Cisco CSS UCS Platform Series User Guide, CPS-UCSM4-1RU-K9 / CPS-UCSM4-2RU-K9

Revised: September 02, 2016

CONTENTS

Preface

Purpose

This document summarizes the requirements and supported features of the following Cisco Connected Safety and Security UCS Platform Series servers:

- CPS-UCSM4-1RU-K9
- CPS-UCSM4-2RU-K9

This document also includes a summary of common installation and configuration topics, and links to detailed instructions. Additional summaries are included for the applications supported on the servers, such as the Cisco Video Surveillance Manager.

Revision History

Table 1   Revision History

Document Revision Date	Change Summary
September 02, 2016	Revised maximum supported HDD capacity in "Server Model Comparison".
August 10, 2016	Revised supported HDD information in "Server Model Comparison".
June, 2016	Initial version created for the following servers only: • CPS-UCSM4-1RU-K9 • CPS-UCSM4-2RU-K9

Related Documentation

For information about the CPS-UCS-1RU-K9 and CPS-UCS-2RU-K9 servers, see Cisco Physical Security UCS Platform Series User Guide, CPS-UCS-1RU-K9 / CPS-UCS-2RU-K9.

See "Related Documentation" for more information.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information about obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*. This document also lists all new and revised Cisco technical documentation. It is available at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Tip See "Related Documentation" for more information and links to Cisco Video Surveillance documentation.

Command Syntax Conventions

Table 2 describes the syntax used with the commands in this document.

Table 2   Command Syntax Guide

Convention	Description
boldface	Commands and keywords.
italic	Command input that is supplied by you.
[ ]	Keywords or arguments that appear within square brackets are optional.
{ x	x	x }	A choice of keywords (represented by x) appears in braces separated by vertical bars. You must select one.
^ or Ctrl	Represent the key labeled *Control*. For example, when you read *^D* or *Ctrl-D*, you should hold down the Control key while you press the D key.
screen font	Examples of information displayed on the screen.
boldface screen font	Examples of information that you must enter.
< >	Nonprinting characters, such as passwords, appear in angled brackets.
[ ]	Default responses to system prompts appear in square brackets.

CHAPTER 1

Overview

The Cisco Connected Safety and Security UCS Platform Series servers provide a hardware platform for Connected Safety and Security applications, such as the Cisco Video Surveillance Manager. This document describes the features and requirements of the supported server models and includes references to detailed installation and configuration instructions available in related documentation.

The server is orderable in the following versions:

- CPS-UCSM4-1RU-K9—A 1RU server that holds up to four 3.5-inch SAS hard drives (Figure 1-1).
- CPS-UCSM4-2RU-K9—A 2RU server that holds up to 12 3.5-inch SAS hard drives (Figure 1-3).

Note For information about the previous release of these servers, see Cisco Physical Security UCS Platform Series User Guide, CPS-UCS-1RU-K9 / CPS-UCS-2RU-K9.

Refer to the following topics for more information.

■ **System Overview**

System Overview

The Cisco Connected Safety and Security UCS series servers are adapted from the Cisco UCS C-Series Rack Servers, and support a subset of the features available on the Cisco UCS series servers.

Refer to the following topics for an overview of the supported server models and features.

Server Model Comparison

The Cisco Connected Safety and Security UCS series servers are available in a 1RU and 2RU configuration and include the following features:

Table 1-1   ***Supported Hardware Feature Comparison***

Feature	CPS-UCSM4-1RU-K9	CPS-UCSM4-2RU-K9
Form-Factor	1 RU	2 RU
Processor	Single Intel Xeon E5-2600 v3 Series processor	Dual Intel Xeon E5-2600 v3 Series processors
Memory	16GB	32GB
HDD[1]	Up to four 4TB drives for a maximum capacity of 16TB.	Up to twelve 16 TB drives for a maximum capacity of 72TB.

1. 3.5-inch large form factor (LFF) SAS hard drives

Note   The supported features described in Table 1-1 are a sub-set of the features supported by the Cisco UCS C-Series Rack Server platform.

Cisco CSS UCSM4 1RU Overview

The Cisco Connected Safety and Security UCSM4 1RU is a 1RU server available in the large form factor (LFF) only, which supports up to four 3.5-inch SAS hard drives.

Note   The small form-factor (SFF) version of the Cisco UCS C220 M4 1RU Server is not supported for Cisco Connected Safety and Security applications.

Cisco CSS UCSM4 1RU Front Panel

Figure 1-1 shows the front panel features of server.

Figure 1-1   Cisco CSS UCSM4 1RU Server (LFF Drives, 4-Drive) Front Panel Features
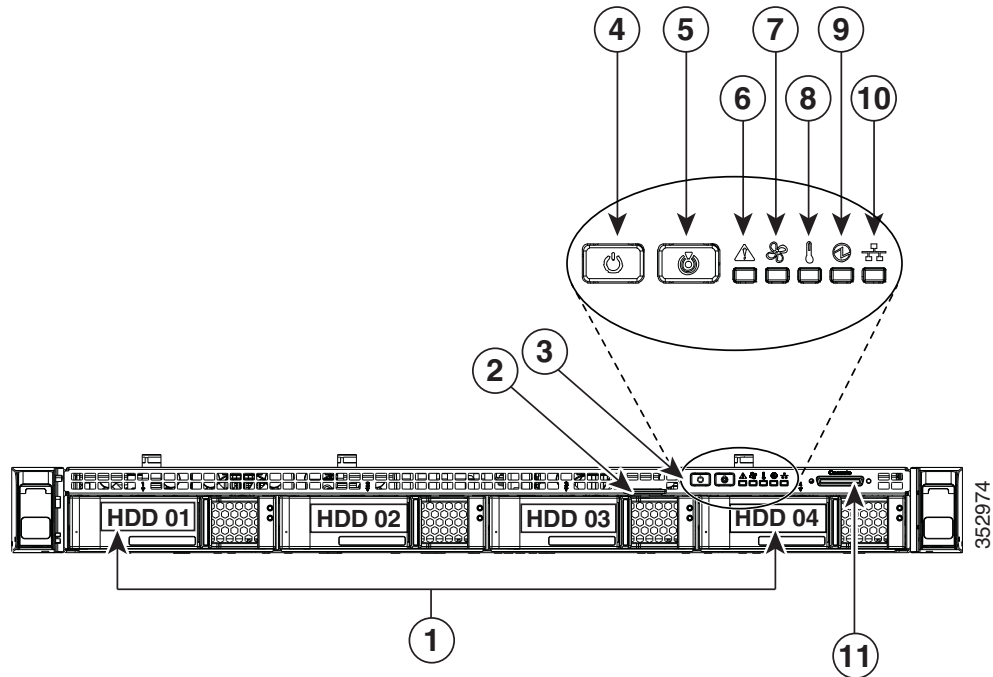
1	Drives (up to four 3.5-inch drives)	7	Fan status LED
2	Pull-out asset tag	8	Temperature status LED
3	Operations panel buttons and LEDs	9	Power supply status LED
4	Power button/power status LED	10	Network link activity LED
5	Unit identification button/LED	11	KVM connector (used with KVM cable that provides two USB 2.0, one VGA, and one serial connector)
6	System status LED		

Cisco CSS UCSM4 1RU Rear Panel

Figure 1-2 shows the rear panel features of the server.

Figure 1-2   Cisco CSS UCSM4 1RU Server Rear Panel Features
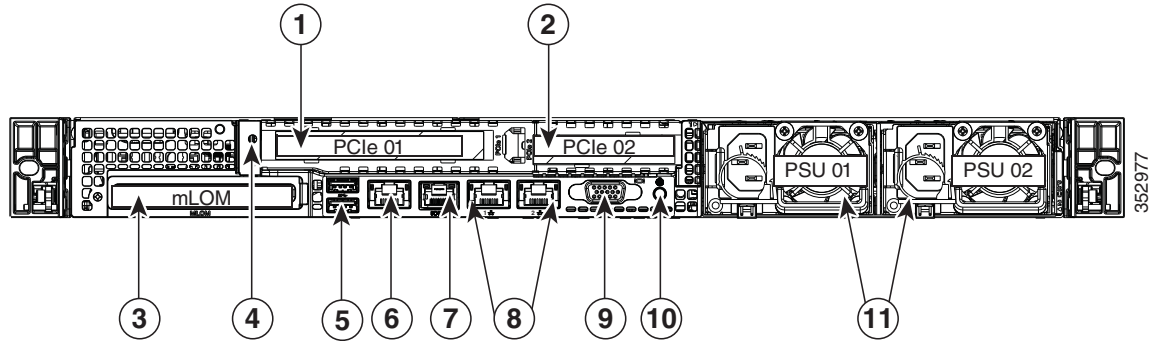
1	PCIe riser 1/slot 1	7	Serial port (RJ-45 connector)
2	PCIe riser 2/slot 2	8	Dual 1-Gb Ethernet ports (LAN1 and LAN2)
3	Modular LAN-on-motherboard (mLOM) card slot	9	VGA video port (DB-15)
4	Grounding-lug hole (for DC power supplies)	10	Rear unit identification button/LED
5	USB 3.0 ports (two)	11	Power supplies (up to two, redundant as 1+1)
6	1-Gb Ethernet dedicated management port		

Tip   See the "Cisco CSS UCSM4 1RU LEDs and Buttons" section on page 1-10 for more information.

Summary of Cisco CSS UCSM4 1RU Server Features

Table 1-2 lists the features of the server.

.

Table 1-2   Cisco CSS UCSM4 1RU Server Features

Feature	Description
Chassis	One rack-unit (1RU) chassis.
Processors	Up to two Intel Xeon E5-2600 v3 Series processors.
Memory	16 DDR4
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 Ethernet LOM ports, or a Cisco virtual interface card.

Table 1-2   Cisco CSS UCSM4 1RU Server Features (continued)

Feature	Description (continued)
Network and management I/O	Supported connectors: • One 1-Gb Ethernet dedicated management port • Two 1-Gb BASE-T Ethernet LAN ports • One RS-232 serial port (RJ-45 connector) • One 15-pin VGA[1] connector • Two USB[2] 3.0 connectors • One front-panel KVM connector that is used with the KVM cable, which provides two USB 2.0, one VGA, and one serial (DB-9) connector.
WoL	1-Gb BASE-T Ethernet LAN ports support the wake-on-LAN (WoL) standard.
Power	AC power supplies 770 W AC each. Do not mix power supply types or wattages in the server. Redundant as 1+1. See Power Specifications, page A-2.
ACPI	The advanced configuration and power interface (ACPI) 4.0 standard is supported.
Cooling	Six hot-swappable fan modules for front-to-rear cooling.
PCIe I/O	Two horizontal PCIe[3] expansion slots on two risers (single riser assembly). See Replacing Additional Hardware Components (Related Documentation), page 4-14 for more information.
Storage	Drives are installed into front-panel drive bays. The Cisco UCS C220 M4 uses Large form factor (LFF) drives, with four-drive backplane. Holds up to four 3.5-inch SAS drives.
Internal USB	One internal USB 3.0 port on the motherboard that you can use with a USB thumb drive for additional storage.
Disk Management (RAID)	The server has a dedicated internal riser for a PCIe-style Cisco modular RAID controller card.
RAID Backup	The server has a mounting bracket for the supercap power module that is used with Cisco modular RAID controller card.
Video	VGA video resolution up to 1920 x 1200, 16 bpp at 60 Hz, and up to 256 MB of video memory.

1. VGA = video graphics array

2. USB = universal serial bus

3. PCIe = peripheral component interconnect express

Cisco CSS UCSM4 2RU Overview

The Cisco CSS UCSM4 2RU (CPS-UCS-2RU-K9) is available in the large form factor (LFF) only, which supports up to 12 3.5-inch hard drives.

Note   The small form-factor (SFF) versions of the Cisco UCS C-Series Rack Servers are not supported for Connected Safety and Security applications.

- Cisco CSS UCSM4 2RU Front Panel, page 1-6
- Cisco CSS UCSM4 2RU Rear Panel, page 1-7
- Summary of Cisco CSS UCSM4 2RU Server Features, page 1-8

Cisco CSS UCSM4 2RU Front Panel

Figure 1-1 shows the front panel features of the server. This version of the server has a 12-drive backplane with an integrated expander.

Figure 1-3   Cisco UCS C240 M4 Server (LFF Drives, 12-Drive) Front Panel Features
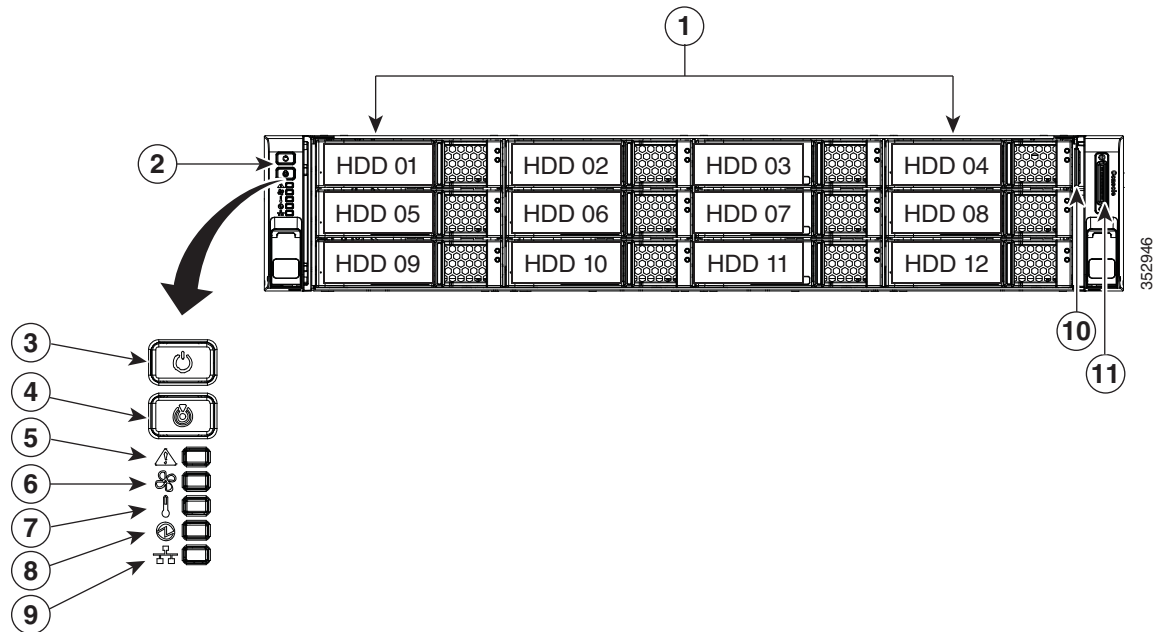
1	Drive bays 1–12 (up to 12 3.5-inch drives)	**7**	Temperature status LED
2	Operations panel buttons and LEDs	**8**	Power supply status LED
3	Power button/LED	**9**	Network link activity LED

4	Unit Identification button/LED	**10**	Pull-out asset tag
5	System status LED	**11**	KVM connector (used with KVM cable that provides two USB 2.0, one VGA, and one serial connector)
6	Fan status LED		

Tip See the "Cisco CSS UCSM4 2RU LEDs and Buttons" section on page 1-16 for more information.

