 meters (39,370 feet)
Maximum Operating Duration	Unlimited
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.

770 W AC Power Supply

This section lists the specifications for each 770 W AC power supply (Cisco part number UCSC-PSU1-770W).

Table 12: 770 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	9.5 A at 100 VAC 4.5 A at 208 VAC
Maximum input volt-amperes	950 VA at 100 VAC
Maximum inrush current	15 A (sub-cycle duration)
Maximum hold-up time	12 ms at 770 W
Maximum output power per PSU	770 W
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 AC Power Supply

This section lists the specifications for each 1050 W AC power supply (Cisco part number UCSC-PSU1-1050W).

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

1600 W AC Power Supply

This section lists the specifications for each 1600 W AC power supply (Cisco part number UCSC-PSU1-1600W).

Table 14: 1600 W AC Specifications

Description	Specification
AC Input Voltage	Nominal range: 200–240 VAC (Range: 180–264 VAC)
AC Input Frequency	Nominal range: 50 to 60Hz (Range: 47–63 Hz)
Maximum AC Input current	9.5 A at 200 VAC
Maximum input volt-amperes	1250 VA at 200 VAC
Maximum inrush current	30 A at 35° C
Maximum hold-up time	80 ms at 1600 W
Maximum output power per PSU	1600 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-PSUV2-1050DC).

Table 15: 1050 W DC Specifications

Description	Specification
DC Input Voltage	Nominal range: -48 to -60 VDC (Range: -40 to -72 VDC)
Maximum DC input current	32 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

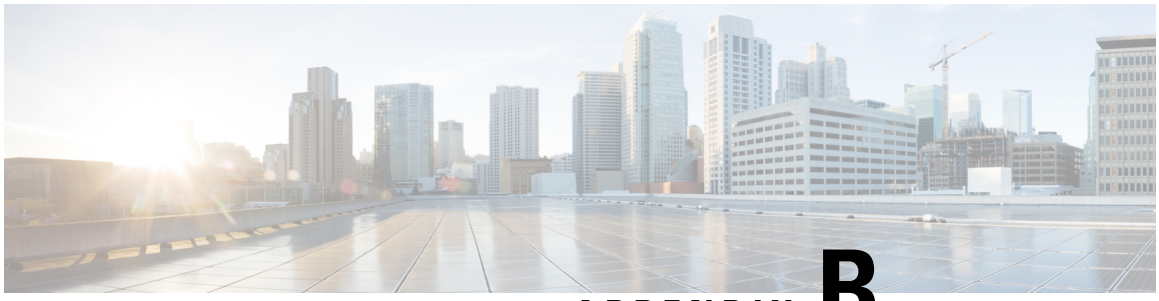
Each power supply in the server has a power cord. Standard power cords or jumper power cords are available for connection to the server. The shorter jumper power cords, for use in racks, are available as an optional alternative to the standard power cords.

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

Table 16: 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

This server supports a single, PCIe-style, SAS RAID or HBA controller that plugs into a dedicated internal riser. Alternatively, the server has a software-based SATA RAID controller embedded in the system.

Note Do not mix controller types in the server. Do not use the embedded SATA controller and a hardware-based RAID controller card at the same time. This combination is not supported and could result in data loss.

Note NVMe PCIe SSDs cannot be controlled by a SAS/SATA RAID controller.

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

Controller	Server Version/Maximum Drives Controlled	RAID Levels	Optional Supercap Backup?	Required Cables

Embedded RAID (PCH SATA)	This controller is supported only in these server versions: • All server versions can use the embedded SATA controller to control two internal SATA M.2 drives. • SFF 10-drives (C220M5SX): 8 front-loading SATA drives (drive bays 1 - 8) • LFF 4-drives (C220M5L): 4 front-loading SATA drives	0, 1, 10	No	Use SAS/SATA cable included with chassis to connect interposer board to drive backplane.
Cisco 12G Modular RAID Controller Controller is orderable only as UCSC-MRAID1G-KIT	This controller is supported only in this server version: • LFF 4-drives (C220M5L): 4 front-loading SAS/SATA drives	0, 1, 5, 6, 10, 50, 60 JBOD mode is also supported.	Yes	Use SAS/SATA cable included with chassis to connect controller to drive backplane.
Cisco 12G Modular RAID Controller with 2-GB cache UCSC-RAID-M5 Includes 2-GB cache	This controller is supported only in these server versions: • SFF 10-drives (C220M5SX): 10 front-loading SAS/SATA drives	0, 1, 5, 6, 10, 50, 60 JBOD mode is also supported.	Yes	Use SAS/SATA cable included with chassis to connect controller to drive backplane.
Cisco 12G Modular SAS HBA UCSC-SAS-M5	This controller is supported only in these server versions: • SFF 10-drives (C220M5SX): 10 front-loading SAS/SATA drives	Non-RAID	No	Use SAS/SATA cable included with chassis to connect controller to drive backplane.
Cisco 12G 9400-8e HBA for external JBOD attach UCSC-9400-8E	Supported in all server versions: 8 external SAS/SATA ports, controlling up to 1024 external drives.	Non-RAID	No	External drive cables not sold by Cisco. NOTE: This HBA does not support optical cables for connection to external storage (copper only).
Cisco Boot-Optimized M.2 RAID Controller UCS-M2-HWRAID	Supported in all server versions. Controls two SATA M.2 drives that mount to this controller.	1 JBOD mode is also supported.	No	None. Controller connects to motherboard socket.

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 Cisco Host Upgrade Utility (HUU) for your firmware release to bring it to a compatible level.

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.

Note **For servers running in standalone mode only:** After you replace controller hardware, you must run the Cisco 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.

RAID Backup (Supercap)

This server supports installation of one supercap unit. The unit mounts to a bracket in-line with the fan modules.

The optional SCPM provides approximately three years of backup for the disk write-back cache DRAM in the case of a sudden power loss by offloading the cache to the NAND flash.

For supercap unit replacement instructions, see Replacing the Supercap (RAID Backup), on page 95.

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

For this server and other Cisco Generation M5 servers, the default write-cache policy for the Cisco Modular RAID controller 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.

Mixing Drive Types in RAID Groups

The following table lists the technical capabilities for mixing hard disk drive (HDD) and solid state drive (SSD) types in a RAID group. However, see the recommendations that follow for the best performance.

Table 17: Mixing Drive Types

Mix of Drive Types in RAID Group	Allowed?
SAS HDD + SATA HDD	Yes
SAS SSD + SATA SSD	Yes
HDD + SSD	No

Drive Type Mixing Best Practices

For the best performance follow these guidelines:

- Use either all SAS or all SATA drives in a RAID group.
- Use the same capacity for each drive in the RAID group.
- Never mix HDDs and SSDs in the same RAID group.

