



## **Cisco Application Services Engine Hardware Installation Guide**

**First Published:** 2019-10-15

### **Americas Headquarters**

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





## CONTENTS

---

### CHAPTER 1

#### Overview 1

- Overview 1
- External Features 1
- Serviceable Component Locations 4
- Summary of Server Features 6

---

### CHAPTER 2

#### Installing the Server 9

- Preparing for Installation 9
  - Installation Warnings and Guidelines 9
  - Rack Requirements 11
- Installing the Server in a Rack 12
- Installing the Cable Management Arm (Optional) 14
- Reversing the Cable Management Arm (Optional) 15
- Initial Server Setup 16
- Connecting to the Server Locally For Setup 17
- Connecting to the Server Remotely For Setup 18
- Updating the BIOS and Cisco IMC Firmware 19
- Accessing the System BIOS 19
- Smart Access Serial 20

---

### CHAPTER 3

#### Maintaining the Server 21

- Status LEDs and Buttons 21
  - Front-Panel LEDs 21
  - Rear-Panel LEDs 24
  - Internal Diagnostic LEDs 25
- Preparing For Component Installation 26

Required Equipment For Service Procedures	26
Shutting Down and Removing Power From the Server	27
Shutting Down Using the Power Button	27
Shutting Down Using The Cisco IMC GUI	27
Shutting Down Using The Cisco IMC CLI	28
Removing the Server Top Cover	28
Serial Number Location	29
Hot Swap vs Hot Plug	29
Removing and Replacing Components	30
Serviceable Component Locations	30
Replacing SAS/SATA Hard Drives or Solid State Drives	32
SAS/SATA Drive Population Guidelines	32
4K Sector Format SAS/SATA Drives Considerations	33
Replacing a SAS/SATA Drive	33
Replacing a Front-Loading NVMe SSD	34
Front-Loading NVMe SSD Population Guidelines	34
Front-Loading NVMe SSD Requirements and Restrictions	35
Enabling Hot-Plug Support in the System BIOS	35
Replacing a Front-Loading NVMe SSD	36
Installing a PCIe Cable For Front-Loading NVMe SSDs	37
Replacing Fan Modules	38
Replacing CPUs and Heatsinks	39
CPU Configuration Rules	39
Tools Required For CPU Replacement	39
Replacing a CPU and Heatsink	40
Moving an M5 Generation CPU	46
Replacing Memory DIMMs	51
DIMM Population Rules and Memory Performance Guidelines	51
Replacing DIMMs	53
Replacing a Mini-Storage Module	53
Replacing a Mini-Storage Module Carrier	54
Replacing an M.2 SSD in a Mini-Storage Carrier For M.2	55
Replacing an Internal USB Drive	56
Replacing a USB Drive	56



Enabling or Disabling the Internal USB Port	57
Replacing the RTC Battery	58
Replacing Power Supplies	59
Replacing AC Power Supplies	59
Replacing a PCIe Card	60
PCIe Slot Specifications	60
Replacing a PCIe Card	61
Cisco Virtual Interface Card (VIC) Considerations	64
Replacing an mLOM Card	65
Replacing an mRAID Riser (Riser 3)	66
Replacing a SAS Storage Controller Card (RAID or HBA) in Riser 3	68
Storage Controller Card Firmware Compatibility	68
Replacing a SAS Storage Controller Card (RAID or HBA)	69
Replacing a Boot-Optimized M.2 RAID Controller Module	70
Cisco Boot-Optimized M.2 RAID Controller Considerations	70
Replacing a Cisco Boot-Optimized M.2 RAID Controller	71
Replacing the Supercap (RAID Backup)	73
Replacing a SATA Interposer Card	75
Replacing a Chassis Intrusion Switch	76
Installing a Trusted Platform Module (TPM)	77
TPM Considerations	77
Service Headers and Jumpers	78
Using the Clear CMOS Header (J38, Pins 9 - 10)	79
Using the BIOS Recovery Header (J38, Pins 11 - 12)	80
Procedure 1: Reboot With recovery.cap File	80
Procedure 2: Use BIOS Recovery Header and bios.cap Recovery File	81
Using the Clear Password Header (J38, Pins 13 - 14)	81
Using the Boot Alternate Cisco IMC Image Header (J39, Pins 1 - 2)	82
Using the Reset Cisco IMC Password to Default Header (J39, Pins 3 - 4)	83
Using the Reset Cisco IMC to Defaults Header (J39, Pins 5 - 6)	84
<b>APPENDIX A</b>	<b>Server Specifications 85</b>
	Server Specifications 85
	Physical Specifications 85

Environmental Specifications	85
Power Specifications	86
1050 W AC Power Supply	86
Power Cord Specifications	87

---

**APPENDIX B**

<b>Storage Controller Considerations</b>	<b>91</b>
Supported Storage Controllers and Cables	91
Storage Controller Card Firmware Compatibility	92
RAID Backup (Supercap)	92
Write-Cache Policy for Cisco 12G SAS Modular RAID Controller	92
Mixing Drive Types in RAID Groups	93
RAID Controller Migration	93
Storage Controller and Backplane Connectors	94
Embedded SATA RAID Controller	96
Embedded SATA RAID Requirements	97
Embedded SATA RAID Controller Considerations	97
Embedded SATA RAID: Two SATA Controllers	98
Enabling SATA Mode For the Embedded Controllers	98
Accessing the Software RAID Configuration Utility	99
For More RAID Utility Information	99



# CHAPTER 1

## Overview

---

- [Overview, on page 1](#)
- [External Features, on page 1](#)
- [Serviceable Component Locations, on page 4](#)
- [Summary of Server Features, on page 6](#)

## Overview

Cisco Application Services Engine provides a common platform for deploying Cisco Data Center applications. These applications provide real time analytics, visibility and assurance for policy and infrastructure.

The Cisco Application Services Engine server is required for installing and hosting the Cisco Application Services Engine application.

The server is orderable in the following version:

- SE-CL-L3 — 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.

## External Features

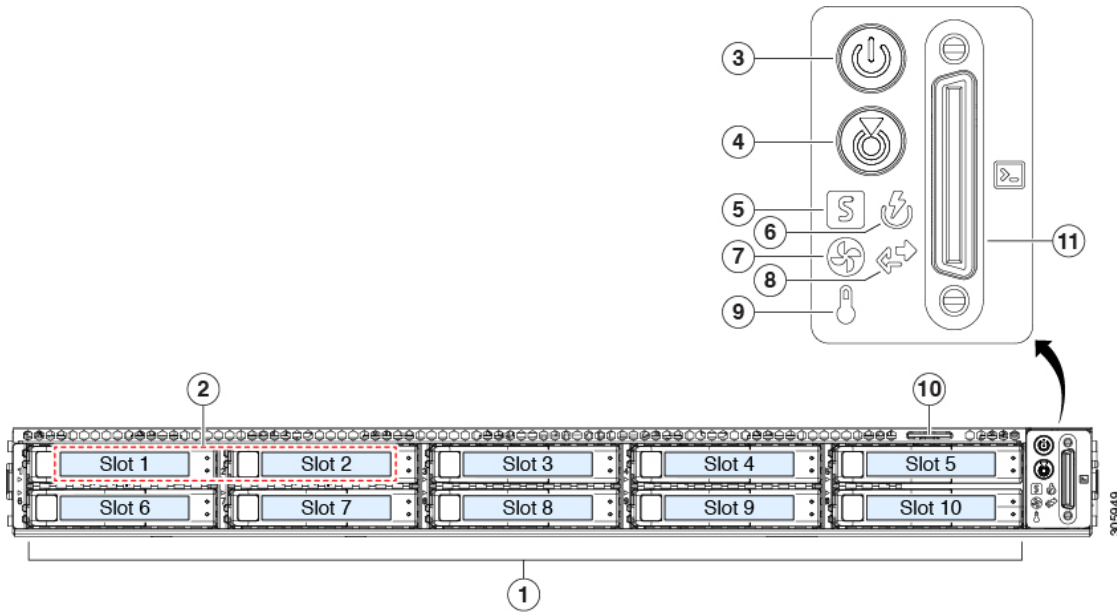
This topic shows the external features of the server versions.

### **Cisco SE-CL-L3 (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 21](#).

Figure 1: Cisco SE-CL-L3 (SFF Drives) Front Panel



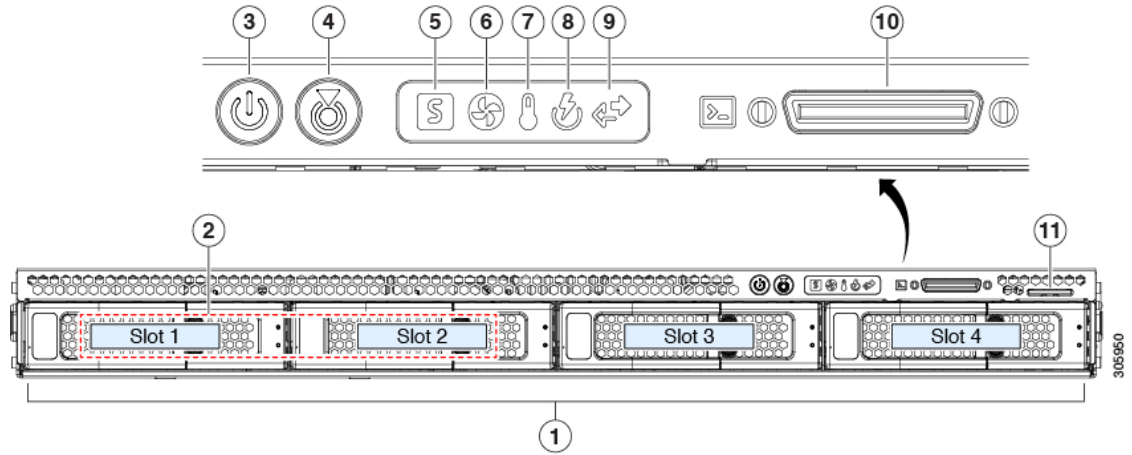
1	Drive bays 1 – 10 support SAS/SATA hard disk drives (HDDs) and solid state drives (SSDs)	7	Fan status LED
2	<ul style="list-style-type: none"> <li>SE-CL-L3 : Drive bays 1 and 2 support NVMe PCIe SSDs.</li> </ul>	8	Network link activity LED
3	Power button/power status LED	9	Temperature status LED
4	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	-	

**SE-CL-L3 (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 21](#).

Figure 2: SE-CL-L3 (LFF Drives) Front Panel



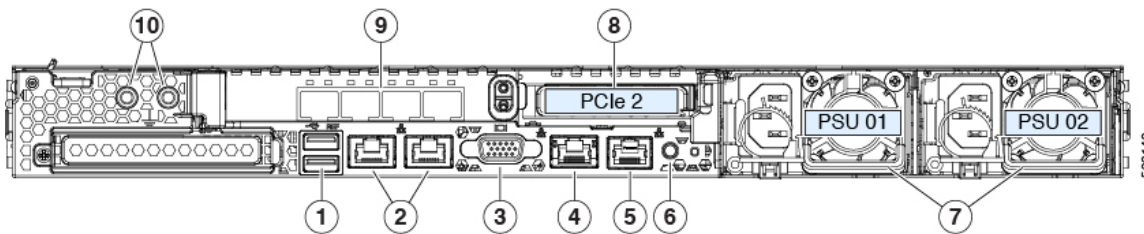
1	Drive bays 1 – 4 support SAS/SATA HDDs and SSDs	7	Temperature status LED
2	Drive bays 1 and 2 support NVMe PCIe SSDs. A size-converter drive sled is required if 2.5-inch SSDs are used.	8	Power supply status LED
3	Power button/power status LED	9	Network link activity LED
4	Unit identification button/LED	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	-	

**SE-CL-L3 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 24.

Figure 3: SE-CL-L3 Rear Panel



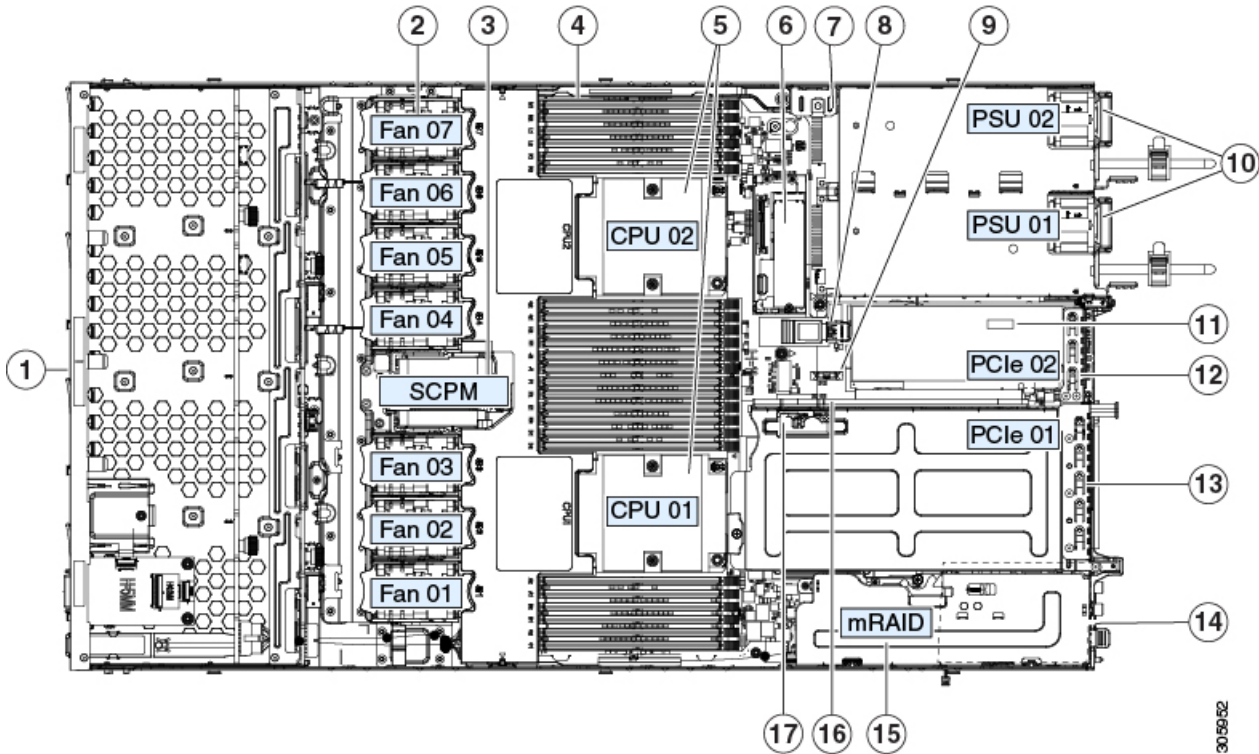
1	USB 3.0 ports (two)	6	Rear unit identification button/LED
---	---------------------	---	-------------------------------------

2	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.  These correspond to <code>eth1-1</code> ( <code>eth0</code> ) and <code>eth1-2</code> ( <code>eth1</code> ) respectively.	7	Power supplies (two, redundant as 1+1)
3	VGA video port (DB-15 connector)	8	PCIe riser 1/slot 1 (x16 lane)  Includes PCIe cable connectors for front-loading NVMe SSDs (x8 lane)
4	1-Gb Ethernet dedicated management port	9	Quad 10-Gb/25-Gb ports.  These correspond to <code>eth 2-1</code> to <code>eth 2-4</code> .  Only 2 interfaces out of the 4 are active at a time ( <code>eth2-1/2-2</code> or <code>eth2-3/2-4</code> ) in active/standby mode.
5	Serial port (RJ-45 connector)	10	Threaded holes for dual-hole grounding lug

## 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: SE-CL-L3 , Serviceable Component Locations



<p><b>1</b></p>	<p>Front-loading drive bays 1–10 support SAS/SATA drives.</p> <ul style="list-style-type: none"> <li>• SE-CL-L3 : Drive bays 1 and 2 support NVMe PCIe SSDs.</li> </ul>	<p><b>10</b></p>	<p>Power supplies (hot-swappable when redundant as 1+1)</p>
<p><b>2</b></p>	<p>Cooling fan modules (seven, hot-swappable)</p>	<p><b>11</b></p>	<p>Trusted platform module (TPM) socket on motherboard (not visible in this view)</p>
<p><b>3</b></p>	<p>Supercap unit mounting bracket (RAID backup)</p>	<p><b>12</b></p>	<p>PCIe riser 2/slot 2 (half-height, x16 lane) Includes PCIe cable connectors for front-loading NVMe SSDs (x8 lane)</p>
<p><b>4</b></p>	<p>DIMM sockets on motherboard (12 per CPU)</p>	<p><b>13</b></p>	<p>PCIe riser 1/slot 1 (full-height, x16 lane) Includes socket for Micro-SD card</p>
<p><b>5</b></p>	<p>CPUs and heatsinks (up to two)</p>	<p><b>14</b></p>	<p>Modular LOM (mLOM) card bay on chassis floor (x16 PCIe lane), not visible in this view</p>

<b>6</b>	Mini-storage module socket. Options: <ul style="list-style-type: none"> <li>• SD card module with two SD card slots</li> <li>• M.2 module with slots for either two SATA M.2 drives or two NVMe M.2 drives</li> <li>• 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)</li> </ul>	<b>15</b>	Modular RAID (mRAID) riser, can optionally be a riser that supports either: <ul style="list-style-type: none"> <li>• Hardware RAID controller card</li> <li>• Interposer card for embedded SATA RAID</li> </ul>
<b>7</b>	Chassis intrusion switch (optional)	<b>16</b>	PCIe cable connectors for front-loading NVMe SSDs on PCIe riser 2
<b>8</b>	Internal USB 3.0 port on motherboard	<b>17</b>	Micro-SD card socket on PCIe riser 1
<b>9</b>	RTC battery, vertical socket	-	