Cisco CSS UCSM4 2RU Rear Panel

Figure 1-2 shows the rear panel features of the server.

Figure 1-4   Cisco CSS UCSM4 2RU Server Rear Panel Features
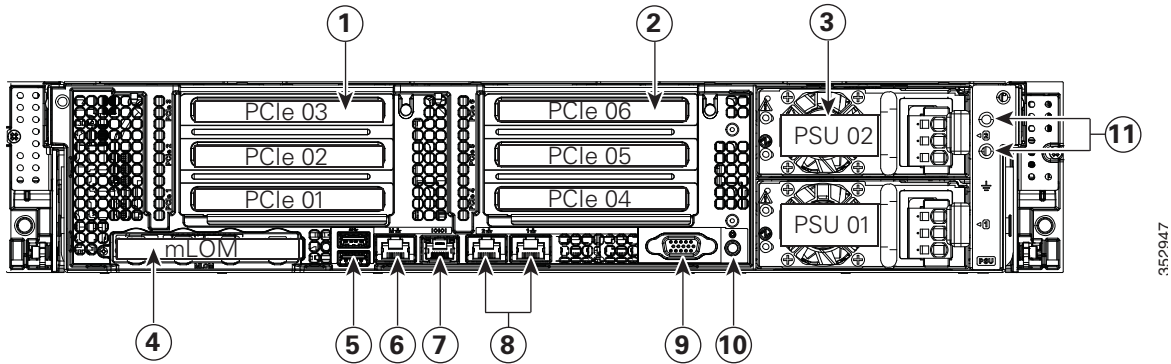
1	PCIe riser 1 (slots 1, 2, 3*) *Slot 3 not present in all versions. See Replacing Additional Hardware Components (Related Documentation), page 4-14 for riser options and slot specifications.	**7**	Serial port (RJ-45 connector)
2	PCIe riser 2 (slots 4, 5, 6)	**8**	Dual 1-Gb Ethernet ports (LAN1, LAN2)
3	Power supplies (DC power supplies shown) See Power Specifications, page A-4 for specifications and options.	**9**	VGA video port (DB-15 connector)
4	Modular LAN-on-motherboard (mLOM) card slot	**10**	Rear Unit Identification button/LED
5	USB 3.0 ports (two)	**11**	Grounding-lug holes (for DC power supplies)
6	1-Gb dedicated management port		

Tip See the "Cisco CSS UCSM4 2RU LEDs and Buttons" section on page 1-16 for more information.

Summary of Cisco CSS UCSM4 2RU Server Features

Table 1-2 lists a summary of server features.

.

Table 1-3   *Cisco CSS UCSM4 2RU Server Features*

Chassis	Two rack-unit (2RU) chassis.
Processors	Up to two Intel Xeon E5-2600 v3 Series processors.
Memory	32 DDR4
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 Ethernet LOM ports, or a Cisco virtual interface card.
Network and management I/O	The server provides these connectors: • One 1-Gb Ethernet dedicated management port • Two 1-Gb BASE-T Ethernet LAN ports • One RS-232 serial port (RJ-45 connector) • One 15-pin VGA[1] connector • Two USB[2] 3.0 connectors • One front-panel KVM connector that is used with the KVM cable, which provides two USB 2.0, one VGA, and one serial (DB-9) connector.
WoL	1-Gb BASE-T Ethernet LAN ports support the wake-on-LAN (WoL) standard.
Power	AC power supplies optionally 650 W AC, 1200 W AC, or 1400 W AC each. Do not mix power supply types or wattages in the server. Redundant as 1+1. See also Power Specifications, page A-4.
ACPI	The advanced configuration and power interface (ACPI) 4.0 standard is supported.
Cooling	Six hot-swappable fan modules for front-to-rear cooling.
PCIe I/O	Up to six horizontal PCIe[3] expansion slots on two risers. Riser 1 can be ordered as one of three different versions: • With slots 1, 2, and 3. • With slots 1 and 2, and a blank slot to accommodate GPU card width. • With slots 1 and 2, plus two connectors for SATA boot drives. Riser 2 contains slots 4, 5, and 6. See Replacing Additional Hardware Components (Related Documentation), page 4-14 for specifications of the slots.

Table 1-3   ***Cisco CSS UCSM4 2RU Server Features (continued)***

Storage	Drives are installed into front-panel drive bays that provide hot-swappable access for SAS drives.
	The Cisco UCS C240 M4 supports large form-factor (LFF) drives with 12-drive backplane and integrated expander. This version holds up to 12 3.5-inch SAS hard drives.
	Note You cannot change the backplane type after-factory. To change a front panel/backplane configuration, a chassis replacement is required.
Internal USB	One internal USB 3.0 port on the motherboard that you can use with a USB thumb drive for additional storage.
Disk Management (RAID)	Dedicated internal socket for a PCIe-style RAID controller card.
RAID Backup	Mounting point on the air baffle for the supercap power module that is used with the Cisco modular RAID controller card.
Video	VGA video resolution up to 1920 x 1200, 16 bpp at 60 Hz, and up to 256 MB of video memory.

1. VGA = video graphics array

2. USB = universal serial bus

3. PCIe = peripheral component interconnect express

Status LEDs and Buttons

This section describes the location and meaning of LEDs and buttons and includes the following topics:

- Cisco CSS UCSM4 1RU LEDs and Buttons, page 1-10
- Cisco CSS UCSM4 2RU LEDs and Buttons, page 1-16

Cisco CSS UCSM4 1RU LEDs and Buttons

This section describes the location and meaning of LEDs and buttons and includes the following topics:

- Front Panel LEDs, page 1-16
- Rear Panel LEDs and Buttons, page 1-19
- Internal Diagnostic LEDs, page 1-22

Front Panel LEDs

Figure 1-5 shows the front panel LEDs. Table 1-7 defines the LED states.

Figure 1-5   Front Panel LEDs
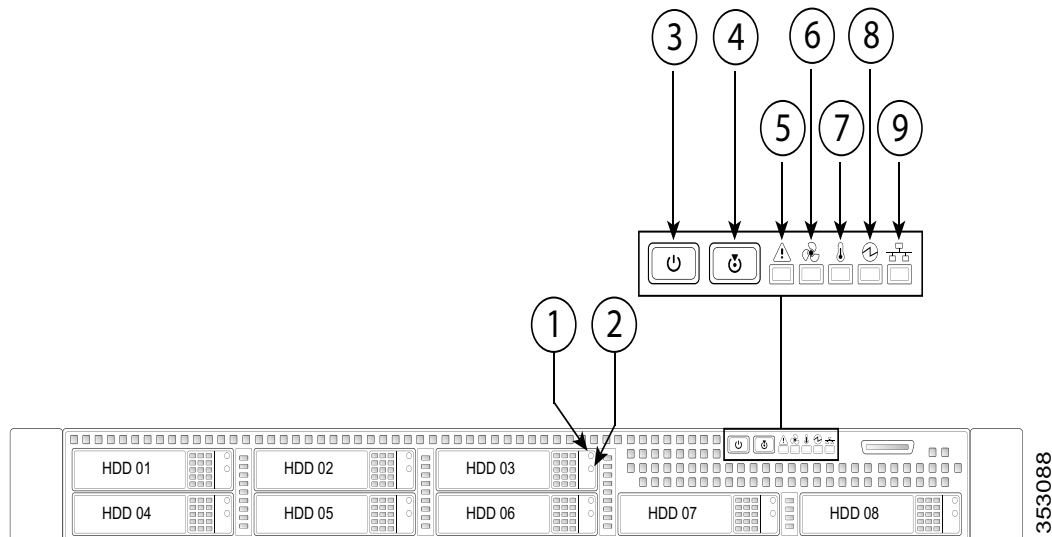
1	Hard drive fault LED	6	Fan status LED
2	Hard drive activity LED	7	Temperature status LED
3	Power button/power status LED	8	Power supply status LED
4	Identification button/LED	9	Network link activity LED
5	System status LED		

Table 1-4   Front Panel LEDs, Definitions of States

	LED Name	State
1 **SAS**	SAS drive fault	• Off—The hard drive is operating properly. • Amber—Drive fault detected. • Amber, blinking—The device is rebuilding. • Amber, blinking with one-second interval—Drive locate function activated.
2 **SAS**	SAS drive activity	• Off—There is no hard drive in the hard drive tray (no access, no fault). • Green—The hard drive is ready. • Green, blinking—The hard drive is reading or writing data.
3	Power button/LED	• Off—There is no AC power to the server. • Amber—The server is in standby power mode. Power is supplied only to the Cisco IMC and some motherboard functions. • Green—The server is in main power mode. Power is supplied to all server components.
4	Unit identification	• Off—The unit identification function is not in use. • Blue—The unit identification function is activated.

5	System status	• Green—The server is running in normal operating condition.
		• Green, blinking—The server is performing system initialization and memory check.
		• Amber, steady—The server is in a degraded operational state. For example:
		  – Power supply redundancy is lost.
		  – CPUs are mismatched.
		  – At least one CPU is faulty.
		  – At least one DIMM is faulty.
		  – At least one drive in a RAID configuration failed.
		• Amber, blinking—The server is in a critical fault state. For example:
		  – Boot failed.
		  – Fatal CPU and/or bus error is detected.
		  – Server is in an over-temperature condition.

6	Fan status	• Green—All fan modules are operating properly. • Amber, steady—One or more fan modules breached the critical threshold. • Amber, blinking—One or more fan modules breached the non-recoverable threshold.
7	Temperature status	• Green—The server is operating at normal temperature. • Amber, steady—One or more temperature sensors breached the critical threshold. • Amber, blinking—One or more temperature sensors breached the non-recoverable threshold.

Table 1-4   *Front Panel LEDs, Definitions of States (continued)*

	LED Name	State
8	Power supply status	• Green—All power supplies are operating normally.
		• Amber, steady—One or more power supplies are in a degraded operational state.
		• Amber, blinking—One or more power supplies are in a critical fault state.
9	Network link activity	• Off—The Ethernet link is idle.
		• Green—One or more Ethernet LOM ports are link-active, but there is no activity.
		• Green, blinking—One or more Ethernet LOM ports are link-active, with activity.

Rear Panel LEDs and Buttons

Figure 1-9 shows the rear panel LEDs and buttons. Table 1-8 defines the LED states.

Figure 1-6   Rear Panel LEDs and Buttons
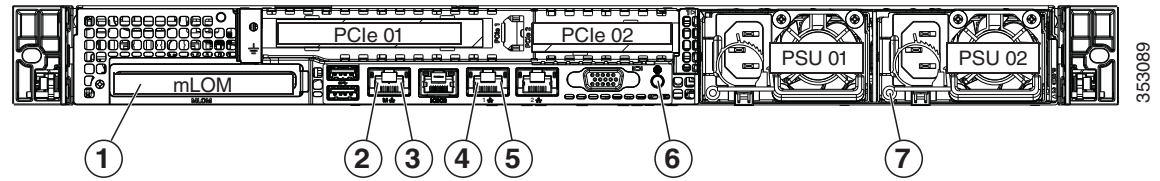
1	Optional mLOM card LEDs (not shown, see Table 1-8)	**5**	1-Gb Ethernet link status LED
2	1-Gb Ethernet dedicated management link status LED	**6**	Rear unit identification button/LED
3	1-Gb Ethernet dedicated management link speed LED	**7**	Power supply status LED
4	1-Gb Ethernet link speed LED		

Table 1-5   Rear Panel LEDs, Definitions of States

	LED Name	**State**
1	Optional mLOM 10-Gb SFP+ (there is a single status LED)	• Off—No link is present. • Green, steady—Link is active. • Green, blinking—Traffic is present on the active link.
1	Optional mLOM 10-Gb BASE-T link speed	• Off—Link speed is 10 Mbps. • Amber—Link speed is 100 Mbps/1 Gbps. • Green—Link speed is 10 Gbps.
1	Optional mLOM 10-Gb BASE-T link status	• Off—No link is present. • Green—Link is active. • Green, blinking—Traffic is present on the active link.
2	1-Gb Ethernet dedicated management link speed	• Off—Link speed is 10 Mbps. • Amber—Link speed is 100 Mbps. • Green—Link speed is 1 Gbps.
3	1-Gb Ethernet dedicated management link status	• Off—No link is present. • Green—Link is active. • Green, blinking—Traffic is present on the active link.
4	1-Gb Ethernet link speed	• Off—Link speed is 10 Mbps. • Amber—Link speed is 100 Mbps. • Green—Link speed is 1 Gbps.