RAID Controller Migration

This server supports SAS/SATA hardware RAID (controller card) and embedded software SATA RAID. You cannot use hardware RAID and software RAID at the same time. See the table below for which data migrations are allowed and a summary of migration steps.

Starting RAID Controller	Migrate to Hardware RAID Allowed?	Migrate to Software RAID Allowed?
None (no drives). Embedded RAID is disabled in the BIOS.	Allowed 1. Install RAID card. 2. Install SAS cables.	Allowed 1. Install SATA interposer card. 2. Install SATA cables. 3. Enable embedded RAID in BIOS.

Embedded software RAID. Embedded RAID is enabled in the BIOS.	**Caution** Data migration from software RAID to hardware RAID is *not* supported and could result in data loss. Allowed only before there is data on the drives; data migration is not supported. **1.** Disable embedded RAID in the BIOS. **2.** Install RAID card. **3.** Install SAS cables.	-
Hardware RAID. Embedded RAID is disabled in the BIOS.	-	Not allowed.

Storage Controller and Backplane Connectors

This section describes cabling connections for the storage controllers and the backplane. The SAS/SATA cables are factory-installed and are used for all supported internal controllers in both the SFF 10-drive (UCSC-C220-M5SX) and LFF 4-drive (UCSC-C220-M5L) versions of the server.

This section also contains diagrams that show the cable-to-drive mapping.

Note The SFF 10-drive version UCSC-C220-M5S*N* supports NVMe drives only, and so does not use SAS or SATA RAID. This version of the server comes with an NVMe-switch card factory-installed in the internal mRAID riser and a PCIe cable connected to PCIe riser 2. The NVMe switch card is not orderable separately.

Embedded RAID

This SW RAID option can control up to 8 SATA drives in the SFF 10-drive version and up to 4 SATA drives in the LFF 4-drive version.

This embedded RAID option requires that you have a SATA interposer card installed in internal mRAID riser 3. Use the SAS/SATA cables that came with the server.

1. Connect SAS/SATA cable A1 from the A1 interposer connector to the A1 backplane connector.
2. Connect SAS/SATA cable A2 from the A2 interposer connector to the A2 backplane connector.

Note See the following figures that illustrate cable connections and which drives are controlled by each cable. In the SFF 10-drive version, drives 5 and 10 cannot be controlled by the embedded SATA RAID controller.

Storage Controller Considerations

Figure 55: Embedded RAID Interposer Cable-to-Drive Backplane Mapping, LFF 4-Drive Version

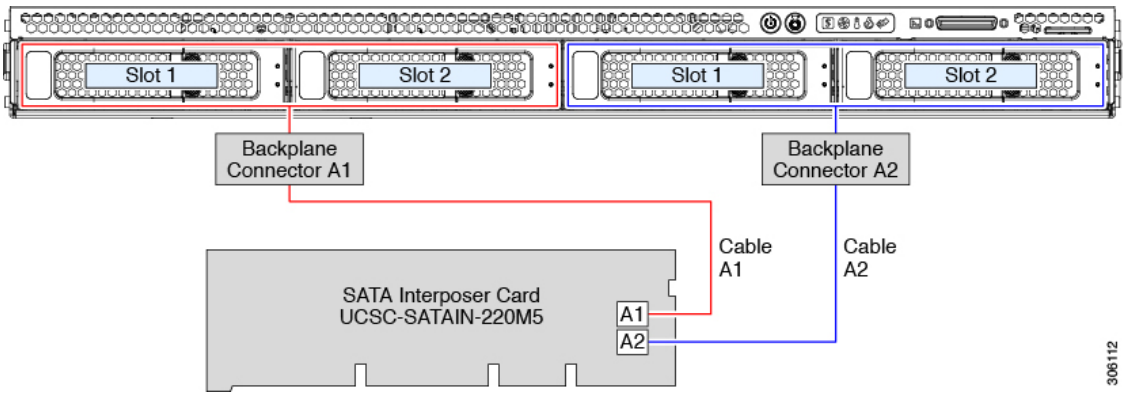
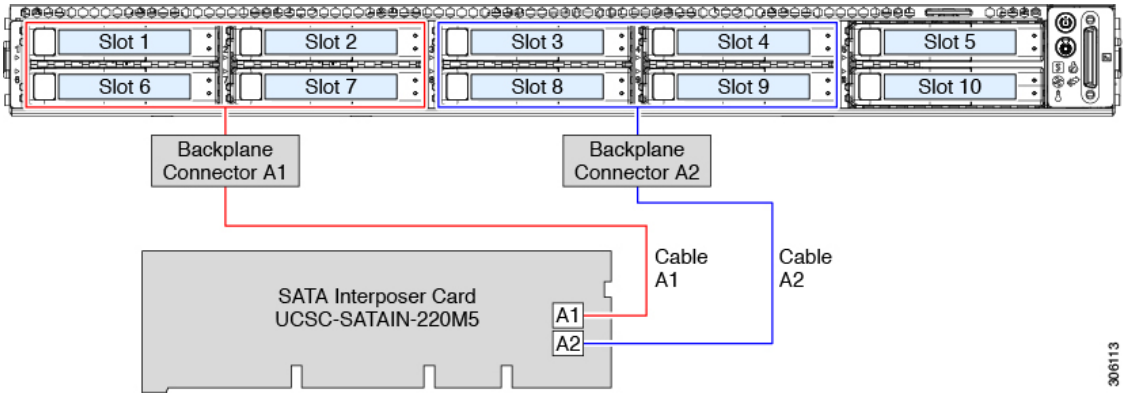


Figure 56: Embedded RAID Interposer Cable-to-Drive Backplane Mapping, SFF 10-Drive Version



Cisco 12G Modular SAS RAID Controller or HBA

This HW RAID option can control up to 10 SAS/SATA drives in the SFF 10-drive version and up to 4 SAS/SATA drives in the LFF 4-drive version.

This option requires that you have a SAS RAID or HBA card installed in internal mRAID riser 3. Use the SAS/SATA cables that came with the server.

1. Connect SAS/SATA cable A1 from the A1 card connector to the A1 backplane connector.
2. Connect SAS/SATA cable A2 from the A2 card connector to the A2 backplane connector.
3. For SFF-10-drive servers only: Connect SAS/SATA cable B2 from the B2 card connector to the B2 backplane connector.

Note See the following figures that illustrate cable connections and which drives are controlled by each cable.