## 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: <ul style="list-style-type: none"> <li>• Intel Xeon Silver 4XXX Processors</li> </ul>
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	<p>Rear panel:</p> <ul style="list-style-type: none"> <li>• One 1-Gb Ethernet dedicated management port (RJ-45 connector)</li> <li>• Two 1-Gb/10-Gb BASE-T Ethernet LAN ports (RJ-45 connectors)</li> </ul> <p>The dual LAN ports can support 1 Gbps and 10 Gbps, depending on the link partner capability.</p> <ul style="list-style-type: none"> <li>• One RS-232 serial port (RJ-45 connector)</li> <li>• One VGA video connector port (DB-15 connector)</li> <li>• Two USB 3.0 ports</li> </ul> <p>Front panel:</p> <ul style="list-style-type: none"> <li>• 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.</li> </ul>
Modular LOM	One dedicated socket (x16 PCIe lane) that can be used to add an mLOM card for additional rear-panel connectivity.
Power	<p>One power supply:</p> <ul style="list-style-type: none"> <li>• AC power supplies 1050 W AC each</li> </ul>
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	<p>Two horizontal PCIe expansion slots on a PCIe riser assembly.</p> <p>See <a href="#">PCIe Slot Specifications, on page 60</a> for specifications of the slots.</p>
InfiniBand	The PCIe bus slots in this server support the InfiniBand architecture.
Storage, front-panel	<p>The server is orderable in three different versions, each with a different front panel/drive-backplane configuration.</p> <ul style="list-style-type: none"> <li>• SE-CL-L3 , 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.</li> </ul>

Feature	Description
Storage, internal	<p>The server has these internal storage options:</p> <ul style="list-style-type: none"> <li>• One USB port on the motherboard.</li> <li>• One micro-SD card socket on PCIe riser 1.</li> <li>• Mini-storage module socket, optionally with either: <ul style="list-style-type: none"> <li>• SD card module. Supports up to two SD cards.</li> <li>• M.2 SSD module. Supports either two SATA M.2 SSDs or two NVMe M.2 SSDs.</li> <li>• 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)</li> </ul> </li> </ul>
Storage management	<p>The server has a dedicated internal mRAID riser that supports one of the following storage-controller options:</p> <ul style="list-style-type: none"> <li>• A PCIe-style Cisco modular RAID controller card (SAS/SATA).</li> <li>• A PCIe-style interposer card for the server's embedded SATA RAID controller.</li> </ul> <p>For a detailed list of storage controller options, see <a href="#">Supported Storage Controllers and Cables, on page 91</a>.</p>
RAID backup	<p>The server has a mounting bracket near the cooling fans for the supercap unit that is used with the Cisco modular RAID controller card.</p>
Integrated video	<p>Integrated VGA video.</p>



## CHAPTER 2

# Installing the Server

---

- [Preparing for Installation](#), on page 9
- [Installing the Server in a Rack](#), on page 12
- [Installing the Cable Management Arm \(Optional\)](#), on page 14
- [Reversing the Cable Management Arm \(Optional\)](#), on page 15
- [Initial Server Setup](#), on page 16
- [Connecting to the Server Locally For Setup](#), on page 17
- [Connecting to the Server Remotely For Setup](#), on page 18
- [Updating the BIOS and Cisco IMC Firmware](#), on page 19
- [Accessing the System BIOS](#), on page 19
- [Smart Access Serial](#), on page 20

## 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 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.

- 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 85](#).
- 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 86](#). 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:

- Cisco part UCSC-RAILB-M4= (ball-bearing slide rail kit)

### 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.**

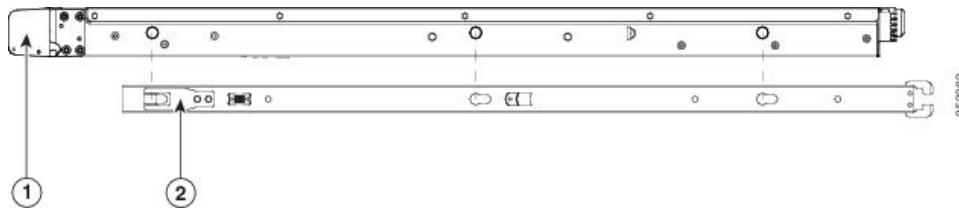
**If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.**

Statement 1006

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

- 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.
- 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.
- Install the second inner rail to the opposite side of the server.

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

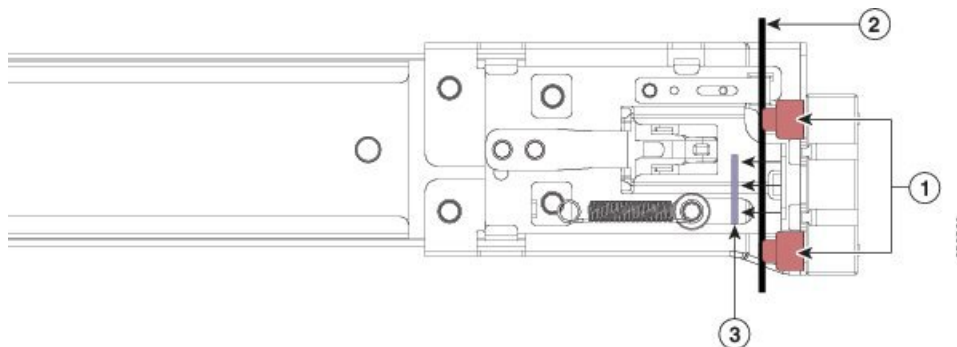


1	Front of server	2	Locking clip on front of inner rail
---	-----------------	---	-------------------------------------

**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



<b>1</b>	Front mounting pegs	<b>3</b>	Securing plate shown pulled back to the open position
<b>2</b>	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.

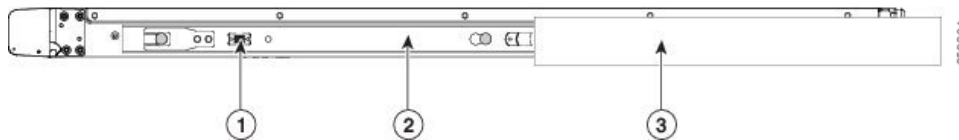
- e) Attach the second slide-rail assembly to the opposite side of the rack. Ensure that the two slide-rail assemblies are at the same height and are level front-to-back.
- f) Pull the inner slide rails on each assembly out toward the rack front until they hit the internal stops and lock in place.

**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)

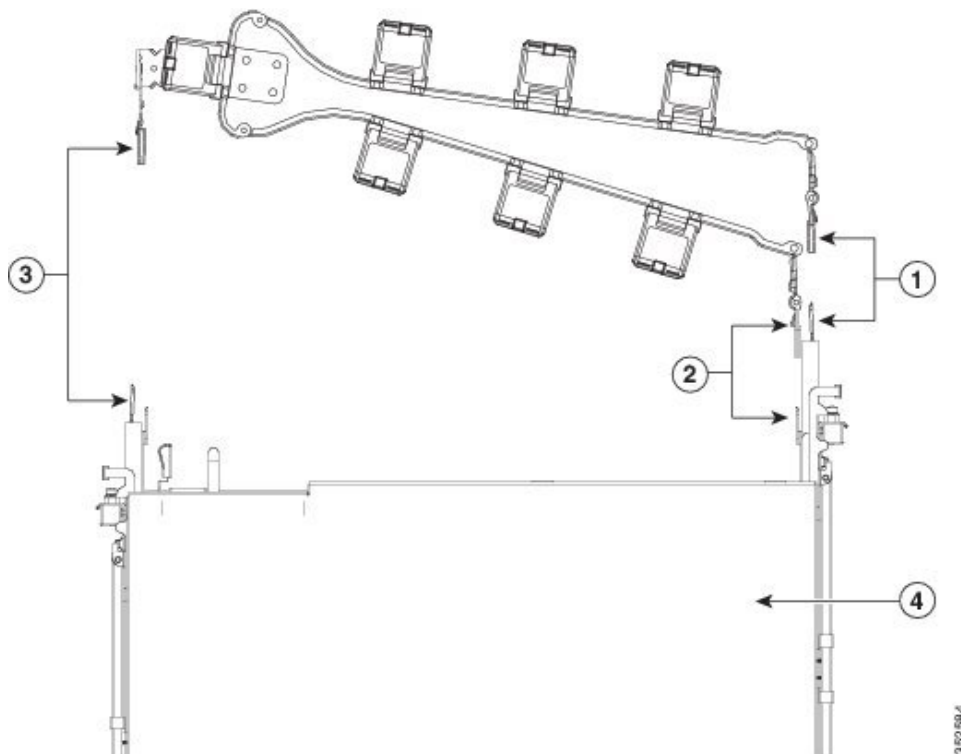


**Note** The cable management arm (CMA) is reversible left-to-right. To reverse the CMA, see [Reversing the Cable Management Arm \(Optional\)](#), on page 15 before installation.

**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



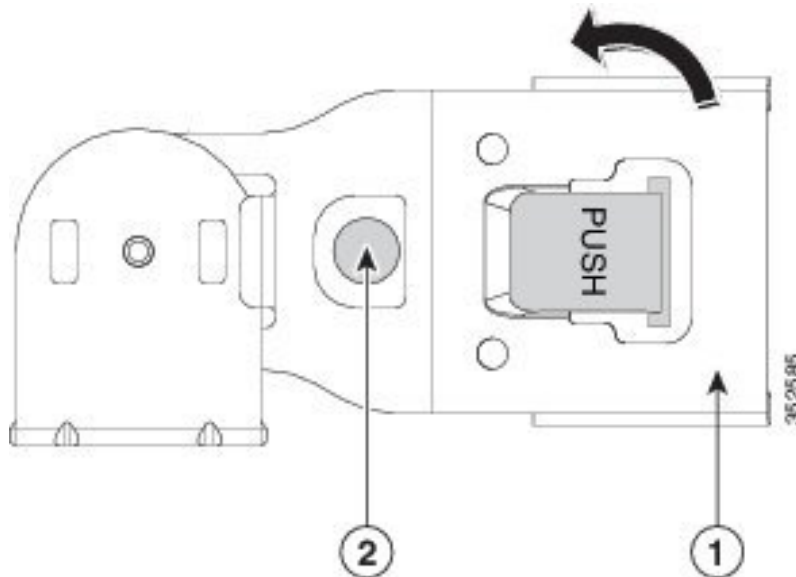
1	CMA tab on arm farthest from server attaches to end of stationary outer slide rail.	3	CMA tab on width-adjustment slider attaches to end of stationary outer slide rail.
2	CMA tab on arm closest to the server attaches to end of inner slide rail attached to server.	4	Rear of server

- 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.

### 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).
- 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 !, @, #, \$, %, ^, &, \*, -, \_, =, “

---

## 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 !, @, #, \$, %, ^, &, \*, -, \_, =, “

---

## 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.

---

## 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`.



# CHAPTER 3

## Maintaining the Server

- [Status LEDs and Buttons](#), on page 21
- [Preparing For Component Installation](#), on page 26
- [Removing and Replacing Components](#), on page 30
- [Service Headers and Jumpers](#), on page 78

### Status LEDs and Buttons

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

#### Front-Panel LEDs

Figure 10: Front Panel LEDs

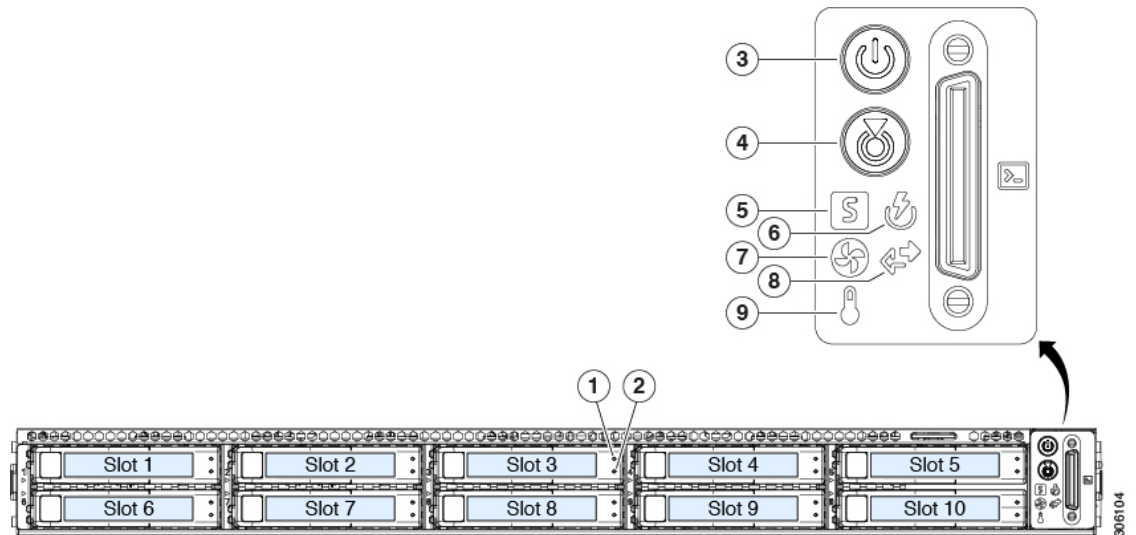


Table 1: Front Panel LEDs, Definition of States

LED Name	States
----------	--------

<b>1</b>  <b>SAS</b>	SAS/SATA drive fault  <b>Note</b> NVMe solid state drive (SSD) drive tray LEDs have different behavior than SAS/SATA drive trays.	<ul style="list-style-type: none"> <li>• Off—The hard drive is operating properly.</li> <li>• Amber—Drive fault detected.</li> <li>• Amber, blinking—The device is rebuilding.</li> <li>• Amber, blinking with one-second interval—Drive locate function activated in the software.</li> </ul>
<b>2</b>  <b>SAS</b>	SAS/SATA drive activity LED	<ul style="list-style-type: none"> <li>• Off—There is no hard drive in the hard drive tray (no access, no fault).</li> <li>• Green—The hard drive is ready.</li> <li>• Green, blinking—The hard drive is reading or writing data.</li> </ul>
<b>1</b>  <b>NVMe</b>	NVMe SSD drive fault  <b>Note</b> NVMe solid state drive (SSD) drive tray LEDs have different behavior than SAS/SATA drive trays.	<ul style="list-style-type: none"> <li>• Off—The drive is not in use and can be safely removed.</li> <li>• Green—The drive is in use and functioning properly.</li> <li>• Green, blinking—the driver is initializing following insertion or the driver is unloading following an eject command.</li> <li>• Amber—The drive has failed.</li> <li>• Amber, blinking—A drive Locate command has been issued in the software.</li> </ul>
<b>2</b>  <b>NVMe</b>	NVMe SSD activity	<ul style="list-style-type: none"> <li>• Off—No drive activity.</li> <li>• Green, blinking—There is drive activity.</li> </ul>
<b>3</b>	Power button/LED	<ul style="list-style-type: none"> <li>• Off—There is no AC power to the server.</li> <li>• Amber—The server is in standby power mode. Power is supplied only to the Cisco IMC and some motherboard functions.</li> <li>• Green—The server is in main power mode. Power is supplied to all server components.</li> </ul>
<b>4</b>	Unit identification	<ul style="list-style-type: none"> <li>• Off—The unit identification function is not in use.</li> <li>• Blue, blinking—The unit identification function is activated.</li> </ul>



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

## Rear-Panel LEDs

Figure 11: Rear Panel LEDs

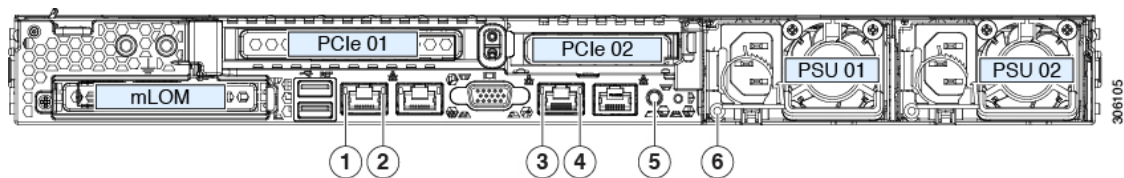


Table 2: Rear Panel LEDs, Definition of States

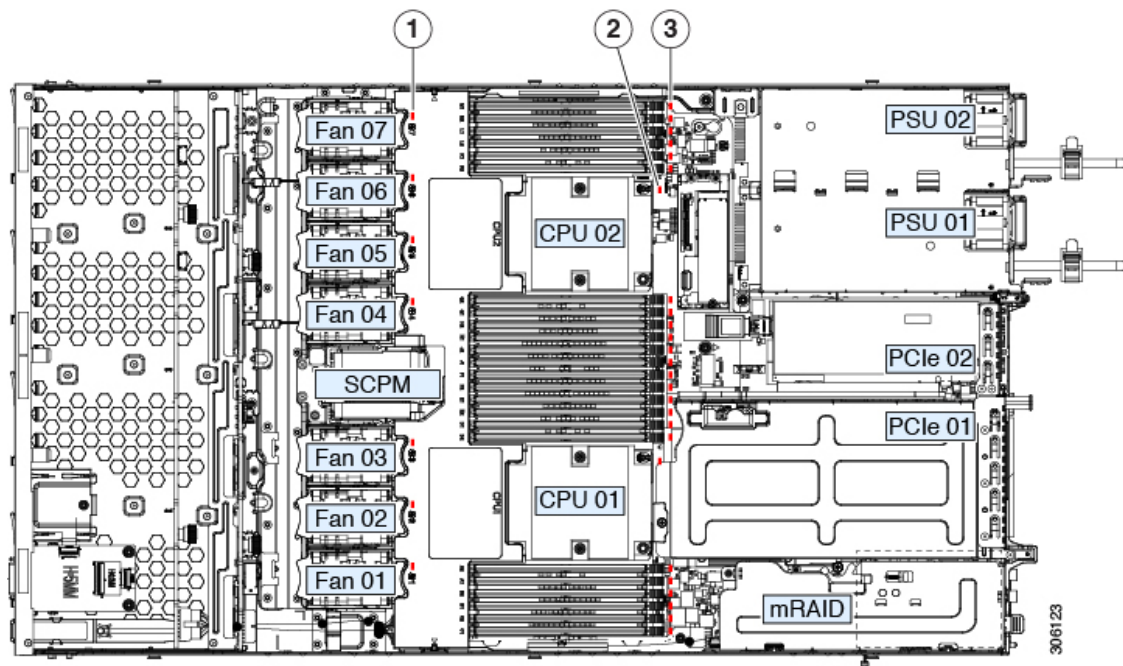
	LED Name	States
1	1-Gb/10-Gb Ethernet link speed (on both LAN1 and LAN2)	<ul style="list-style-type: none"> <li>• Amber—Link speed is 100 Mbps.</li> <li>• Amber—Link speed is 1 Gbps.</li> <li>• Green—Link speed is 10 Gbps.</li> </ul>
2	1-Gb/10-Gb Ethernet link status (on both LAN1 and LAN2)	<ul style="list-style-type: none"> <li>• Off—No link is present.</li> <li>• Green—Link is active.</li> <li>• Green, blinking—Traffic is present on the active link.</li> </ul>
3	1-Gb Ethernet dedicated management link speed	<ul style="list-style-type: none"> <li>• Off—Link speed is 10 Mbps.</li> <li>• Amber—Link speed is 100 Mbps.</li> <li>• Green—Link speed is 1 Gbps.</li> </ul>
4	1-Gb Ethernet dedicated management link status	<ul style="list-style-type: none"> <li>• Off—No link is present.</li> <li>• Green—Link is active.</li> <li>• Green, blinking—Traffic is present on the active link.</li> </ul>
5	Rear unit identification	<ul style="list-style-type: none"> <li>• Off—The unit identification function is not in use.</li> <li>• Blue, blinking—The unit identification function is activated.</li> </ul>

