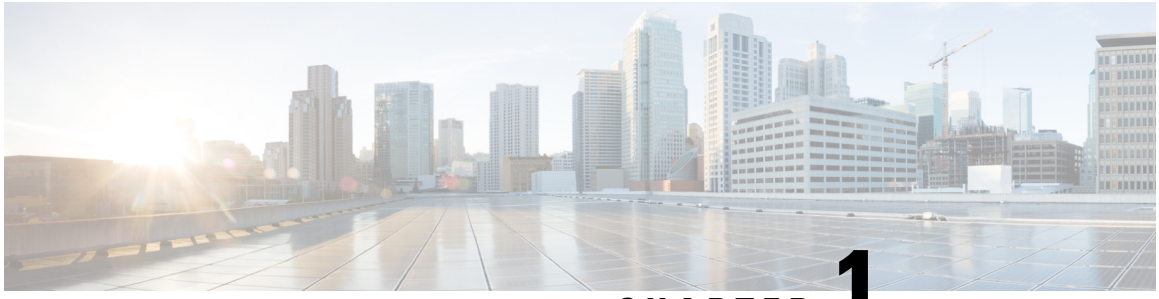
Cisco Secure Firewall 4200 Series Hardware Installation Guide

First Published: 2023-09-07

Last Modified: 2024-04-23

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

CONTENTS



CHAPTER 1

Overview

Features

The Cisco Secure Firewall 4200 is a standalone modular security services platform that includes the Secure Firewall 4215, 4225, and 4245.

The Secure Firewall 4200 supports Cisco Firepower Threat Defense and Cisco ASA software. See the Cisco Secure Firewall Threat Defense Compatibility Guide and the Cisco Secure Firewall ASA Compatibility guide, which provide Cisco software and hardware compatibility, including operating system and hosting environment requirements, for each supported version.

The following figure shows the Secure Firewall 4200.

Figure 1: Secure Firewall 4200

The following table lists the features for the Secure Firewall 4200.

Table 1: Secure Firewall 4200 Features

Feature	4215	4225	4245
Form factor	1 RU Fits a standard 19-inch (48.3-cm) square-hole rack		
Rack mount	Two slide-rail mounting brackets and two slide rails 4-post Electronic Industries Association (EIA)-310-D rack		
Airflow	Front to rear (I/O side to non-I/O side) Cold aisle to hot aisle		
Core count	Single socket 32-core	Single socket 64-core	Dual socket two 64-cores
System memory	8 x 32 GB (256 GB) at 3200 Mt/s	8 x 64 GB (512 GB) at 3200 Mt/s	16 x 64 GB (1 TB) at 3200 Mt/s
Management ports	Two 1/10/25-Gbps SFP28 ports		
Console port	One RJ-45 serial port		
USB port	One USB 3.0 with 5 W Type A port		
Network ports	Eight fixed 1/10/25-Gbps SFP28 fiber ports Named Ethernet 1/1 through 1/8		
Network module slots	Two (hot-swappable) **Note** Hot-swapping of identical modules is supported, but if you replace a network module with another type, you must reboot the system so that the new network module is recognized.		

Feature	4215	4225	4245
Network modules	• 8-port 1/10Gb SFP+ (FPR-X-NM-8X10G) • 8-port 1/10/25Gb SFP+ (FPR-X-NM-8X25G) • 4-port 40-Gb QSFP/QSFP+ (FPR-X-NM-4X40G) • 4-port 40/100/200-Gb QSFP28/QSFP (FPR-X-NM-4X200G) **Note** 200-Gb traffic is not supported until a later release. • 2-port 100-Gb QSFP56/QSFP28/QSFP (FPR-XNM-2X100G) • 6-port 10-Gb SFP SR multimode hardware bypass (FPR-X-NM-6X10SRF) • 6-port 10-Gb SFP LR single mode hardware bypass (FPR-X-NM-6X10LRF) • 6-port 25-Gb SFP SR multimode hardware bypass (FPR-X-NM-6X25SRF) • 6-port 25-Gb SFP LR single mode hardware bypass (FPR-X-NM-6X25LRF) • 8-port copper 1-Gb 1000Base-T hardware bypass (FPR-X-NM-8X1GF)		
AC power supply	Ships with one 1900 W AC power supply (second power supply is optional) Hot-swappable	Ships with two 1900 W AC power supplies Hot-swappable	
Redundant power	Yes **Note** You must order a second power supply.	Yes **Note** Ships with two power supplies.	
Fans	Three dual fan modules (hot-swappable)		
Storage	Two Nonvolatile Memory Express (NVMe) SSD slots for EDSFF (Enterprise & Datacenter SSD Form Factor) SSD drives Ships with two 1.8-TB SSDs; factory-configured for RAID1.		
Pullout asset card	Displays the serial number and a QR code that points to the Documentation Portal		
Grounding	Grounding pad on the left side of chassis near the rear power switch; use the grounding lug kit that ships with the chassis.		
Power switch	On rear panel		
Reset button	Resets the system to factory default without requiring serial console access **Note** The reset button is recessed. Press with a pin and hold longer than 5 seconds to set the system back to the factory default.		

Deployment Options

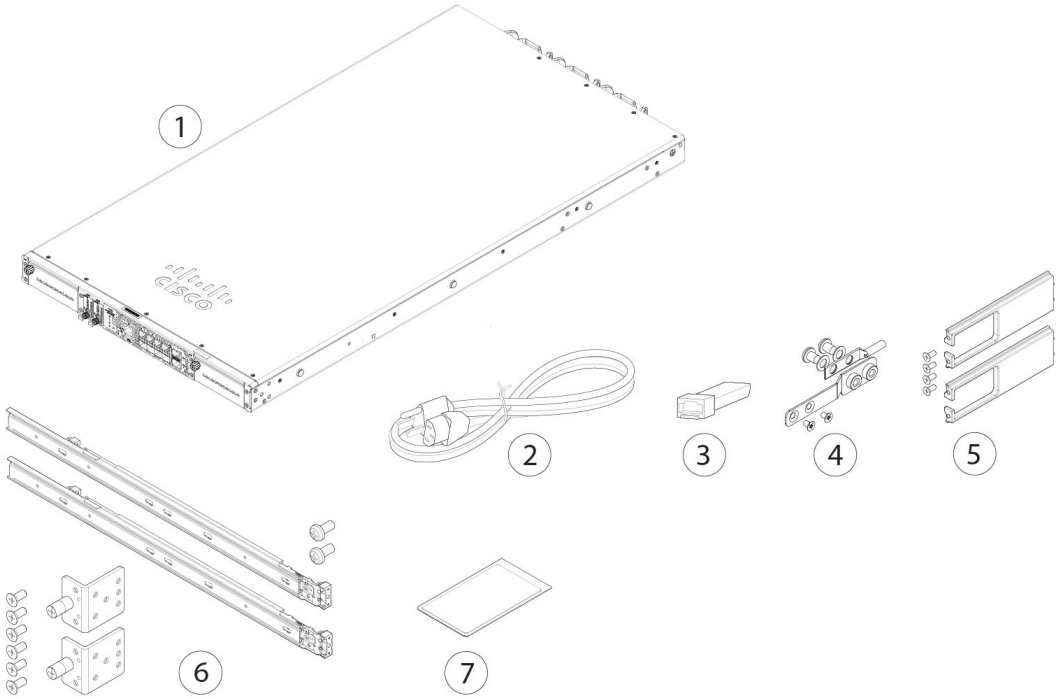
Here are some examples of how you can deploy the Secure Firewall 4200:

- As a firewall:
  - At the enterprise internet edge in a redundant configuration
  - At branch offices in either a high availability pair or standalone
  - At data centers in a high availability pair or clustered, which serves the needs of smaller enterprises
- As a device that provides additional application control, URL filtering, or IPS/threat-centered capabilities:
  - Behind an enterprise internet edge firewall in an inline configuration or as a standalone (requires hardware fail-open network module support)
  - Deployed passively off a SPAN port on a switch or a tap on a network, or standalone
- As a branch native SD-WAN solution that offers remote deployment and can be managed over a 4G LTE
- As a VPN device:
  - For remote access VPN
  - For site-to-site VPN

Package Contents

The following figure shows the package contents for the Secure Firewall 4200. The contents are subject to change and your exact contents contain additional or fewer items depending on whether you order the optional parts. See Product ID Numbers for a list of PIDs associated with the package contents.

Figure 2: Secure Firewall 4200 Package Contents



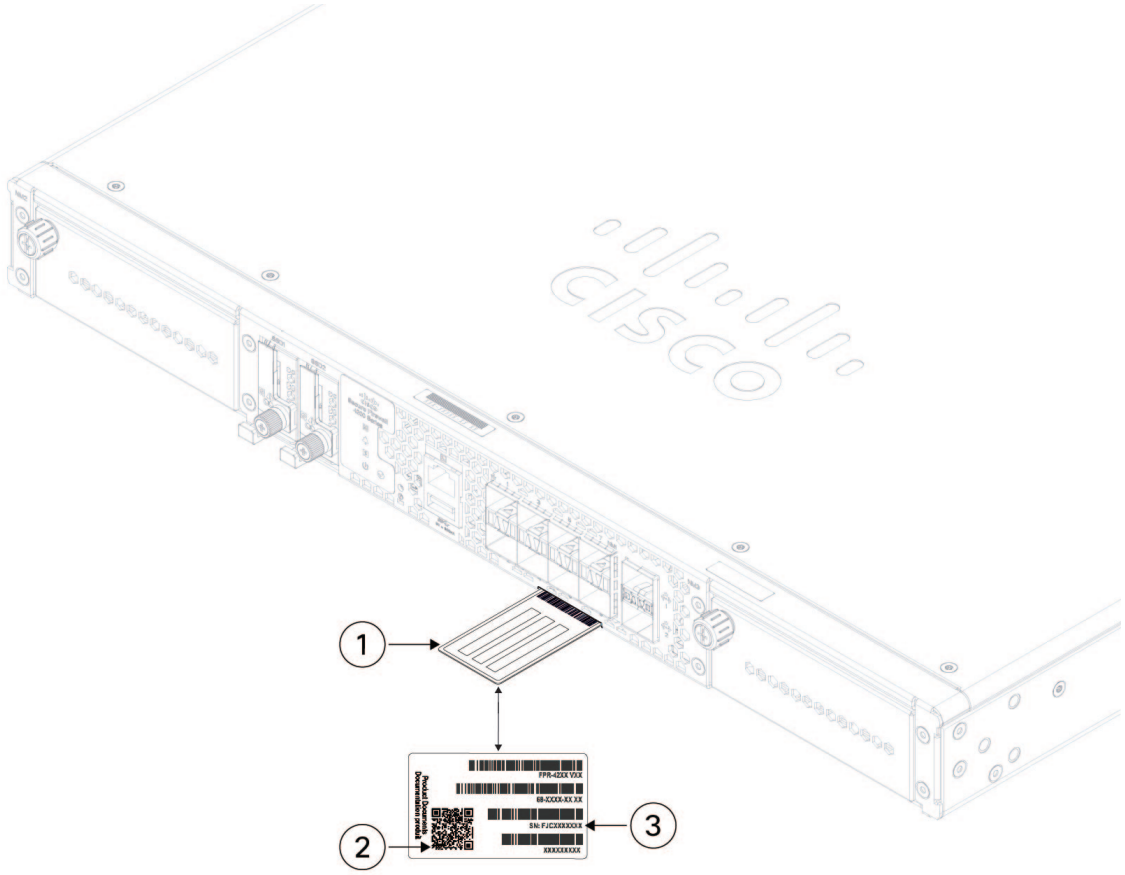
1	Secure Firewall 4200 chassis	**2**	One or two power cords (country-specific) See Power Cord Specifications, on page 41 for a list of supported power cords.
3	SFP transceiver (Optional; in package if ordered)	**4**	Ground lug, screws, and washers • One ground lug (part number 32-100152-01) • One ground lug bracket (part number 700-122528-01) • Two M4.0 x 0.6 mm flat head Phillips screws (part number 48-2030-01) • Two ¼-20 x 0.297-inch screws (part number 48-102252-01) • Two 0.469-inch OD, 0.261-inch ID, 0.025-inch T washers (part number 49-100464-01)

5	Cable management bracket kit (part number 69-101031-01) • Two cable management brackets (part number 700-130991-01) • Four 8-32 x 0.375-inch Phillips screws (part number 48-2696-01) (Optional; in package if ordered)	**6**	Two slide rails (800-109129-01) Slide rail accessories kit (53-101561-01): • Two slide rail mounting brackets (part number 700-121935-01) • Six 8-32 x 0.302-inch slide rail mounting bracket Phillips screws (part number 48-102184-01) for securing the brackets to the chassis • Two M3 x 0.5 x 6-mm Phillips screws (part number 48-101144-01) for securing the chassis to your rack
7	*Cisco Secure Firewall 4200* This document has URLs to the hardware installation guide, regulatory and safety information guide, and warranty and licensing information. It also contains a QR code that points to the Digital Documentation Portal. The portal contains links to the product information page, the hardware installation guide, the regulatory and safety information guide, and the getting started guide		—

Serial Number and Documentation Portal QR Code

The pullout asset card on the front panel of your Secure Firewall 4200 chassis contains the chassis serial number and the Documentation Portal QR code, which points to product information, the getting started guide, the regulatory and compliance guide, and the hardware installation guide.