Table 1-5   Rear Panel LEDs, Definitions of States (continued)

	LED Name	State
5	1-Gb Ethernet link status	• Off—No link is present.
		• Green—Link is active.
		• Green, blinking—Traffic is present on the active link.
6	Rear unit identification	• Off—The unit identification LED is not in use.
		• Blue—The unit identification LED is activated.
7	Power supply status	**AC power supplies:**
		• Off—No AC input (12 V main power off, 12 V standby power off).
		• Green, blinking—12 V main power off; 12 V standby power on.
		• Green, solid—12 V main power on; 12 V standby power on.
		• Amber, blinking—Warning threshold detected but 12 V main power on.
		• Amber, solid—Critical error detected; 12 V main power off (for example, over-current, over-voltage, or over-temperature failure).
		DC power supply (UCSC-PSUV2-1050DC):
		• Off—No DC input (12 V main power off, 12 V standby power off).
		• Green, blinking—12 V main power off; 12 V standby power on.
		• Green, solid—12 V main power on; 12 V standby power on.
		• Amber, blinking—Warning threshold detected but 12 V main power on.
		• Amber, solid—Critical error detected; 12 V main power off (for example, over-current, over-voltage, or over-temperature failure).

Internal Diagnostic LEDs

The server has internal fault LEDs for CPUs, DIMMs, fan modules, SD cards, the RTC battery, and the mLOM card. These LEDs are available only when the server is in standby power mode. An LED lights amber to indicate a faulty component.

See Figure 1-7 for the locations of these internal LEDs.

Figure 1-7   Internal Diagnostic LED Locations
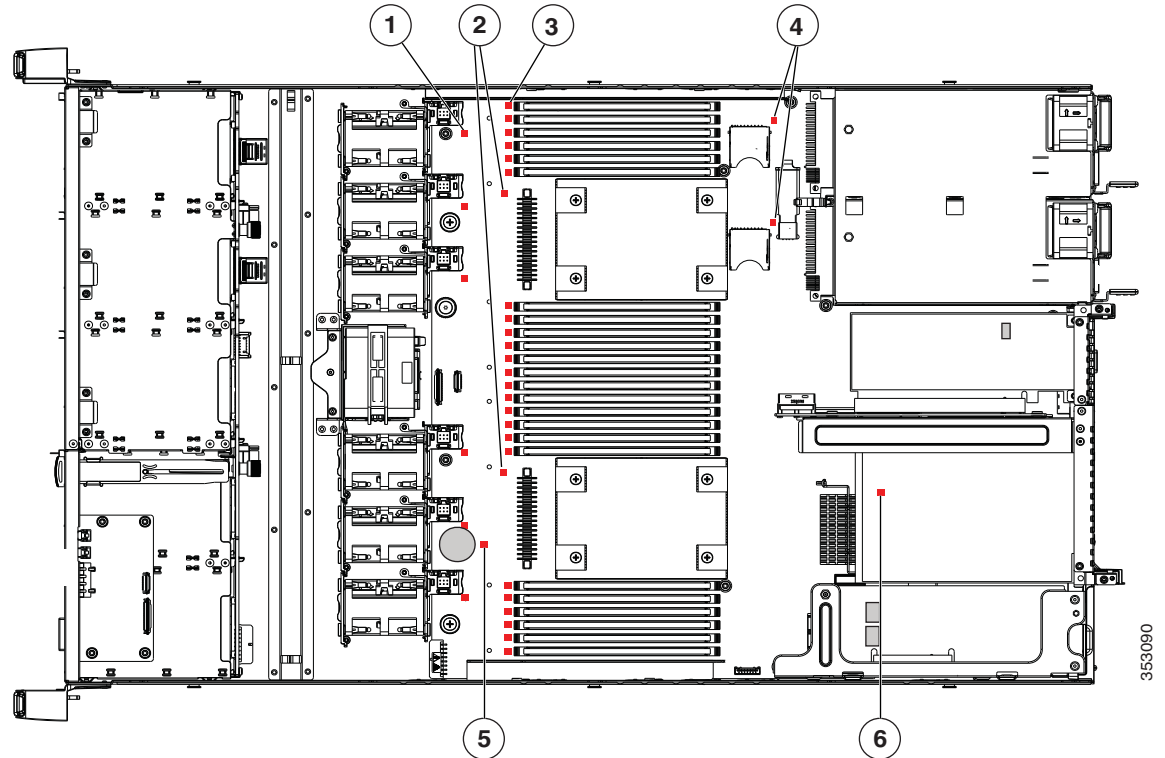
1	Fan module fault LEDs (one next to each fan connector on the motherboard)	**4**	SD card fault LEDs (one next to each bay)
2	CPU fault LEDs (one in front of each CPU)	**5**	RTC battery fault LED
3	DIMM fault LEDs (one in front of each DIMM socket on the motherboard)	**6**	mLOM card fault LED (on motherboard next to mLOM socket)

Table 1-6   Internal Diagnostic LEDs, Definition of States

LED Name	State
Internal diagnostic LEDs (all)	• Off—Component is functioning normally. • Amber—Component has failed.

Cisco CSS UCSM4 2RU LEDs and Buttons

This section describes the location and meaning of LEDs and buttons and includes the following topics

- Front Panel LEDs, page 1-16
- Rear Panel LEDs and Buttons, page 1-19
- Internal Diagnostic LEDs, page 1-22

Front Panel LEDs

Figure 1-8 shows the front panel LEDs. Table 1-7 defines the LED states.

The small form factor (SFF) drives, 24-drive version and the SFF drives, 16-drive version are shown.

Figure 1-8   *Front Panel LEDs*
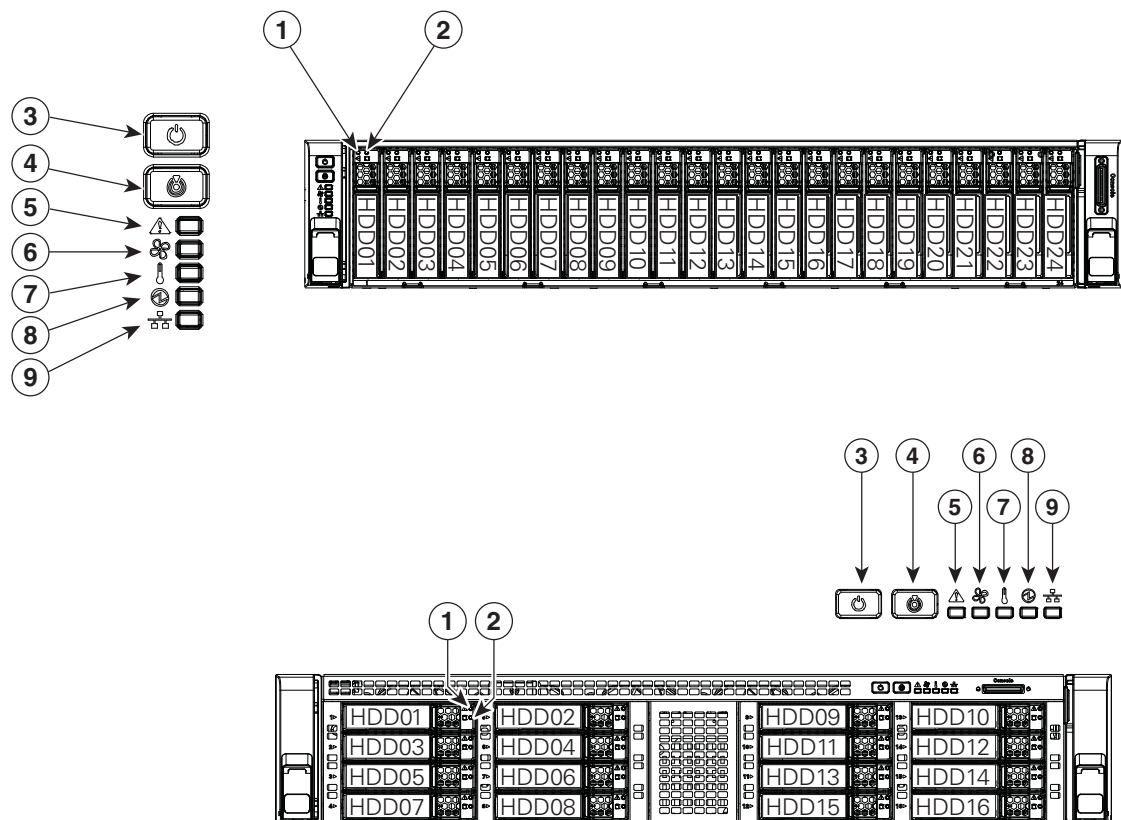
1	Hard drive fault LED (on each drive tray)	6	Fan status LED
2	Hard drive activity LED (on each drive tray)	7	Temperature status LED
3	Power button/power status LED	8	Power supply status LED
4	Unit Identification button/LED	9	Network link activity LED
5	System status LED		

Table 1-7   Front Panel LEDs, Definitions of States

	LED Name	State
1 **SAS**	Hard drive fault	• Off—The hard drive is operating properly. • Amber—Drive fault detected. • Amber, blinking—The device is rebuilding. • Amber, blinking with one-second interval—Drive locate function activated.
2 **SAS**	Hard drive activity	• Off—There is no hard drive in the hard drive tray (no access, no fault). • Green—The hard drive is ready. • Green, blinking—The hard drive is reading or writing data.
3	Power button/LED	• Off—There is no AC power to the server. • Amber—The server is in standby power mode. Power is supplied only to the Cisco IMC and some motherboard functions. • Green—The server is in main power mode. Power is supplied to all server components.
4	Unit Identification	• Off—The unit identification function is not in use. • Blue—The unit identification function is activated.

5	System status	• Green—The server is running in a normal operating condition.
		• Green, blinking—The server is performing system initialization and memory check.
		• Amber, steady—The server is in a degraded operational state. For example:
		  – Power supply redundancy is lost.
		  – CPUs are mismatched.
		  – At least one CPU is faulty.
		  – At least one DIMM is faulty.
		  – At least one drive in a RAID configuration failed.
		• Amber, blinking—The server is in a critical fault state. For example:
		  – Boot failed.
		  – Fatal CPU and/or bus error is detected.
		  – Server is in an over-temperature condition.

6	Fan status	• Green—All fan modules are operating properly. • Amber, steady—One or more fan modules breached the critical threshold. • Amber, blinking—One or more fan modules breached the non-recoverable threshold.
7	Temperature status	• Green—The server is operating at normal temperature. • Amber, steady—One or more temperature sensors breached the critical threshold. • Amber, blinking—One or more temperature sensors breached the non-recoverable threshold.

Table 1-7   Front Panel LEDs, Definitions of States (continued)

	LED Name	State
8	Power supply status	• Green—All power supplies are operating normally. • Amber, steady—One or more power supplies are in a degraded operational state. • Amber, blinking—One or more power supplies are in a critical fault state.
9	Network link activity	• Off—The Ethernet link is idle. • Green—One or more Ethernet LOM ports are link-active, but there is no activity. • Green, blinking—One or more Ethernet LOM ports are link-active, with activity.

Rear Panel LEDs and Buttons

Figure 1-9 shows the rear panel LEDs and buttons. Table 1-8 defines the LED states.

Figure 1-9   Rear Panel LEDs and Buttons
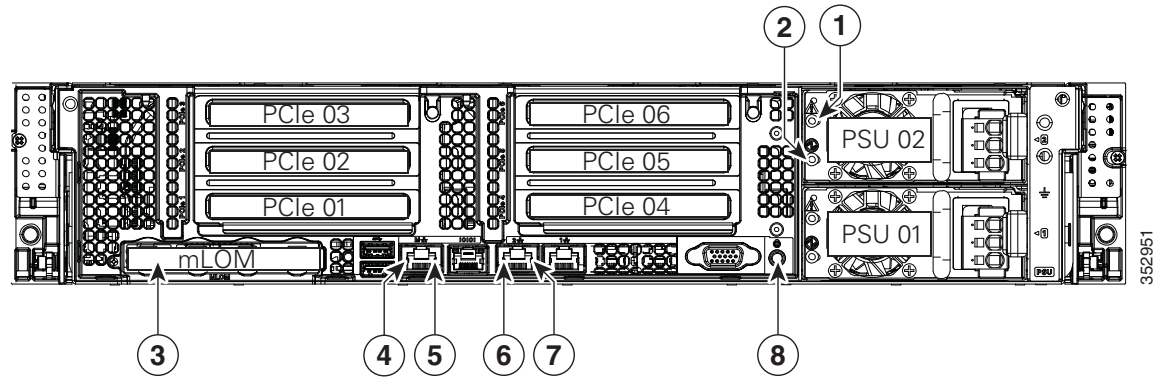
1	Power supply fault LED	**5**	1-Gb Ethernet dedicated management link status LED
2	Power supply AC status LED	**6**	1-Gb Ethernet link speed LED
3	(not shown)	**7**	1-Gb Ethernet link status LED
4	1-Gb Ethernet dedicated management link speed LED	**8**	Unit Identification button/LED

Table 1-8   Rear Panel LEDs, Definitions of States

	LED Name	**State**
1	Power supply fault This is a summary; for advanced power supply LED information, see Table 1-9.	• Off—The power supply is operating normally. • Amber, blinking—An event warning threshold has been reached, but the power supply continues to operate. • Amber, solid—A critical fault threshold has been reached, causing the power supply to shut down (for example, a fan failure or an over-temperature condition).
2	Power supply status This is a summary; for advanced power supply LED information, see Table 1-9.	AC power supplies: • Off—There is no AC power to the power supply. • Green, blinking—AC power OK; DC output not enabled. • Green, solid—AC power OK; DC outputs OK. DC power supplies: • Off—There is no DC power to the power supply. • Green, blinking—DC power OK; DC output not enabled. • Green, solid—DC power OK; DC outputs OK.
3	not shown	•

Table 1-8   *Rear Panel LEDs, Definitions of States (continued)*

	LED Name	State
4	1-Gb Ethernet dedicated management link speed	• Off—Link speed is 10 Mbps. • Amber—Link speed is 100 Mbps. • Green—Link speed is 1 Gbps.
5	1-Gb Ethernet dedicated management link status	• Off—No Link is present. • Green—Link is active. • Green, blinking—Traffic is present on the active link.
6	1-Gb Ethernet link speed	• Off—Link speed is 10 Mbps. • Amber—Link speed is 100 Mbps. • Green—Link speed is 1 Gbps.
7	1-Gb Ethernet link status	• Off—No link is present. • Green—Link is active. • Green, blinking—Traffic is present on the active link.
8	Unit Identification	• Off—The unit identification function is not in use. • Blue—The unit identification function is activated.