6	Power supply status (one LED each power supply unit)	<p><b>AC power supplies:</b></p> <ul style="list-style-type: none"> <li>• Off—No AC input (12 V main power off, 12 V standby power off).</li> <li>• Green, blinking—12 V main power off; 12 V standby power on.</li> <li>• Green, solid—12 V main power on; 12 V standby power on.</li> <li>• Amber, blinking—Warning threshold detected but 12 V main power on.</li> <li>• Amber, solid—Critical error detected; 12 V main power off (for example, over-current, over-voltage, or over-temperature failure).</li> </ul> <p><b>DC power supplies:</b></p> <ul style="list-style-type: none"> <li>• Off—No DC input (12 V main power off, 12 V standby power off).</li> <li>• Green, blinking—12 V main power off; 12 V standby power on.</li> <li>• Green, solid—12 V main power on; 12 V standby power on.</li> <li>• Amber, blinking—Warning threshold detected but 12 V main power on.</li> <li>• Amber, solid—Critical error detected; 12 V main power off (for example, over-current, over-voltage, or over-temperature failure).</li> </ul>
---	--	---

## Internal Diagnostic LEDs

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

Figure 12: Internal Diagnostic LED Locations



<p><b>1</b></p>	<p>Fan module fault LEDs (one behind each fan connector on the motherboard)</p> <ul style="list-style-type: none"> <li>• Amber—Fan has a fault or is not fully seated.</li> <li>• Green—Fan is OK.</li> </ul>	<p><b>3</b></p>	<p>DIMM fault LEDs (one behind each DIMM socket on the motherboard)</p> <p>These LEDs operate only when the server is in standby power mode.</p> <ul style="list-style-type: none"> <li>• Amber—DIMM has a fault.</li> <li>• Off—DIMM is OK.</li> </ul>
<p><b>2</b></p>	<p>CPU fault LEDs (one behind each CPU socket on the motherboard).</p> <p>These LEDs operate only when the server is in standby power mode.</p> <ul style="list-style-type: none"> <li>• Amber—CPU has a fault.</li> <li>• Off—CPU is OK.</li> </ul>	<p>-</p>	

## 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.

---

## Removing the Server Top Cover

---

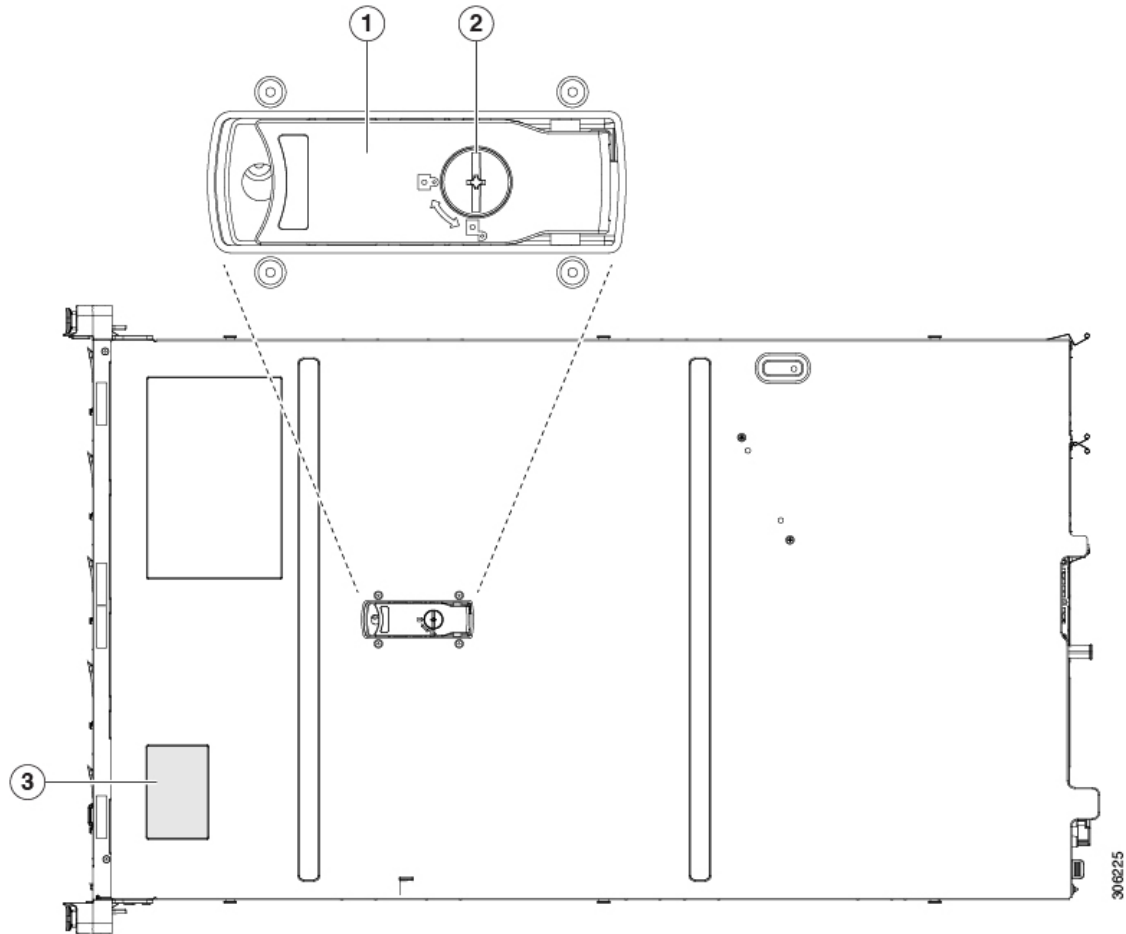
**Step 1** Remove the top cover:

- 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 28](#).

## 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.

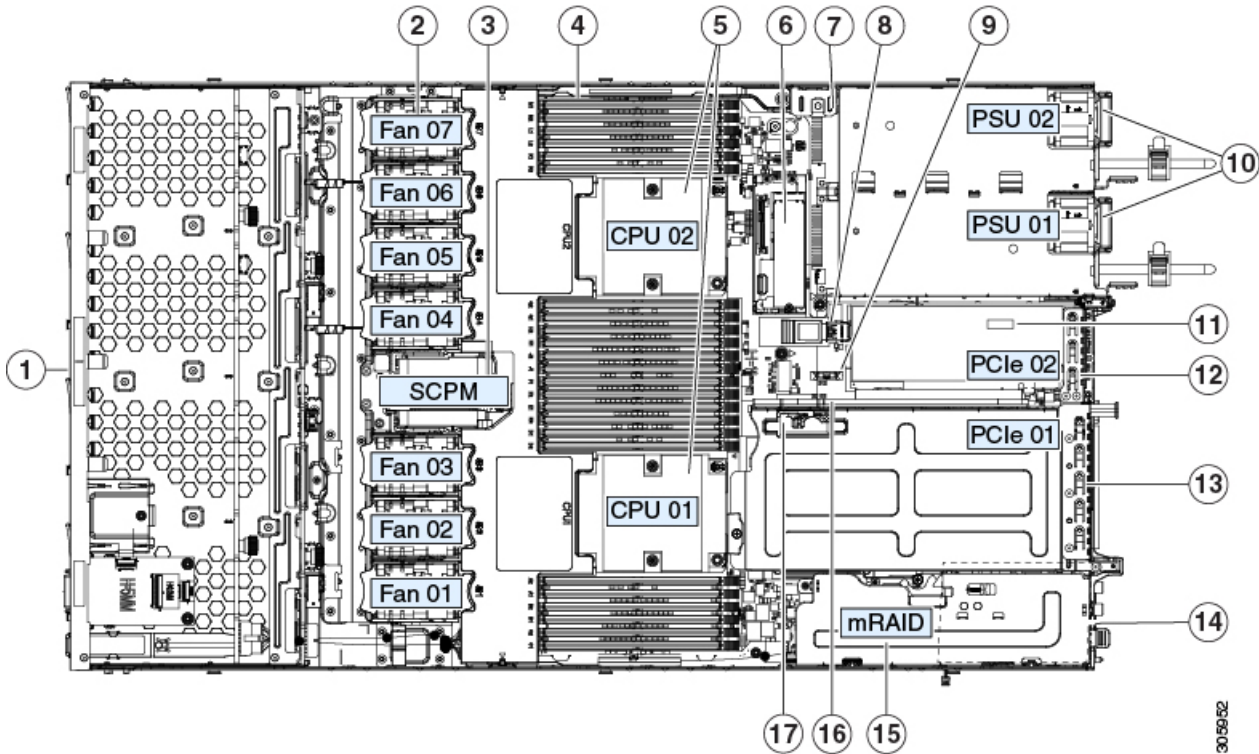
This section describes how to install and replace server components.

## 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: SE-CL-L3 , Serviceable Component Locations



<p><b>1</b></p>	<p>Front-loading drive bays 1–10 support SAS/SATA drives.</p> <ul style="list-style-type: none"> <li>• SE-CL-L3 : Drive bays 1 and 2 support NVMe PCIe SSDs.</li> </ul>	<p><b>10</b></p>	<p>Power supplies (hot-swappable when redundant as 1+1)</p>
<p><b>2</b></p>	<p>Cooling fan modules (seven, hot-swappable)</p>	<p><b>11</b></p>	<p>Trusted platform module (TPM) socket on motherboard (not visible in this view)</p>
<p><b>3</b></p>	<p>Supercap unit mounting bracket (RAID backup)</p>	<p><b>12</b></p>	<p>PCIe riser 2/slot 2 (half-height, x16 lane) Includes PCIe cable connectors for front-loading NVMe SSDs (x8 lane)</p>
<p><b>4</b></p>	<p>DIMM sockets on motherboard (12 per CPU)</p>	<p><b>13</b></p>	<p>PCIe riser 1/slot 1 (full-height, x16 lane) Includes socket for Micro-SD card</p>
<p><b>5</b></p>	<p>CPUs and heatsinks (up to two)</p>	<p><b>14</b></p>	<p>Modular LOM (mLOM) card bay on chassis floor (x16 PCIe lane), not visible in this view</p>

6	Mini-storage module socket. Options: <ul style="list-style-type: none"> <li>• SD card module with two SD card slots</li> <li>• M.2 module with slots for either two SATA M.2 drives or two NVMe M.2 drives</li> <li>• 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)</li> </ul>	15	Modular RAID (mRAID) riser, can optionally be a riser that supports either: <ul style="list-style-type: none"> <li>• Hardware RAID controller card</li> <li>• Interposer card for embedded SATA RAID</li> </ul>
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	-	

## 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 36](#).

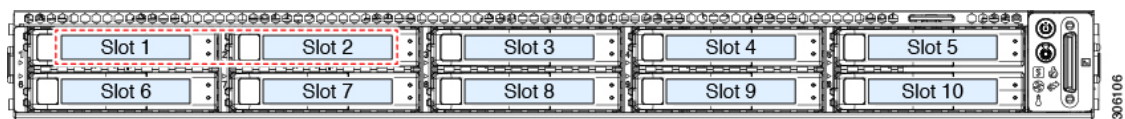
### SAS/SATA Drive Population Guidelines

The server is orderable in the following different version

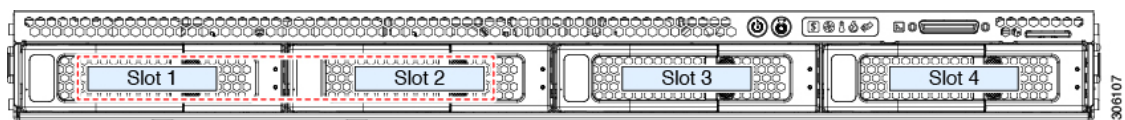
- SE-CL-L3 — Small form-factor (SFF) drives, with 10-drive backplane. Supports up to 10 2.5-inch SAS/SATA drives. Drive bays 1 and 2 support NVMe SSDs.

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

### About this task

- 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.
- Operating system support on 4K sector drives is as follows: Windows: Win2012 and Win2012R2; Linux: RHEL 6.5, 6.6, 6.7, 7.0, 7.2; SLES 11 SP3, and SLES 12. ESXi/Vmware is not supported.

### Setting Up UEFI Mode Booting in the BIOS Setup Utility

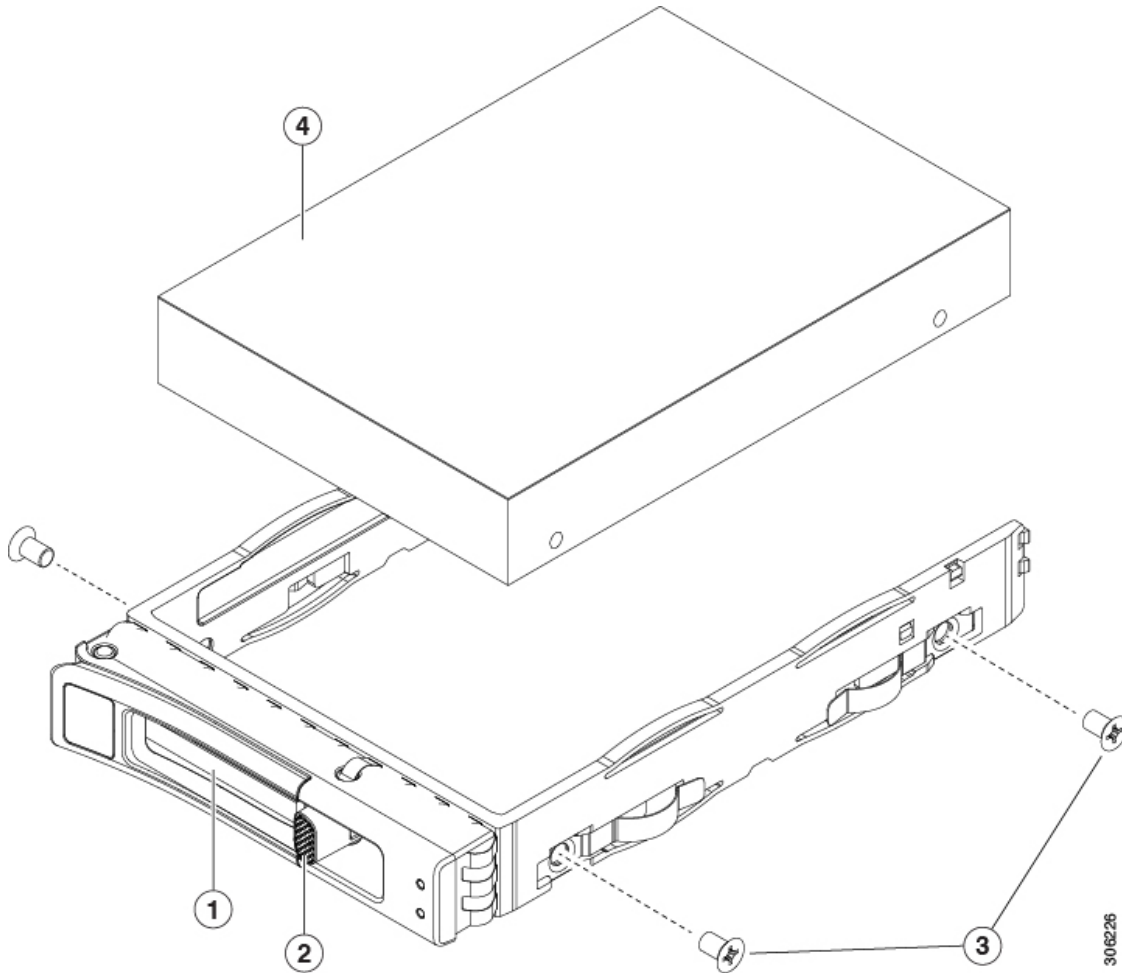
UEFI mode is the system default. Use this procedure if the mode has been changed and must be set back to UEFI mode.

- 
- 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.

### Front-Loading NVMe SSD Population Guidelines

The front drive bay support for 2.5-inch NVMe SSDs:

- SE-CL-L3 — Small form-factor (SFF) drives, with 10-drive backplane. Drive bays 1 and 2 support 2.5-inch NVMe SSDs.