Figure 57: Hardware RAID Card Cable-to-Drive Backplane Mapping, LFF 4-Drive Version

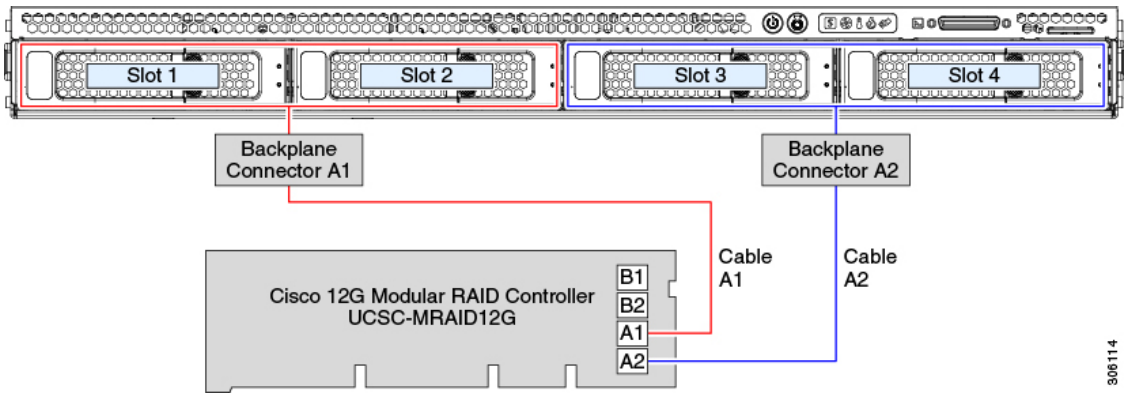
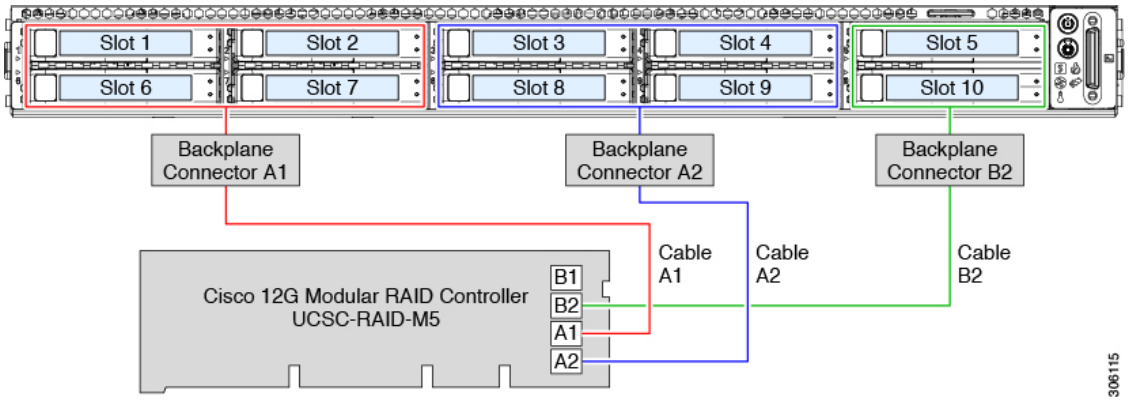


Figure 58: Hardware RAID Card Cable-to-Drive Backplane Mapping, SFF 10-Drive Version



Embedded SATA RAID Controller

This server includes an embedded MegaRAID controller that supports RAID levels 0 and 1. The primary controller can control up to eight front-loading SATA-only drives. The secondary controller can control two internal M.2 SATA drives.

Note The VMware ESX/ESXi operating system is not supported with the embedded SATA MegaRAID controller in SW RAID mode. You can use VMWare in AHCI mode.

Note The Microsoft Windows Server 2016 Hyper-V hypervisor is supported for use with the embedded MegaRAID controller in SW RAID mode, but all other hyperviors are not supported. All Hypervisors are supported in AHCI mode.

Note You cannot control the M.2 SATA SSDs in the server with a HW RAID controller.

Embbeded SATA RAID Requirements

The embedded SATA RAID controller requires the following items:

- Interposer card UCSC-SATAIN-220M5. This must be installed in internal mRAID riser 3.
- The SAS/SATA cables that are preinstalled in the chassis.
- Primary controller: SATA drives only (up to eight, in front drive bays 1–8).
- Secondary controller: M.2 mini-storage module with two SATA M.2 SSDs.
- The embedded SATA RAID controllers must be enabled in the server BIOS. If you ordered the server with embedded SATA RAID, it is enabled at the factory.
- (Optional) LSI MegaSR drivers for Windows or Linux.
- The software RAID controller requires UEFI boot mode; Legacy boot mode is not supported.
- If you use an embedded RAID controller with Linux, both the pSATA and the sSATA controller must be set to `LSI SW RAID` mode.

Embedded SATA RAID Controller Considerations

Note the following considerations:

- The default setting for this embedded controller hub is SATA RAID 0, 1, and 10 support for up to eight front-loading SATA drives, and up to two internal M.2 SATA drives. The hub is divided into two SATA controllers that have different functions. See Embedded SATA RAID: Two SATA Controllers, on page 129.
- When you order the server with this embedded controller, the controller is enabled in the BIOS. Instructions for enabling the controller are included for the case in which a server is reset. See Enabling SATA Mode For the Embedded Controllers , on page 129.
- You cannot downgrade from using a hardware RAID controller card to using the software RAID embedded controller (see RAID Controller Migration, on page 124).

  Caution Data migration from software RAID (embedded RAID) to hardware RAID (a controller card) is not supported and could result in data loss. Migrations from software RAID to hardware RAID are supported only before there is data on the drives, or when there are no drives in the server.

- The required drivers for this controller are already installed and ready to use with the LSI SWRAID Configuration Utility. However, if you will use this controller with Windows or Linux, you must download

and install additional drivers for those operating systems. See Installing LSI MegaSR Drivers For Windows and Linux, on page 131.

Embedded SATA RAID: Two SATA Controllers

The embedded RAID platform controller hub (PCH) is split into two controllers: primary SATA (pSATA) and secondary SATA (sSATA). These two controllers are seen as separate RAID controllers in the Cisco IMC interface and are configurable separately.