In Table 1-9, read the status and fault LED states together in each row to determine the event that cause this combination.

Table 1-9   *Rear Power Supply LED States*

Green PSU Status LED State	Amber PSU Fault LED State	Event
• Solid on	• Off	12V main on (main power mode)
• Blinking	• Off	12Vmain off (standby power mode)
• Off	• Off	No AC power input (all PSUs present)
• Off	• On	No AC power input (redundant supply active)
• Blinking	• Solid on	12V over-voltage protection (OVP)
• Blinking	• Solid on	12V under-voltage protection (UVP)
• Blinking	• Solid on	12V over-current protection (OCP)
• Blinking	• Solid on	12V short-circuit protection (SCP)
• Solid on	• Solid on	PSU fan fault/Lock (before OTP)
• Blinking	• Solid on	PSU fan fault/Lock (after OTP)
• Blinking	• Solid on	Over-temperature protection (OTP)
• Solid on	• Blinking	OTP warning
• Solid on	• Blinking	OCP warning
• Blinking	• Off	12V main off (CR slave PSU is in sleep mode)

Internal Diagnostic LEDs

The server is equipped with a supercap voltage source that can activate internal component fault LEDs up to 30 minutes after AC power is removed. The server has internal fault LEDs for CPUs, DIMMs, fan modules, SD cards, the RTC battery, and the mLOM card.

To use these LEDs to identify a failed component, press the front or rear Unit Identification button (see Figure 1-8 or Figure 1-9) with AC power removed. An LED lights amber to indicate a faulty component.

See Figure 1-10 for the locations of these internal LEDs.

Figure 1-10   Internal Diagnostic LED Locations
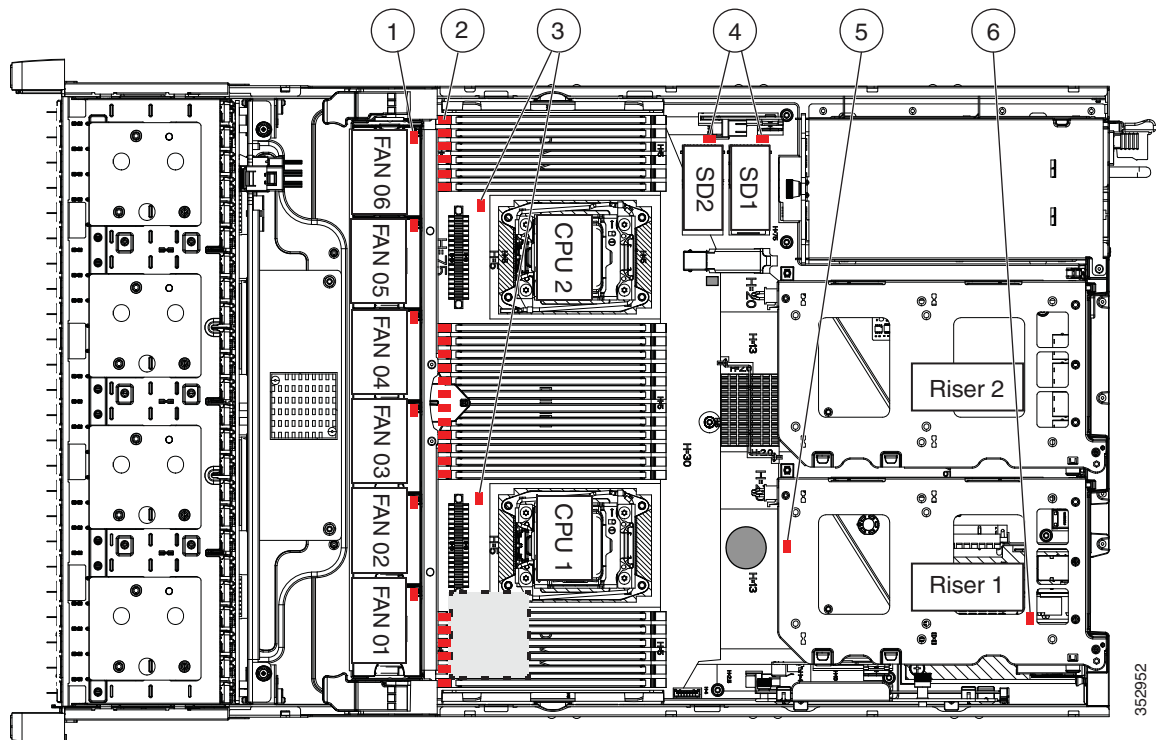
1	Fan module fault LEDs (one on each fan module)	**4**	SD card fault LEDs
2	DIMM fault LEDs (one directly in front of each DIMM socket on the motherboard)	**5**	RTC battery fault LED (under PCIe riser 1)
3	CPU fault LEDs	**6**	mLOM card fault LED (under PCIe riser 1)

Table 1-10   Internal Diagnostic LEDs, Definition of States

LED Name	State
Internal diagnostic LEDs (all)	• Off—Component is functioning normally. • Amber—Component has a fault.

Supported Cisco Connected Safety and Security Hardware Configurations

Supported NIC (GigE) Ports (Cisco Video Surveillance)

The Cisco Connected Safety and Security UCS series servers support the following:

- One 1-Gb Ethernet dedicated management port
- Two 1-Gb Base-T Ethernet ports

See the "System Overview" section on page 1-2 for port locations.

Note
- The LAN Ethernet posts are referred to as "Eth 0" and "Eth1" in the Cisco Connected Safety and Security applications, such as Cisco Video Surveillance.

- The Cisco Connected Safety and Security UCS series servers do NOT support the NIC redundancy modes. Only the *None* option is supported: the Ethernet ports operate independently and do not fail over if there is a problem.

Server and Accessories Part Numbers

The following servers and field replaceable units (FRUs) are supported by the Cisco Connected Safety and Security UCS Platform Series servers. Refer to these PIDs when ordering new or replacement components.

Table 1-11   Part Numbers for the Cisco Connected Safety and Security UCS Platform Series

Type	Part Number (PID)	Description
Server appliance	CPS-UCS-1RU-K9=	Cisco Connected Safety and Security UCSM4 1RU server
	CPS-UCS-2RU-K9=	Cisco Connected Safety and Security UCSM4 2RU server
Hard Drives	UCS-HDD2TI2F213	2 TB SAS 7.2K RPM 3.5 inch HDD
	UCS-HD4T7KS3-E	4TB SAS 7.2K RPM 3.5 inch HDD
	UCS-HD6T7KL4K	6 TB SAS 7.2K RPM 3.5 inch HDD
RAID Controller	UCSC-MRAID12G	Cisco 12G SAS Modular Raid Controller
Fiber Channel PCIe Card	N2XX-AEPCI05	Emulex LPe 12002 Dual Port 8Gb Fibre Channel HBA
Memory	UCS-MR-1X162RU-A	16GB DDR4-2133-MHz RDIMM/PC4-17000/dual rank/x4/1.2v
Power Supplies	CPS-PSU-650W=	650W power supply for CPS-UCS-M4-2RU-K9 server
	CPS-PSU1-770W	770W power supply for CPS-UCS-M4-1RU-K9 server

Server Monitoring and Management Tools

The following software tools are used to monitor server health and events:

- Cisco Integrated Management Interface (CIMC), page 1-24
- Cisco Video Surveillance Management Console, page 1-24

Cisco Integrated Management Interface (CIMC)

You can monitor the server inventory, health, and system event logs by using the built-in Cisco Integrated Management Controller (CIMC) GUI or CLI interfaces. See the user documentation for your firmware release at the following URL:

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

For example: see the Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide, Release 1.5.

Cisco Video Surveillance Management Console

For the Cisco Video Surveillance Manager application, use the browser-based Cisco VSM Management Console to configure, manage and monitor the server.

See the following documents for more information:

- Cisco Video Surveillance Management Console Administration Guide
- Cisco Video Surveillance Manager: Install and Upgrade Guide

Supported Applications

The current release of the Cisco Connected Safety and Security UCS series servers support the Cisco Video Surveillance Manager and associated servers and devices. See the following for more information:

- Supported Applications, page 2-1
- Related Documentation, page B-1
- The Cisco Video Surveillance 7 Documentation Roadmap available at http://www.cisco.com/go/physicalsecurity/vsm/roadmap. This document provides descriptions and links to Cisco Video Surveillance documentation, server and storage platform documentation, and other related documentation.

Supported Applications

The CPS-UCSM4-1RU-K9 and CPS-UCSM4-2RU-K9 servers support the following application:

- Cisco Video Surveillance Manager, Release 7.7 and Higher, page 2-1

Note The previous versions of these servers (CPS-UCS-1RU-K9 and CPS-UCS-2RU-K9) support Cisco VSM Release 7.2 and higher. See the Cisco Physical Security UCS Platform Series User Guide, CPS-UCS-1RU-K9 / CPS-UCS-2RU-K9 for more information.

Cisco Video Surveillance Manager, Release 7.7 and Higher

- Overview, page 2-1
- Initial Setup Procedure, page 2-2
- Upgrading the Cisco VSM System Software, page 2-2
- Recovering the Cisco VSM System Software, page 2-3
- Supported RAID and Hard Drive Configurations (Cisco VSM), page 2-4
- Supported Hard Drives, page 2-5
- More Information, page 2-6

Overview

The CPS-UCSM4-1RU-K9 and CPS-UCSM4-2RU-K9 servers support the Cisco Video Surveillance Manager (Cisco VSM) Release 7.7 and higher, including associated servers and devices.

These servers are shipped as server appliances, meaning that the Cisco Video Surveillance Manager system software is pre-loaded in a "bare-metal" configuration.

Note These servers do not currently support additional virtual machine (VM) installations. Virtual Machine deployment is supported on separate Cisco UCS Express, and B-, C-, and E- Series platform servers. See the Cisco Video Surveillance Virtual Machine Deployment, Recovery and HA Guide for UCS Platforms for more information.

Initial Setup Procedure

To install and configure a Cisco Connected Safety and Security UCS series server appliance for the first time, complete the following high-level steps:

Procedure

Step 1 Physically install the Cisco Connected Safety and Security UCS series server appliance.

See the "Installing the Server" section on page 3-1.

Step 2 Complete the initial server setup.

See the "Initial Server Setup" section on page 3-16.

Step 3 Use the browser-based Cisco Video Surveillance Management Console to complete the initial server setup for the Cisco Video Surveillance Manager.

See the Cisco Video Surveillance Management Console Administration Guide.

Step 4 Use the browser-based Cisco Video Surveillance Operations Manager to configure additional server options and Cisco VSM features.

See the Cisco Video Surveillance Operations Manager User Guide.

Upgrading the Cisco VSM System Software

To to update the Cisco VSM system software, use the browser-based Cisco VSM Operations Manager or Cisco VSM Management Console to install the upgrade file that contains all required packages and components.

See the Cisco Video Surveillance Manager: Install and Upgrade Guide for your release.

Recovering the Cisco VSM System Software

To create a bootable USB flash drive that can be used to recover an installation or perform a factory installation of Cisco VSM 7.

See the Cisco Video Surveillance Manager: Install and Upgrade Guide for your release.

The recovery options include the following:

Table 2-1   Recovery Options

Option	Description
recovery	Reinstalls the operating system. • Recorded video is preserved. • RAID configurations are preserved (only the OS partitions are formatted).
factory	Restores the server to the factory default settings: • Reinstalls the operating system. • Clears and reconfigures the RAID. You must disconnect any external storage before using this option. • Recorded video and configurations are deleted. • RAID-6 is configured on the Cisco CSS UCSM4 2RU server with 6 to12 internal drives. ⚠ **Caution** This action deletes all data and video files.
factory_raid5	Restores a Cisco CSS UCSM4 2RU server to the factory default settings, including: • Reinstalls the operating system • Clears and reconfigures the RAID. You must disconnect any external storage before using this option. • Recorded video and configurations are deleted • Valid only on the Cisco CSS UCSM4 2RU with 6 to 12 internal drives. See Table 2-2. ⚠ **Caution** This action deletes all data and video files.
rescue	Boot to prompt from USB media. Use this option to recover a password or for other administrative tasks

Supported RAID and Hard Drive Configurations (Cisco VSM)

Table 2-2 defines the drive configurations supported by the Cisco Video Surveillance Manager. The Cisco CSS UCSM4 1RU server supports RAID 1 and 5, while the Cisco CSS UCSM4 2RU server supports RAID levels 1, 5 and 6.

Table 2-2   Supported Drive Configurations

CPS-UCSM4-1RU-K9	2 drives	RAID 1
	4 drives	RAID 5
CPS-UCSM4-2RU-K9	2 drives	RAID 1
	6 -12 drives	RAID 5 or RAID 6

Requirements and Conditions

The following notes apply to drive configurations, recovery and expansion.

- All drives must be installed in the lowest numbered available slot.
- Hot Standby drives are not supported.
- Mixing RAID configurations is not supported. For example, 6 drives in RAID 6, and 6 drives in RAID 5).
- RAID expansion is not supported during a "Recovery" installation (RAID configuration remains the same during a "Recovery" installation).
- RAID configuration may be changed during a "Factory" reimage (note that all data will be lost unless backed up prior to the procedure).

Supported RAID Upgrade Paths

Table 2-3 defines the supported paths to add additional drives.