## 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.

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 33](#).
- You cannot control NVMe PCIe SSDs with a SAS RAID controller because NVMe SSDs interface with the server via the PCIe bus.
- 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 35](#)

---

### 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 37](#).

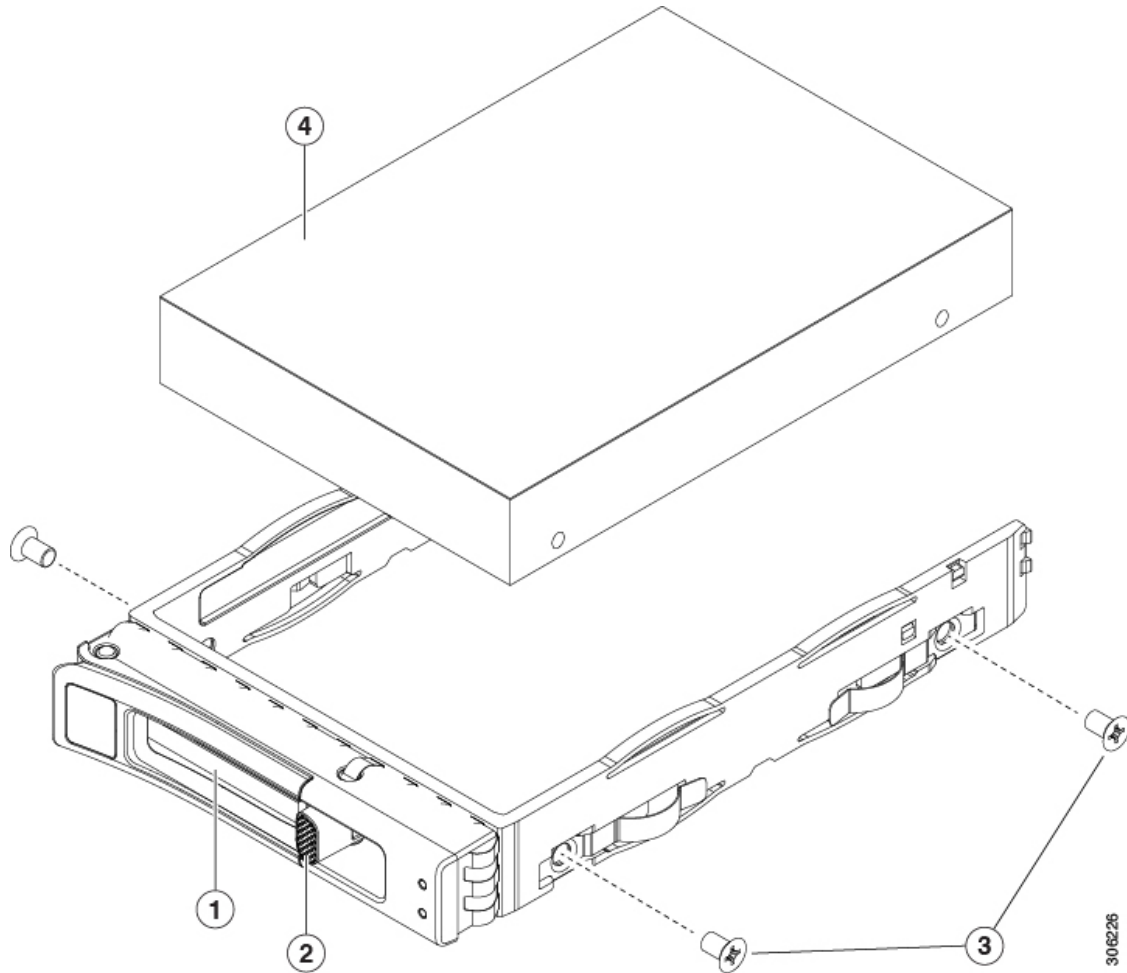
### Step 2 Install a new front-loading NVMe SSD:

- 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

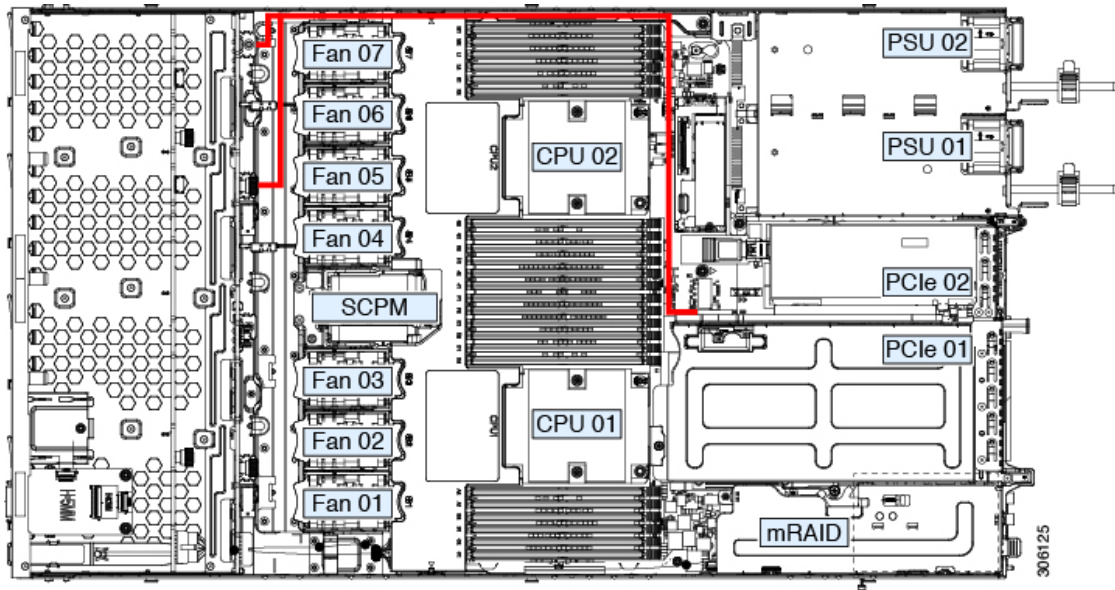
## Installing a PCIe Cable For Front-Loading NVMe SSDs

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 Fan Modules

The seven fan modules in the server are numbered as shown in the figure 1.



**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 28](#).
- 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:

### CPU Configuration Rules

This server has two CPU sockets on the motherboard. Each CPU supports six DIM channels (12 DIMM slots). See [DIMM Population Rules and Memory Performance Guidelines, on page 51](#).

- The server operates with two identical CPUs installed.
- 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.

### 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.

## 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 27](#).
- 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.

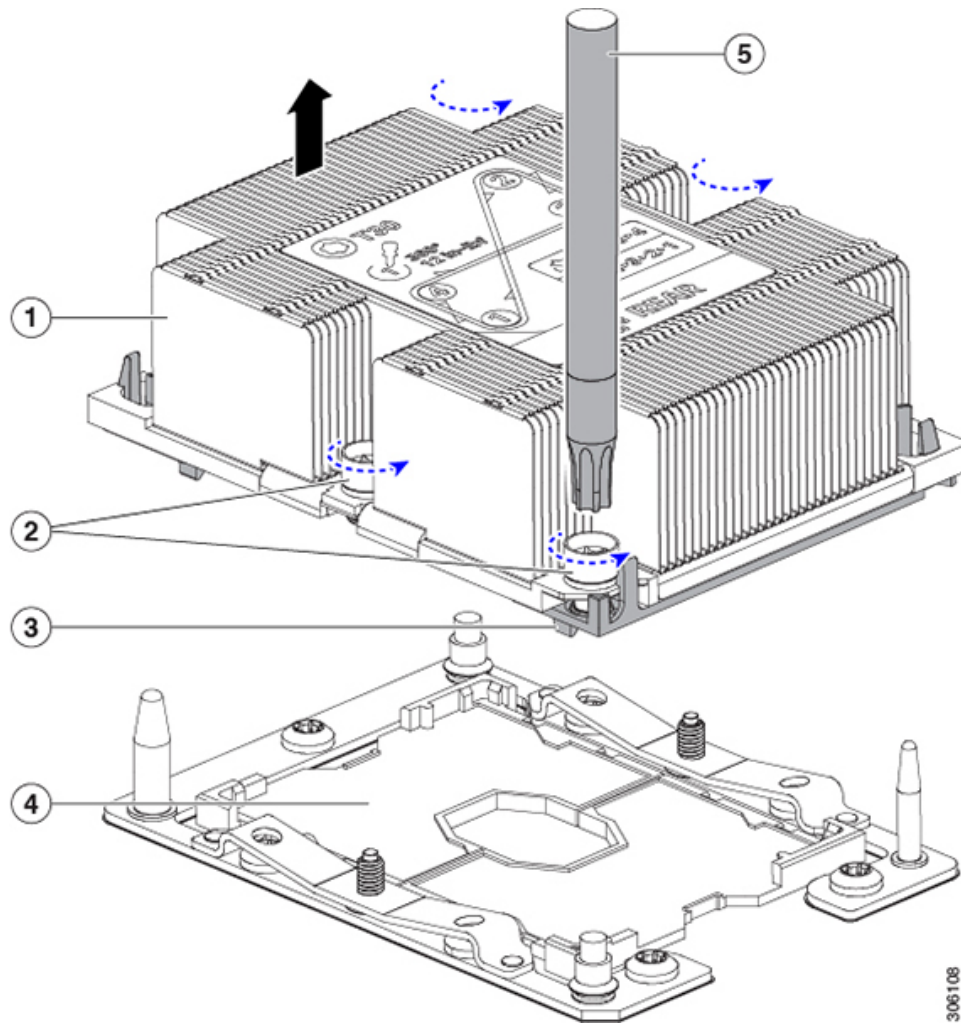
**Caution** If you cannot safely view and access the component, remove the server from the rack.

- c) Remove the top cover from the server as described in [Removing the Server Top Cover, on page 28](#).
- 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 20: 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)	-	

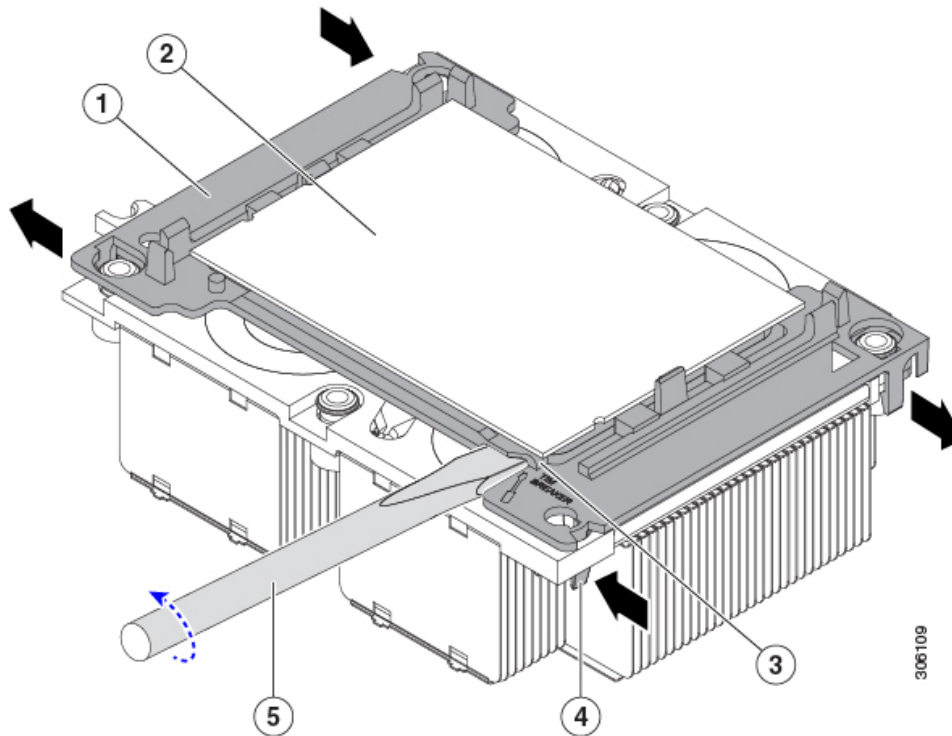
**Step 2**

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 21: 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.

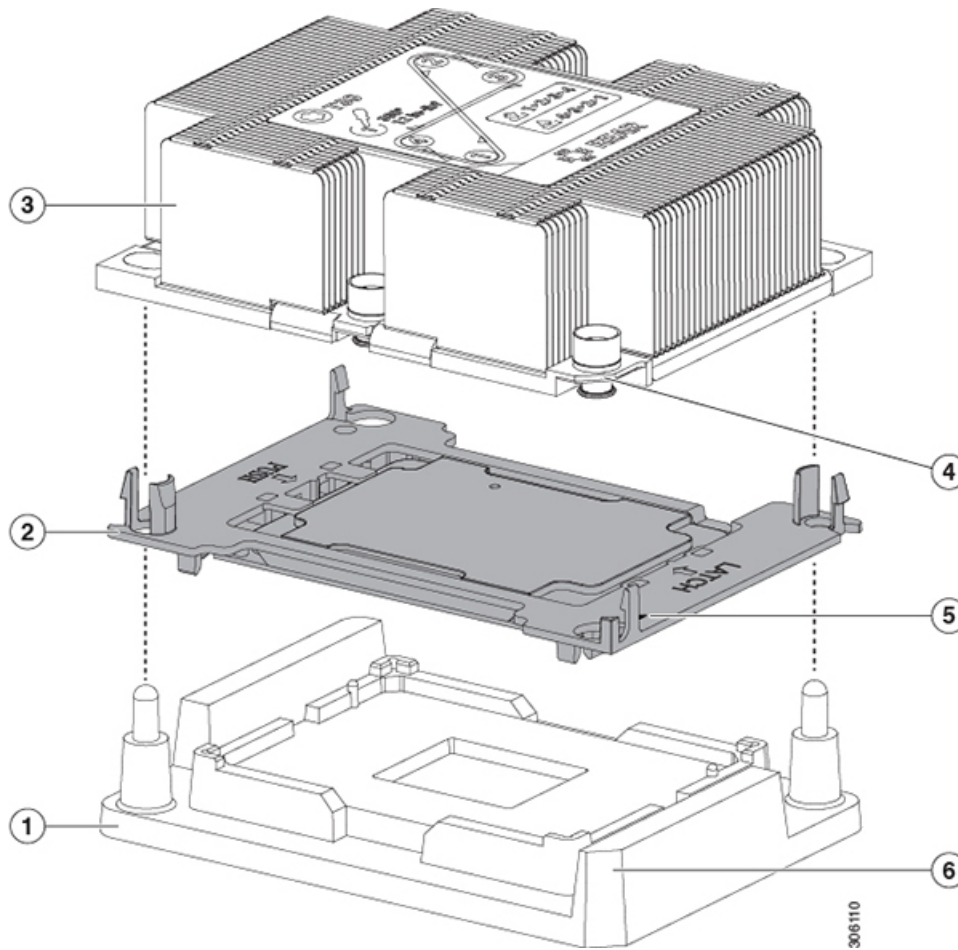
**Note** Handle the CPU-assembly by the plastic carrier only. Do not touch the CPU surface. Do not separate the CPU from the carrier.

**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 22: CPU Assembly Tool, CPU Assembly, and Heatsink Alignment Features*



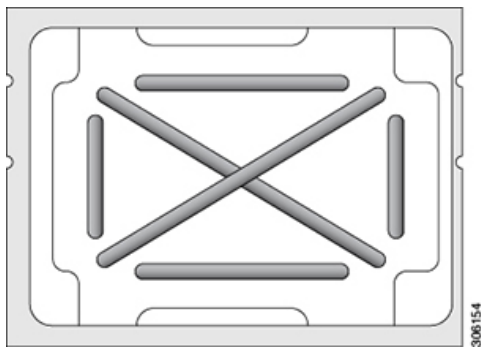
1	CPU assembly tool	4	Angled corner on heatsink (pin 1 alignment feature)
2	CPU assembly (CPU in plastic carrier)	5	Triangle cut into carrier (pin 1 alignment feature)
3	Heatsink	6	Angled corner on CPU assembly tool (pin 1 alignment feature)

**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 4 cubic centimeters of thermal interface material to the top of the CPU. Use the pattern shown below to ensure even coverage.

**Figure 23: 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.

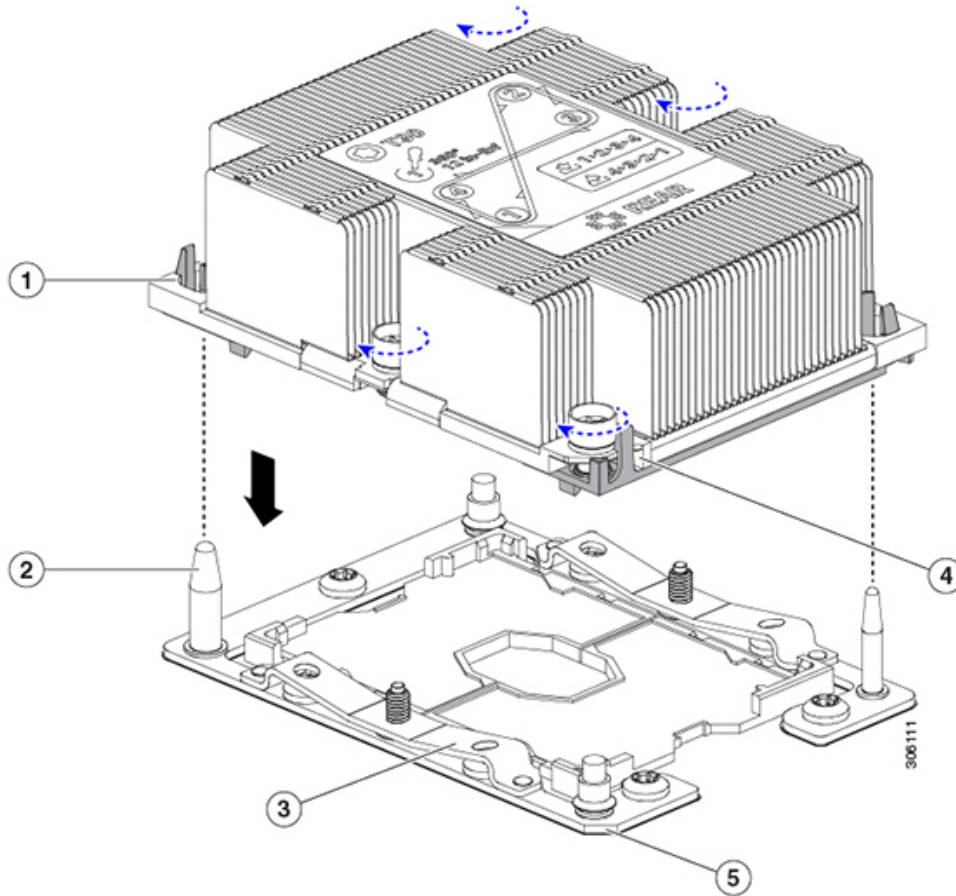
**Caution** In the following step, use extreme care to avoid touching or damaging the CPU contacts or the CPU socket pins.