Figure 3: Pullout Asset Card



1	Pullout asset tag	**2**	Documentation Portal QR code
3	Chassis serial number		—

The compliance label on the bottom of the chassis contains the chassis serial number, regulatory compliance marks, and also the Documentation Portal QR code that points to the guides listed above. The following figure shows an example compliance label found on the bottom of the chassis.

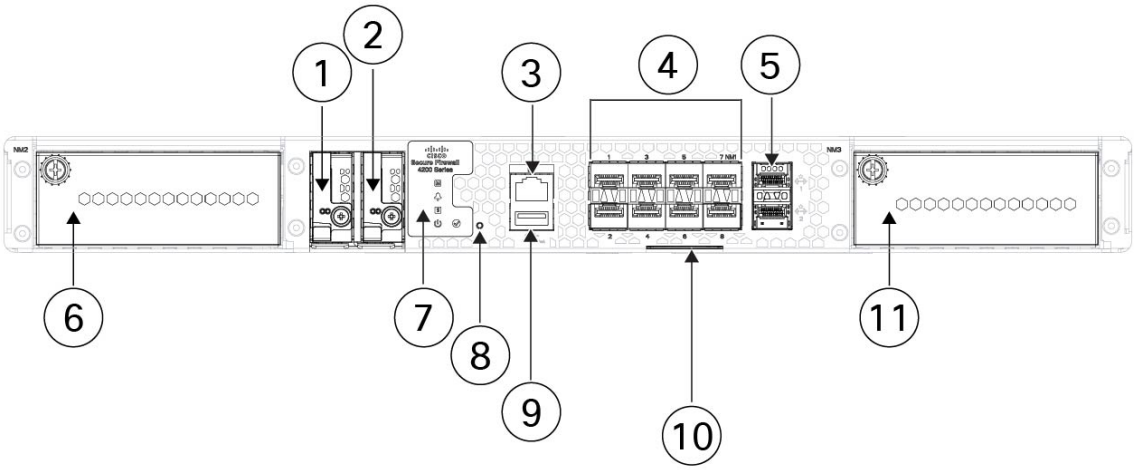
Figure 4: Example Compliance Label

1	Chassis model number	**2**	Documentation Portal QR code
3	Serial number		—

Front Panel

The following figure shows the front panel of the Secure Firewall 4200. See Front Panel LEDs, on page 11 for a description of the LEDs.

Figure 5: Secure Firewall 4200 Front Panel



1	SSD slot (SSD-1)	**2**	SSD slot (SSD-2)
3	RJ-45 console port	**4**	Eight 1/10/25-Gb SFP28 fixed fiber ports (NM-1) Fiber ports named 1/1 through 1/8 left to right
5	Dual stacked management ports (supports 1/10/25-Gb Gigabit Ethernet) Top port: • Secure Firewall Threat Defense—Management 0 (also referred to as Management 1/1) • ASA—Management 1/1 Bottom port: • Secure Firewall Threat Defense—Management 1 (also referred to as Management 1/2) • ASA—Management 1/2	**6**	Network module slot (NM-2)
7	System LEDs	**8**	Recessed factory reset button
9	Type A USB 3.0 port	**10**	Pullout asset card with chassis serial number and QR code to the Digital Documentation Portal that has links to the getting started guide, hardware guide, and regulatory and compliance guide.
11	Network module slot (NM-3)		—

Management Port

The Secure Firewall 4200 chassis management port is a 1/10/25-Gb SFP port that supports fiber as well as DAC or GLC-TE.

RJ-45 Console Port

The Secure Firewall 4200 does not ship with an RJ-45 serial cable unless you order it with the chassis. You can obtain a cable, for example, a USB-to-RJ-45 serial cable. You can use the CLI to configure your 4200 through the RJ-45 serial console port by using a terminal server or a terminal emulation program on a computer.

The RJ-45 (8P8C) port supports RS-232 signaling to an internal UART controller. The console port does not have any hardware flow control, and does not support a remote dial-in modem. The default console port settings are displayed as follows:

- 9,600 bits per second
- 8 data bits
- No parity
- 1 stop bit
- No flow control

Type A USB 3.0 Port

You can use the external Type A USB port to attach a data-storage device. The external USB drive identifier is `usb:`. The Type A USB port supports the following:

- Hot swapping
- USB drive formatted with FAT32
- Boot kickstart image from ROMMON for discovery recovery purposes
- Copy files to and from workspace:/ and volatile:/ within local-mgmt. The most relevant files are:
  - Core files
  - Ethanalyzer packet captures
  - Tech-support files
  - Security module log files
- Platform bundle image upload using **download image usbA:**

The Type A USB port does *not* support Cisco Secure Package (CSP) image upload support.

Network Ports

The Secure Firewall 4200 chassis has two network module slots that support the following network modules:

- 4-port 40-Gb QSFP/QSFP+ (FPR-X-NM-4X40G)
- 4-port 40/100/200-Gb QSFP28/QSFP (FPR-X-NM-4X200G)
- 2-port 100-Gb QSFP56/QSFP28/QSFP (FPR-X-NM-2X100G)

- 8-port 1/10-Gb SFP (FPR-X-NM-8X10G)
- 8-port 1/10/25-Gb ZSFP (FPR-X-NM-8X25G)
- 6-port 10-Gb SFP SR multimode hardware bypass (FPR-X-NM-6X10SR-F)
- 6-port 10-Gb SFP LR single mode hardware bypass (FPR-X-NM-6X10LR-F)
- 6-port 25-Gb SFP SR multimode hardware bypass (FPR-X-NM-6X25SR-F)
- 6-port 25-Gb SFP LR single mode hardware bypass (FPR-X-NM-6X25LR-F)
- 8-port 1-Gb 1000Base-T hardware bypass (FPR-X-NM-8X1G-F)

Factory Reset Button

The Secure Firewall 4200 chassis has a recessed reset button that resets the system to the factory default. Pressing the button down for five seconds deletes the current configuration and current files.

Note Use the reset button if the current credentials are lost and you want to initialize the box without having console access.

The following occurs:

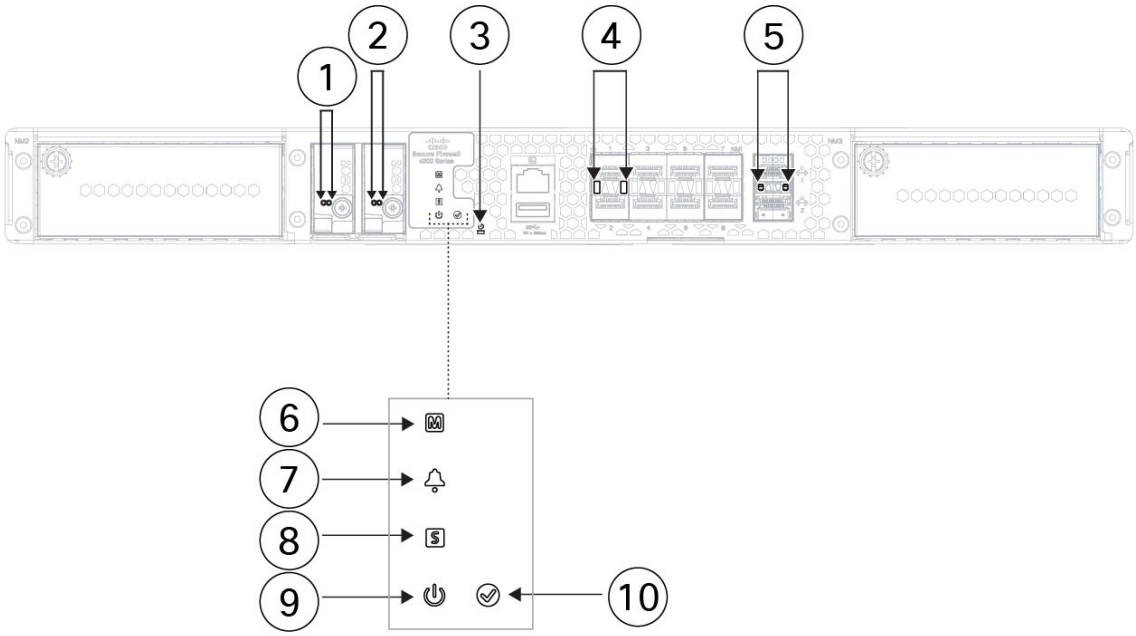
- ROMMON NVRAM is cleared and returned to default.
- All extra images are removed; the current running image remains.
- FXOS logs, core files, SSH keys, certificates, FXOS configuration, and Apache configuration are removed.

Note If power is lost between when you pushed the reset button and when the reset process is complete, the process stops and you have to push the button again after the system powers back on.

Front Panel LEDs

The following figure shows the Secure Firewall 4200 front panel LEDs.

Figure 6: Secure Firewall 4200 Front Panel LEDs



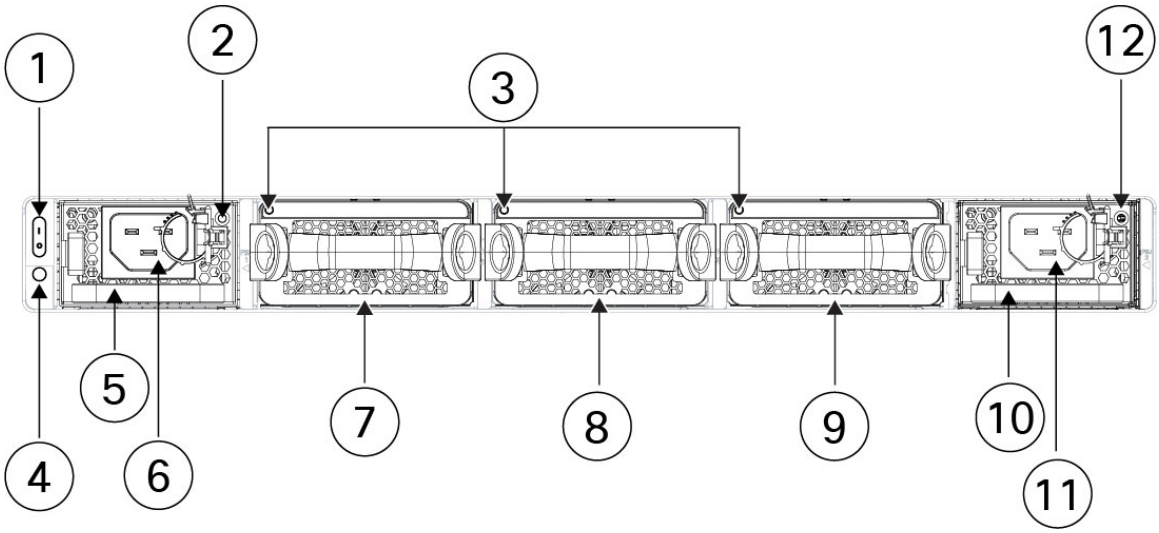
1	**SSD-1 Status** **Note** The left LED is active. The right LED is always off. • Off—The SSD is not present. • Green—The SSD is present; no activity. • Green, flashing—The SSD is active. • Amber—The SSD has a problem or failure.	2	**SSD-2 Status** **Note** The left LED is active. The right LED is always off. • Off—The SSD is not present. • Green—The SSD is present; no activity. • Green, flashing—The SSD is active. • Amber—The SSD has a problem or failure.
3	**Factory Reset Button Status** • Green, flashing—Flashes 5 seconds after you depress the button. • Off—Reset is complete. **Note** The factory reset button begins flashing after it has been depressed for at least 5 seconds, and persists until the software has completely applied all factory default settings or it is interrupted by a power cycle.	4	**Fiber Port Link/Activity Status** Each fiber port has one dual color LED under the SFP cage. • Off—No SFP. • Green—Link up. • Green, flashing—Network activity at >1G is detected. • Amber—No link or network failure.

5	**Management Port Status** The 1/10/25-Gb fiber management port has a bicolor LED under the SFP cage that indicates link/activity/fault: • Off—No SFP. • Green—Link up. • Green, flashing—Network activity. • Amber—SFP present, but no link.	6	**Managed Status** Reserved for future use.
7	**Alarm Status** • Off—No alarms. • Amber—Environmental error. • Green—Status is ok.	8	**System Status** • Off—System has not booted up yet. • Green, flashing quickly—System is booting up. • Green—Normal system function. • Amber—System boot up has failed. • Amber, flashing—Alarm condition, system needs service or attention and may not boot properly.
9	**Power Status** • Off—System is powered off. If the AC power cord is plugged in, and the LED on the power supply is blinking green, standby power is still on. **Note** If the LED is off, then the power switch is set to OFF or there is no input power. • Green, flashing—The system has detected a power switch toggle event, and initiated the shutdown sequence. If the power switch is in the OFF position, the system powers off after shutdown is completed. Do not remove the AC or DC power source while this LED is blinking so that the system has time to perform a graceful shutdown. • Amber—The system is powering up (before the BIOS boots). This takes one to five seconds at most. • Green—The system is fully powered up.	10	**Activity Status** (Role of a high-availability pair) • Off—The unit is not configured or enabled in a high-availability pair. • Green—The unit is in active mode. • Amber—The unit is in standby mode.

Rear Panel

The following figure shows the rear panel of the Secure Firewall 4200.