Table 2-3   Supported Upgrade Paths

	From	To	Notes
Cisco CSS UCSM4 1RU	2 drives	4 Drives/RAID 5	RAID Change, Factory Reimage required

Table 2-3   Supported Upgrade Paths (continued)

Cisco CSS UCSM4 2RU	2 drives/RAID 1	6+ Drives/RAID 5	RAID Change, Factory Reimage required
	2 drives/RAID 1	6+ Drives/RAID 6	
	2 drives/RAID 1	up to 12 Drives/RAID 5	
	2 drives/RAID 1	up to 12 Drives/RAID 6	
	6+ drives/RAID 5	up to 12 Drives/RAID 6	
	6+ drives/RAID 6	up to 12 Drives /RAID 5	
	6+ drives/RAID 5	up to 12 Drives (as 1 RAID Group) /RAID 5	Factory Reimage required. Dynamic expansion of existing VD, /media partitions not supported
	6+ drives/RAID 6	up to 12 Drives (as 1 RAID Group) /RAID 6	

> **Note** You can order drives in bundles of 2 drives. The bundles are for replacement and for expansion to get to four drives. These drives that are shipped are of the same capacity. They can be 2TB, 4TB, or 6TB. See the "Server and Accessories Part Numbers" section on page 1-23 for more information.

> **Note** RAID configuration changes require a "Factory" reimage. All data will be lost unless backed up prior to the procedure.

Supported Hard Drives

You can order drives in bundles of 2 drives. The bundles are for replacement and for expansion to get to four drives. These drives that are shipped are of the same capacity. They can be 2TB, 4TB or 6TB.

Requirements for All Servers

- Drives are not rebuilt when the same drive is removed and reinserted. The removed drive must be replaced with a new drive. The rebuild will start automatically.

- All drives must be of the same capacity. Drives of different capacities are not supported (for example, you cannot mix 2TB, 4TB and/or 6TB drives in the same server).

- Installation is supported only if all hard drives are in optimal state.

- You can order drives in bundles of 2 drives for replacement or expansion. See the "Server and Accessories Part Numbers" section on page 1-23.

- See the "Replacing Hard Drives" section on page 4-9 for more information.

Cisco CSS UCSM4 1RU Hard Disk Configuration

- The Cisco CSS UCSM4 1RU server ships with 2 or 4 disk drives (other combinations are not supported).
- Up to four large form factor (LFF) disk drives (3.5" hard drives) of 2TB, 4TB, and 6TB are supported. These are driven directly from the RAID controller and do not require any expander.
- RAID levels 1, 5 are supported. See the "Supported RAID and Hard Drive Configurations (Cisco VSM)" section on page 2-4.

Cisco CSS UCSM4 2RU Hard Disk Configuration

- Cisco CSS UCSM4 2RU server ships with 2 or 12 disk drives.
- Up to 12 large form factor (LFF) disk drives (3.5" hard drives) of 2TB, 4TB, and 6TB are supported. These are driven directly from the RAID controller and do not require any expander.
- RAID levels 1, 5 and 6 are supported. See the "Supported RAID and Hard Drive Configurations (Cisco VSM)" section on page 2-4.

More Information

See the following for more information:

- Replacing Hard Drives, page 4-9
- Related Documentation, page B-1
- The Cisco Video Surveillance 7 Documentation Roadmap available at http://www.cisco.com/go/physicalsecurity/vsm/roadmap. This document provides descriptions and links to Cisco Video Surveillance documentation, server and storage platform documentation, and other related documentation.

CHAPTER **3**

Installing the Server

This chapter describes how to install the server, and it includes the following sections:

Note   Before you install, operate, or service a server, review the *Regulatory Compliance and Safety Information for Cisco UCS C-Series Servers* for important safety information.

Warning   **IMPORTANT SAFETY INSTRUCTIONS**

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

Unpacking and Inspecting the Server

⚠️

Caution   When handling internal server components, wear an ESD strap and handle modules by the carrier edges only.

🔍

Tip   Keep the shipping container in case the server requires shipping in the future.

✎

Note   The chassis is thoroughly inspected before shipment. If any damage occurred during transportation or any items are missing, contact your customer service representative immediately.

Step 1   Remove the server from its cardboard container and save all packaging material.

Step 2   Compare the shipment to the equipment list provided by your customer service representative. Verify that you have all items.

Step 3   Check for damage and report any discrepancies or damage to your customer service representative. Have the following information ready:

- Invoice number of shipper (see the packing slip)
- Model and serial number of the damaged unit
- Description of damage
- Effect of damage on the installation

Preparing for Server Installation

This section provides information about preparing for server installation, and it includes the following topics:

- Installation Guidelines, page 3-3
- Rack Requirements, page 3-4
- Equipment Requirements, page 3-4
- Slide Rail Adjustment Range and Cable Management Arm Dimensions, page 3-5

Installation Guidelines

Warning   **To prevent the system from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of: 40° C (104° 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

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

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

- Plan your site configuration and prepare the site before installing the server. See the *Cisco UCS Site Preparation Guide* for the recommended site planning tasks.

- Ensure that there is adequate space around the server to allow for servicing 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 "Server Specifications".
- Ensure that the cabinet or rack meets the requirements listed in the "Rack Requirements" section on page 3-4.
- Ensure that the site power meets the power requirements listed in the "Server Specifications". If available, you can use an uninterruptible power supply (UPS) to protect against power failures.

Rack Requirements

CPS-UCSM4-1RU-K9

This section provides the requirements for the standard open racks.

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 supplied slide rails.
- The minimum vertical rack space per server must be one RU, equal to 1.75 in. (44.45 mm).

CPS-UCSM4-2RU-K9

This section provides the requirements for the standard open racks.

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 supplied slide rails.
- The minimum vertical rack space per server must be two RUs, equal to 3.5 in. (88.9 mm).

Equipment Requirements

CPS-UCSM4-1RU-K9

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

CPS-UCSM4-2RU-K9

The slide rails supplied by Cisco Systems for this server do not require tools for installation if you install them in a rack that has square 0.38-inch (9.6 mm), round 0.28-inch (7.1 mm), or #12-24 UNC threaded holes.

Supported Slide Rail Kits

CPS-UCSM4-1RU-K9

This server supports two rail kit options:

- Cisco part UCSC-RAILB-M4= (ball-bearing rail kit).
- Cisco part UCSC-RAILF-M4= (friction rail kit).

Do not attempt to use a rail kit that was for the Cisco UCS C220 M3 server; the rail kits for the Cisco UCS C220 M4 server have been designed specifically for it.

CPS-UCSM4-2RU-K9

This server supports one rail kit option: Cisco part UCSC-RAILB-M4= (ball-bearing rail kit).

Do not attempt to use a rail kit that was for the Cisco UCS C240 M3 server; the rail kit for the Cisco UCS C240 M4 server has been designed specifically for it.

Slide Rail Adjustment Range 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 CPS-UCSM4-1RU-K9 Server In a Rack

This section contains the following sections:

Installing the Slide Rails

This section describes how to install the server in a rack using the rack kits that are sold by Cisco.

⚠ **Warning**

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

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

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

If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.
Statement 1006

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

   a. Align an inner rail with one side of the server so that the three keyed slots in the rail align with the three pegs on the side of the server (see Figure 3-1).

   b. Set the keyed slots over the pegs, and then slide the rail toward the front to lock it in place on the pegs. The front slot has a metal clip that locks over the front peg.

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

Figure 3-1   Attaching Inner Rail to Side of Server
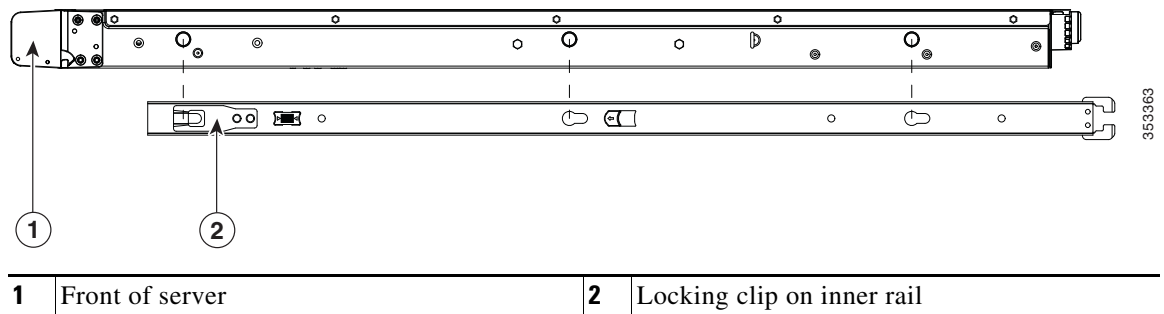
1	Front of server	**2**	Locking clip on inner rail

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 (see Figure 3-2).

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

Figure 3-2   Front Securing Mechanism, Inside of Front End
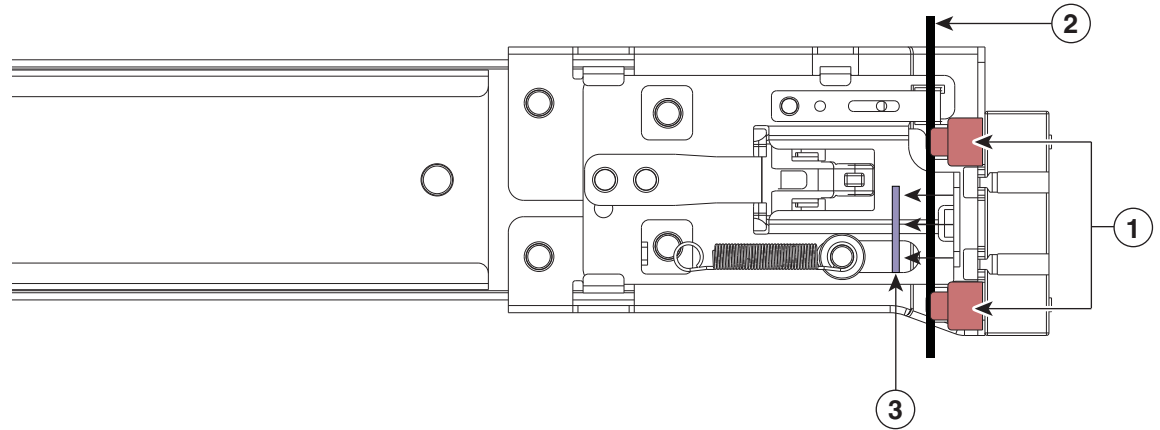
1	Front mounting pegs	**3**	Securing plate shown pulled back to open position
2	Rack post		

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 (see Figure 3-2).

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 with each other 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 67 pounds (59 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 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 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 3-3   Inner Rail Release Clip
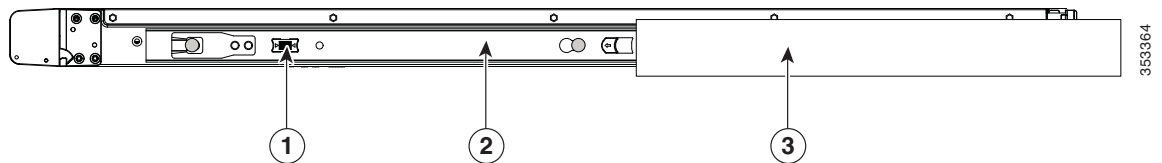
1	Inner rail release clip	**3**	Outer rail attached to rack post
2	Inner rail attached to server and inserted into outer rail		

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 the 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 CMA is reversible left to right. To reverse the CMA, see Reversing the Cable Management Arm (Optional), page 3-10 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 (see Figure 3-4). Slide the tab over the end of the rail until it clicks and locks.

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 (see Figure 3-4). 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 (see Figure 3-4).

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 (see Figure 3-4). 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.

Figure 3-4 Attaching the Cable Management Arm to the Rear of the Slide Rails

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

Reversing the Cable Management Arm (Optional)

Step 1   Rotate the entire CMA assembly 180 degrees. The plastic cable guides must remain pointing upward.

Step 2   Flip the tabs at the end of each CMA arm 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 3-5   *Reversing the CMA*
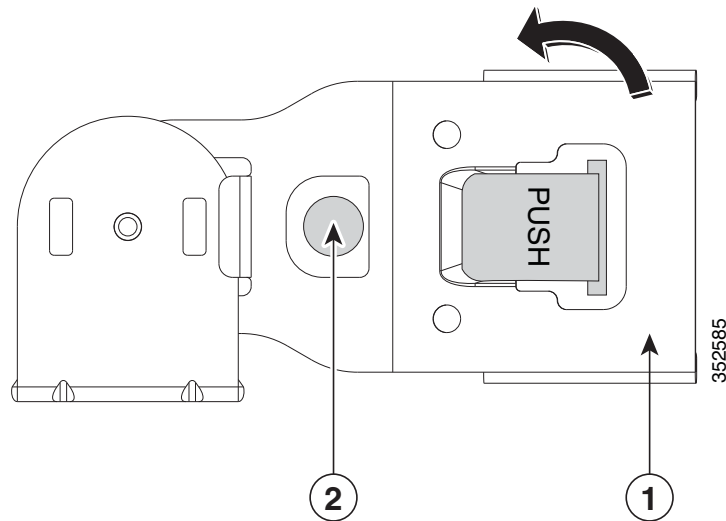
1	CMA tab on end of width-adjustment slider	2	Metal button for rotating

Installing the CPS-UCSM4-2RU-K9 Server In a Rack

This section contains the following sections:

Installing the Slide Rails

This section describes how to install the server in a rack using the rack kits that are sold by Cisco.

Warning   **To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:**
This unit should be mounted at the bottom of the rack if it is the only unit in the rack.
When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.
If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.
Statement 1006

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

a.   Align an inner rail with one side of the server so that the three keyed slots in the rail align with the three pegs on the side of the server (see Figure 3-1).

b.   Set the keyed slots over the pegs, and then slide the rail toward the front to lock it in place on the pegs. The front slot has a metal clip that locks over the front peg.