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



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

- 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.

## 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:

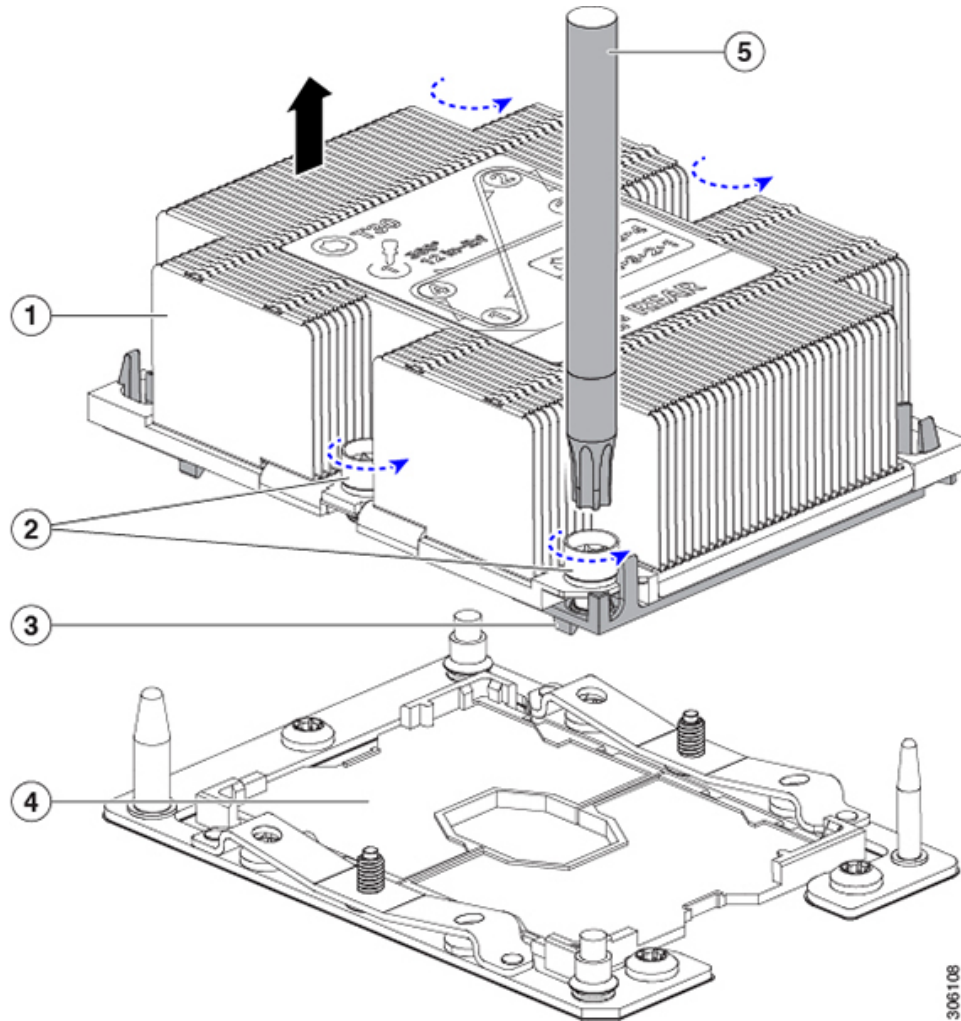
- a) Use a T-30 Torx driver to loosen the four captive nuts that secure the assembly to the board standoffs.

**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 25: 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)	-	

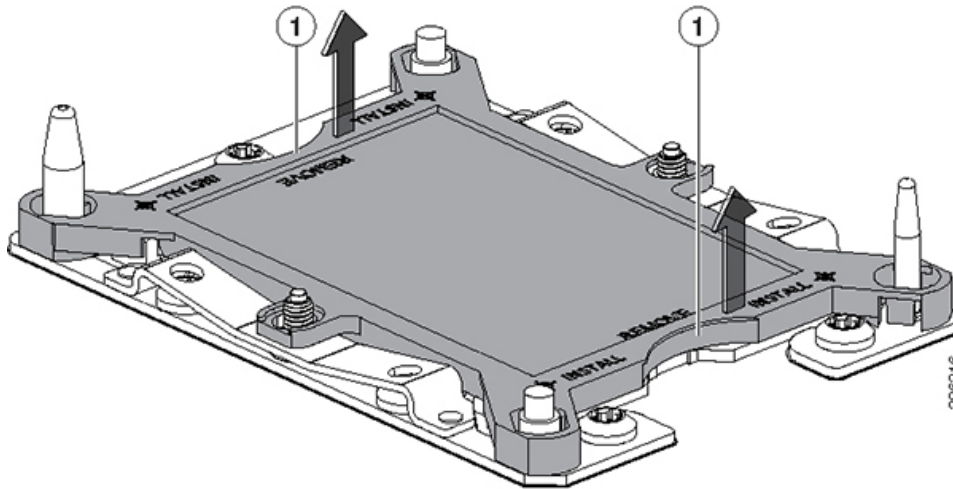
**Step 2**

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 26: Removing a CPU Socket Dust Cover



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

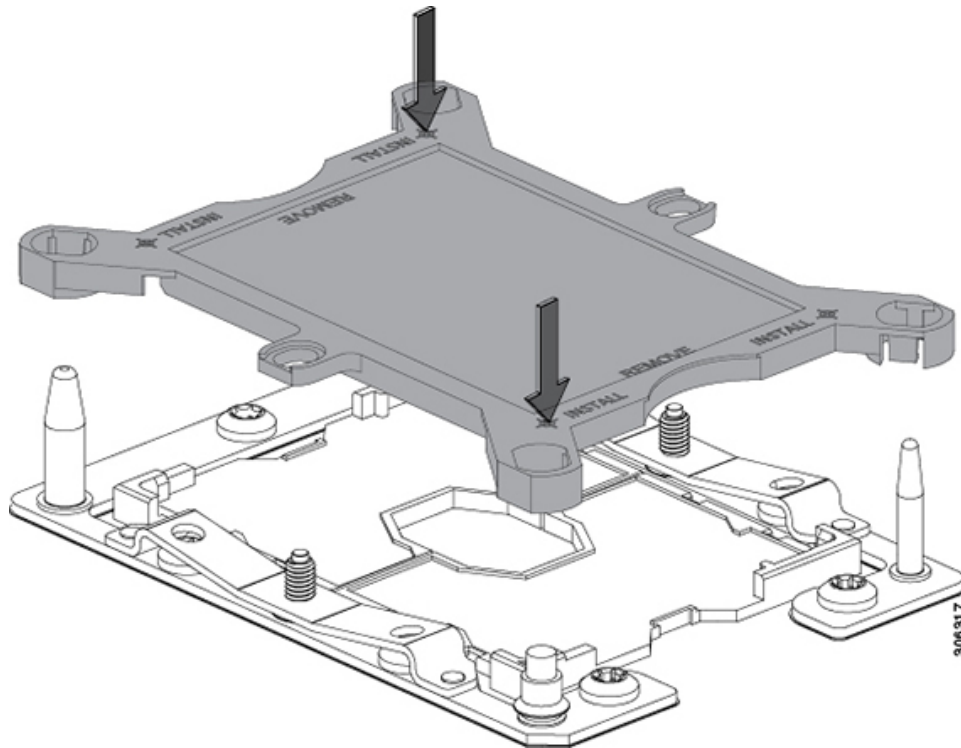
- b) With the wording on the dust cover facing up, set it in place over the CPU socket. Make sure that all alignment posts on the socket plate align with the cutouts on the cover.

**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 27: Installing a CPU Socket Dust Cover



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

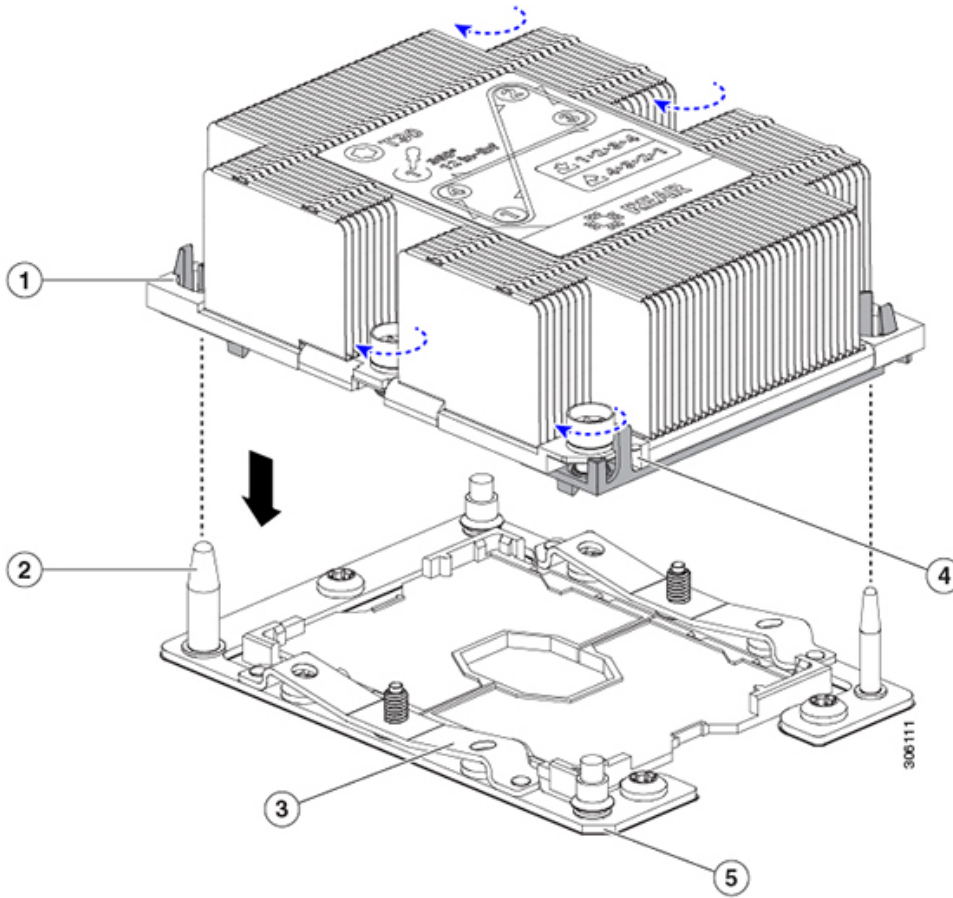
**Step 3**

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 28: 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.

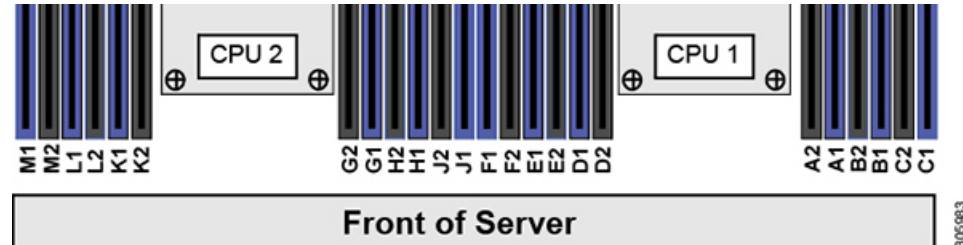
### DIMM Population Rules and Memory Performance Guidelines

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 29: 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 3: 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 4: DIMM Mixing Rules**

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

DIMM type RDIMMs or LRDIMMs	You cannot mix DIMM types in a channel.	You cannot mix DIMM types in a bank.
--------------------------------	---	--------------------------------------

### Memory Mirroring

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

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

## Replacing DIMMs

### Identifying a Faulty DIMM

Each DIMM socket has a corresponding DIMM fault LED, directly in front of the DIMM socket. See [Internal Diagnostic LEDs, on page 25](#) 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 27](#).
- 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 28](#).
- 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 51](#).
- 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 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.

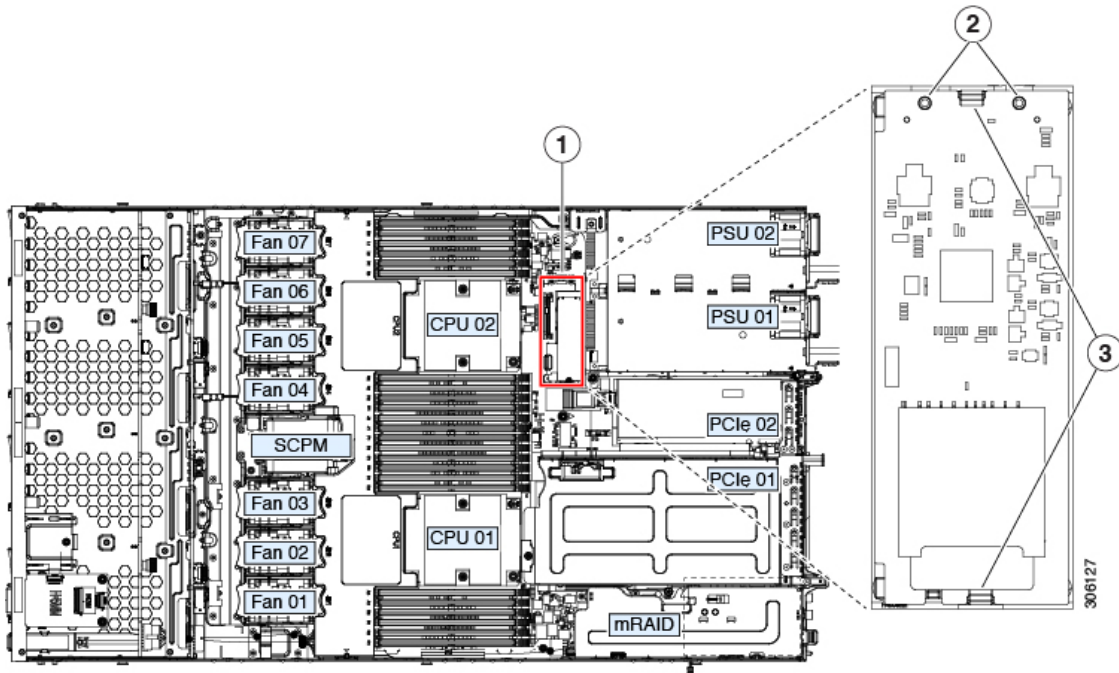
## Replacing a Mini-Storage Module Carrier

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 27](#).
- 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 28](#).
- Step 4** Remove a carrier from its socket:
- Locate the mini-storage module carrier in its socket just in front of power supply 1.
  - At each end of the carrier, push outward on the clip that secures the carrier.
  - Lift both ends of the carrier to disengage it from the socket on the motherboard.
  - Set the carrier on an anti-static surface.
- Step 5** Install a carrier to its socket:
- 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.
  - Gently push down the socket end of the carrier so that the two pegs go through the two holes on the carrier.
  - 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 30: Mini-Storage Module Carrier



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

## 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 96](#).

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 54](#).
- Step 2** Remove an M.2 SSD:
- Use a #1 Phillips-head screwdriver to remove the single screw that secures the M.2 SSD to the carrier.
  - Remove the M.2 SSD from its socket on the carrier.
- Step 3** Install a new M.2 SSD:
- 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.
  - Press the M.2 SSD flat against the carrier.
  - 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 54](#).
- 

## 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



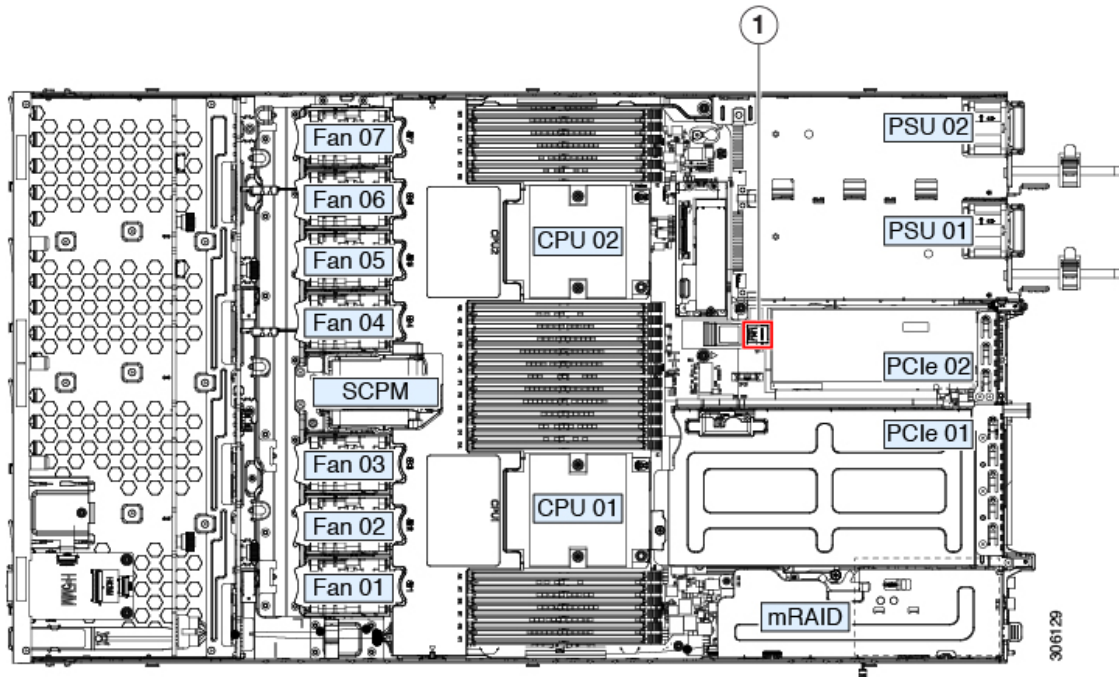

---

**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:
- Shut down and remove power from the server as described in [Shutting Down and Removing Power From the Server, on page 27](#).
  - Slide the server out the front of the rack far enough so that you can remove the top cover. You might have to detach cables from the rear panel to provide clearance.
- Caution** If you cannot safely view and access the component, remove the server from the rack.
- Remove the top cover from the server as described in [Removing the Server Top Cover, on page 28](#).
  - Locate the USB socket on the motherboard, directly in front of PCIe riser 2.
  - Grasp the USB drive and pull it horizontally to free it from the socket.
- Step 2** Install a new internal USB drive:
- Align the USB drive with the socket.
  - Push the USB drive horizontally to fully engage it with the socket.
  - Replace the top cover to the server.
  - Replace the server in the rack, replace cables, and then fully power on the server by pressing the Power button.