- SFF 10-drives server UCSC-C220-M5SX:
  - The pSATA controller controls up to eight front SATA drives (drive bays 1–8).
  - The sSATA controller controls two internal SATA M.2 drives, when they are present in the M.2 mini-storage module option.
  - If the M.2 mini-storage module is not present, or if M.2 NVMe drives are installed in the mini-storage module, the sSATA controller is automatically disabled.
- SFF 10-drives NVMe-optimized server UCSC-C220-M5SN:
  - The pSATA controller is disabled.
  - The sSATA controller controls two internal SATA M.2 drives, when they are present in the M.2 mini-storage module option.
  - If the M.2 mini-storage module is not present, or if M.2 NVMe drives are installed in the mini-storage module, the sSATA controller is automatically disabled.
- LFF 4-drives server UCSC-C220-M5L:
  - The pSATA controller controls front-loading SATA drives in bays 1-4.
  - The sSATA controller controls two internal SATA M.2 drives, when they are present in the M.2 mini-storage module option.
  - If the M.2 mini-storage module is not present, or if M.2 NVMe drives are installed in the mini-storage module, the sSATA controller is automatically disabled.
- Each controller is listed separately in the BIOS. You can enable or disable the controllers in the BIOS. See Embedded SATA RAID: Two SATA Controllers, on page 129.

Enabling SATA Mode For the Embedded Controllers

This procedure uses the server's BIOS Setup Utility.

Note If you use an embedded RAID controller with Linux, both the pSATA and the sSATA controller must be set to `LSI SW RAID` mode.

Step 1 Boot the server and press **F2** when prompted to enter the BIOS Setup utility.

Step 2 Set the SATA mode:

a) Choose the **Advanced** tab, and then choose **LOM and PCIe Slots Configuration**.

b) For the primary pSATA controller, select **pSATA** and then choose one of the options from the dialog:

- LSI SW RAID—Enable the embedded pSATA RAID controller.

  Note This menu option does not appear when the server is set to boot in Legacy mode (UEFI mode is required). To change the boot mode, use the BIOS setting for **Boot Options > Boot Mode**.

- Disabled—Disable the embedded pSATA RAID controller.

c) For the secondary sSATA controller, select **M.2** and then choose one of the options from the dialog:

- LSI SW RAID—Enable the embedded sSATA RAID controller for control of internal SATA M.2 drives.

  Note This menu option does not appear when the server is set to boot in Legacy mode (UEFI mode is required). To change the boot mode, use the BIOS setting for **Boot Options > Boot Mode**.

  Note This menu option does not appear when the server has no M.2 mini storage module, or when no SATA M.2 drive is installed in the mini-storage module.

- AHCI—Enable control of the internal SATA M.2 drives by AHCI through your OS rather than the embedded RAID controller.
- Disabled—Disable the embedded sSATA RAID controller.

Step 3 Press **F10** to save your changes and exit the utility.

Accessing the Software RAID Configuration Utility

To configure RAID settings for the embedded SATA RAID controllers, use the utility that is built into the BIOS. Each controller is controlled by its own instance of the utility.

Step 1 Boot the server and press **F2** when prompted to enter the BIOS Setup utility.

Step 2 Choose the **Advanced** tab.

Step 3 Select the instance of the utility that is for the controller that you want to manage (primary or secondary):

- For the pSATA controller, select **LSI Software RAID Configuration Utility (SATA)**.
- For the sSATA controller, select **LSI Software RAID Configuration Utility (sSATA)**.

Installing LSI MegaSR Drivers For Windows and Linux

Note The required drivers for this controller are already installed and ready to use. However, if you will use this controller with Windows or Linux, you must download and install additional drivers for those operating systems.

This section explains how to install the LSI MegaSR drivers for the following supported operating systems:

- Microsoft Windows Server
- Red Hat Enterprise Linux (RHEL)
- SUSE Linux Enterprise Server (SLES)

For the specific supported OS versions, see the Hardware and Software Compatibility Matrix for your server release.

Downloading the MegaSR Drivers

The MegaSR drivers are included in the C-Series driver ISO for your server and OS.

Step 1 Find the drivers ISO file download for your server online and download it to a temporary location on your workstation:

a) See the following URL: http://www.cisco.com/cisco/software/navigator.html.
b) Type the name of your server in the **Select a Product** search field and then press **Enter**.
c) Click **Unified Computing System (UCS) Drivers**.
d) Click the release number that you are downloading.
e) Click the Download icon to download the drivers ISO file.

Step 2 Continue through the subsequent screens to accept the license agreement and then browse to a location where you want to save the driver ISO file.

Microsoft Windows Server Drivers

Installing Microsoft Windows Server Drivers

The Windows Server operating system automatically adds the driver to the registry and copies the driver to the appropriate directory.

Before you begin

Before you install this driver on an embedded controller, you must configure a RAID drive group on the embedded controller for the drives where you will install the OS (pSATA and/or sSATA).

To access the configuration utility, open the BIOS Setup Utility, go to the **Advanced** tab, and then choose the utility instance for the embedded controller:

- For pSATA, select **LSI Software RAID Configuration Utility (SATA)**
- For sSATA, select **LSI Software RAID Configuration Utility (sSATA)**

Step 1 Download the Cisco UCS C-Series drivers' ISO, as described in Downloading the MegaSR Drivers, on page 131.

Step 2 Prepare the drivers on a USB thumb drive:

a) Burn the ISO image to a disk.
b) Browse the contents of the drivers folders to the location of the embedded MegaRAID drivers: /<OS>/Storage/Intel/C600-M5/
c) Expand the Zip file, which contains the folder with the MegaSR driver files.
d) Copy the expanded folder to a USB thumb drive.

Step 3 Start the Windows driver installation using one of the following methods:

- To install from local media, connect an external USB DVD drive to the server and then insert the first Windows installation disk into the drive. Skip to Step 6.
- To install from remote ISO, log in to the server's Cisco IMC interface and continue with the next step.

Step 4 Launch a Virtual KVM console window and click the **Virtual Media** tab.

a) Click **Add Image** and browse to select your remote Windows installation ISO file.
b) Check the check box in the **Mapped** column for the media that you just added, and then wait for mapping to complete.

Step 5 Power cycle the server.

Step 6 Press **F6** when you see the F6 prompt during bootup. The Boot Menu window opens.

Step 7 On the Boot Manager window, choose the physical disk or virtual DVD and press **Enter**. The Windows installation begins when the image is booted.

Step 8 Press **Enter** when you see the prompt, "Press any key to boot from CD."

Step 9 Observe the Windows installation process and respond to prompts in the wizard as required for your preferences and company standards.

Step 10 When Windows prompts you with "Where do you want to install Windows," install the drivers for embedded MegaRAID:

a) Click **Load Driver**. You are prompted by a Load Driver dialog box to select the driver to be installed.
b) Connect the USB thumb drive that you prepared in Step 3 to the target server.
c) On the Windows Load Driver dialog, click **Browse**.
d) Use the dialog box to browse to the location of the drivers folder on the USB thumb drive, and then click **OK**.