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

Figure 3-6   *Attaching Inner Rail to Side of Server*
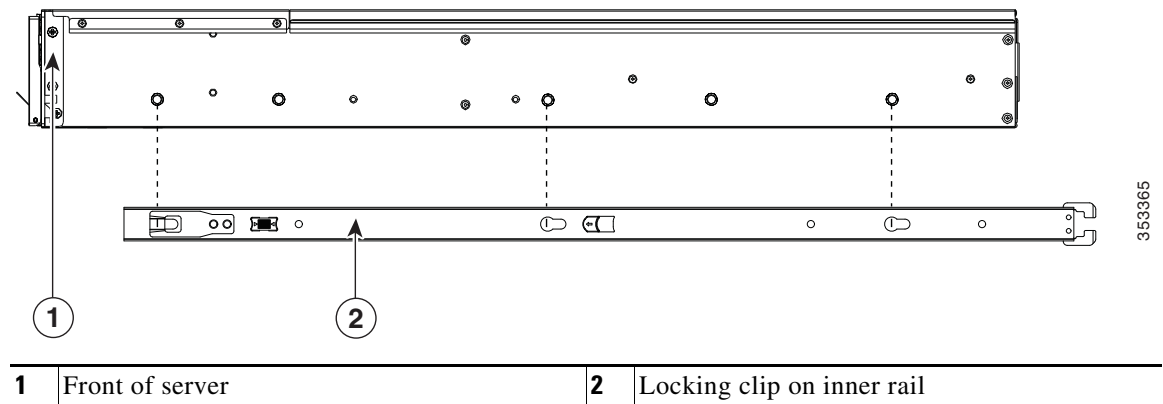
1	Front of server	2	Locking clip on inner rail

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 (see Figure 3-2).

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

Figure 3-7   Front Securing Mechanism, Inside of Front End
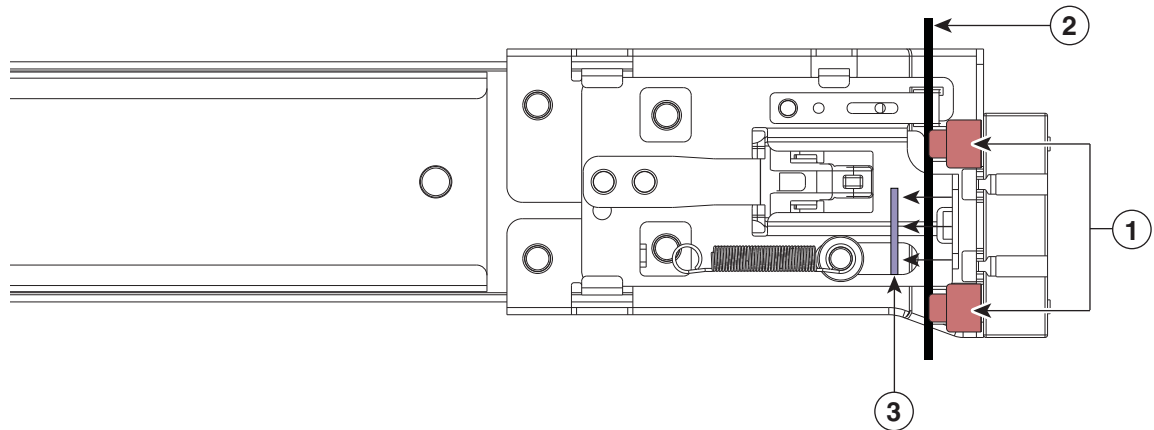
1	Front mounting pegs	3	Securing plate shown pulled back to open position
2	Rack post		

Step 3   Install the slide rails into the rack:

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

The slide rail front-end wraps around the outside of the rack post and the mounting pegs enter the rack-post holes from the outside-front (see Figure 3-2).

✎
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 with each other 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 67 pounds (59 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 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 release clip toward the rear on both inner rails (Figure 3-8), and then continue pushing the server into the rack until its front slam latches engage with the rack posts.

Figure 3-8   Inner Rail Release Clip
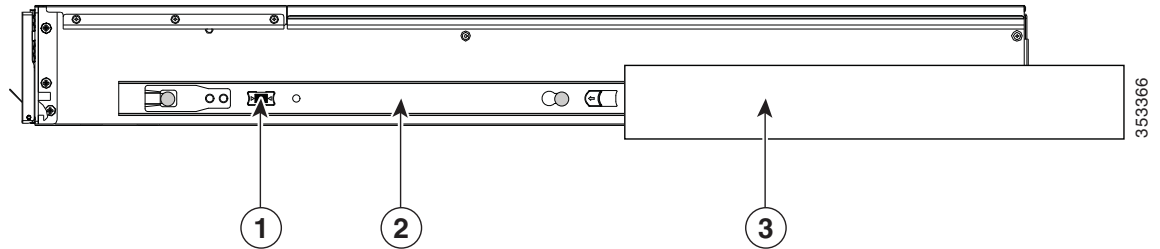
1	Inner rail release clip	**3**	Outer rail attached to rack post
2	Inner rail attached to server		

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 the 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 CMA is reversible left to right. To reverse the CMA, see Reversing the Cable Management Arm (Optional), page 3-10 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 (see Figure 3-4). Slide the tab over the end of the rail until it clicks and locks.

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 (see Figure 3-4). 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 (see Figure 3-4).

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 (see Figure 3-4). 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.

Figure 3-9   Attaching the Cable Management Arm to the Rear of the Slide Rails

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

Reversing the Cable Management Arm (Optional)

Step 1 Rotate the entire CMA assembly 180 degrees. The plastic cable guides must remain pointing upward.

Step 2 Flip the tabs at the end of each CMA arm 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 3-10   *Reversing the CMA*
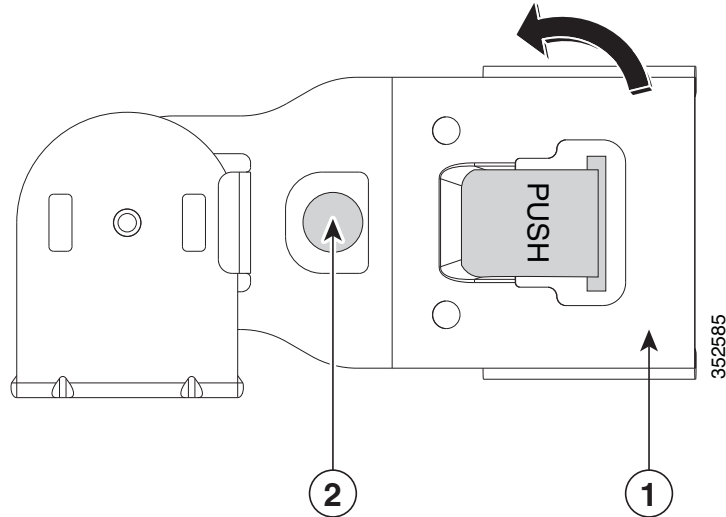
1	CMA tab on end of width-adjustment slider	**2**	Metal button for rotating

Initial Server Setup

This section includes the following topics:

Connecting and Powering On the Server (Standalone Mode)

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*.

> **Note**   UCS integration mode is not supported.

The server is shipped with these default settings:

- The NIC mode is Shared LOM EXT.

    Shared LOM EXT mode enables the 1-Gb Ethernet ports and the ports on any installed Cisco virtual interface card (VIC) to access Cisco Integrated Management Interface (Cisco IMC). If you want to use the 10/100/1000 dedicated management ports to access Cisco IMC, you can connect to the server and change the NIC mode as described in Step 1 of the following procedure.

- The NIC redundancy is active-active. All Ethernet ports are utilized simultaneously.

- DHCP is enabled.

- IPv4 is enabled. You can change this to IPv6.

The following method is supported for connecting to the system for initial setup:

- Local setup—Use this procedure to connect a keyboard and monitor to the system for setup. This procedure requires a KVM cable (Cisco PID N20-BKVM). See Local Connection Procedure, page 3-16.

Local Connection Procedure

Step 1   Attach a power cord to each power supply in your server, and then attach each power cord to a grounded AC power outlet. See Power Specifications, page A-2 for power specifications.

Wait for approximately two minutes to let the server boot in standby power during the first bootup.

You can verify system power status by looking at the system Power Status LED on the front panel (see External Features Overview, page 1-1). 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 a USB keyboard and VGA monitor to the corresponding connectors on the rear panel (see External Features Overview, page 1-1).

- Connect an optional KVM cable (Cisco PID N20-BKVM) to the KVM connector on the front panel (see External Features Overview, page 1-1 for the connector location). Connect your USB keyboard and VGA monitor to the KVM cable.

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.

       This utility has two windows that you can switch between by pressing F1 or F2.

Step 4   Continue with .

Cisco IMC Configuration Utility Setup

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

Step 1   Set NIC mode and NIC redundancy:

    a. Set the NIC mode to choose which ports to use to access Cisco IMC for server management (see Figure 1-5 for identification of the ports):

    • Shared LOM EXT (default)—This is the shared LOM extended mode, the factory-default setting. With this mode, the shared LOM and Cisco Card interfaces are both enabled.

       In this mode, DHCP replies are returned to both the shared LOM ports and the Cisco card ports. If the system determines that the Cisco card connection is not getting its IP address from a Cisco UCS Manager system because the server is in standalone mode, further DHCP requests from the Cisco card are disabled. Use the Cisco Card NIC mode if you want to connect to Cisco IMC through a Cisco card in standalone mode.

    • Dedicated—The dedicated management port is used to access Cisco IMC. You must select a NIC redundancy and IP setting.

    • Shared LOM—The 1-Gb Ethernet ports are used to access Cisco IMC. You must select a NIC redundancy and IP setting.

    • Cisco Card—The ports on an installed Cisco UCS virtual interface card (VIC) are used to access Cisco IMC. You must select a NIC redundancy and IP setting.

       See also the required VIC Slot setting below.

    • VIC Slot—If you use the Cisco Card NIC mode, you must select this setting to match where your VIC is installed. The choices are Riser1, Riser2, or Flex-LOM (the mLOM slot).

       – If you select Riser1, slot 2 is the primary slot, but you can use slot 1.

       – If you select Riser2, slot 5 is the primary slot, but you can use slot 4.

       – If you select Flex-LOM, you must use an mLOM-style VIC in the mLOM slot.

    b. Use this utility to change the NIC redundancy to your preference. This server has three possible NIC redundancy settings:

       – None—The Ethernet ports operate independently and do not fail over if there is a problem. This setting can be used only with the Dedicated NIC mode.

       – Active-standby—If an active Ethernet port fails, traffic fails over to a standby port.

       – Active-active—All Ethernet ports are utilized simultaneously. Shared LOM EXT mode can have only this NIC redundancy setting. Shared LOM and Cisco Card modes can have both Active-standby and Active-active settings.

Step 2   Choose whether to enable DHCP for dynamic network settings, or to enter static network settings.

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

The static IPv4 and IPv6 settings include the following:

- The Cisco IMC IP address.
- The prefix/subnet.

    For IPv6, valid values are 1–127.

- The gateway.

    For IPv6, if you do not know the gateway, you can set it as none by entering **::** (two colons).

- The preferred DNS server address.

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

Step 3   (Optional) Use this utility to make VLAN settings.

Step 4   Press **F1** to go to the second settings window, then continue with the next step.

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

Step 5   (Optional) Set a hostname for the server.

Step 6   (Optional) Enable dynamic DNS and set a dynamic DNS (DDNS) domain.

Step 7   (Optional) If you check the Factory Default check box, the server reverts to the factory defaults.

Step 8   (Optional) Set a default user password.

Step 9   (Optional) Enable auto-negotiation of port settings or set the port speed and duplex mode manually.

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

Step 10   (Optional) Reset port profiles and the port name.

Step 11   Press **F5** to refresh the settings that you made. You might have to wait about 45 seconds until the new settings appear and the message, "Network settings configured" is displayed before you reboot the server in the next step.

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

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

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

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

To manage the server, see the *Cisco UCS C-Series Rack-Mount Server Configuration Guide* or the *Cisco UCS C-Series Rack-Mount Server CLI Configuration Guide* for instructions on using those interfaces. The links to these documents are in the C-Series documentation roadmap:

http://www.cisco.com/go/unifiedcomputing/c-series-doc

System BIOS and CIMC Firmware

This section includes information about the system BIOS and it includes the following sections:

- Updating the BIOS and Cisco IMC Firmware, page 3-20
- Accessing the System BIOS, page 3-21

Updating the BIOS and Cisco IMC Firmware

⚠

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

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

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

- **Recommended method for system components firmware update**: Use the Cisco Host Upgrade Utility to simultaneously upgrade Cisco IMC, BIOS, LOM, LSI storage controller, and Cisco UCS VIC firmware to compatible levels.

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

- You can upgrade the BIOS using the EFI interface, or upgrade from a Windows or Linux platform.

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

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

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

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

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

For links to the documents listed above, see the documentation roadmap at the following URL:

http://www.cisco.com/go/unifiedcomputing/c-series-doc

Accessing the System BIOS

You can change the BIOS settings for your server. Detailed instructions are also printed on the BIOS screens.

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**.

Replacing Hardware Components

This chapter describes how to install or replace hardware components.

Refer to the following topics for more information:

Preparing for Server Component Installation

This section describes how to prepare for component installation, and it includes the following topics:

For more information, see the following:

- Cisco CSS UCSM4 1RU: "Preparing for Server Component Installation" in the Cisco UCS C220 Server Installation and Service Guide.
- Cisco CSS UCSM4 2RU: "Preparing for Server Component Installation" in the Cisco UCS C240 Server Installation and Service Guide.

Required Equipment

The following equipment is used to perform the procedures in this chapter:

- Number 2 Phillips-head screwdriver
- Electrostatic discharge (ESD) strap or other grounding equipment such as a grounded mat

Shutting Down and Powering Off the Server

The server can run in 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 the cooling fans and it is safe to power off the server from this mode.