Figure 31: 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]

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

**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 27](#).
- 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 28](#).
- 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.

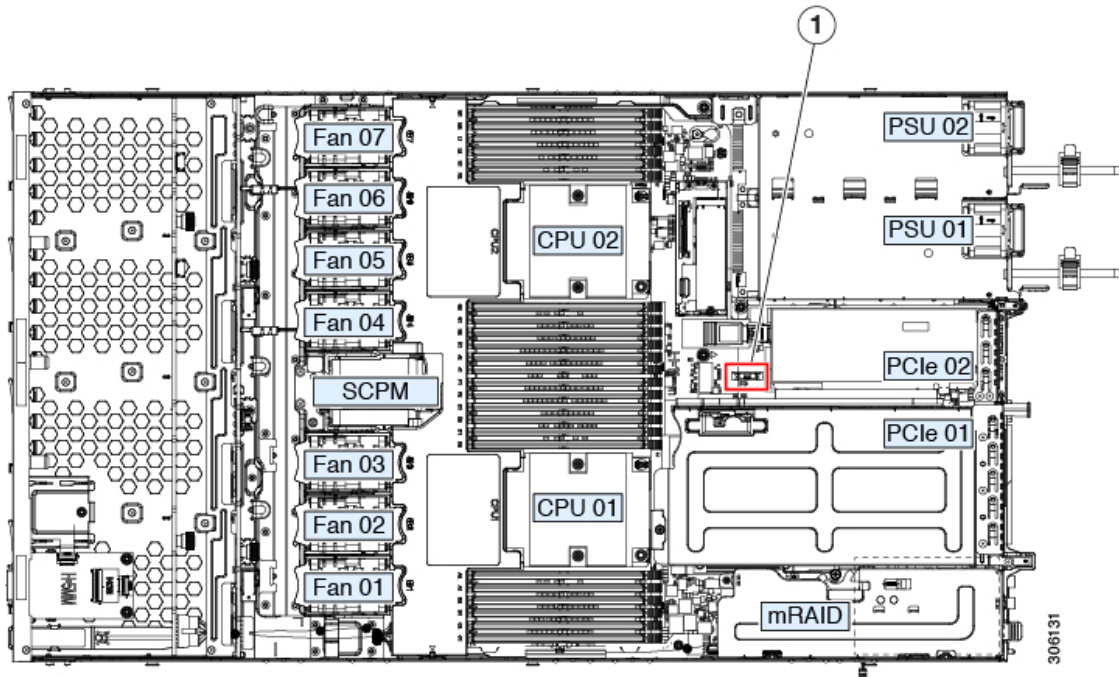
**Step 2** Install a new RTC battery:

- 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 32: RTC Battery Location on Motherboard



1	RTC battery in vertical socket	-	
---	--------------------------------	---	--

## Replacing Power Supplies

The server has one power supply.

- See also [Power Specifications, on page 86](#) for more information about the power supplies.
- See also [Rear-Panel LEDs, on page 24](#) for information about the power supply LEDs.

This section includes procedures for replacing AC power supply units.

- [Replacing AC Power Supplies, on page 59](#)

## Replacing AC Power Supplies



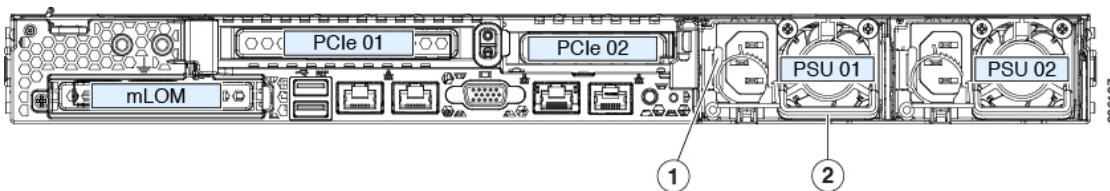
**Note** If you have ordered a server with power supply redundancy (two power supplies), you do not have to power off the server to replace a power supply because they are redundant as 1+1.



**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:
- 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 27](#).
    - If your server has two power supplies, you do not have to shut down the server.
  - Remove the power cord from the power supply that you are replacing.
  - Grasp the power supply handle while pinching the release lever toward the handle.
  - Pull the power supply out of the bay.
- Step 2** Install a new power supply:
- Grasp the power supply handle and insert the new power supply into the empty bay.
  - Push the power supply into the bay until the release lever locks.
  - Connect the power cord to the new power supply.
  - Only if you shut down the server, press the Power button to boot the server to main power mode.

**Figure 33: Replacing AC Power Supplies**



1	Power supply release lever	2	Power supply handle
---	----------------------------	---	---------------------

## Replacing a PCIe Card

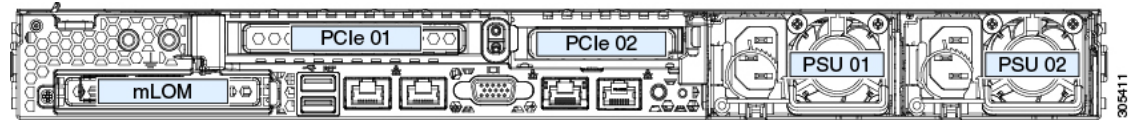


**Note** Cisco supports all PCIe cards qualified and sold by Cisco. PCIe cards not qualified or sold by Cisco are the responsibility of the customer. Although Cisco will always stand behind and support the C-Series rack-mount servers, customers using standard, off-the-shelf, third-party cards must go 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 34: Rear Panel, Showing PCIe Slot Numbering



The following tables describe the specifications for the slots.

Table 5: 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 6: 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 Virtual Interface Card, there are prerequisite considerations. See [Cisco Virtual Interface Card \(VIC\) Considerations](#), on page 64.



**Note** RAID controller cards install into a separate mRAID riser. See [Replacing a SAS Storage Controller Card \(RAID or HBA\)](#), on page 69.

### 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 27.

- 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 28](#).
- 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.

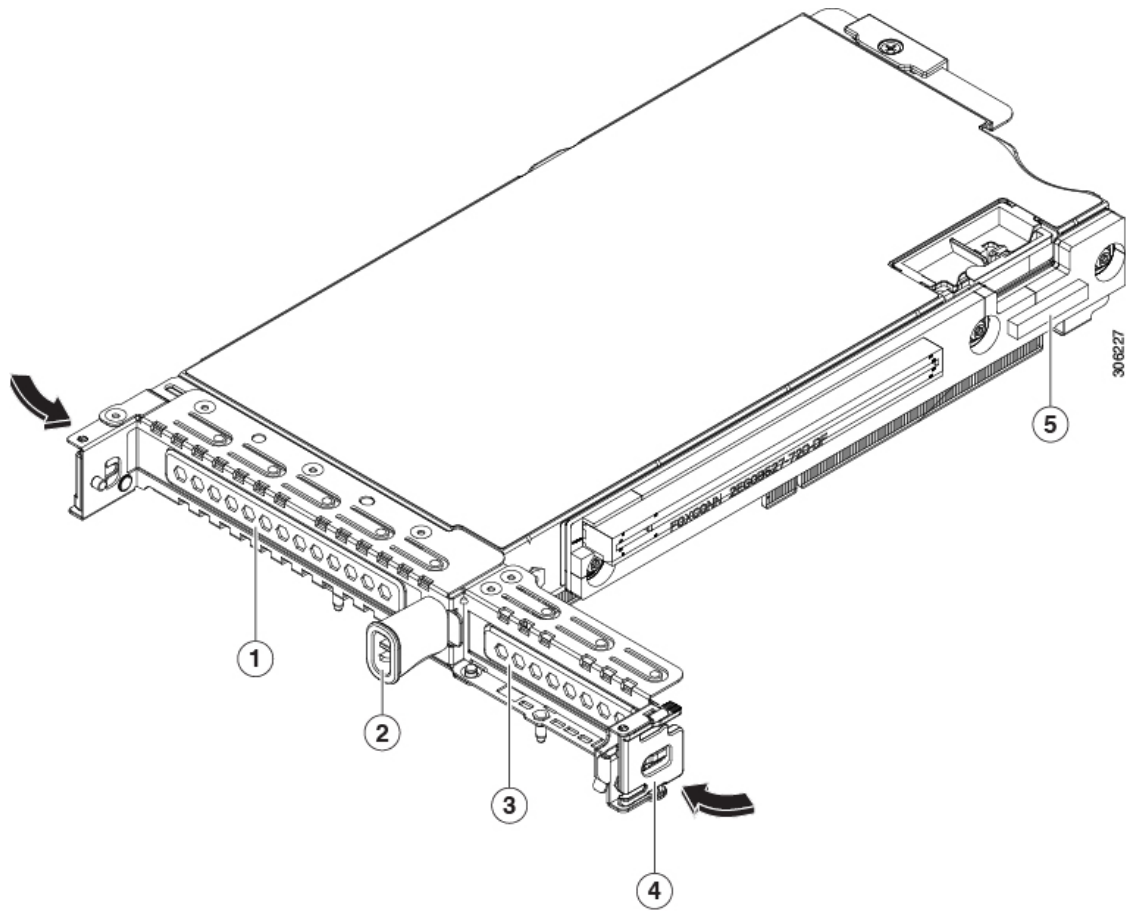
If the riser has no card, remove the blanking panel from the rear opening of the riser.

## 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.



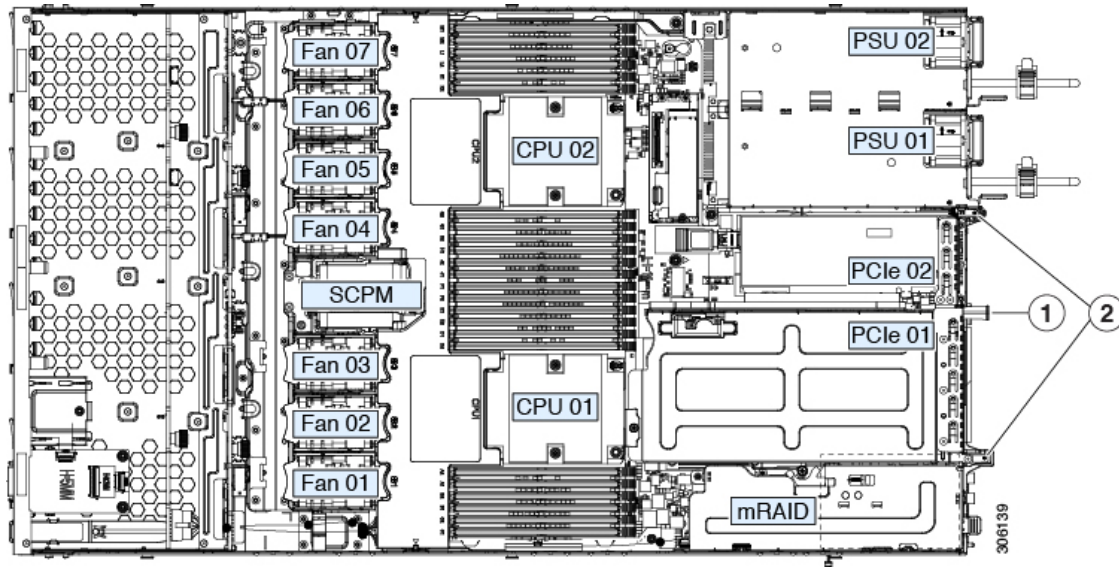
Figure 35: PCIe Riser Assembly



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 36: 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.

Table 7: 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 <i>Cisco Card</i> 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 27](#).
- 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 28](#).
- 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.

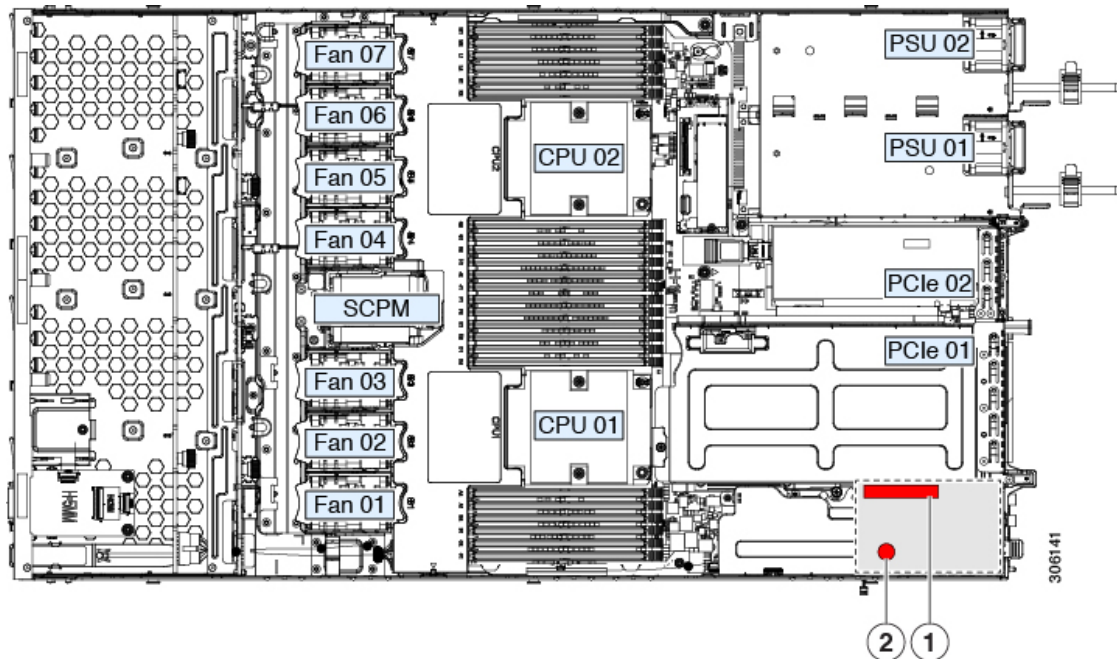
**Step 2** Install a new mLOM card:

- 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 37: Location of the mLOM Card Socket Below the mRAID Riser**



<b>1</b>	Position of horizontal mLOM card socket	<b>2</b>	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 \(RAID or HBA\)](#), on page 69.

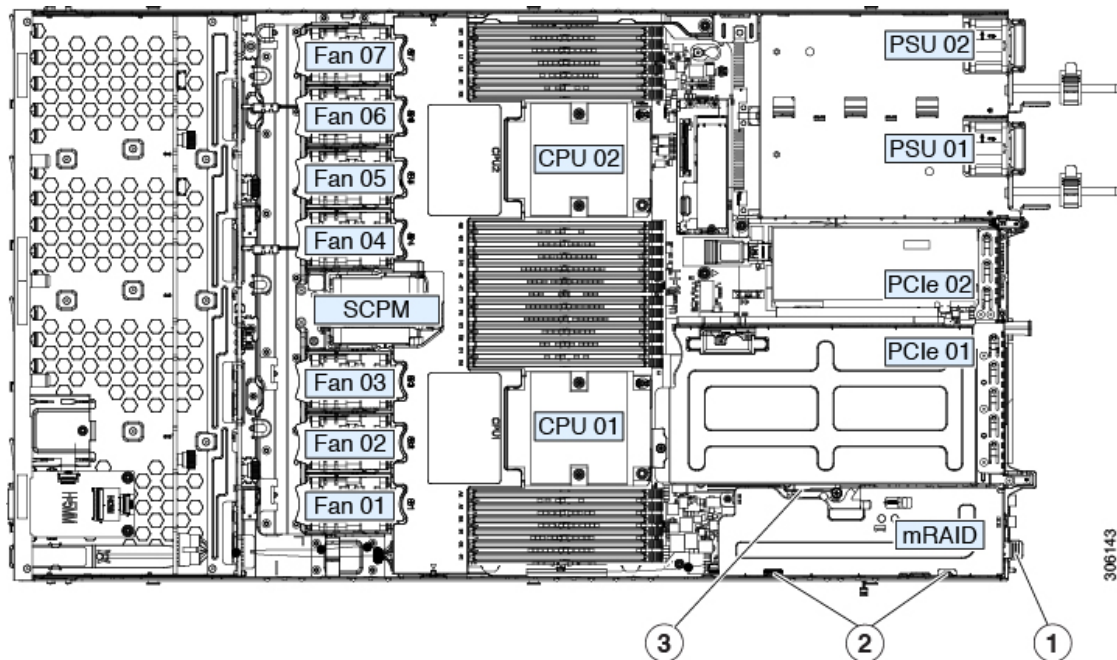
See also [Replacing the Supercap \(RAID Backup\)](#), on page 73.

- 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 75.