Figure 7: Secure Firewall 4200 Rear Panel



1	Power on/off switch	**2**	Power supply LED (PSU-1)
3	Dual fan modules (FAN-1, FAN-2, FAN-3) LEDs	**4**	System power LED This system power LED has the same behavior as the front panel LED. See Front Panel LEDs, on page 11 for more information. **Note** Power supply module 1 (PSU-1)
5	Power supply module 1 (PSU-1)	**6**	Power supply module 1 (PSU-1) connector
7	Dual fan module 1 (FAN-1)	**8**	Dual fan module 2 (FAN-2)
9	Dual fan module 3 (FAN-3)	**10**	Power supply module 2 (PSU-2)
11	Power supply module 2 (PSU-2) connector		Power supply LED (PSU-2)

Power Switch

The power switch is located to the left of PSU-1 on the rear of the chassis. It is a toggle switch that controls power to the system. Turning the switch to OFF starts the graceful shutdown process. During the shutdown process the power LEDs flash green indicating that the process has started. Once the shutdown is complete, the system is powered off. Wait for the system power LEDs to turn off before unplugging the AC power cables. See Front Panel LEDs, on page 11 for the power status LED description.

Note Threat defense requires a graceful shutdown. See the Cisco Secure 4200 Getting Started Guide for the procedure.

Caution If you remove the system power cords before the graceful shutdown is complete, disk corruption can occur. You can move the power switch to OFF before the shutdown. The system ignores it.

Note After removing power from the chassis by unplugging the power cord, wait at least 10 seconds before turning power back ON. You want to keep the system power off, including the standby power, for 10 seconds.

8-Port 1/10/25-Gb Network Module

The Secure Firewall chassis has two network module slots named NM-2 and NM-3 (left to right on the front panel). Network modules are optional, removable I/O modules that provide either additional ports or different interface types. The network module plugs into the chassis on the front panel. See Front Panel, on page 8 for the location of the network module slots on the chassis.

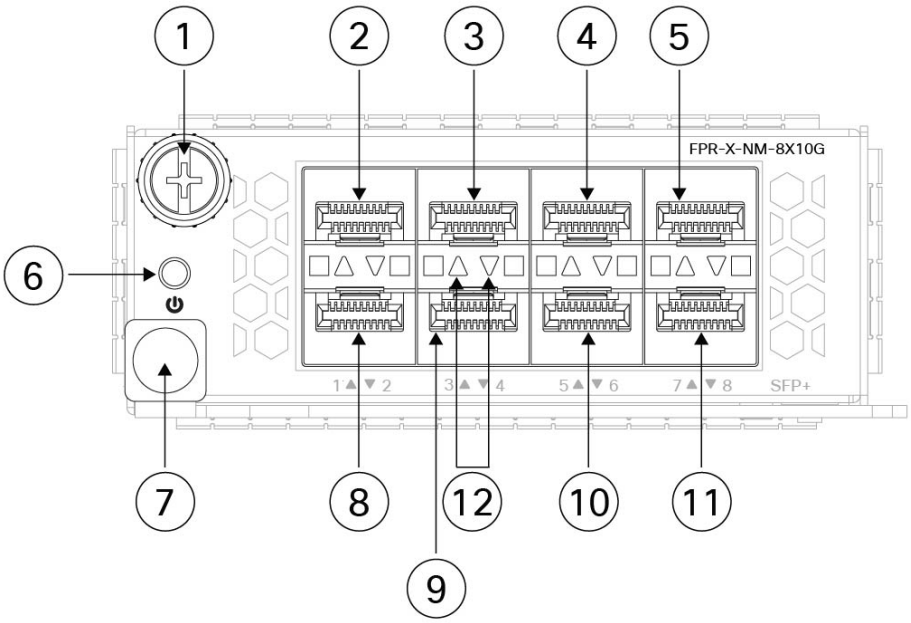
FPR-X-NM-8X10G supports 1 Gb and 10 Gb full-duplex Ethernet traffic per port and is supported on all Secure Firewall 4200s. FPR-X-NM-8X25G supports 1 Gb, 10 Gb, or 25 Gb full-duplex Ethernet traffic per port and is supported on all Secure Firewall 4200s.

The top ports are numbered from left to right—Ethernet 2/1 or 3/1, Ethernet 2/3 or 3/3, Ethernet 2/5 or 3/5, and Ethernet 2/7 or 3/7. The bottom ports are numbered from left to right—Ethernet 2/2 or 3/2, Ethernet 2/4 or 3/4, Ethernet 2/6 or 3/6, and Ethernet 2/8 or 3/8 (see the figure below). Up arrows are the top ports and down arrows are the bottom ports (see the figure below). This network module supports SFP/SFP+/SFP28 transceivers. See Supported SFP/SFP+/QSFP+ Transceivers , on page 33 for the list of Cisco-supported transceivers.

Note The hardware and the system support hot swapping if you are replacing a network module with the same type of network module. You must first disable the network port and then reenable it after replacement. If you replace the 8-port 1/10/25-Gb network module with another supported network module, you must reboot the chassis so that the new network module is recognized. See the configuration guide for your operating system for the detailed procedures for managing network modules.

The following figure shows the front panel of the 1/10-Gb and 1/10/25-Gb network module.

Figure 8: 8-Port 1/10-Gb (FPR-X-NM-8X10G) and 8-Port 1/10/25-Gb (FPR-X-NM-8X25G) Network Module



1	Captive screw	**2**	Ethernet 2/1 or 3/1
3	Ethernet 2/3 or 3/3	**4**	Ethernet 2/5 or 3/5
5	Ethernet 2/7 or 3/7	**6**	Power on LED
7	Ejector handle	**8**	Ethernet 2/2 or 3/2
9	Ethernet 2/4 or 3/4	**10**	Ethernet 2/6 or 3/6
11	Ethernet 2/8 or 3/8	**12**	Network activity LEDs The up arrows represent the top ports and the down arrows represent the bottom ports. • Off—No SFP. • Amber—No link or network failure. • Green—Link up. • Green, flashing—Network activity.

For More Information

- See 4-Port 40-Gb Network Module, on page 17 for a description of the 40-Gb network module.
- See 6-Port 10-Gb SR/10-Gb LR/25-Gb SR/25-Gb LR Network Module with Hardware Bypass , on page 26 for a description of the 1/10/25-Gb network module.
- See 8-Port 1000Base-T Network Module with Hardware Bypass, on page 23 for a description of the 10/100/1000Base-T network module.

- See Install, Remove, and Replace the Network Module, on page 65 for the procedure for removing and replacing network modules.

4-Port 40-Gb Network Module

The Secure Firewall 4200 chassis has two network module slots named NM-2 and NM-3 (left to right on the front panel). Network modules are optional, removable I/O modules that provide either additional ports or different interface types. The network module plugs into the chassis on the front panel. See Front Panel, on page 8 for the location of the network module slots on the chassis.

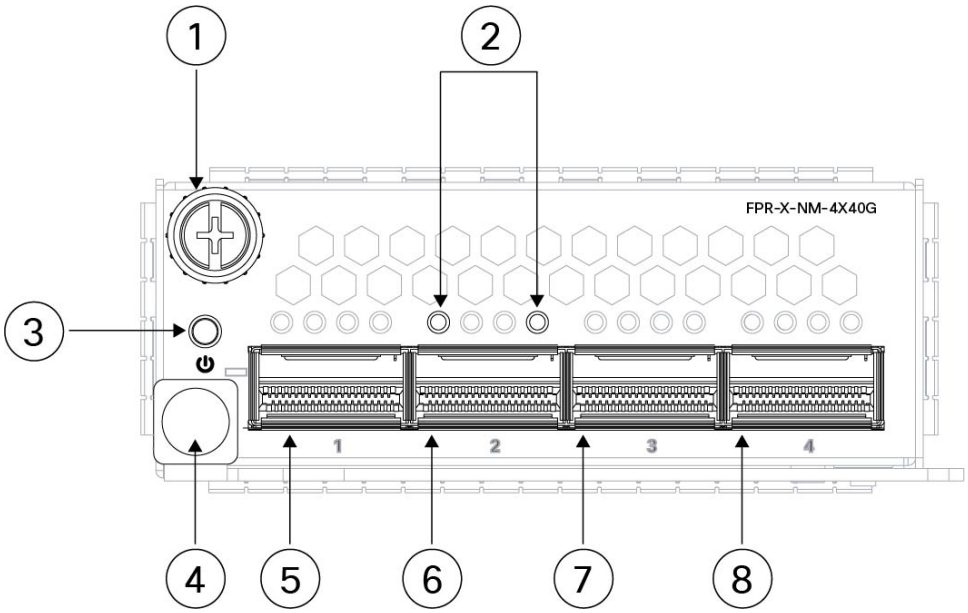
The FPR-X-NM-4X40G supports 40-Gb operation. This network module provides full-duplex Ethernet traffic per port. The 40-Gb network module has four QSFP+ ports. The 40-Gb ports are numbered left to right, Ethernet 2/1 or 3/1 through Ethernet 2/4 or 3/4. See Supported SFP/SFP+/QSFP+ Transceivers , on page 33 for the list of Cisco-supported transceivers.

You can break each of the four 40-Gb ports into four 10-Gb ports using the supported breakout cables (see Supported SFP/SFP+/QSFP+ Transceivers , on page 33 for a list of the breakout cables). With the four-port 40-Gb network module, you now have 16 10-Gb interfaces. The added interfaces are Ethernet 2/1/1 or 3/1/1 through Ethernet 2/4/4 or 3/4/4.

Note The hardware and the system support hot swapping if you are replacing a network module with the same type of network module. If you replace the 4-port 40-Gb network module with another supported network module, you must reboot the chassis so that the new network module is recognized. See the configuration guide for your operating system for the detailed procedures for managing network modules.

The following figure shows the front panel of the 4-port 40-Gb network module.

Figure 9: 4-Port 40-Gb Network Module (FPR-X-NM-4X40G)



1	Captive screw	**2**	Network activity LEDs The up arrows represent the top ports and the down arrows represent the bottom ports. • Off—No SFP. • Amber—No link or a network failure. • Green—Link is up. • Green, flashing—Network activity.
3	Power on LED	**4**	Ejector handle
5	Ethernet 2/1 or 3/1	**6**	Ethernet 2/2 or 3/2
7	Ethernet 2/3 or 3/3	**8**	Ethernet 2/4 or 3/4

For More Information

- See 8-Port 1/10/25-Gb Network Module, on page 15 for a description of the 1/10/25-Gb network module.
- See 6-Port 10-Gb SR/10-Gb LR/25-Gb SR/25-Gb LR Network Module with Hardware Bypass , on page 26 for a description of the 1/10/25-Gb network module.
- See 8-Port 1000Base-T Network Module with Hardware Bypass, on page 23 for a description of the 1-Gb network module.
- See Install, Remove, and Replace the Network Module, on page 65 for the procedure for removing and replacing network modules.

2-Port 100-Gb Network Module

The Secure Firewall 4200 chassis has two network module slots named NM-2 and NM-3 (left to right on the front panel). Network modules are optional, removable I/O modules that provide either additional ports or different interface types. The network module plugs into the chassis on the front panel. See Front Panel, on page 8 for the location of the network module slots on the chassis.

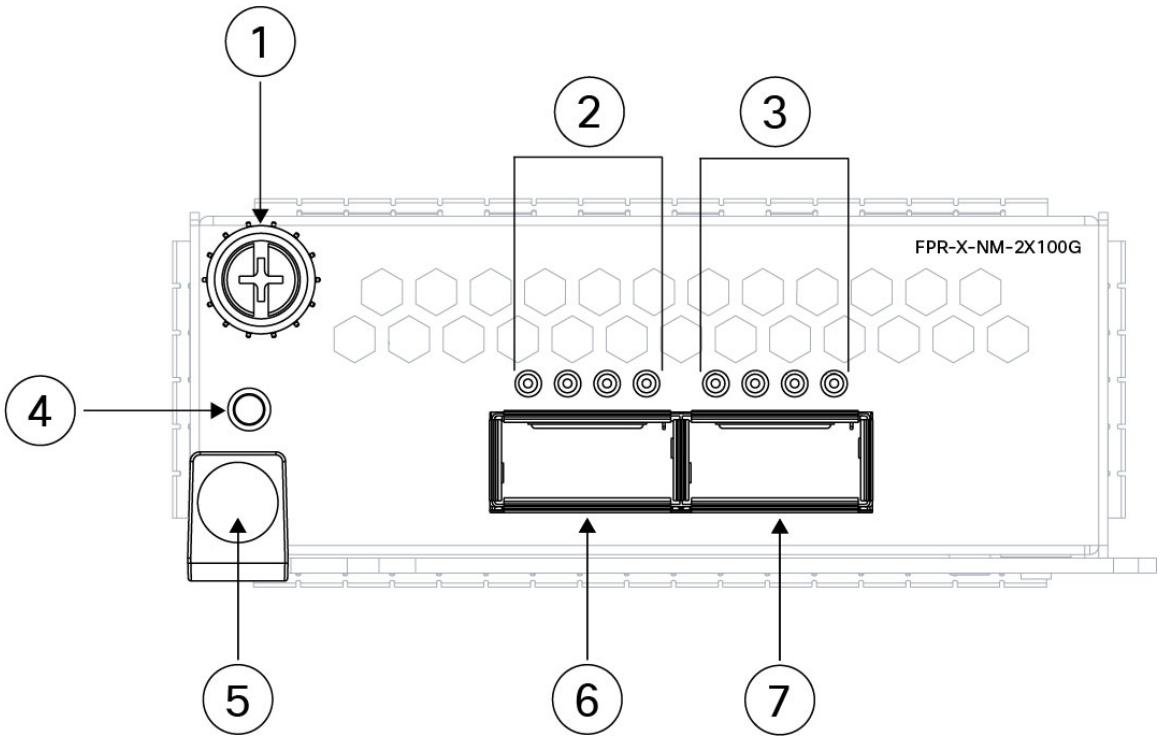
The FPR-X-NM-2X100G supports 40/100-Gb operation. This network module has two QSFP/QSFP28 ports and provides full-duplex Ethernet traffic per port. The maximum bandwidth supported is 200 Gb full duplex, where each port operates at 100 Gb. The 100-Gb ports are numbered left to right, Ethernet 2/1 or 3/1 through Ethernet 2/2 or 3/2. See Supported SFP/SFP+/QSFP+ Transceivers , on page 33 for the list of Cisco-supported transceivers.