You can invoke a graceful shutdown or a hard shutdown by using either of the following methods:

- Use the Cisco IMC management interface.
- Use the **Power** button on the server front panel. To use the **Power** button, follow these steps:

Step 1   Check the color of the Power Status LED (see the "Status LEDs and Buttons" section on page 1-10).

- Green—The server is in main power mode and must be shut down before it can be safely powered off. Go to Step 2.
- Amber—The server is already in standby mode and can be safely powered off. Go to Step 3.

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 Status 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   Disconnect the power cords from the power supplies in your server to completely power off the server.

Removing and Replacing the Server Top Cover

- Cisco CSS UCSM4 1RU Top Cover, page 4-3
- Cisco CSS UCSM4 2RU Top Cover, page 4-4

Cisco CSS UCSM4 1RU Top Cover

To remove or replace the top cover of the Cisco CSS UCSM4 1RUserver, follow these steps:

Step 1   Remove the top cover (see Figure 4-1).

    a.   If the cover latch is locked, use a screwdriver to turn the lock 90-degrees counterclockwise to unlock it. See Figure 4-1.

    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:

> **Note**   The latch must be in the fully open position when you set the cover back in place, which allows the opening in the latch to sit over a peg that is on the fan tray.

    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 4-1   *Removing the Top Cover*

1	Top cover	2	Locking cover latch

Cisco CSS UCSM4 2RU Top Cover

To remove or replace the top cover of the Cisco CSS UCSM4 1RU server, follow these steps:

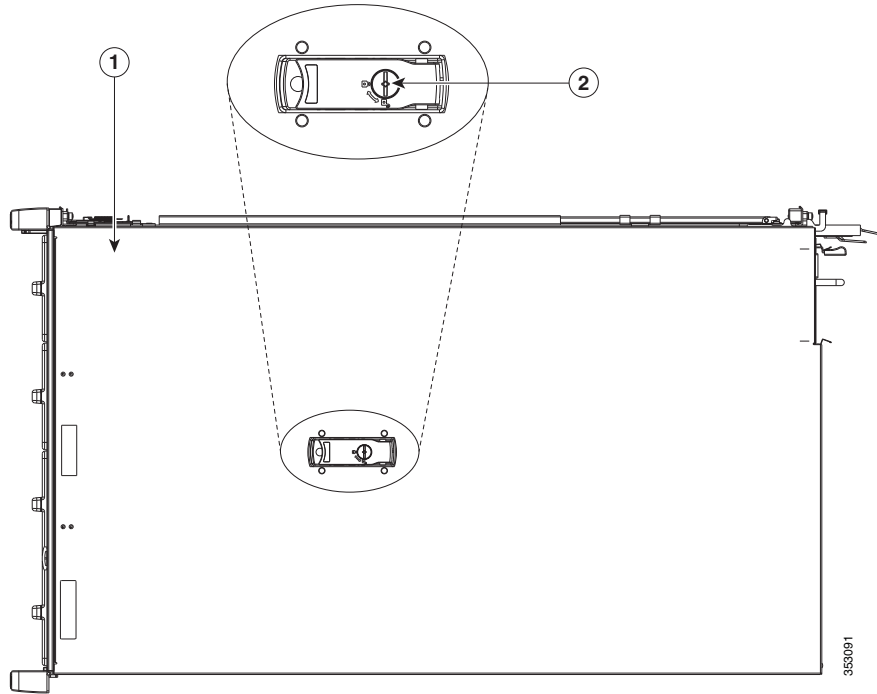**Step 1**   Remove the top cover (see Figure 4-1).

   a.   If the cover latch is locked, use a screwdriver to turn the lock 90-degrees counterclockwise to unlock it. See Figure 4-1.

   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:

   ✎

   Note   The latch must be in the fully open position when you set the cover back in place, which allows the opening in the latch to sit over a peg that is on the fan tray.

   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 4-2   Removing the Top Cover
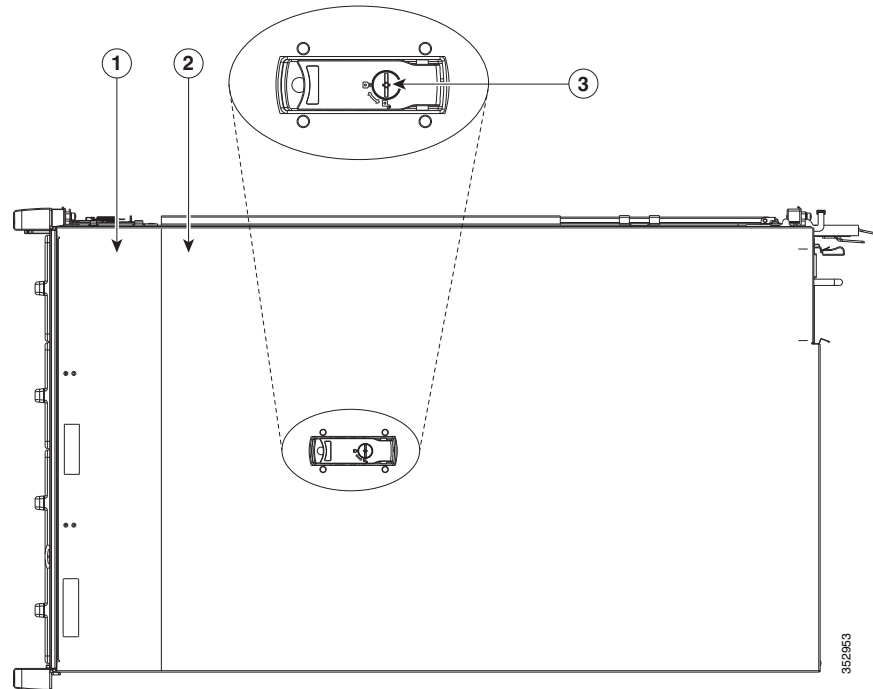
1	Front cover panel	**3**	Locking cover latch
2	Top cover		

Serial Number Location

The serial number (SN) for the server is printed on a label on the top of the server, near the front.

Hot-Swap or Hot-Plug Replacement

Some components can be removed and replaced without powering off and removing AC power from the server.

- Hot-swap replacement—You do not have to precondition or shut down the component in the software before you remove it for the following components:

    - SAS hard drives or SSDs

    - Cooling fan modules

    - Power supplies (when 1+1 redundant)

- **Hot-plug replacement**—You must take the component offline before removing it for the following component:
  - NVMe PCIe SSDs

Replaceable Component Locations

Cisco CSS UCSM4 1RU Replaceable Component Locations

This section shows the locations of the field-replaceable components. The view in Figure 4-3 is from the top down with the top cover and air baffle removed.

Figure 4-3   Replaceable Component Locations
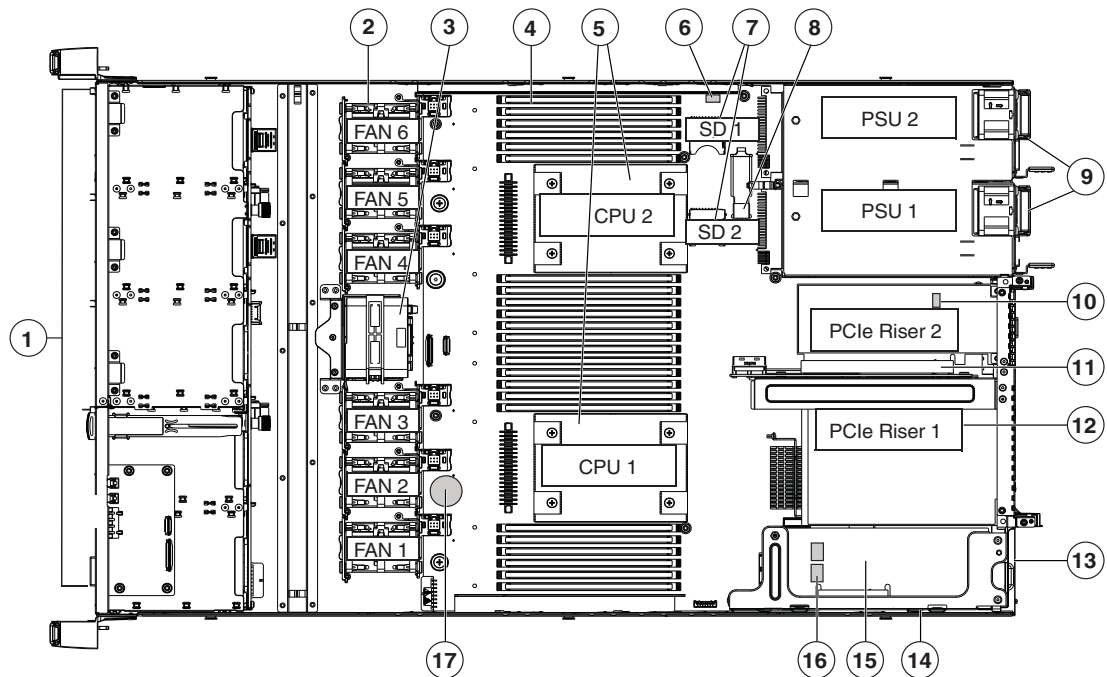
1	Drive bays 1–8 support SAS drives. SFF, 8-drive version only: Drive bays 1 and 2 support SAS and NVMe PCIe SSDs. NVMe SSDs require PCIe riser version 2B in the server to provide the PCIe bus connection.	**10**	Trusted platform module (TPM) socket on motherboard (not visible in this view)
2	Cooling fan modules (six)	**11**	PCIe riser 2 (half-height PCIe slot 2)
3	Supercap Power Module (RAID backup) mounting bracket	**12**	PCIe riser 1 (full-height PCIe slot 1)
4	DIMM sockets on motherboard (24)	**13**	Modular LOM (mLOM) connector on chassis floor

5	CPUs and heatsinks (up to two)	14	Cisco modular RAID controller PCIe riser (dedicated riser with horizontal socket)
6	Embedded SATA RAID header for RAID 5 key	15	Cisco modular RAID controller card
7	SD card bays on motherboard (two)	16	Embedded SATA RAID mini-SAS connectors on motherboard (not visible in this view)
8	Internal USB 3.0 port on motherboard	17	RTC battery on motherboard
9	Power supplies (up to two, hot-swappable when redundant as 1+1)		

The Technical Specifications Sheets for all versions of this server, which include supported component part numbers, are at Cisco UCS Servers Technical Specifications Sheets.

Cisco CSS UCSM4 2RU Replaceable Component Locations

Figure 4-4 shows the locations of the components that are supported as field-replaceable. The view shown is from the top down, with the top covers and air baffle removed.

Figure 4-4   Replaceable Component Locations

1	Drives bays. All drive bays support SAS drives.	10	PCIe riser 2 (PCIe slots 4, 5, 6)
	SFF, 8-, 16-, and 24-drive versions only: Drive bays 1 and 2 support SAS drives and NVMe PCIe SSDs. NVMe drives require a PCIe interposer board for PCIe bus connection (see item 6).		
2	Fan modules (six, hot-swappable)	11	PCIe riser 1 (PCIe slots 1, 2, 3*) *Slot 3 not present in all versions.
3	DIMM sockets on motherboard (up to 24 DIMMs)	12	SATA boot drives (two sockets available only on PCIe riser 1 option 1C)
4	CPUs and heatsinks (two)	13	mLOM card socket on motherboard under PCIe riser 1
5	Cisco SD card slots on motherboard (two)	14	Socket for embedded RAID interposer board
6	PCIe interposer board socket	15	Cisco modular RAID controller PCIe slot (dedicated slot and bracket)
7	USB 3.0 slot on motherboard	16	RTC battery on motherboard
8	Power supplies (hot-swappable, accessed through rear panel)	17	Embedded RAID header for RAID 5 key
9	Trusted platform module (TPM) socket on motherboard, under PCIe riser 2	18	Supercap power module (RAID backup) mounting location on air baffle (not shown)

The Technical Specifications Sheets for all versions of this server, which include supported component part numbers, are at Cisco UCS Servers Technical Specifications Sheets.

Installing or Replacing Server Components

Refer to the following topics for information on the components and configurations supported by the Cisco Connected Safety and Security UCS series servers.

- Replacing Hard Drives, page 4-9
- Replacing Additional Hardware Components (Related Documentation), page 4-14

✎ **Note** The Cisco Connected Safety and Security UCS series servers support a sub-set of the hardware and features available in the Cisco UCS series servers. Review the following information carefully.

Replacing Hard Drives

Refer to the following topics for more information:

- Cisco CSS UCSM4 1RU: Replacing SAS Hard Drives or Solid State Drives, page 4-9
- Cisco CSS UCSM4 2RU: Replacing a Hard Drive, page 4-11

Cisco CSS UCSM4 1RU: Replacing SAS Hard Drives or Solid State Drives

The Cisco Connected Safety and Security UCSM4 1RU (CPS-UCSM4-1RU-K9) is available in the large form factor (LFF) only.

✎ **Note** The small form-factor (SFF) version of the server is not supported Connected Safety and Security applications.

See the "Supported Hard Drives" section on page 2-5 for more information.
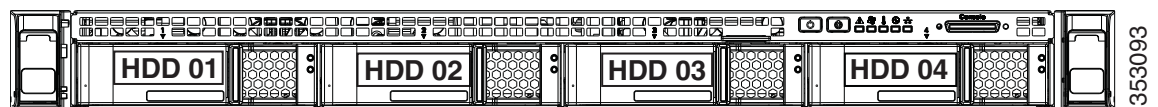
This section includes the following information:

- SAS Drive Population Guidelines, page 4-9
- Replacing a SAS Drive, page 4-10

SAS Drive Population Guidelines

The large form factor (LFF) server can hold up to four 3.5-inch SAS hard drives.

The drive-bay numbering is shown in Figure 4-5.

Figure 4-5   *Drive Numbering, LFF Drives, Four-Drive Version*

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 hard drives and SAS SSDs in the same server (the LFF version of the server does not support SSDs). 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 hard drives or all SAS SSDs.