- 
- Step 1** Prepare the server for component installation:
- Shut down and remove power from the server as described in [Shutting Down and Removing Power From the Server, on page 27](#).
  - Slide the server out the front of the rack far enough so that you can remove the top cover. You might have to detach cables from the rear panel to provide clearance.  
**Caution** If you cannot safely view and access the component, remove the server from the rack.
  - Remove the top cover from the server as described in [Removing the Server Top Cover, on page 28](#).
- Step 2** Remove the existing mRAID riser:
- 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.
  - Lift the riser straight up to disengage it from the motherboard socket.
  - Set the riser upside down on an antistatic surface.
  - 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:
- Install your card into the new riser. Close the card-ejector lever on the card to lock it into the riser.
  - Connect cables to the installed card.
  - 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.
  - 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 38: 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 96](#) 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)

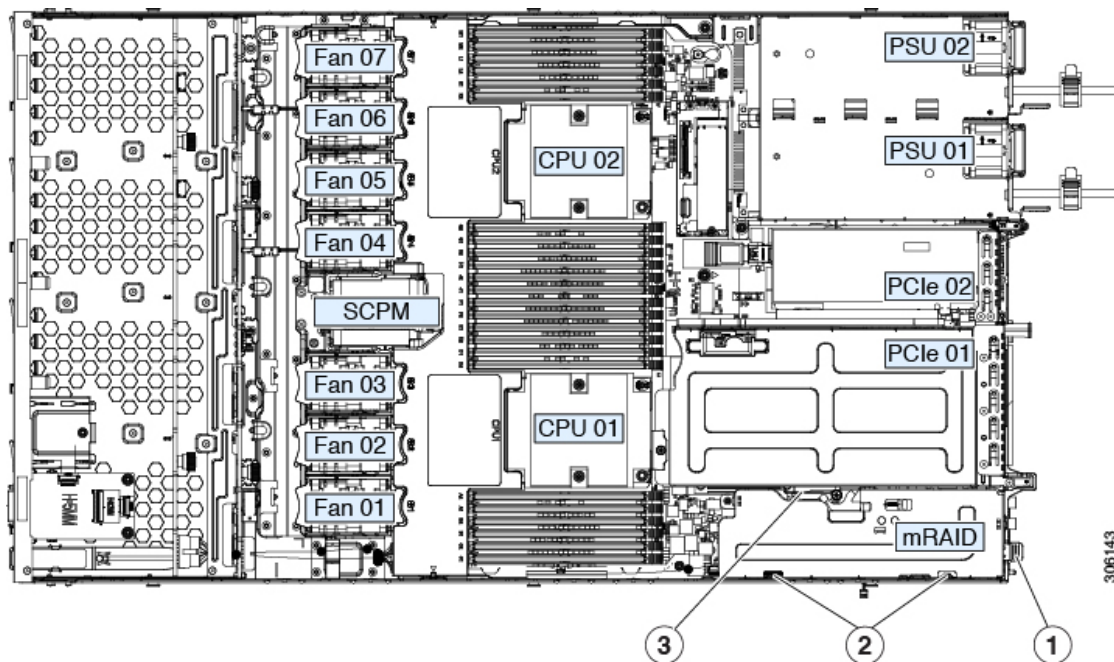
- Step 1** Prepare the server for component installation:
- Shut down and remove power from the server as described in [Shutting Down and Removing Power From the Server, on page 27](#).
  - Slide the server out the front of the rack far enough so that you can remove the top cover. You might have to detach cables from the rear panel to provide clearance.  
**Caution** If you cannot safely view and access the component, remove the server from the rack.
  - Remove the top cover from the server as described in [Removing the Server Top Cover, on page 28](#).
- Step 2** Remove the mRAID riser (riser 3) from the server:
- 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.
  - Lift the riser straight up to disengage it from the motherboard socket.
  - Set the riser upside down on an antistatic surface.
- Step 3** Remove any existing card from the riser:
- Disconnect cables from the existing card.
  - Open the blue card-ejector lever on the back side of the card to eject it from the socket on the riser.
  - Pull the card from the riser and set it aside.
- Step 4** Install a new storage controller card to the riser:
- With the riser upside down, set the card on the riser.
  - Push on both corners of the card to seat its connector in the riser socket.
  - Close the card-ejector lever on the card to lock it into the riser.
  - Connect cables to the installed card.
- Step 5** Return the riser to the server:
- 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.
  - 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 Host Upgrade Utility to update the controller firmware and program the correct suboem-id for the controller.

After you replace controller hardware (APIC-RAID-M5), 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.

Figure 39: 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:

- The minimum version of Cisco IMC that support this controller is 4.0(4) and later.
- This controller supports RAID 1 (single volume) and JBOD mode.
- 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 M2STOR-RAID.
  - A drive in Slot 1 is mapped as drive 253; a drive in slot 2 is mapped as drive 254.



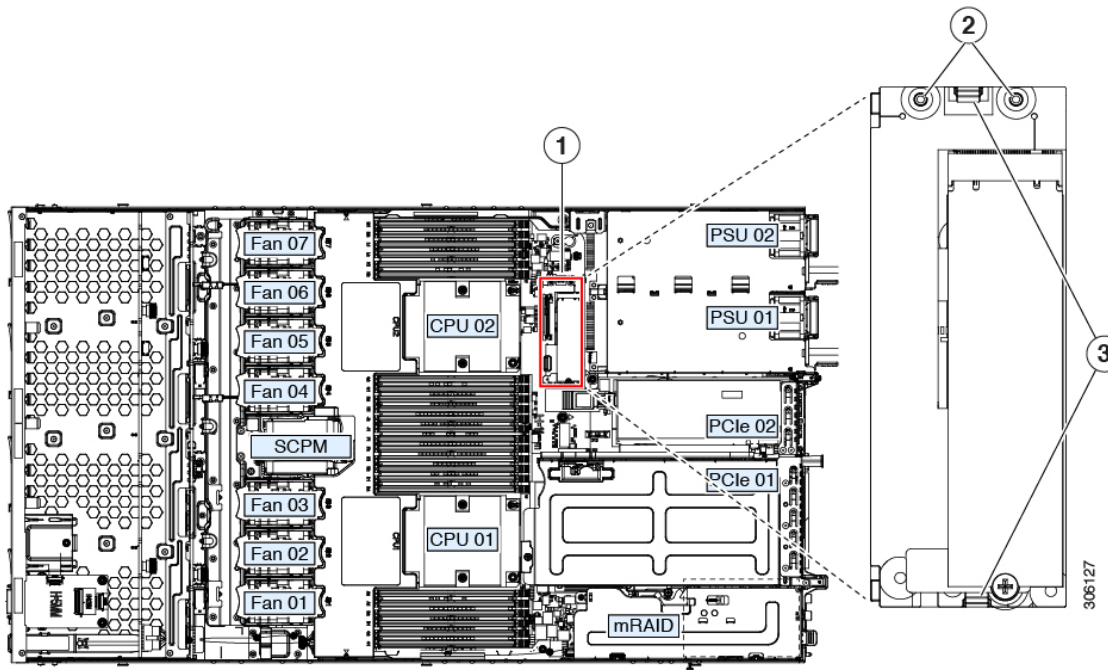
- When using RAID, we recommend that both SATA M.2 drives are the same capacity. If different capacities are used, the smaller capacity of the two drives is used to create a volume and the rest of the drive space is unusable.  
JBOD mode supports mixed capacity SATA M.2 drives.
- Hot-plug replacement 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. They can also be monitored using other utilities such as UEFI HII, PMCLI, XMLAPI, and Redfish.
- 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 27](#).
- 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 28](#).
- 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 40: Cisco Boot-Optimized M.2 RAID Controller on Motherboard



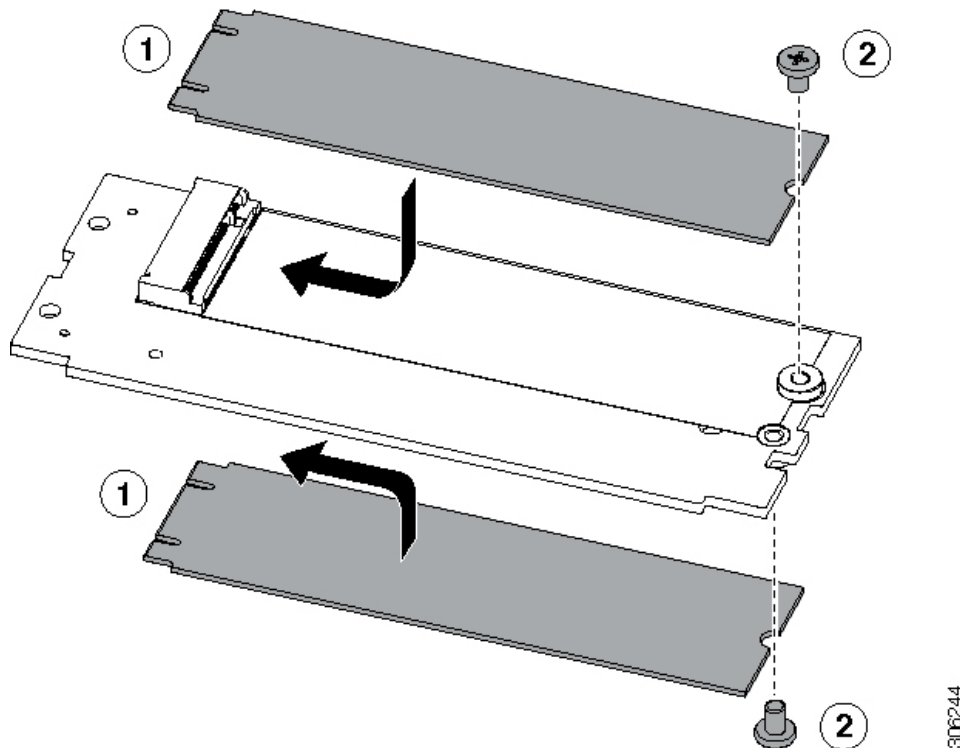
1	Location of socket on motherboard	3	Securing clips
2	Alignment pegs	-	

**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 41: Cisco Boot-Optimized M.2 RAID Controller, Showing M.2 Drive Installation



- Step 6** Install the controller to its socket on the motherboard:
- 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.
  - Gently push down the socket end of the controller so that the two pegs go through the two holes on the controller.
  - 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:
- Shut down and remove power from the server as described in [Shutting Down and Removing Power From the Server, on page 27](#).
  - 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.

## Replacing the Supercap (RAID Backup)

**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 28](#).

**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.

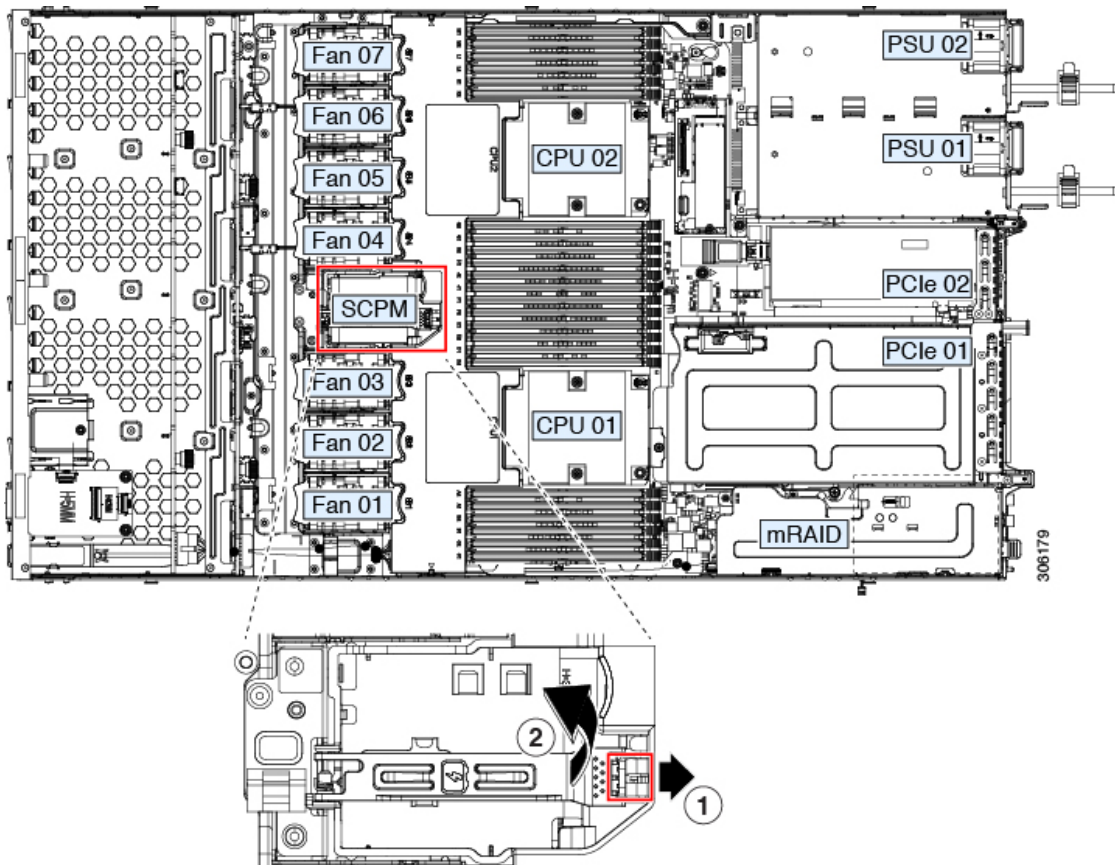
**Step 3** Install a new supercap:

- 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 42: 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).

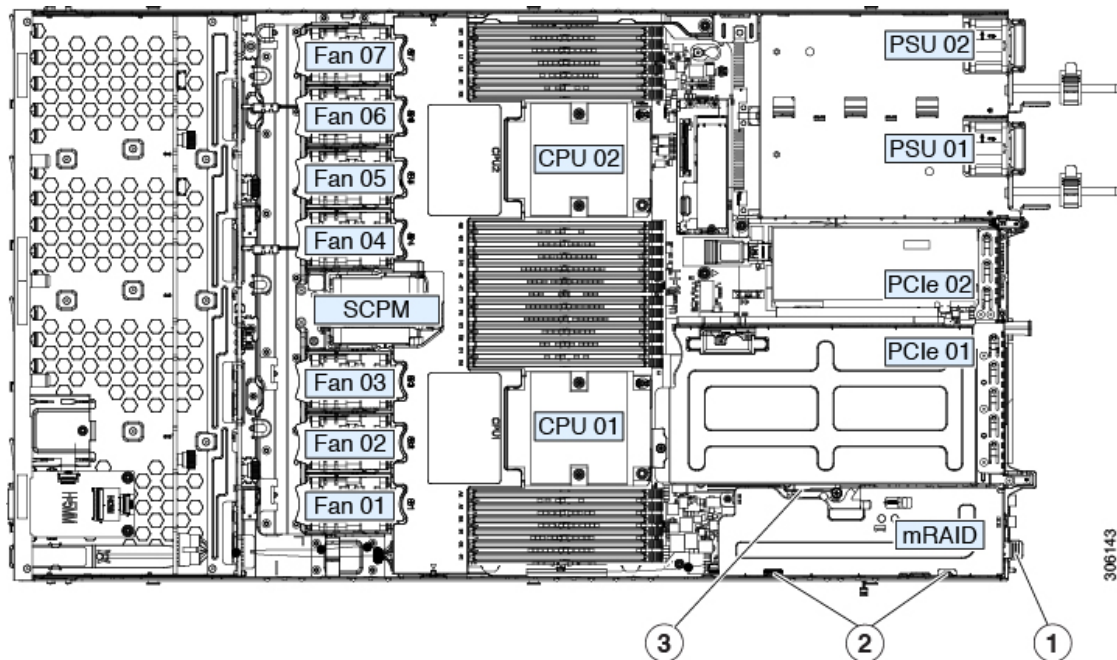


**Note** You cannot use a hardware RAID controller card and the embedded software RAID controller at the same time. See [Embedded SATA RAID Controller, on page 96](#) for details about RAID support.

- Step 1** Prepare the server for component installation:
- Shut down and remove power from the server as described in [Shutting Down and Removing Power From the Server, on page 27](#).
  - Slide the server out the front of the rack far enough so that you can remove the top cover. You might have to detach cables from the rear panel to provide clearance.
 

**Caution** If you cannot safely view and access the component, remove the server from the rack.
  - Remove the top cover from the server as described in [Removing the Server Top Cover, on page 28](#).
- Step 2** Remove the mRAID riser (riser 3) from the server:
- 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.
  - Lift the riser straight up to disengage it from the motherboard socket.
  - Set the riser upside down on an antistatic surface.
- Step 3** Remove any existing card from the riser:
- Disconnect cables from the existing card.
  - Open the blue card-ejector lever on the back side of the card to eject it from the socket on the riser.
  - Pull the card from the riser and set it aside.
- Step 4** Install a new card to the riser:
- With the riser upside down, set the card on the riser.
  - Push on both corners of the card to seat its connector in the riser socket.
  - Close the card-ejector lever on the card to lock it into the riser.
- Step 5** Return the riser to the server:
- 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.
  - 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 43: 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 is an optional security feature that logs an event in the system event log (SEL) whenever the cover is removed from the chassis.

**Step 1** Prepare the server for component installation:

- Shut down and remove power from the server as described in [Shutting Down and Removing Power From the Server, on page 27](#).
- Slide the server out the front of the rack far enough so that you can remove the top cover. You might have to detach cables from the rear panel to provide clearance.

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

- Remove the top cover from the server as described in [Removing the Server Top Cover, on page 28](#).

**Step 2** Remove an existing intrusion switch:

- Disconnect the intrusion switch cable from the socket on the motherboard.
- Use a #1 Phillips-head screwdriver to loosen and remove the single screw that holds the switch mechanism to the chassis wall.
- Slide the switch mechanism straight up to disengage it from the clips on the chassis.