   Windows loads the drivers from the folder and when finished, the driver is listed under the prompt, "Select the driver to be installed."

e) Click **Next** to install the drivers.

Updating Microsoft Windows Server Drivers

Step 1 Click **Start**, point to **Settings**, and then click **Control Panel**.

Step 2 Double-click **System**, click the **Hardware** tab, and then click **Device Manager**. Device Manager starts.

Step 3 In Device Manager, double-click **SCSI and RAID Controllers**, right-click the device for which you are installing the driver, and then click **Properties**.

Step 4 On the Driver tab, click **Update Driver** to open the Update Device Driver wizard, and then follow the wizard instructions to update the driver.

Linux Drivers

Dowloading the Driver IMG or ISO File

See Downloading the MegaSR Drivers, on page 131 for instructions on downloading the drivers. Within the Cisco UCS Drivers ISO image, the MegaSR driver is included in a `dud-[driver version].img` (or dd.iso).

Note The LSI MegaSR drivers that Cisco provides for RHEL and SLES are for the original GA versions of those distributions. The drivers do not support updates to those OS kernels.

Preparing Physical Thumb Drive for Linux

This topic describes how to prepare physical Linux thumb drive from the driver image files.

This procedure requires a CD or DVD drive that you can use to burn the ISO image to disk; and a USB thumb drive.

Alternatively, you can mount the dud.img file as a virtual disk, as described in the installation procedures.

For RHEL and SLES, you can use a driver disk utility to create disk images from image files.

Step 1 Download the Cisco UCS C-Series drivers ISO, as described in Downloading the MegaSR Drivers, on page 131 and save it to your Linux system.

Step 2 Extract the dud.img or dd.iso driver file:

Note For RHEL 7.1 and later, there is no dud.img file--the driver is contained in a dd.iso file.

a) Burn the Cisco UCS C-Series Drivers ISO image to a disc.
b) Browse the contents of the drivers folders to the location of the embedded MegaRAID drivers: /<OS>/Storage/Intel/C600-M5/
c) Expand the Zip file, which contains the folder with the driver files.

Step 3 Copy the driver update disk image `dud-[driver version].img` (or dd.iso) to your Linux system.

Step 4 Insert a blank USB thumb drive into a port on your Linux system.

Step 5 Create a directory and mount the dud.img or dd.iso image to that directory:

Example:

```
mkdir <destination_folder>
mount -oloop <driver_image> <destination_folder>
```

Step 6 Copy the contents in the directory to your USB thumb drive.

Installing the Red Hat Enterprise Linux Driver

For the specific supported OS versions, see the Hardware and Software Compatibility Matrix for your server release.

This topic describes the fresh installation of the RHEL device driver on systems that have the embedded MegaRAID stack.

Note If you use an embedded RAID controller with Linux, both the pSATA and the sSATA controller must be set to `LSI SW RAID` mode.

Before you begin

Before you install this driver on an embedded controller, you must configure a RAID drive group on the embedded controller that controls the drives where you will install the OS (pSATA and/or sSATA).

To access the configuration utility, open the BIOS Setup Utility, go to the **Advanced** tab, and then choose the utility instance for the embedded controller:

- For pSATA, select **LSI Software RAID Configuration Utility (SATA)**
- For sSATA, select **LSI Software RAID Configuration Utility (sSATA)**

Step 1 Prepare the `dud.img` (or dd.iso) file using one of the following methods:

Note For RHEL 7.1 and later, there is no dud.img file--the driver is contained in a dd.iso file.

- To install from physical drive, use the procedure in Preparing Physical Thumb Drive for Linux, on page 133, then continue with step 3.
- To install from *virtual* disk, download the Cisco UCS C-Series drivers' ISO, as described in Downloading the MegaSR Drivers, on page 131, then continue with the next step.

Step 2 Extract the `dud.img` (or dd.iso) file:

a) Burn the Cisco UCS C-Series Drivers ISO image to a disk.
b) Browse the contents of the drivers folders to the location of the embedded MegaRAID drivers: /<OS>/Storage/Intel/C600-M5/
c) Copy the `dud-<driver version>.img` (or dd.iso) file to a temporary location on your workstation.
d) If you are using RHEL 7.x, rename the saved dd.iso to dd.img.

Note If you are using RHEL 7.x, renaming the dd.iso file to dd.img simplifies this procedure and saves time. The Cisco UCS virtual drive mapper can map only one .iso at a time, and only as a virtual CD/DVD. Renaming the file to dd.img allows you to mount the RHEL installation ISO as a virtual CD/DVD and the renamed dd.img as a virtual floppy disk or removable disk at the same time. This avoids the steps of unmounting and remounting the RHEL ISO when the dd.iso driver file is prompted for.

Step 3 Start the Linux driver installation using one of the following methods:

- To install from local media, connect an external USB CD/DVD drive to the server and then insert the first RHEL installation disk into the drive. Then continue with Step 5.

- To install from virtual disk, log in to the server's Cisco IMC interface. Then continue with the next step.

Step 4 Launch a Virtual KVM console window and click the **Virtual Media** tab.

a) Click **Add Image** and browse to select your remote RHEL installation ISO image.

Note An .iso file can be mapped only as a virtual CD/DVD.

b) Click **Add Image** again and browse to select your RHEL 6.x `dud.img` or the RHEL 7.x dd.img file that you renamed in step 2.

Note Map the .img file as a virtual floppy disk or virtual removable disk.

c) Check the check boxes in the **Mapped** column for the media that you just added, then wait for mapping to complete.

Step 5 Power-cycle the target server.

Step 6 Press **F6** when you see the F6 prompt during bootup. The Boot Menu window opens.

Note Do not press Enter in the next step to start the installation. Instead, press **e** to edit installation parameters.

Step 7 On the Boot Menu window, use the arrow keys to select **Install Red Hat Enterprise Linux** and then press **e** to edit installation parameters.

Step 8 Append one of the following blacklist commands to the end of the line that begins with **linuxefi**:

- For RHEL 6.x (32- and 64-bit), type:

```
linux dd blacklist=isci blacklist=ahci nodmraid noprobe=<ata drive number>
```

Note The noprobe values depend on the number of drives. For example, to install RHEL 6.x on a RAID 5 configuration with three drives, type:

```
Linux dd blacklist=isci blacklist=ahci nodmraid noprobe=ata1 noprobe=ata2
```

- For RHEL 7.x (32- and 64-bit), type:

```
linux dd modprobe.blacklist=ahci nodmraid
```

Step 9 **Optional:** To see full, verbose installation status steps during installation, delete the **Quiet** parameter from the line.