Replacing a SAS Drive

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

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. See Figure 4-6.

    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 4-6   Replacing Hard Drives
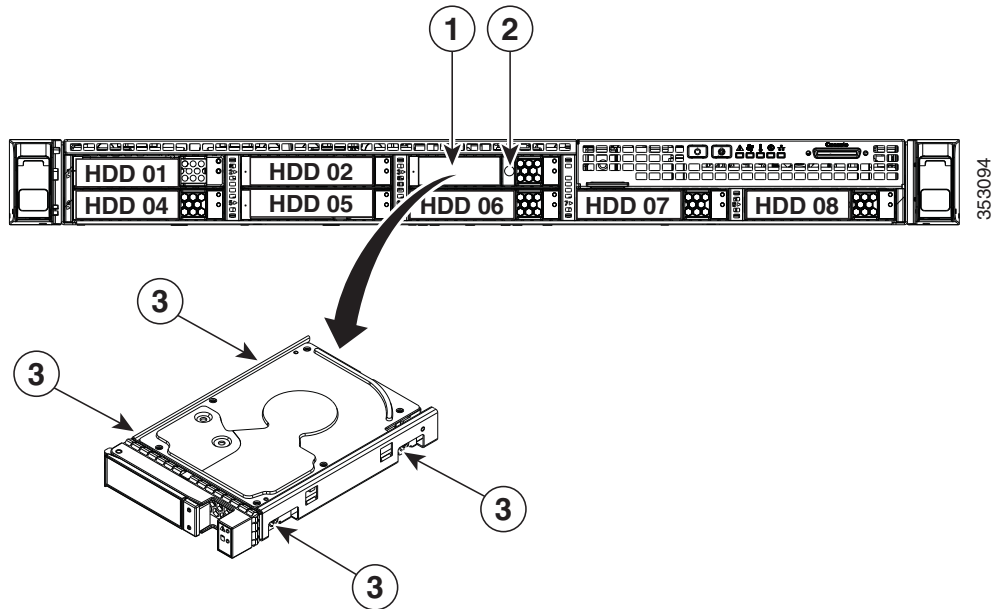
1	Ejector lever	**3**	Drive tray securing screws (4)
2	Release button		–

Cisco CSS UCSM4 2RU: Replacing a Hard Drive

The Cisco Connected Safety and Security UCSM4 2RU (CPS-UCSM4-2RU-K9) is available in the large form factor (LFF) only.

Note   The small form-factor (SFF) server is not supported for Cisco Connected Safety and Security applications.

See the "Supported Hard Drives" section on page 2-5 for more information.

This section includes the following information:

- SAS Drive Population Guidelines, page 4-11
- Replacing SAS Drives, page 4-12

SAS Drive Population Guidelines

The server is orderable in the large form-factor (LFF) drive version only, which holds up to twelve 3.5-inch hard drives.

- CPS-UCSM4-2RU-K9—Large form-factor (LFF) drives, with 12-drive backplane and integrated expander. This version holds up to 12 3.5-inch SAS hard drives. SAS drives are hot-swappable.

Note You cannot change the backplane type after-factory. To change a front panel/backplane configuration, a chassis replacement is required.

The drive-bay numbering for all server versions is shown in Figure 4-7.

Figure 4-7   Drive Numbering, LFF Drives, 12-Drive Version
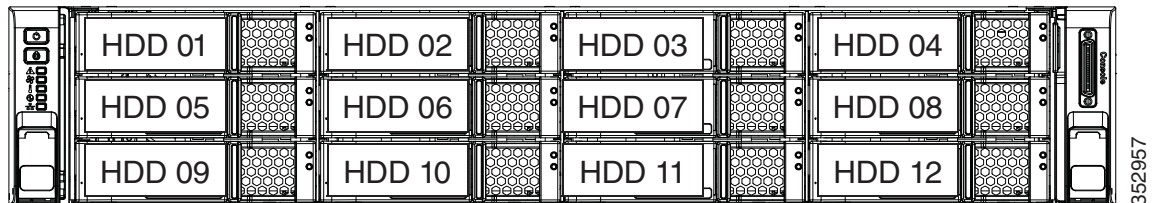
Observe these drive population guidelines for optimal performance:

- When populating drives, add drives in the lowest numbered bays first.

- Keep an empty drive blanking tray in any unused bays to ensure optimal airflow and cooling.

- You can mix hard drives and solid state drives 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 hard drives or all SSDs.

Replacing SAS Drives

Tip You do not have to shut down or power off the server to replace SAS hard drives or solid state drives (SSDs) because they are hot-swappable.

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

a. Press the release button on the face of the drive tray. See Figure 4-6.

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 replace 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 4-8   *Replacing Drives*
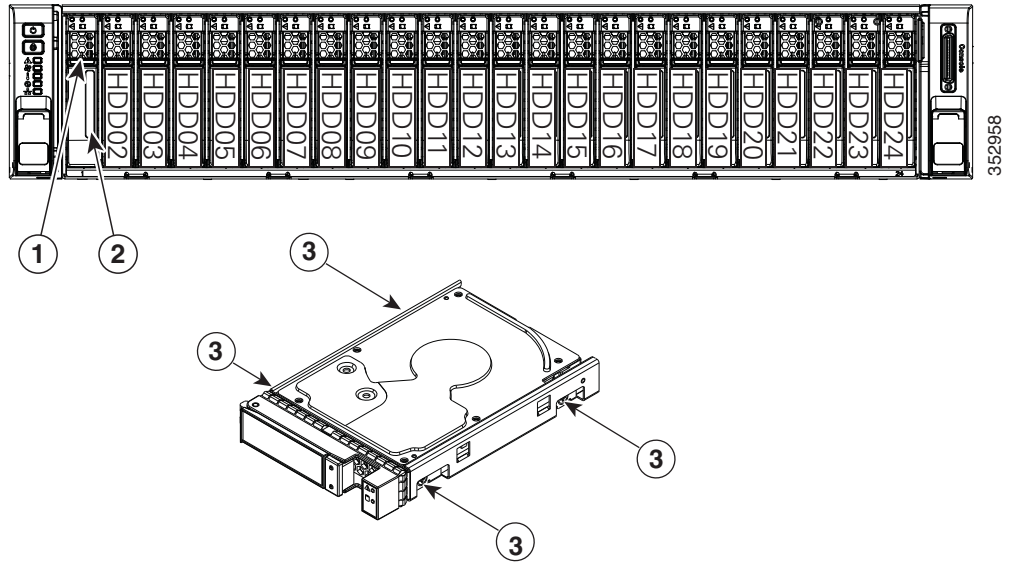
1	Release button	**3**	Drive tray securing screws (four)
2	Ejector lever		–

Replacing Additional Hardware Components (Related Documentation)

The Cisco Connected Safety and Security UCS series servers support a sub-set of the hardware and features available in the Cisco UCS series servers. Review the information in this document carefully, including the "Overview" section on page 1-1.

For instructions to replace additional hardware components, refer to the following documentation:

- Cisco CSS UCSM4 1RU: "Installing or Replacing Server Components" in the Cisco UCS C220 M4 Server Installation and Service Guide.

- Cisco CSS UCSM4 2RU: "Installing or Replacing Server Components" in the Cisco UCS C240 M4 Server Installation and Service Guide.

This documentation includes the following topics:

- Replacing Hard Drives

- Replacing Fan Modules

- Replacing a PCIe Card

- Replacing Power Supplies

See Cisco UCS C-Series Rack Servers for complete documentation on the UCS C220 M4 Rack Server (1RU) and UCS C240 M4 Rack Server (2RU).

See also the "Related Documentation" section on page B-1 and www.cisco.com/go/unifiedcomputing/c-series-doc for links to additional information on the Cisco UCS-series servers.

APPENDIX **A**

Server Specifications

This appendix lists the technical specifications for the server and includes the following sections:

Cisco Connected Safety and Security UCSM4 2RU Specifications

Physical Specifications

Table A-1 lists the physical specifications for the server.

Table A-1   Physical Specifications

Description	Specification
Height	1.7 in. (4.3 cm)
Width	16.9 in. (42.9 cm)
Depth (length)	29.8 in. (75.8 cm)
Maximum weight (fully loaded chassis)	LFF 4-drive: 39.9 lb. (18.1 Kg)

Environmental Specifications

Table A-2 lists the environmental specifications for the server.

Table A-2   Environmental Specifications

Description	Specification
Temperature, operating	41 to 95°F (5 to 35°C) Derate the maximum temperature by 1°C per every 305 meters of altitude above sea level.
Temperature, non-operating (when the server is stored or transported)	–40 to 149°F (–40 to 65°C)
Humidity (RH), operating	10 to 90%
Humidity, non-operating	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)	5.4
Sound pressure level Measure A-weighted per ISO7779 LpAm (dBA) Operation at 73°F (23°C)	37

Power Specifications

The CPS-UCSM4-1RU-K9 server supports the following power supply option:

770 W AC Power Supply

Table A-3 lists the specifications for each 770 W AC power supply
(Cisco part number UCSC-PSU1-770W).

Table A-3   Power Supply Specifications

Description	Specification
AC input voltage	Nominal range: 100–120 VAC, 200–240 VAC (Range: 90–132 VAC, 180–264 VAC)
AC input frequency	Nominal range: 50 to 60Hz (Range: 47–63 Hz)
Maximum AC input current	9.5 A at 100 VAC 4.5 A at 208 VAC
Maximum input volt-amperes	950 VA at 100 VAC
Maximum output power per PSU	770 W

Table A-3   Power Supply Specifications

Description	Specification
Maximum inrush current	15 A (sub-cycle duration)
Maximum hold-up time	12 ms at 770 W
Power supply output voltage	12 VDC
Power supply standby voltage	12 VDC
Efficiency rating	Climate Savers Platinum Efficiency (80Plus Platinum certified)
Form factor	RSP2
Input connector	IEC320 C14

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

http://ucspowercalc.cisco.com

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

Cisco Connected Safety and Security UCSM4 2RU Specifications

- Physical Specifications, page A-1
- Power Specifications, page A-2
- Environmental Specifications, page A-5

Physical Specifications

Table A-1 lists the physical specifications for the server.

Table A-4   Physical Specifications

Description	Specification
Height	3.4 in. (8.70 cm)
Width (including slam latches)	19.0 in. (48.26 cm)
Depth (length)	29.0 in. (73.70 cm)
Depth, including slam latches and power supply handles	31.5 in. (80.00 cm)
Maximum Weight (fully loaded)	LFF 12-drive: 67.5 lb. (30.6 Kg)

Power Specifications

The CPS-UCSM4-2RU-K9 server supports the following power supply option:

650 W AC Power Supply

Table A-3 lists the specifications for each 650 W AC power supply
(Cisco part number UCSC-PSU2V2-650W=).

Table A-5   Power Supply 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	7.6 A at 100 VAC 3.65 A at 208 VAC
Maximum input volt-amperes	760 VA at 100 VAC
Maximum output power per PSU	650 W

Table A-5   Power Supply Specifications

Description	Specification
Maximum inrush current	35 A (sub-cycle duration)
Maximum hold-up time	12 ms at 650 W
Power supply output voltage	12 VDC
Power supply standby voltage	3.3 VDC
Efficiency rating	Climate Savers Platinum Efficiency (80Plus Platinum certified)
Form factor	RSP1
Input connector	IEC320 C14

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

http://ucspowercalc.cisco.com

Environmental Specifications

Table A-2 lists the environmental specifications for the server.

Table A-6   Environmental Specifications

Description	Specification
Temperature, operating	41 to 95°F (5 to 35°C) Derate the maximum temperature by 1°C per every 305 meters of altitude above sea level.
Temperature, nonoperating (when the server is in storage or is transported)	–40 to 149°F (–40 to 65°C)
Humidity (RH), operating	10 to 90%
Humidity, non-operating	5 to 93%
Altitude, operating	0 to 10,000 feet
Altitude, nonoperating (when the server is in storage or is transported)	0 to 40,000 feet
Sound power level Measure A-weighted per ISO7779 LwAd (Bels) Operation at 73°F (23°C)	5.8
Sound pressure level Measure A-weighted per ISO7779 LpAm (dBA) Operation at 73°F (23°C)	43

Related Documentation

This document describes installation of the following Cisco Connected Safety and Security servers:

- CPS-UCSM4-1RU-K9
- CPS-UCSM4-2RU-K9

Note For information about the CPS-UCS-1RU-K9 and CPS-UCS-2RU-K9 servers, see Cisco Physical Security UCS Platform Series User Guide, CPS-UCS-1RU-K9 / CPS-UCS-2RU-K9.

You can access the most current information and documentation online at the following URLs:

Cisco Physical Security UCS Platform Series User Guide, CPS-UCSM4-1RU-K9 / CPS-UCSM4-2RU-K9 (this document):

www.cisco.com/go/physicalsecurity/ucs/install

Cisco UCS C-Series Server Installation Documentation:

- Cisco UCS C-Series Rack Servers

    – Cisco CSS UCSM4 1RU: Cisco UCS C220 M4 Server Installation and Service Guide.

    – Cisco CSS UCSM4 2RU: Cisco UCS C240 M4 Server Installation and Service Guide.

Cisco UCS C-Series Server Documentation Roadmap:

www.cisco.com/go/unifiedcomputing/c-series-doc

Cisco UCS C-Series Regulatory Compliance and Safety Information:

www.cisco.com/go/physicalsecurity/ucs/rcsi

Cisco Connected Safety and Security Product Information:

www.cisco.com/go/physicalsecurity/

Cisco Video Surveillance 7 Documentation Roadmap:

Descriptions and links to Cisco Video Surveillance documentation, server and storage platform documentation, and other related documentation.

http://www.cisco.com/go/physicalsecurity/vsm/roadmap

Cisco Video Surveillance Manager Documentation Website:

www.cisco.com/go/physicalsecurity/vsm/docs