You can break each 100-Gb port into four 10-Gb or 25-Gb ports using the supported breakout cables. With the two-port 100-Gb network module, you now have 8 10-Gb or 25-Gb interfaces. The added interfaces are Ethernet 2/1/1 or 3/1/1 through Ethernet 2/1/8 or 3/1/8

Note The hardware and the system support hot swapping if you are replacing a network module with the same type of network module. If you replace the 100-Gb network module with another supported network module, you must reboot the chassis so that the new network module is recognized. See the configuration guide for your operating system for the detailed procedures for managing network modules.

The following figure shows the front panel of the 2-port 100-Gb network module.

Figure 10: 2-Port 100-Gb Network Module (FPR-X-NM-2X100G)



1	Captive screw	**2**	Network activity LEDs • Off—No SFP. • Amber—No link or a network failure. • Green—Link is up. • Green, flashing—Network activity.
3	Network activity LEDs • Off—No SFP. • Amber—No link or a network failure. • Green—Link is up. • Green, flashing—Network activity.	**4**	Power on LED

5	Ejector handle	**6**	Ethernet 2/1 or 3/1
7	Ethernet 2/2 or 3/2		—

For More Information

- See 8-Port 1/10/25-Gb Network Module, on page 15 for a description of the 1/10/25-Gb network module.
- See 6-Port 10-Gb SR/10-Gb LR/25-Gb SR/25-Gb LR Network Module with Hardware Bypass , on page 26 for a description of the 1/10/25-Gb network module.
- See 8-Port 1000Base-T Network Module with Hardware Bypass, on page 23 for a description of the 1-Gb network module.
- See Install, Remove, and Replace the Network Module, on page 65 for the procedure for removing and replacing network modules.

4-Port 200-Gb Network Module

The Secure Firewall 4200 chassis has two network module slots NM-2 and NM-3 (left to right on the front panel). Network modules are optional, removable I/O modules that provide either additional ports or different interface types. The network module plugs into the chassis on the front panel. See Front Panel, on page 8 for the location of the network module slots on the chassis.

The FPR-X-NM-4X200G supports 40/100/200-Gb operation. This network module provides full-duplex Ethernet traffic per port. The 200-Gb network module has four QSFP+ ports. The ports are numbered left to right, Ethernet 2/1 or 3/1 through Ethernet 2/4 or 3/4. See Supported SFP/SFP+/QSFP+ Transceivers , on page 33 for the list of Cisco-supported transceivers.

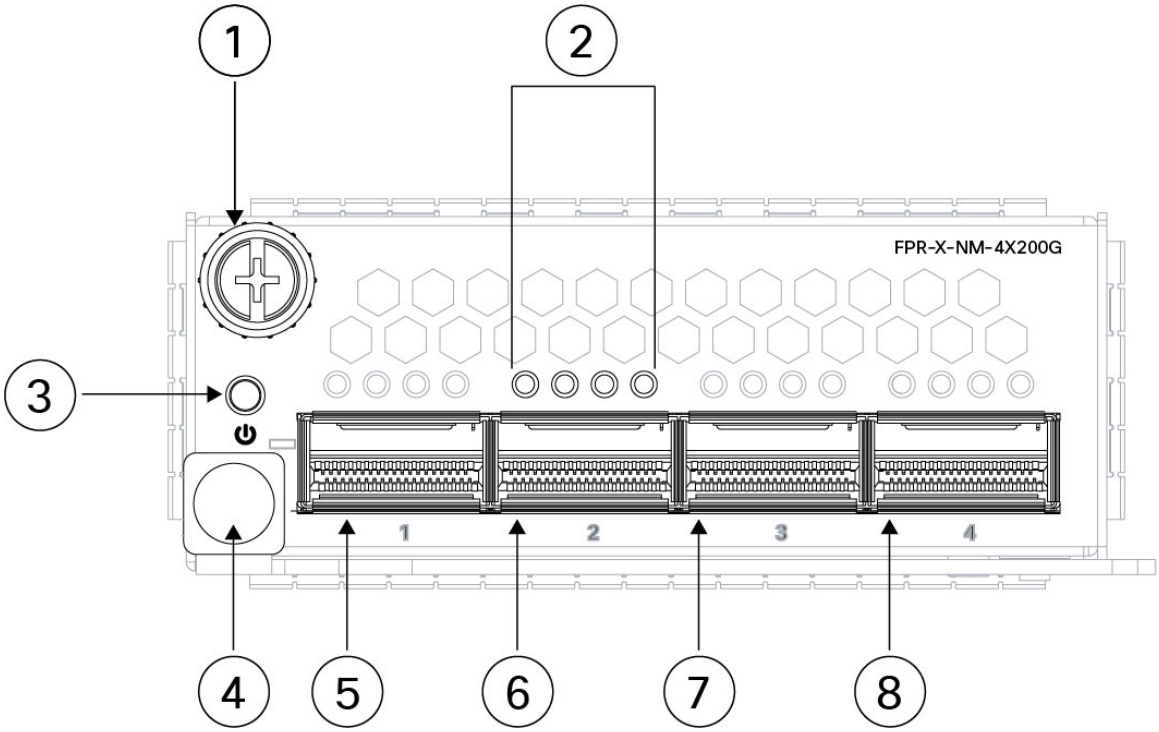
Note The FPR-X-NM-4X200G supports 40/100 Gb operation initially. Support for 200 Gb is added in a future software release.

You can break each 100-Gb port into four 10-Gb or 25-Gb ports using the supported breakout cables. With the two-port 100-Gb network module, you now have 8 10-Gb or 25-Gb interfaces. The added interfaces are Ethernet 2/1/1 or 3/1/1 through Ethernet 2/4/4 or 3/4/4.

Note The hardware and the system support hot swapping if you are replacing a network module with the same type of network module. If you replace the 4-port 200-Gb network module with another supported network module, you must reboot the chassis so that the new network module is recognized. See the configuration guide for your operating system for the detailed procedures for managing network modules.

The following figure shows the front panel of the 4-port 200-Gb network module.

Figure 11: 4-Port 200-Gb Network Module (FPR-X-NM-4X200G)



1	Captive screw	**2**	Network activity LEDs The up arrows represent the top ports and the down arrows represent the bottom ports. • Off—No SFP. • Amber—No link or a network failure. • Green—Link is up. • Green, flashing—Network activity.
3	Power on LED	**4**	Ejector handle
5	Ethernet 2/1 or 3/1	**6**	Ethernet 2/2 or 3/2
7	Ethernet 2/3 or 3/3	**8**	Ethernet 2/4 or 3/4

For More Information

- See 8-Port 1/10/25-Gb Network Module, on page 15 for a description of the 8-port 1/10/25-Gb network module.
- See 8-Port 1000Base-T Network Module with Hardware Bypass, on page 23 for a description of the 8-port 10/100/1000Base-T network module.
- See Install, Remove, and Replace the Network Module, on page 65 for the procedure for removing and replacing network modules.

2-Port 400-Gb Network Module

The Secure Firewall 4200 chassis has two network module slots named NM-2 and NM-3 (left to right on the front panel). Network modules are optional, removable I/O modules that provide either additional ports or different interface types. The network module plugs into the chassis on the front panel. See Front Panel, on page 8 for the location of the network module slots on the chassis.

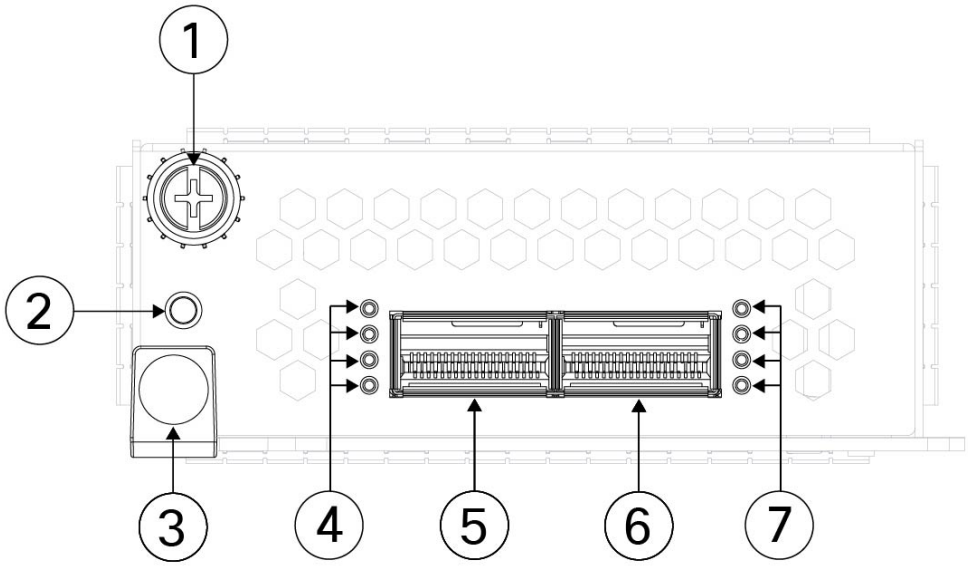
Note The FPR-X-NM-2X400G is first supported in FTD 7.6 and ASA 9.22.1.

The FPR-X-NM-2X400G supports 400-Gb operation, and is also designed to support 200-Gb, 100-Gb, and 40-Gb per port. This network module provides full-duplex Ethernet traffic per port. The 400-Gb network module supports two QSFP-DD transceivers and is designed to also support 200-Gb QSFP56, 100-Gb QSFP28, and 40-Gb QSFP+ transceivers. The 400-Gb ports are numbered left to right, Ethernet 2/1 or 3/1 through Ethernet 2/2 or 3/2. See Supported SFP/SFP+/QSFP+ Transceivers , on page 33 for the full list of Cisco-supported transceivers.

Note The hardware and the system support hot swapping if you are replacing a network module with the same type of network module. If you replace the 2-port 400-Gb network module with another supported network module, you must reboot the chassis so that the new network module is recognized. See the configuration guide for your operating system for the detailed procedures for managing network modules.

The following figure shows the front panel of the 2-port 400-Gb network module.

Figure 12: 2-Port 400-Gb Network Module (FPR-X-NM-2X400G)



1	Captive screw	**2**	Power on LED

3	Ejector handle	**4**	Network activity LEDs • Off—No SFP. • Amber—No link or a network failure. • Green—Link is up. • Green, flashing—Network activity.
5	Ethernet 2/1 or 3/1	**6**	Ethernet 2/2 or 3/2
5	Network activity LEDs • Off—No SFP. • Amber—No link or a network failure. • Green—Link is up. • Green, flashing—Network activity.	**6**	—

For More Information

- See 8-Port 1/10/25-Gb Network Module, on page 15 for a description of the 1/10/25-Gb network module.
- See 6-Port 10-Gb SR/10-Gb LR/25-Gb SR/25-Gb LR Network Module with Hardware Bypass , on page 26 for a description of the 1/10/25-Gb network module.
- See 8-Port 1000Base-T Network Module with Hardware Bypass, on page 23 for a description of the 1-Gb network module.
- See Install, Remove, and Replace the Network Module, on page 65 for the procedure for removing and replacing network modules.

8-Port 1000Base-T Network Module with Hardware Bypass

The Secure Firewall 4200 chassis has two network module slots named NM-2 and NM-3 (left to right on the front panel). Network modules are optional, removable I/O modules that provide either additional ports or different interface types. The network module plugs into the chassis on the front panel. See Front Panel, on page 8 for the location of the network module slots on the chassis.

FPR4K-XNM-8X1GF is an 8-port 1000Base-T hardware bypass network module. The eight ports are numbered from top to bottom, left to right. Ports 1 and 2, 3 and 4, 5 and 6, and 7 and 8 are paired for hardware bypass mode. In hardware bypass mode, data is not processed by the Secure Firewall 4200 but is routed to the paired port.

Hardware bypass (also known as fail-to-wire) is a physical layer (Layer 1) bypass that allows paired interfaces to go into bypass mode so that the hardware forwards packets between these port pairs without software intervention. Hardware bypass provides network connectivity when there are software or hardware failures. Hardware bypass is useful on ports where the secure firewall is only monitoring or logging traffic. The hardware bypass network modules have a switch that is capable of connecting the two ports when needed.

Note Hardware bypass is only supported with threat defense, although you can use these modules in nonbypass mode in threat defense or ASA.

Hardware bypass is supported only on a fixed set of ports. You can pair Port 1 with Port 2, Port 3 with Port 4, but you cannot pair Port 1 with Port 4 for example.

Note When the appliance switches from normal operation to hardware bypass or from hardware bypass back to normal operation, traffic may be interrupted for several seconds. A number of factors can affect the length of the interruption; for example, behavior of the link partner such as how it handles link faults and debounce timing; spanning tree protocol convergence; dynamic routing protocol convergence; and so on. During this time, you may experience dropped connections.