Step 10 On the Boot Menu window, press **Ctrl+x** to start the interactive installation.

Step 11 Below **Driver disk device selection**, select the option to install your driver .img file. (Type **r** to refresh the list if it is not populated.)

Note The installer recognizes the driver file as an .iso file, even though you renamed it to dd.img for mapping.

Type the number of the driver device ISO in the list. Do *not* select the RHEL ISO image. In the following example, type **6** to select device sdb:

```
5) sr0 iso9660 RHEL-7.6\x20Server.x

6) sdb iso9660 CDROM

# to select, 'r' - refresh, or 'c' -continue: 6
```

The installer reads the driver file and lists the drivers.

Step 12 Under **Select drivers to install**, type the number of the line that lists the megasr driver. In the following example, type **1**:

```
1) [ ] /media/DD-1/rpms/x86_61/kmod-megasr-18.01.2010.1107_e17.6-1.x86_61.rpm
# to toggle selection, or 'c' -continue: 1
```

Your selection is displayed with an X in brackets.

```
1) [X] /media/DD-1/rpms/x86_61/kmod-megasr-18.01.2010.1107_e17.6-1.x86_61.rpm
```

Step 13 Type **c** to continue.

Step 14 Follow the RHEL installation wizard to complete the installation.

Step 15 When the wizard's Installation Destination screen is displayed, ensure that **LSI MegaSR** is listed as the selection. If it is not listed, the driver did not load successfully. In that case, select **Rescan Disc**.

Step 16 After the installation completes, reboot the target server.

Installing the SUSE Linux Enterprise Server Driver

For the specific supported OS versions, see the Hardware and Software Compatibility Matrix for your server release.

This topic describes the fresh installation of the SLES driver on systems that have the embedded MegaRAID stack.

Note If you use an embedded RAID controller with Linux, both the pSATA and the sSATA controller must be set to `LSI SW RAID` mode.

Before you begin

Before you install this driver on an embedded controller, you must configure a RAID drive group on the embedded controller that controls the drives where you will install the OS (pSATA and/or sSATA).

To access the configuration utility, open the BIOS Setup Utility, go to the **Advanced** tab, and then choose the utility instance for the embedded controller:

- For pSATA, select **LSI Software RAID Configuration Utility (SATA)**
- For sSATA, select **LSI Software RAID Configuration Utility (sSATA)**

Step 1 Prepare the `dud.img` file using one of the following methods:

- To install from physical disk, use the procedure in Preparing Physical Thumb Drive for Linux, on page 133, then continue with step 4.
- To install from *virtual* disk, download the Cisco UCS C-Series drivers ISO, as described in Downloading the MegaSR Drivers, on page 131, then continue with the next step.

Step 2 Extract the `dud.img` file that contains the driver:

a) Burn the ISO image to a disk.

b) Browse the contents of the drivers folders to the location of the embedded MegaRAID drivers: /<OS>/Storage/Intel/C600-M5/...

c) Within the SLES folder for your version, the `dud-<driver version>.img` file is packaged in a compressed `.gz` file. Extract the .img file from the .gz file.
d) Copy the `dud-<driver version>.img` file to a temporary location on your workstation.

Step 3 Start the Linux driver installation using one of the following methods:

- To install from local media, connect an external USB DVD drive to the server and then insert the first SLES installation disk into the drive. Then continue with Step 5.
- To install from remote ISO, log in to the server's Cisco IMC interface. Then continue with the next step.

Step 4 Launch a Virtual KVM console window and click the **Virtual Media** tab.

a) Click **Add Image** and browse to select your remote SLES installation ISO file.
b) Click **Add Image** again and browse to select your `dud-<driver version>.img` file.
c) Check the check boxes in the **Mapped** column for the media that you just added, then wait for mapping to complete.

Step 5 Power-cycle the target server.

Step 6 Press **F6** when you see the F6 prompt during bootup. The Boot Menu window opens.

Step 7 On the Boot Manager window, select the physical or virtual SLES installation ISO and press **Enter**.

The SLES installation begins when the image is booted.

Step 8 When the first SLES screen appears, select **Installation**.

Step 9 Press **e** to edit installation parameters.

Step 10 Append the following parameter to the end of the line that begins with **linuxefi**:

```
brokenmodules=ahci
```

Step 11 **Optional**: To see detailed status information during the installation, add the following parameter to the line that begins with **linuxefi**:

```
splash=verbose
```

Step 12 Press **Ctrl+x** to start the installation.

The installation proceeds. The installer finds the LSI driver automatically in the `dud-<driver version>.img` file that you provided. With verbose status messages, you see the driver being installed when `LSI MegaRAID SW RAID Module` is listed.

Step 13 Follow the SLES installation wizard to complete the installation. Verify installation of the driver when you reach the **Suggested Partitioning** screen:

a) On the **Suggested Partitioning** screen, select **Expert Partitioner**.
b) Navigate to **Linux > Hard disks** and verify that there is a device listed for the `LSI - LSI MegaSR` driver. The device might be listed as a type other than sda. For example:

```
dev/sdd: LSI - LSI MegaSR
```

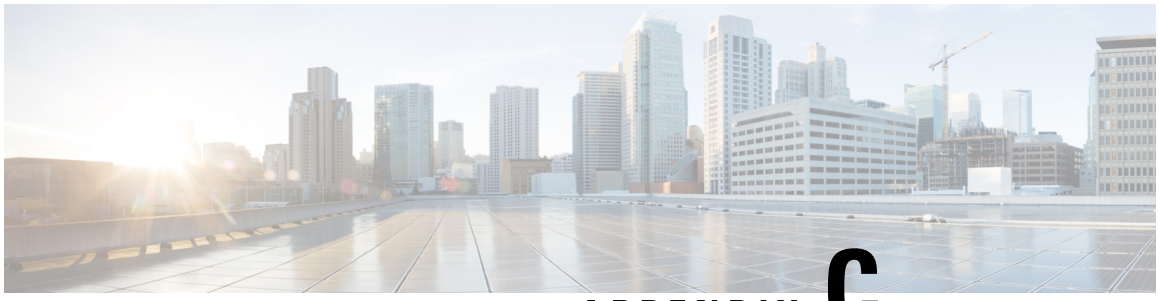
If no device is listed, the driver did not install properly. In that case, repeat the steps above.

Step 14 When installation is complete, reboot the target server.

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 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 for the supported GPU cards.