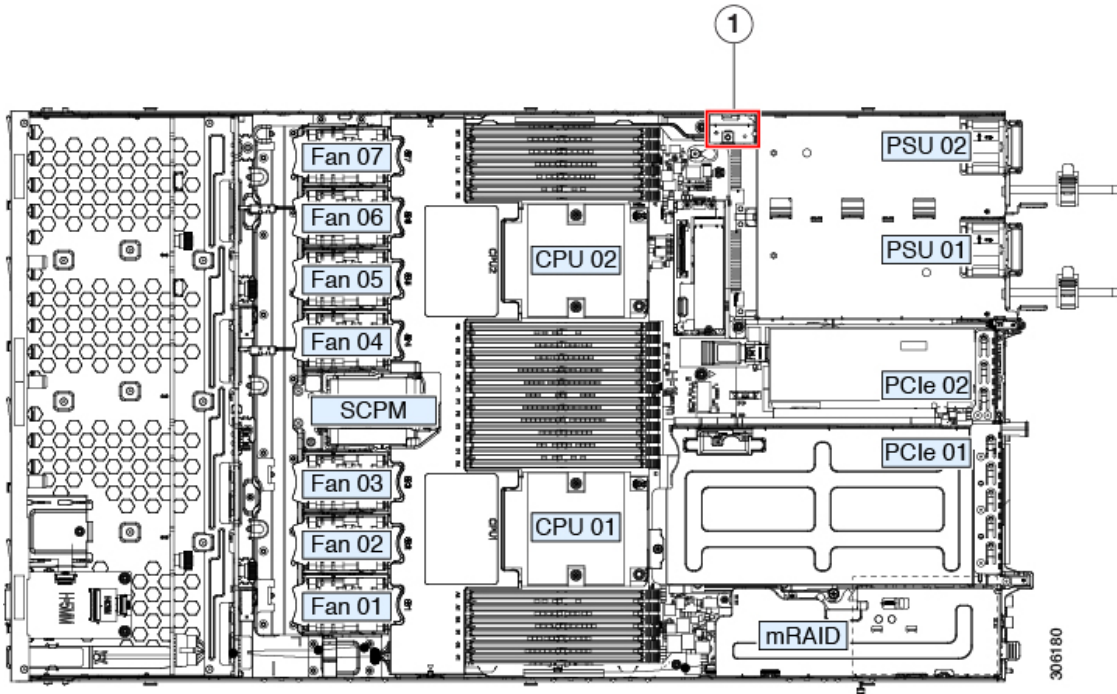


- Step 3** Install a new intrusion switch:
- a) Slide the switch mechanism down into the clips on the chassis wall so that the screwhole lines up.
  - b) Use a #1 Phillips-head screwdriver to install the single screw that secures the switch mechanism to the chassis wall.
  - c) Connect the switch cable 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 44: 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 TPM version 2.0.
- Field replacement of a TPM is not supported.

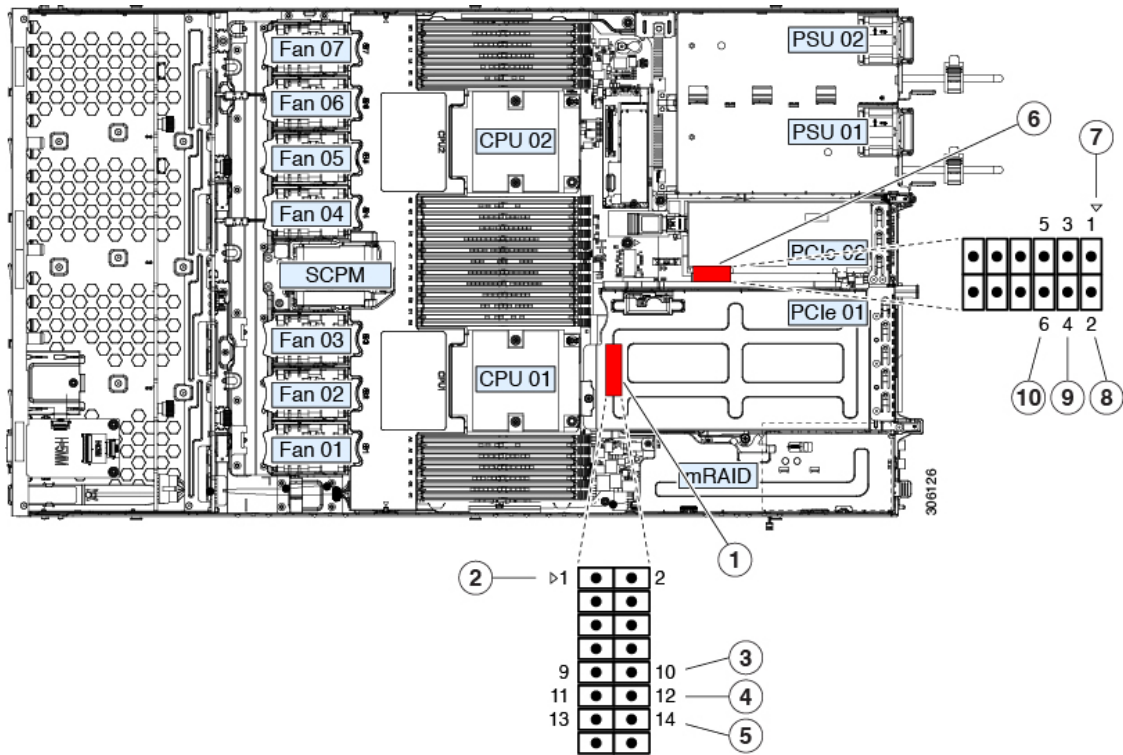
# Service Headers and Jumpers

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

This section contains the following topics:

- Using the Clear CMOS Header (J38, Pins 9 - 10), on page 79
- Using the BIOS Recovery Header (J38, Pins 11 - 12), on page 80
- Using the Clear Password Header (J38, Pins 13 - 14), on page 81
- Using the Boot Alternate Cisco IMC Image Header (J39, Pins 1 - 2), on page 82
- Using the Reset Cisco IMC Password to Default Header (J39, Pins 3 - 4), on page 83
- Using the Reset Cisco IMC to Defaults Header (J39, Pins 5 - 6), on page 84

Figure 45: 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 27](#). 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 28](#).
- Step 4** Locate header block J38 and pins 9-10, as shown in [Service Headers and Jumpers, on page 78](#).
- 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 27](#). 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 28](#).
- Step 6** Locate header block J38 and pins 11-12, as shown in [Service Headers and Jumpers, on page 78](#).
- 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 27](#). 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 28](#).
- Step 4** Locate header block J38 and pins 13-14, as shown in [Service Headers and Jumpers, on page 78](#).
- 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 27](#). 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 28](#).
- Step 4** Locate header block J39, pins 1-2, as shown in [Service Headers and Jumpers, on page 78](#).
- 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 27](#). 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 28](#).
- Step 4** Locate header block J39, pins 3-4, as shown in [Service Headers and Jumpers, on page 78](#).
- 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 27](#). 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 28](#).
- Step 4** Locate header block J39, pins 5-6, as shown in [Service Headers and Jumpers, on page 78](#).
- 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 settings 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, on page 85](#)

### Server Specifications

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

- [Physical Specifications, on page 85](#)
- [Environmental Specifications, on page 85](#)
- [Physical Specifications, on page 85](#)

### Physical Specifications

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

**Table 8: 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.

Table 9: Environmental Specifications

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

## Power Specifications

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

### 1050 W AC Power Supply

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



Table 10: 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

## 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 11: Supported Power Cords

Description	Length (Feet)	Length (Meters)
CAB-48DC-40A-8AWG DC power cord, -48 VDC, 40 A, 8 AWG Three-socket Mini-Fit connector to three-wire	11.7	3.5

CAB-C13-C14-AC AC power cord, 10 A; C13 to C14, recessed receptacle	9.8	3.0
CAB-250V-10A-AR AC power cord, 250 V, 10 A Argentina	8.2	2.5
CAB-C13-C14-2M-JP AC Power Cord, C13 to C14 Japan PSE Mark	6.6	2.0
CAB-9K10A-EU AC Power Cord, 250 V, 10 A; CEE 7/7 Plug Europe	8.2	2.5
CAB-250V-10A-IS AC Power Cord, 250 V, 10 A Israel	8.2	2.5
CAB-250V-10A-CN AC power cord, 250 V, 10 A PR China	8.2	2.5
CAB-ACTW AC power cord, 250 V, 10 A Taiwan	7.5	2.3
CAB-C13-CBN AC cabinet jumper power cord, 250, 10 A, C13 to C14	2.2	0.68
CAB-C13-C14-2M AC cabinet jumper power cord, 250 V, 10 A, C13 to C14	6.6	2.0
CAB-9K10A-AU AC power cord, 250 V, 10 A, 3112 plug, Australia	8.2	2.5
CAB-N5K6A-NA AC power cord, 200/240 V, 6 A, North America	8.2	2.5

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





## APPENDIX **B**

# Storage Controller Considerations

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

- [Supported Storage Controllers and Cables, on page 91](#)
- [Storage Controller Card Firmware Compatibility, on page 92](#)
- [RAID Backup \(Supercap\), on page 92](#)
- [Write-Cache Policy for Cisco 12G SAS Modular RAID Controller, on page 92](#)
- [Mixing Drive Types in RAID Groups, on page 93](#)
- [RAID Controller Migration, on page 93](#)
- [Storage Controller and Backplane Connectors, on page 94](#)
- [Embedded SATA RAID Controller, on page 96](#)
- [For More RAID Utility Information, on page 99](#)

## 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: <ul style="list-style-type: none"> <li>All server versions can use the embedded SATA controller to control two internal SATA M.2 drives.</li> <li>8 front-loading SATA drives (drive bays 1 - 8)</li> </ul>	0, 1, 10	No	Use SAS/SATA cable included with chassis to connect interposer board 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: <ul style="list-style-type: none"> <li>10 front-loading SAS/SATA drives</li> </ul>	0, 1, 5, 6, 10, 50, 60	Yes	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	Controls two SATA M.2 drives that mount to this controller.	1	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.

## 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 73.

## 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 12: 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 <ol style="list-style-type: none"><li>1. Install RAID card.</li><li>2. Install SAS cables.</li></ol>	Allowed <ol style="list-style-type: none"><li>1. Install SATA interposer card.</li><li>2. Install SATA cables.</li><li>3. Enable embedded RAID in BIOS.</li></ol>
Embedded software RAID. Embedded RAID is enabled in the BIOS.	<b>Caution</b> Data migration from software RAID to hardware RAID is <i>not</i> supported and could result in data loss.  Allowed only before there is data on the drives; data migration is not supported. <ol style="list-style-type: none"><li>1. Disable embedded RAID in the BIOS.</li><li>2. Install RAID card.</li><li>3. Install SAS cables.</li></ol>	-
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 the SFF 10-drive of the SE-CL-L3 .

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

### 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.

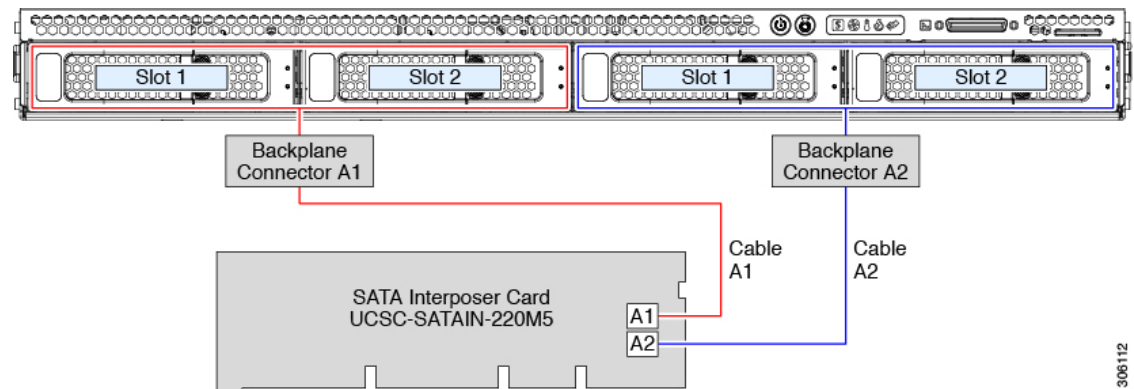
1. Connect SAS/SATA cable A1 from the A1 interposer connector to the A1 backplane connector.
2. Connect SAS/SATA cable A2 from the A2 interposer connector to the A2 backplane connector.



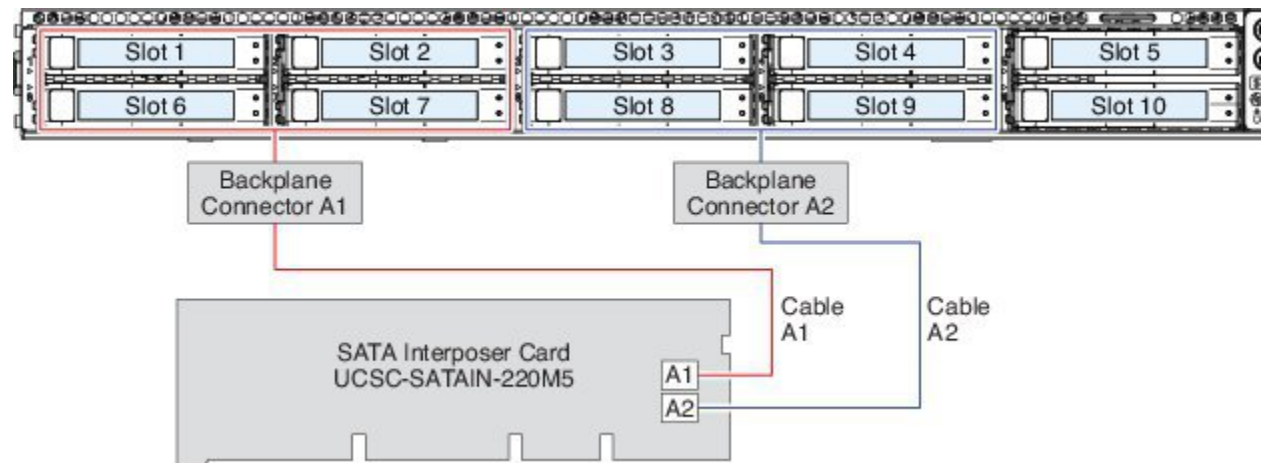
**Note** See the following figures that illustrate cable connections and which drives are controlled by each cable. In the SFF 10-drive version, drives 5 and 10 cannot be controlled by the embedded SATA RAID controller.



**Figure 46: Embedded RAID Interposer Cable-to-Drive Backplane Mapping, LFF 4-Drive Version**



**Figure 47: 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 48: Hardware RAID Card Cable-to-Drive Backplane Mapping, LFF 4-Drive Version

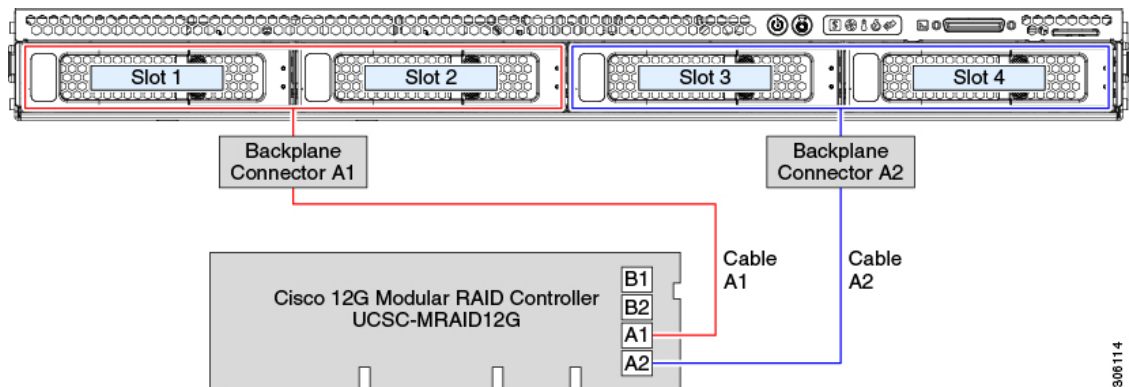
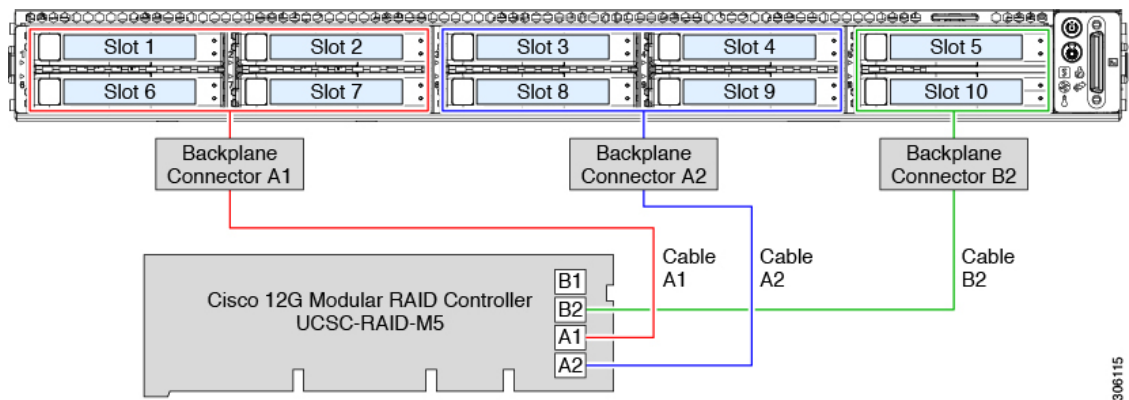


Figure 49: Hardware RAID Card Cable-to-Drive Backplane Mapping, SFF 10-Drive Version



## 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 hypervisors 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.

---

## Embedded 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 98](#).
- 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 98](#).
- You cannot downgrade from using a hardware RAID controller card to using the software RAID embedded controller (see [RAID Controller Migration, on page 93](#)).



---

**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.

## 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 SE-CL-L3 :
  - 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.

## 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)**.
- 

## 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](#).