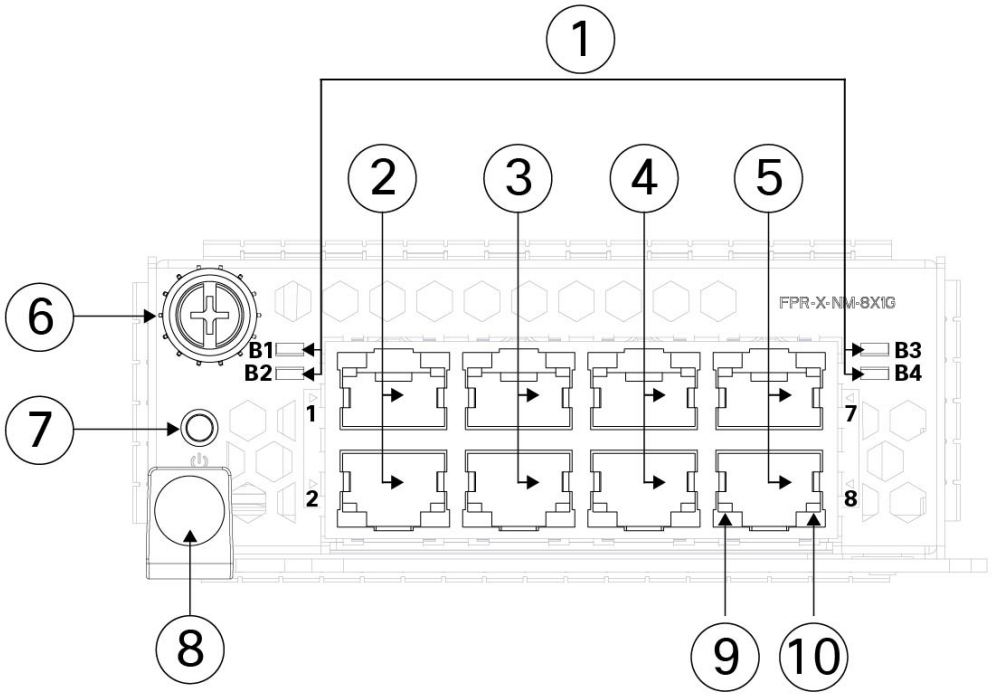
Note If you have an inline interface set with a mix of hardware bypass and nonhardware bypass interfaces, you cannot enable hardware bypass on this inline interface set. You can only enable hardware bypass on an inline interface set if all the pairs in the inline set are valid hardware bypass pairs.

Note The hardware and the system support hot swapping if you are replacing a network module with the same type of network module. If you replace the 8-port 10/100/1000Base-T network module with another supported network module, you must reboot the chassis so that the new network module is recognized. See the configuration guide for your operating system for the detailed procedures for managing network modules.

Note Make sure you have the correct firmware package and software version installed to support this network module. See the configuration guide for your software for the procedures for updating the firmware package and verifying the software version. See the Cisco Secure Firewall Threat Defense Compatibility Guide and the Cisco Secure Firewall ASA Compatibility guide, which provide Cisco software and hardware compatibility, including operating system and hosting environment requirements, for each supported version.

The following figure shows the front panel of the 8-port 1000Base-Tnetwork module.

Figure 13: 8-Port 1000Base-T Network Module (FPR-X-NM-8X1GF)



1	Bypass LEDs B1 through B4 • Green—In standby mode. • Amber, flashing—Port is in hardware bypass mode, failure event.	**2**	Ethernet 2/1 and 2/2 or Ethernet 3/1 and 3/2 Ports 1 and 2 are paired together to form a hardware bypass pair. LED B1 applies to this paired port.
3	Ethernet 2/3 and Ethernet 2/4 or Ethernet 3/3 and 3/4 Ports 3 and 4 are paired together to form a hardware bypass pair. LED B2 applies to this paired port.	**4**	Ethernet 2/5 and 2/6 or Ethernet 3/5 and 3/6 Ports 5 and 6 are paired together to form a hardware bypass pair. LED B3 applies to this paired port.
5	Ethernet 2/7 and 2/8 or Ethernet 3/7 and 3/8 Ports 7 and 8 are paired together to form a hardware bypass pair. LED B4 applies to this paired port.	**6**	Captive screw
7	Power LED	**8**	Handle
9	Left Port LED • Unlit—No connection or port is not in use. • Green—Link up. • Green, flashing—Network activity.	**10**	Right Port LED • Unlit—No connection or port is not in use. • Green—Link up. • Green, flashing—Network activity.

For More Information

- See 6-Port 10-Gb SR/10-Gb LR/25-Gb SR/25-Gb LR Network Module with Hardware Bypass , on page 26 for a description of the 1/10/25-Gb network module.
- See 4-Port 40-Gb Network Module, on page 17 for a description of the 40-Gb network module.
- See 8-Port 1/10/25-Gb Network Module, on page 15 for a description of the 1/10/25-Gb network module.
- See Install, Remove, and Replace the Network Module, on page 65 for the procedure for removing and replacing network modules.

6-Port 10-Gb SR/10-Gb LR/25-Gb SR/25-Gb LR Network Module with Hardware Bypass

The Secure Firewall 4200 chassis has two network module slots named NM-2 and NM-3 (left to right on the front panel). Network modules are optional, removable I/O modules that provide either additional ports or different interface types. The network module plugs into the chassis on the front panel. See Front Panel, on page 8 for the location of the network module slots on the chassis.

The FPR-X-NM-6X10SRF, FPR-X-NM-6X10LRF, FPR-X-NM-6X25SRF, and FPR-X-NM-6X25LRF hardware bypass network modules have six ports that are numbered from top to bottom, left to right. Pair ports 1 and 2, 3 and 4, and 5 and 6 to form hardware bypass paired sets. In hardware bypass mode, data is not processed by the Secure Firewall 4200 but is routed to the paired port. This network module has built-in SPF transceivers. Hot swapping and field replacement of transceivers are not supported.

Hardware bypass (also known as fail-to-wire) is a physical layer (Layer 1) bypass that allows paired interfaces to go into bypass mode so that the hardware forwards packets between these port pairs without software intervention. Hardware bypass provides network connectivity when there are software or hardware failures. Hardware bypass is useful on ports where the secure firewall is only monitoring or logging traffic. The hardware bypass network modules have a switch that is capable of connecting the two ports when needed. This hardware bypass network module has built-in SFPs.

Note Hardware bypass is only supported with threat defense, although you can use these modules in nonbypass mode in threat defense or ASA.

Hardware bypass is supported only on a fixed set of ports. You can pair Port 1 with Port 2, Port 3 with Port 4, but you cannot pair Port 1 with Port 4 for example.

Note When the appliance switches from normal operation to hardware bypass or from hardware bypass back to normal operation, traffic may be interrupted for several seconds. A number of factors can affect the length of the interruption; for example, behavior of the link partner such as how it handles link faults and debounce timing; spanning tree protocol convergence; dynamic routing protocol convergence; and so on. During this time, you may experience dropped connections.

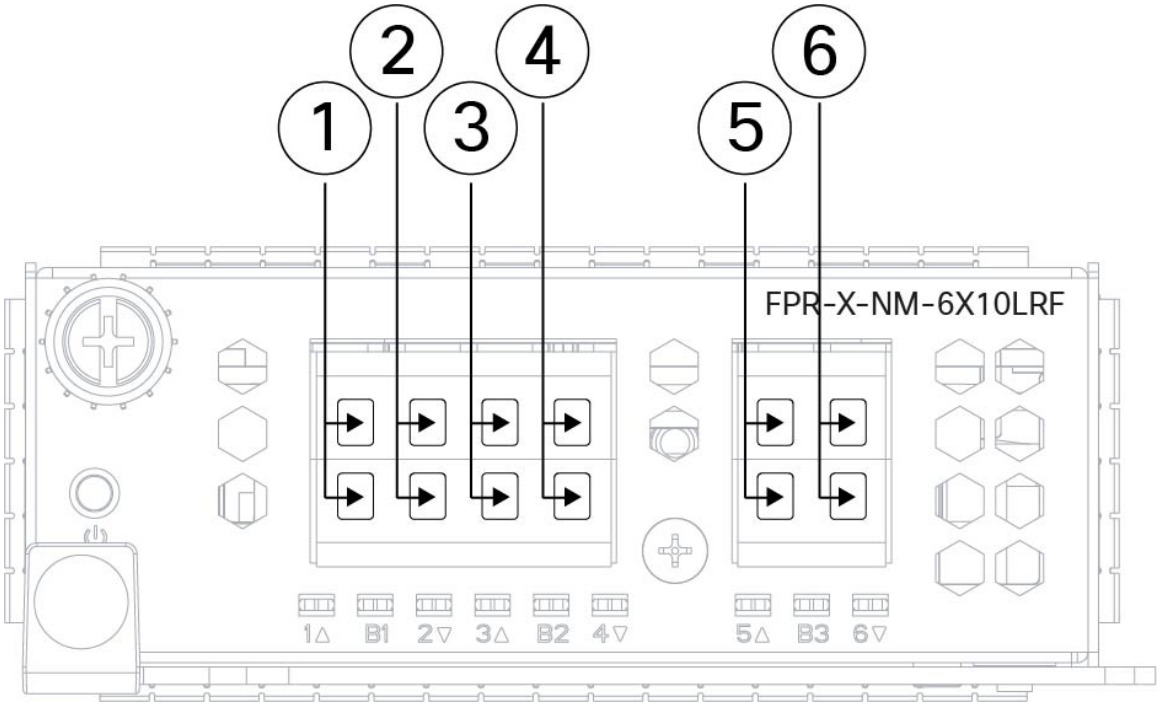
Note If you have an inline interface set with a mix of hardware bypass and nonhardware bypass interfaces, you cannot enable hardware bypass on this inline interface set. You can only enable hardware bypass on an inline interface set if all the pairs in the inline set are valid hardware bypass pairs.

Note The hardware and the system support hot swapping if you are replacing a network module with the same type of network module. If you replace the 6-port 1/10/25-Gb network module with another supported network module, you must reboot the chassis so that the new network module is recognized. See the configuration guide for your operating system for the detailed procedures for managing network modules.

Note Make sure you have the correct firmware package and software version installed to support this network module. See the configuration guide for your software for the procedure to verify your firmware package and software version. See the Cisco Secure Firewall Threat Defense Compatibility Guide and the Cisco Secure Firewall ASA Compatibility guide, which provide Cisco software and hardware compatibility, including operating system and hosting environment requirements, for each supported version

The following figure shows the front panel of the 6-port 1/10/25-Gb network module.

Figure 14: 6-Port 1/10/25-Gb Network Module (FPR-X-NM-6X10SRF, FPR-X-NM-6X10LRF, FPR-X-NM-6X25SRF, and FPR-X-NM-6X25LRF)



1	Ethernet 2/1 or 3/1 (top port) Ethernet 2/2 or 3/2 (bottom port) Ports 1 and 2 are paired together to form a hardware bypass pair.	**2**	Ethernet 2/3 or 3/3 (top port) Ethernet 2/4 or 3/4 (bottom port) Ports 3 and 4 are paired together to form a hardware bypass pair.
3	Ethernet 2/5 or 3/5 (top port) Ethernet 2/6 or 3/6 (bottom port) Ports 5 and 6 are paired together to form a hardware bypass pair.	**4**	Ethernet 2/7 or 3/7 (top port) Ethernet 2/8 or 3/8 (bottom port) Ports 7 and 8 are paired together to form a hardware bypass pair.
5	Ethernet 2/9 or 3/9 (top port) Ethernet 2/10 or 3/10 (bottom port) Ports 9 and 10 are paired together to form a hardware bypass pair.	**6**	Ethernet 2/11 or 3/11 (top port) Ethernet 2/12 or 3/12 (bottom port) Ports 11 and 12 are paired together to form a hardware bypass pair.
7	Bypass LEDs B1 through B3: • Off—Bypass mode is disabled. • Green—Port is in standby mode. • Amber, flashing—Port is in hardware bypass mode, failure event.	**8**	Captive screw
9	Power LED	**10**	Handle ejector
11	Six network activity LEDs: • Amber—No connection, or port is not in use, or no link or network failure. • Green—Link up, no network activity. • Green, flashing—Network activity.		—

For More Information

- See 8-Port 1000Base-T Network Module with Hardware Bypass, on page 23 for a description of the 1-Gb network module.
- See 8-Port 1/10/25-Gb Network Module, on page 15 for a description of the 1/10/25-Gb network module.
- See 4-Port 40-Gb Network Module, on page 17 for a description of the 40-Gb network module.
- See Install, Remove, and Replace the Network Module, on page 65 for the procedure for removing and replacing network modules.

Power Supply Module

The Secure Firewall 4200 supports two AC power supply modules so that dual power supply redundancy protection is available. Facing the back of the chassis, the power supply modules are numbered left to right—PSU-1 and PSU-2.

The power supply module is hot-swappable.

Note After removing power from the chassis by unplugging the power cord, wait at least 10 seconds before turning power back ON. You want to keep the system power off, including the standby power, for 10 seconds.