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 Tesla P4	3.1(3) **Note** The NVIDIA Tesla P4 GPU is not supported with Second Generation Intel Xeon Scalable processors.
NVIDIA T4	4.0(2e) **Note** The minimum version of Cisco UCS Manager that supports this card is 4.0(2c).

GPU Card Configuration Rules

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

- You can install up to two single-wide GPU cards in the server, in PCIe slots 1 and 2.
- Use the UCS power calculator at the following link to determine the power needed based on your server configuration: http://ucspowercalc.cisco.com
- Do not mix different brands or models of GPU cards 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.

Replacing a Single-Wide GPU Card

Step 1 Remove an existing GPU card from the PCIe riser:

a) Shut down and remove power from the server as described in Shutting Down and Removing Power From the Server, on page 33.

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 35.
d) Use two hands to grasp the external riser handle and the blue area at the front of the riser.
e) Lift straight up to disengage the riser's connectors from the two sockets on the motherboard. Set the riser upside-down on an antistatic surface.
f) Open the hinged plastic retainer that secures the rear-panel tab of the card.
g) Pull evenly on both ends of the GPU card to remove it from the socket on the PCIe riser.

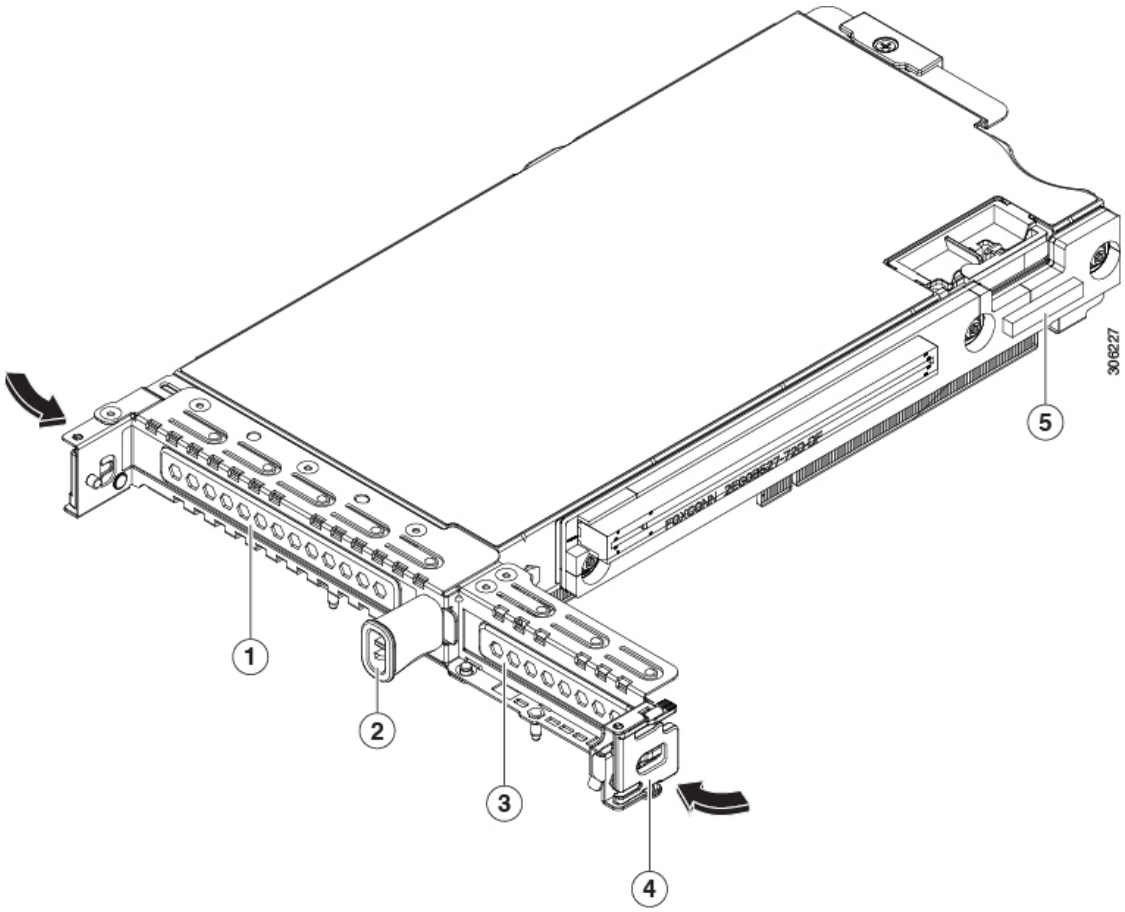
If the riser has no card, remove the blanking panel from the rear opening of the riser.

Step 2 Install a new GPU card:

Note The NVIDIA Tesla P4 and Tesla T4 are half-height, half-length cards. If one is installed in full-height PCIe slot 1, it requires a full-height rear-panel tab installed to the card.

a) With the hinged tab retainer open, align the new GPU card with the empty socket on the PCIe riser.
b) Push down evenly on both ends of the card until it is fully seated in the socket.
c) Ensure that the card’s rear panel tab sits flat against the riser rear-panel opening and then close the hinged tab retainer over the card’s rear-panel tab.