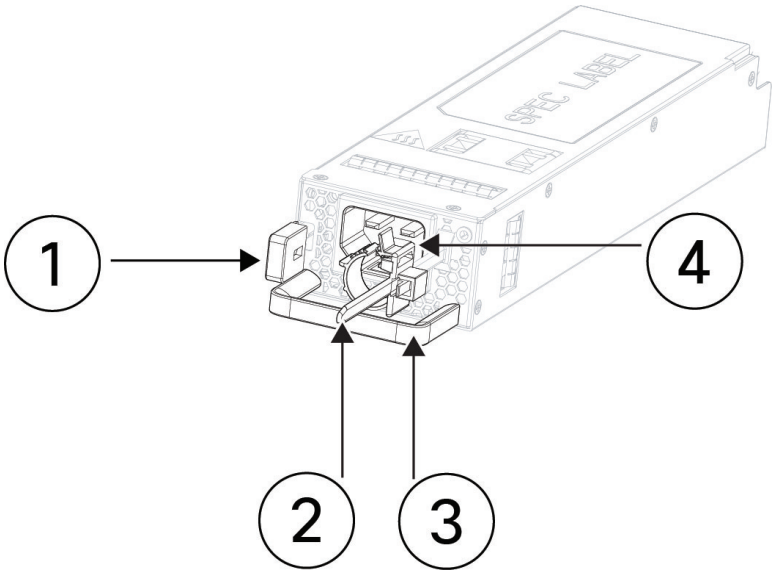
Attention Make sure that one power supply module is always active.

AC Power Supply

The dual power supplies can supply up to 1900-W power across the input voltage range. The load is shared when both power supply modules are plugged in and running at the same time.

Note The system does not consume more than the capacity of one power supply module, so it always operates in full redundancy mode when two power supply modules are installed.

Figure 15: Power Supply Module



1	Release tab	**2**	Cord retention mechanism
3	Handle	**4**	Power cord connector

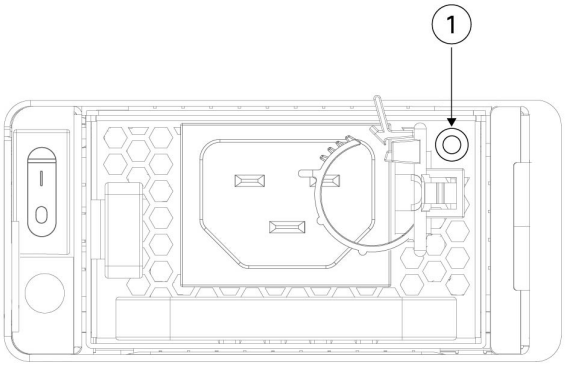
Table 2: AC Power Supply Module Hardware Specifications

Specification	4215	4225	4245
Dimensions	1.575 x 2.657 x 9.92 inches (40.0 x 67.5 x 252 mm)		
Hot-swappable	Yes		
Redundancy	1+1 maximum in parallel		
Input voltage	100 to 120 VAC (low line) 200 to 240 VAC (high line)		Only 200 to 240 VAC (high line)
Input current (maximum)	14 A at 100 VAC or 13 A at 200 VAC		
Input voltage frequency	50 to 60 Hz (nominal)		
Output main voltage at current	12 V +/- 5% at 100 A (low line) 12 V +/- 5% at 158 A (high line)		
Output standby voltage at current	12 V at 2.5 A		
Output power	1200 W (low line) 1900 W (high line)		
Energy efficiency	> 90% (platinum)		
Temperature (operating)	100% load at 6000 ft (1828.8 m): 23 to 113 °F (-5 to 45°C) 100% load at 10000 ft (3000 m): 23 to 95°F (-5 to 35°C)		
Temperature (nonoperating)	-40 to 158°F (-40 to 70°C)		
Altitude (nonoperating)	-1000 to 40000 ft (-305 to 12200 m)		
Humidity (operating and nonoperating)	5 to 90% (noncondensing)		

Power Supply Module LED

The following figure shows the bicolor power supply LED on the AC power supply module.

Figure 16: Power Supply Module LED



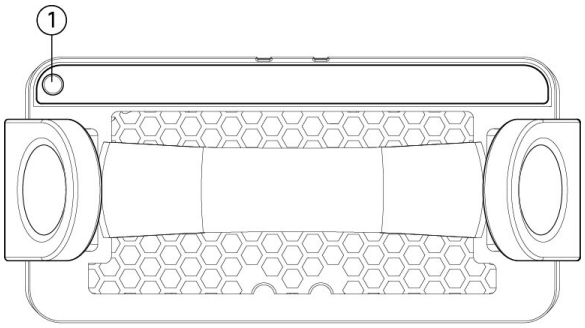
1	Power supply LED • Active mode—Green • Standby mode—Green, flashing • Boot loading process—Green, flashing • No AC power, but the other power supply module in the system is operating—Amber • Fan fault—Amber • No input power—Off

Dual Fan Modules

The Secure Firewall 4200 has three dual fan modules. There are two fans per module and each fan has dual rotors. When one fan fails, the other dual fan modules spin at maximum speed so that the system continues to function. The dual fan modules are hot-swappable and installed in the rear of the chassis.

The following figure shows the location of the fan LED on the fan module.

Figure 17: Fan LED



1	Two-color LED

The fan module has one two-color LED, which is located on the upper left corner of the fan.

- Off—No power or the system is powering up.
- Green—Fans are running normally. It may take up to one minute for the LED status to turn green after power is on.
- Amber, flashing—One or more fan rotor RPMs is not normal. Immediate attention is required.
- Amber—One or more fan rotors have failed. The system can continue to operate normally, but fan service is required.

For More Information

- See Product ID Numbers, on page 38 for a list of the PIDs associated with the Secure Firewall 4200 fans.
- See Remove and Replace the Dual Fan Module, on page 68 for the procedure for removing and replacing the dual fan modules.

SSDs

The Secure Firewall 4200 has two SSD slots that each hold one NVMe 1.8-TB SSD. By default the Secure Firewall 4200 ships with two 1.8-TB SSDs installed in slot 1 and slot 2. Software RAID1 is shipped already configured.

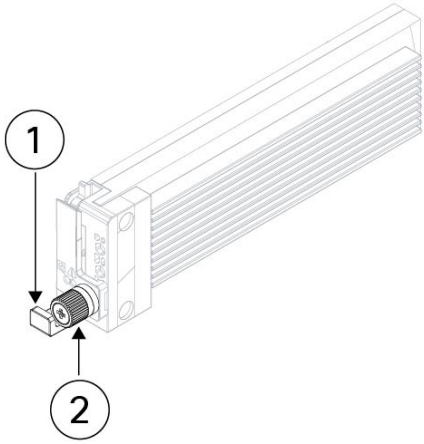
Hot swapping is supported. You can swap SSDs without powering off the chassis. However, before hot swapping SSDs you must issue the **raid remove-secure local-disk 1|2** command to prepare the SSD for removal. This command preserves the data on the SSD. After you remove and replace the SSD, you must add it again to the RAID1 configuration using the **raid add local-disk 1|2** command. See Hot Swap an SSD on the Secure Firewall 3100/4200 for the procedures for safely removing an SSD.

Caution The **raid remove-secure local disk** command securely erases the specified SSD data.

Caution You cannot swap SSDs between different platforms. For example, you cannot use a 3100 series SSD in a 4200 series model.

The SSD drive identifiers are `disk0:` and `disk1:`.

Figure 18: SSD

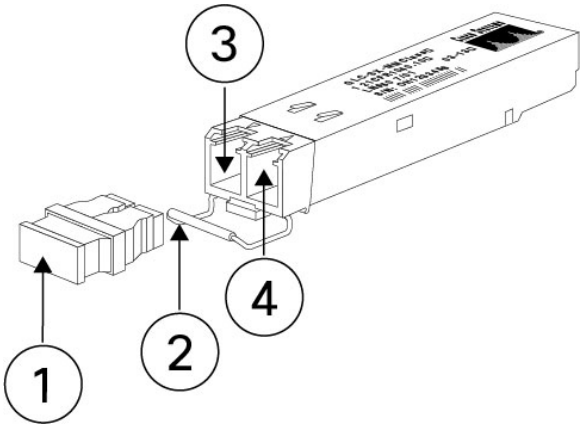


1	SSD release tab		Captive screw

Supported SFP/SFP+/QSFP+ Transceivers

The SFP/SFP+/QSFP+ transceiver is a bidirectional device with a transmitter and receiver in the same physical package. It is a hot-swappable optical or electrical (copper) interface that plugs into the SFP/SFP+/QSFP+ ports on the fixed ports and the network module ports, and provides Ethernet connectivity.

Figure 19: SFP Transceiver



1	Dust plug	**2**	Bail clasp
3	Receive optical bore	**4**	Transmit optical bore

Safety Warnings

Take note of the following warnings:

Warning **Statement 1055**—Class 1/1M Laser

Invisible laser radiation is present. Do not expose to users of telescopic optics. This applies to Class 1/1M laser products.

Warning **Statement 1056**—Unterminated Fiber Cable

Invisible laser radiation may be emitted from the end of the unterminated fiber cable or connector. Do not view directly with optical instruments. Viewing the laser output with certain optical instruments, for example, eye loupes, magnifiers, and microscopes, within a distance of 100 mm, may pose an eye hazard.

Warning **Statement 1057**—Hazardous Radiation Exposure

Use of controls, adjustments, or performance of procedures other than those specified may result in hazardous radiation exposure.

Warning Use appropriate ESD procedures when inserting the transceiver. Avoid touching the contacts at the rear, and keep the contacts and ports free of dust and dirt. Keep unused transceivers in the ESD packing that they were shipped in.

Caution Although non-Cisco SFPs are allowed, we do not recommend using them because they have not been tested and validated by Cisco. Cisco TAC may refuse support for any interoperability problems that result from using an untested third-party SFP transceiver.

The following table lists the supported transceivers for the fixed ports on all 4200 models, and the FPR4K-XNM-8X10G and FPR4K-XNM-8X25G network modules.

Table 3: Supported 1-Gb SFP Transceivers

Optics Type	PID	Comments
1G, 1000Base-T	GLC-TE	1 Gb-copper SFP version
1G multimode	GLC-SX-MMD	850 nm
1G single mode	GLC-LH-SMD	1310 nm
1G SM extended r.	GLC-EX-SMD	40 km
1G SM	GLC-ZX-SMD	80 km

The following table lists the supported transceivers for the fixed ports on all 4200 models, and the FPR4K-XNM-8X10G and FPR4K-XNM-8X25G network modules.

Table 4: Supported 10-Gb SFP Transceivers

Optics Type	PID	Comments
10G-SR	SFP-10G-SR	—
10G-SR	SFP-10G-SR-S	Ethernet only
10G-LR	SFP-10G-LR	—
10G-LR	SFP-10G-LR-S	Ethernet only
10G-ER	SFP-10G-ER-S	—
10G-ER	SFP-10G-ER-S	Ethernet only
10G-ZR	SFP-10G-ZR	—
10G-ZR	SFP-10G-ZR-S	—
10G DAC copper	SFP-H10GB-CUxM	Length 1, 1.5, 2, 2.5, 3, 4, 5 m
10G DAC CU active	QSFP-4X10G-ACUxM	Length 7 and 10 m **Note** You can install the SFP end of the cable in the network modules and chassis ports specified in the introduction sentence of this table. See the 40-Gb and 100-Gb tables for compatibility with the QSFP end of the cable.
10G AOC	SFP-10G-AOCxM	Length 1, 2, 3, 5, 7, 10 m

The following table lists the supported transceivers for the fixed ports on all 4200 models and the FPR4K-X-NM-8X25G network module.

Table 5: Supported 25-Gb SFP Transceivers

Optics Type	PID	Comments
25G-SR	SFP-25G-SR-S	—
25G-CSR	SFP-10/25G-CSR-S	Dual rate, longer reach
25G-LR	SFP-10/25G-LR-S	Dual rate

Optics Type	PID	Comments
25G DAC copper	QSFP-4SFP25G-CUxM	Length 1, 2, 3, 5 m **Note** You can install the SFP end of the cable in the network modules and chassis ports specified in the introduction sentence of this table. See the 40-Gb and 100-Gb tables for compatibility with the QSFP end of the cable.
25G AOC	SFP-25G-AOCxM	Length 1, 2, 3, 4, 5, 7, 10 m

The following table lists the supported transceivers for the FPR4K-X-NM-4X40G, FPR4K-X-NM-2X100G, and FPR4K-X-NM-4X2000G network modules.

Table 6: Supported 40-Gb SFP Transceivers for FPR4K-X-NM-4X40G, FPR4K-X-NM-2X100G, and FPR4K-X-NM-4X200G

Optics Type	PID	Comments
40G-SR4	QSFP-40G-SR4	—
40G-SR4-S	QSFP-40G-SR4-S	Ethernet only
40G-CSR4	QSFP-40G-CSR4	300 m with OM3
40G-SR-BD	QSFP-40G-SR-BD	LC connector
40G-LR4-S	QSFP-40G-LR4-S	Ethernet only
40G-LR4	QSFP-40G-LR4	Ethernet and OTU3
40G-LR4L	WSP-Q40GLR4L	LR4 Lite, up to 2 km
40G-CU	Cisco QSFP-H40G-CUxM	QSFP to QSFP copper direct-attach cables (passive); length 1, 3, 5 m
40G-CU-breakout	QSFP-4SFP10G-CUxM	QSFP to 4xSFP copper direct-attach cables; length 1, 2, 3, 4, 5 m
40G-CU-A	Cisco QSFP-H40G-ACUxM	QSFP to QSFP copper direct-attach cables (active); length 7, 10 m
40G-CU-A-breakout	Cisco QSFP-4X10G-ACUxM	QSFP to QSFP copper direct-attach cables (active); length 7, 10 m

Optics Type	PID	Comments
40G-AOC	QSFP-H40G-AOCxM	QSFP to QSFP active optical cables; length 1, 2, 3, 5, 7, 10, 15, 30 m

The following table lists the supported transceivers for the FPR4K-X-NM-2X100G and FPR4K-X-NM-4X2000G network modules.

Table 7: Supported 100-Gb QSFP Transceivers for FPR4K-X-NM-2X100G and FPR4K-X-NM-4X200G

Optics Type	PID	Comments
100G-SR4	QSFP-100G-SR4-S	100GBASE SR4 QSFP, MPO, 100 m over OM4 MMF
100G-LR4	QSFP-100G-LR4-S	100GBASE LR4 QSFP, LC, 10 km over SMF
40/100G	QSFP-40/100G-SRBD	100 m OM4, LC connector
100G-AOC	QSFP-100G-AOCxM	Multimode up to 30 m (direct attach); length 1, 2, 3, 5, 7, 10,15, 20, 25, 30 m
100G-CR4	QSFP-100G-CUxM	100G copper up to 5 m (direct attach); length 1, 2, 3, 5 m
100G-CR4 breakout	QSFP-4SFP25G-CUxM	100G copper breakout; length 1, 2, 3, 5 m)
100G-FR	QSFP-100G-FR-S	100GBASE FR QSFP transceiver, 2 km over SMF, LC connector
100G-DR	QSFP-100G-DR-S	100GBASE DR QSFP transceiver, 500 m over SMF, LC connector

Hardware Specifications

The following table contains hardware specifications for the Secure Firewall 4200.

Table 8: Secure Firewall 4200 Hardware Specifications

Specification	4215	4225	4245
Chassis dimensions (H x W x D)	1.73 x 16.89 x 32.0 inches (4.39 x 42.9 x 81.28 cm)		
Network module dimensions (H x W x D)	1.41 x 3.66 x 9.94 inches (3.58 x 9.3 x 25.25 cm)		

Specification	4215	4225	4245
Chassis weight (2 power supplies, 2 network modules, 3 fan modules)	43 lb (19.5 kg)	43 lb (19.5 kg)	46 lb (20.8 kg)
Chassis weight (*no* powers supplies, *no* network modules, *no* fan modules)	33 lb (15 kg)	33 lb (15 kg)	36 lb (16.3 kg)
System input power	770 W	870 W	1380 W
Temperature	Operating: 32 to 104°F (-0 to 40°C) Nonoperating: -40 to 149°F (-40 to 65°C) maximum altitude is 40,000 ft		
Humidity	Operating: 5 to 90% noncondensing Nonoperating: 5 to 90% noncondensing		
Altitude	Operating: 0 to 10,000 ft (0 to 1829 m) maximum Nonoperating: 40,000 ft (12,192 m) maximum		
Sound pressure	<=78 dBA (typical) <= 84 dBA (maximum)		
Sound power	<=87 dB (typical) <=92 dB (maximum)		

Product ID Numbers

The following table lists the product IDs (PIDs) associated with the Secure Firewall 4200. All of the PIDs in the table are field-replaceable. If you need to get a return material authorization (RMA) for any component, see Cisco Returns Portal for more information.

Note See the **show inventory** command in the Cisco Firepower Threat Defense Command Reference or the Cisco ASA Series Command Reference to display a list of the PIDs for your Secure Firewall 4200.

Table 9: Secure Firewall 4200 PIDs

PID	Description
Chassis	
FPR4215-ASA-K9	Cisco Secure Firewall 4215 ASA chassis 1 RU

PID	Description
FPR4225-ASA-K9	Cisco Secure Firewall 4225 ASA chassis 1 RU
FPR4245-ASA-K9	Cisco Secure Firewall 4245 ASA chassis 1 RU
FPR4215-NGFW-K9	Cisco Secure Firewall 4215 next generation firewall chassis 1 RU
FPR4225-NGFW-K9	Cisco Secure Firewall 4225 next generation firewall chassis 1 RU
FPR4245-NGFW-K9	Cisco Secure Firewall 4245 next generation firewall chassis 1 RU
Accessories	
FPR4200-ACC-KIT=	Accessory kit (spare)
FPR4200-PWR-AC	AC power supply
FPR4200-PWR-AC=	AC power supply (spare)
FPR4200-PSU-BLANK	Power supply blank slot cover
FPR4200-PSU-BLANK=	Power supply blank slot cover (spare)
FPR4200-SSD1800	1800 GB SSD
FPR4200-SSD1800=	1800 GB SSD (spare)
FPR4200-FAN	Dual fan module
FPR4200-FAN=	Dual fan module (spare)
FPR4200-SLD-RAILS	Slide rail kit
FPR4200-SLD-RAILS=	Slide rail kit (spare)
FPR4200-CBL-MGMT	Cable management brackets
FPR4200-CBL-MGMT=	Cable management brackets (spare)
FPR4200-FIPS-KIT	FIPS opacity shield; covers the serial number on the chassis
FPR4200-FIPS-KIT=	FIPS opacity shield; covers the serial number on the chassis (spare)
Network Modules	
FPR4K-XNM-6X10SRF	6-port 10-Gb SFP hardware bypass network module, SR multimode
FPR4K-XNM-6X10SRF=	6-port 10-Gb SFP hardware bypass network module, SR multimode (spare)

PID	Description
FPR4K-XNM-6X10LRF	6-port 10-Gb SFP hardware bypass network module, LR single mode
FPR4K-XNM-6X10LRF=	6-port 10-Gb SFP hardware bypass network module, LR single mode (spare))
FPR4K-XNM-6X25SRF	6-port 25-Gb SFP hardware bypass network module, SR multimode
FPR4K-XNM-6X25SRF=	6-port 25-Gb SFP hardware bypass network module, SR multimode (spare)
FPR4K-XNM-6X25LRF	6-port 25-Gb SFP hardware bypass network module, LR single mode
FPR4K-XNM-6X25LRF=	6-port 25-Gb SFP hardware bypass network module, LR single mode (spare)
FPR4K-XNM-8X1GF	8-port 1000Base-10 hardware bypass network module
FPR4K-XNM-8X1GF=	8-port 1000Base-10 hardware bypass network module (spare)
FPR4K-XNM-8X10G	8-port 1/10-Gb SFP+ network module
FPR4K-XNM-8X10G=	8-port 1/10-Gb SFP+ network module (spare)
FPR4K-XNM-8X25G	8-port 1/10/25-Gb SFP network module
FPR4K-XNM-8X25G=	8-port 1/10/25-Gb SFP network module (spare)
FPR4K-XNM-4X40G	4-port 40-Gb QSFP+ network module
FPR4K-XNM-4X40G=	4-port 40-Gb QSFP+ network module
FPR4K-XNM-2X100G	2-port 100-Gb QSFP+
FPR4K-XNM-2X100G=	2-port 100-Gb QSFP+ (spare)
FPR4K-XNM-4X200G	4-port 40/100/200-Gb QSFP+
FPR4K-XNM-4X200G=	4-port 40/100/200-Gb QSFP+ (spare)
FPR4200-NM-BLANK	Network module blank slot cover
FPR4200-NM-BLANK=	Network module blank slot cover (spare)

Power Cord Specifications

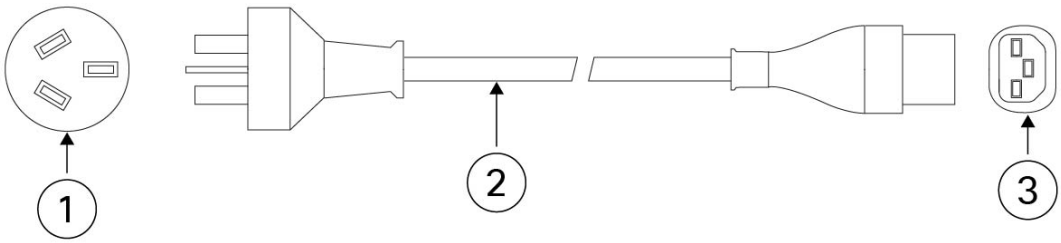
Each power supply has a separate power cord. Standard power cords or jumper power cords are available for connection to the secure firewall. The jumper power cords for use in racks are available as an optional alternative to the standard power cords.

If you do not order the optional power cord with the system, you are responsible for selecting the appropriate power cord for the product. Using a incompatible power cord with this product may result in electrical safety hazard. Orders delivered to Argentina, Brazil, and Japan must have the appropriate power cord ordered with the system.

Note Only the approved power cords or jumper power cords provided with the Secure 4200 are supported.

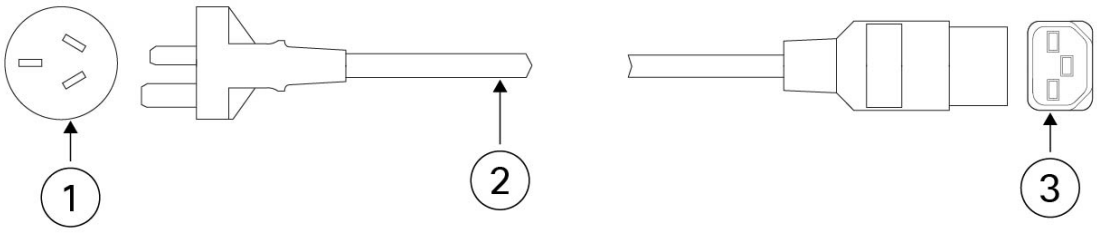
The following power cords are supported.

Figure 20: Argentina



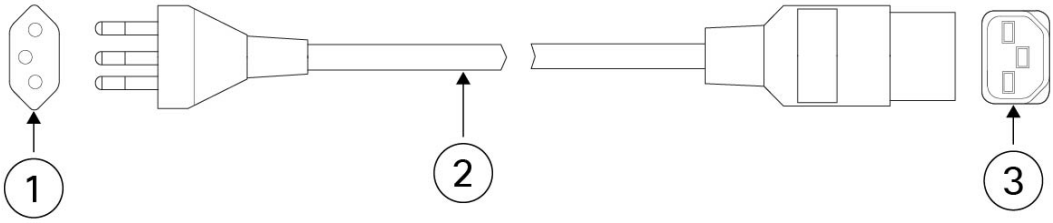
	PID: PWR-CAB-AC-ARG		Part number: 37-1711-01
1	Plug: IRAM 2073	**2**	Cord set rating: 20 A, 250 V
3	Connector: IEC 60320/C21		Cord length: 14 ft (4.25 m)

Figure 21: Australia



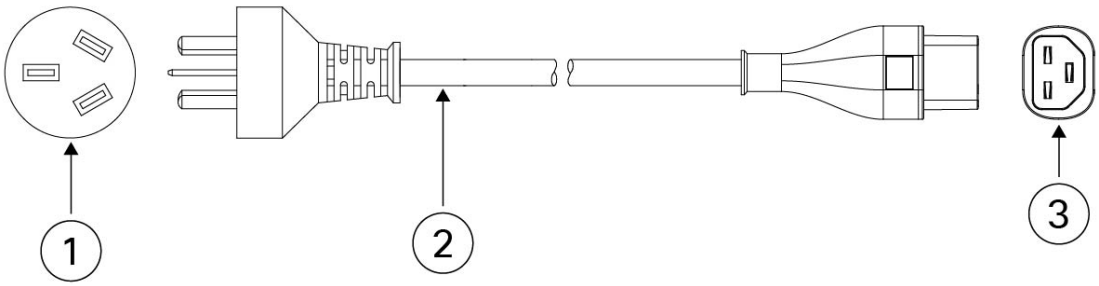
	PID: PWR-CAB-AC-AUS		Part number: 72-5201-01
1	Plug: A.S./NZS 3112	**2**	Cord set rating: 15 A, 250 V
3	Connector: IEC 60320/C21		Cord length: 14 ft (4.3 m)

Figure 22: Brazil



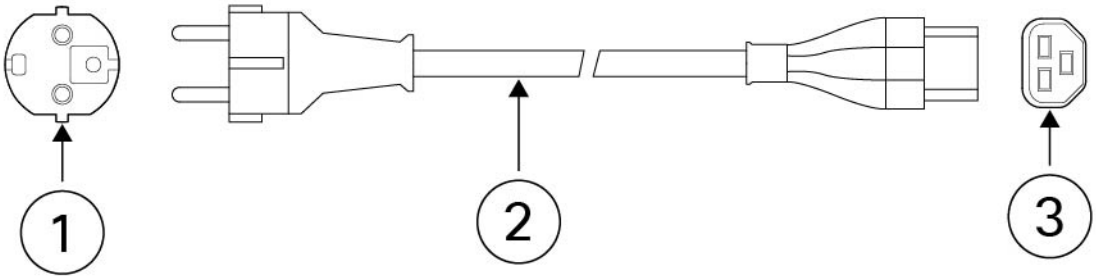
	PID: PWR-CAB-AC-BRA		Part number: 72-5208-01
1	Plug: NBR 14136	**2**	Cord set rating: 16 A, 250 V
3	Connector: IEC 60320/C21		Cord length: 14 ft (4.3 m)