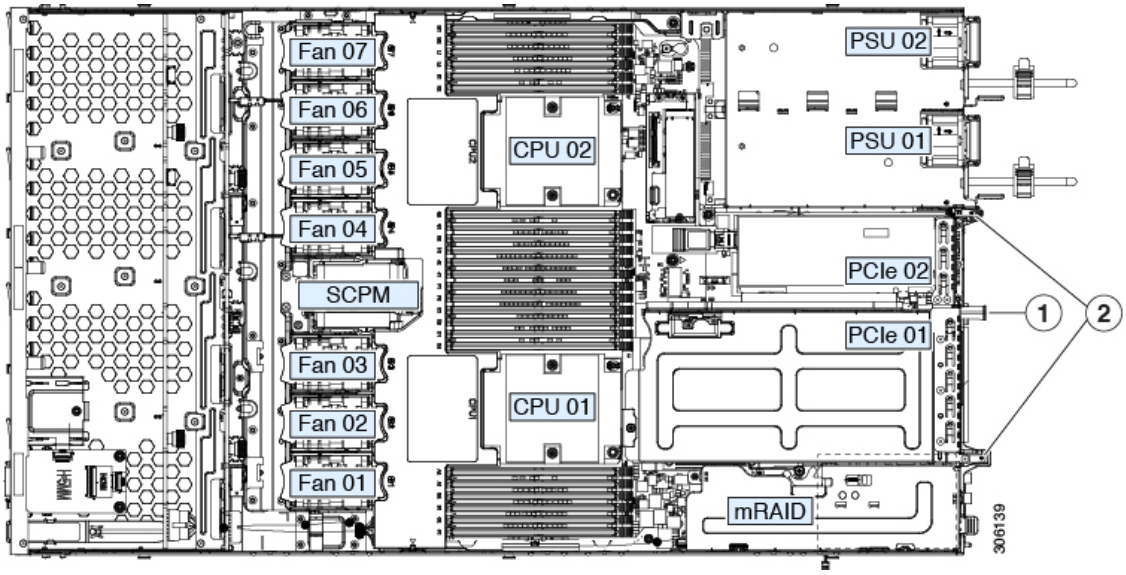
Figure 59: PCIe Riser Assembly



1	PCIe slot 1 rear-panel opening	**4**	Hinged card retainer (one each slot)
2	External riser handle	**5**	PCIe connector for cable that supports front-panel NVMe SSDs
3	PCIe slot 2 rear-panel opening	-	

d) Position the PCIe riser over its two sockets on the motherboard and over the two chassis alignment channels.

Figure 60: PCIe Riser Alignment Features



1	Blue riser handle	**2**	Riser alignment features in chassis

e) Carefully push down on both ends of the PCIe riser to fully engage its two connectors with the two sockets on the motherboard.
f) Replace the top cover to the server.
g) Replace the server in the rack, replace cables, and then fully power on the server by pressing the Power button.

Step 3 Optional: Continue with Installing Drivers to Support the GPU Cards, on page 149.

Note If you installed an NVIDIA Tesla P-Series or T-Series GPU, you must install GRID licenses to use the GRID features. See Using NVIDIA GRID License Server For P-Series and T-Series GPUs, on page 143.

Using NVIDIA GRID License Server For P-Series and T-Series GPUs

This section applies to NVIDIA Tesla P-Series and 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 144

2. Register your product activation keys with NVIDIA.

   Registering Your Product Activation Keys With NVIDIA, on page 145

3. Download the GRID software suite.

   Downloading the GRID Software Suite, on page 145

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

   Installing NVIDIA GRID License Server Software, on page 145

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 146

6. Manage your GRID licenses.

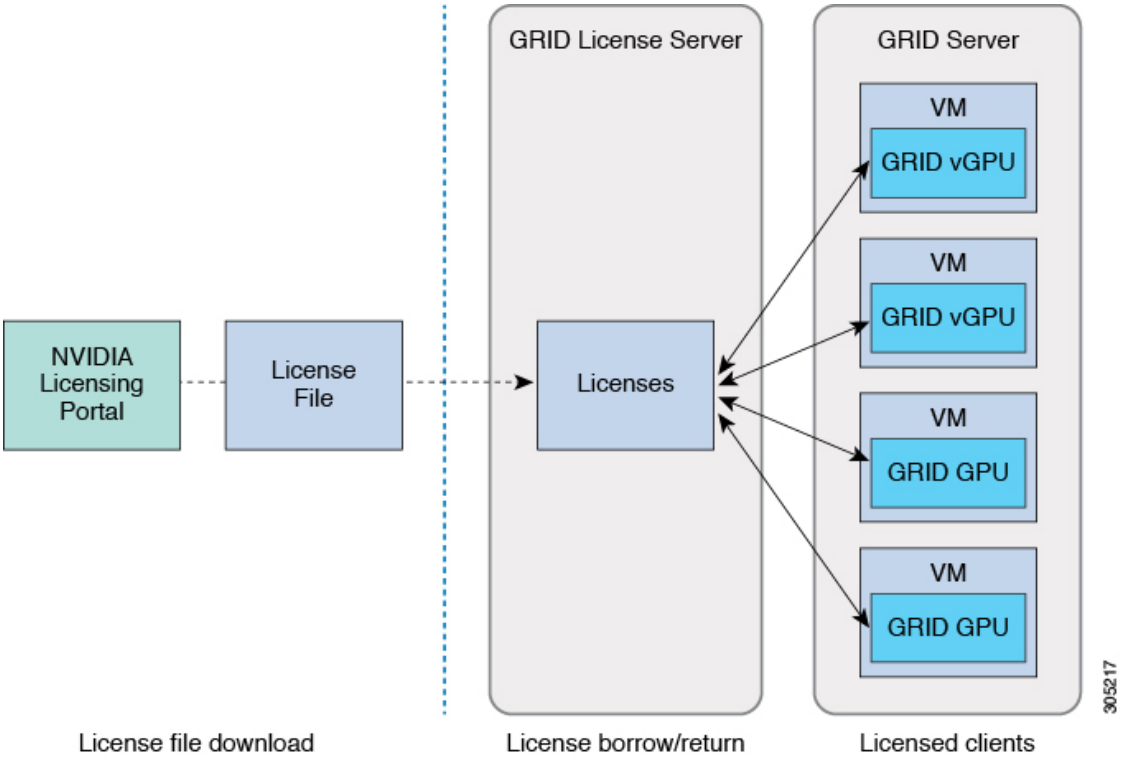
   Managing GRID Licenses , on page 147

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 61: 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 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.

a) Click **Choose File**.

b) Browse to the license .bin file that you want to install and click **Open**.

c) 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 of 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.

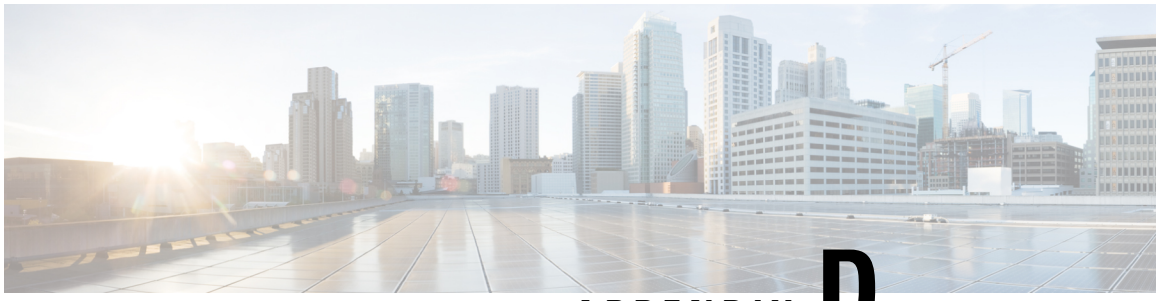
Step 2 Create a virtual machine in your hypervisor. Refer to your hypervisor documentation for instructions.

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

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

Installation For Cisco UCS Manager Integration