Figure 23: China



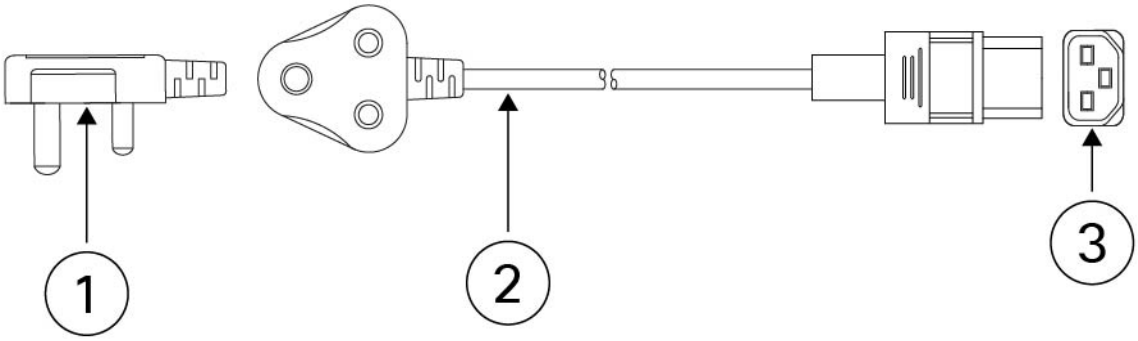
	PID: PWR-CAB-AC-CHN		Part number: 72-5207-01
1	Plug: GB16C	**2**	Cord set rating: 16 A, 250 V
3	Connector: IEC 60320/C21		Cord length: 14 ft (4.3 m)

Figure 24: Europe



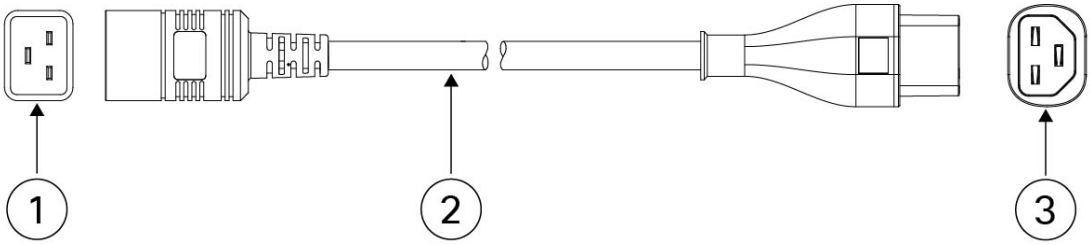
	PID: PWR-CAB-AC-EU		Part number: 37-1808-01
1	Plug: CEE 7/7	**2**	Cord set rating: 16 A, 250 V
3	Connector: IEC 60320/C21		Cord length: 14 ft (4.3 m)

Figure 25: India



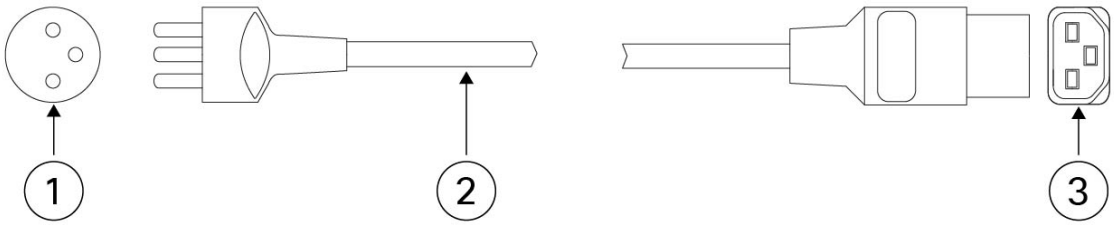
	PID: PWR-CAB-AC-IND		Part number: 37-1857-01
1	Plug: IS 1293	**2**	Cord set rating: 16 A, 250 V
3	Connector: IEC 60320/C21		Cord length: 14 ft (4.3 m)

Figure 26: International



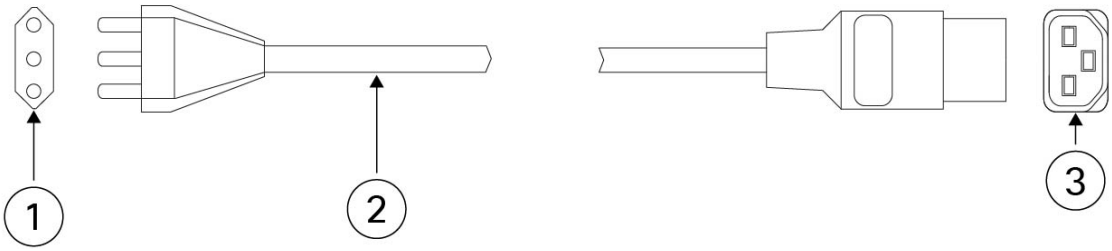
	PID: PWR-CAB-AC-BLK		Part number: 72-5595-01
1	Plug: IEC 60320/20	**2**	Cord set rating: 20 A, 250 V
3	Connector: IEC 60320/C21		Cord length: 14 ft (4.3 m)

Figure 27: Israel



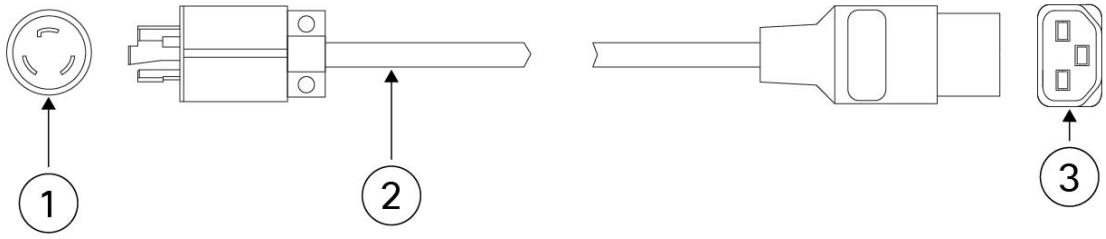
	PID: PWR-CAB-AC-ISRL		Part number: 72-5206-01
1	Plug: SI-32	**2**	Cord set rating: 16 A, 250 V
3	Connector: IEC 60320/C21		Cord length: 14 ft (4.3 m)

Figure 28: Italy



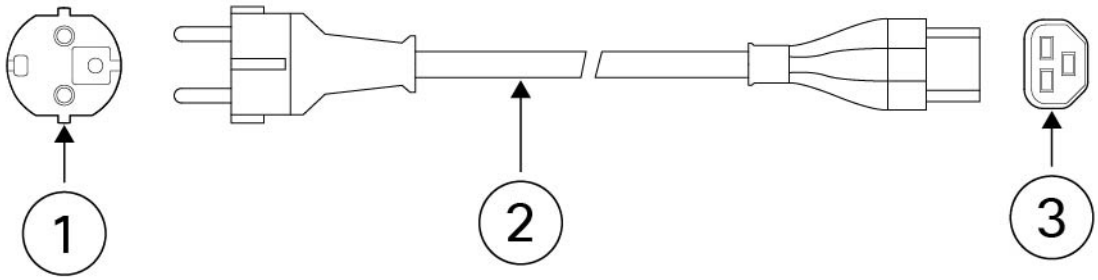
	PID: PWR-CAB-AC-ITA		Part number: 72-5203-01
1	Plug: CEI 23-50	**2**	Cord set rating: 16 A, 250 V
3	Connector: IEC 60320/C21		Cord length: 14 ft (4.3 m)

Figure 29: Japan



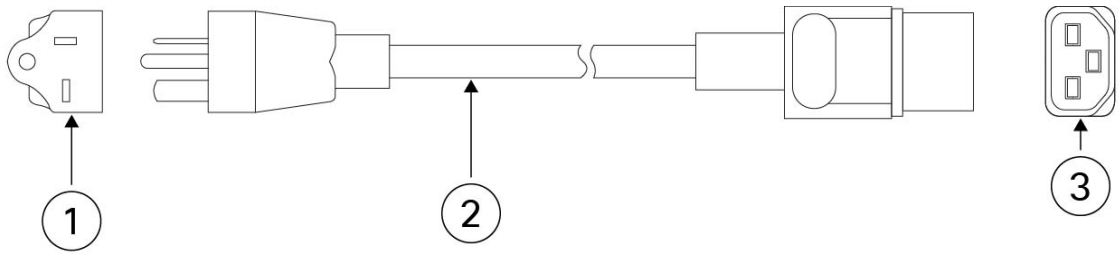
	PID: PWR-CAB-AC-JPN		Part number: 72-5210-01
1	Plug: NEMA L6-20	**2**	Cord set rating: 20 A, 250 V
3	Connector: IEC 60320/C21		Cord length: 14 ft (4.3 m)

Figure 30: Korea



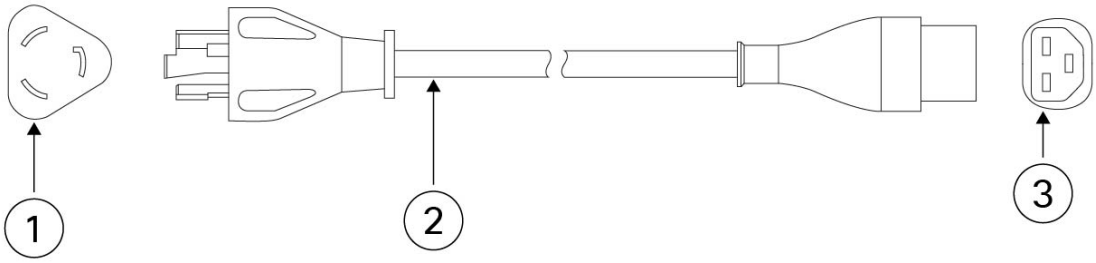
	PID: PWR-CAB-AC-KOR		Part number: 37-1808-01
1	Plug: CEE 7/7	**2**	Cord set rating: 16 A, 250 V
3	Connector: IEC 60320/C21		Cord length: 14 ft (4.3 m)

Figure 31: North America



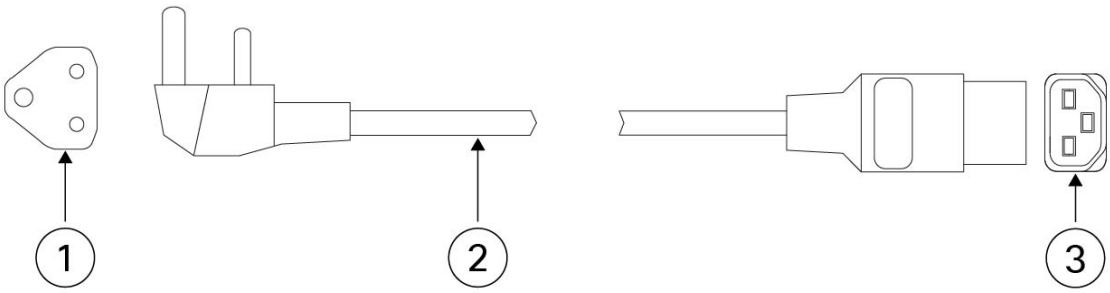
	PID: PWR-CAB-AC-USA520		Part number: 37-1849-01
1	Plug: NEMA 5-20P	**2**	Cord set rating: 20 A, 125 V
3	Connector: IEC 60320/C21		Cord length: 14 ft (4.3 m)

Figure 32: North America



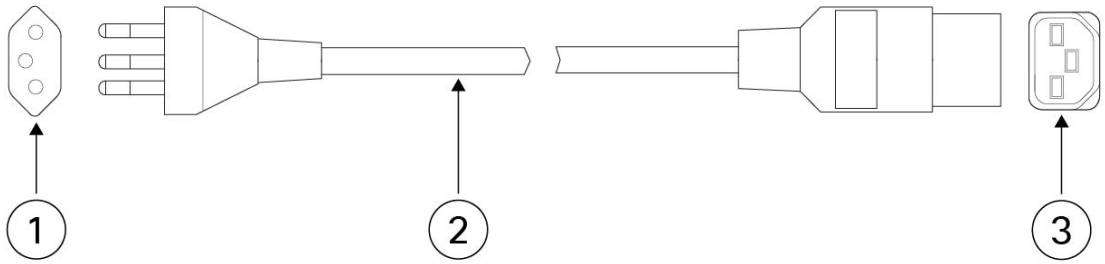
	PID: PWR-CAB-AC-USA		Part number: 72-5200-01
1	Plug: NEMA L6-20P	**2**	Cord set rating: 20 A, 250 V
3	Connector: IEC 60320/C21		Cord length: 14 ft (4.3 m)

Figure 33: South Africa



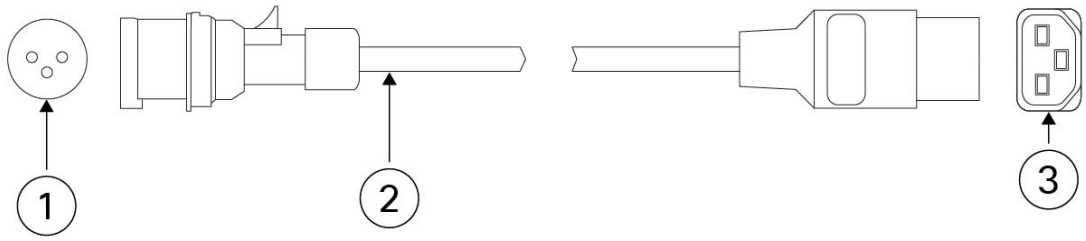
	PID: PWR-CAB-AC-SA		Part number: 72-5204-01
1	Plug: SABS 164	**2**	Cord set rating: 16 A, 250 V
3	Connector: IEC 60320/C21		Cord length: 14 ft (4.3 m)

Figure 34: Switzerland

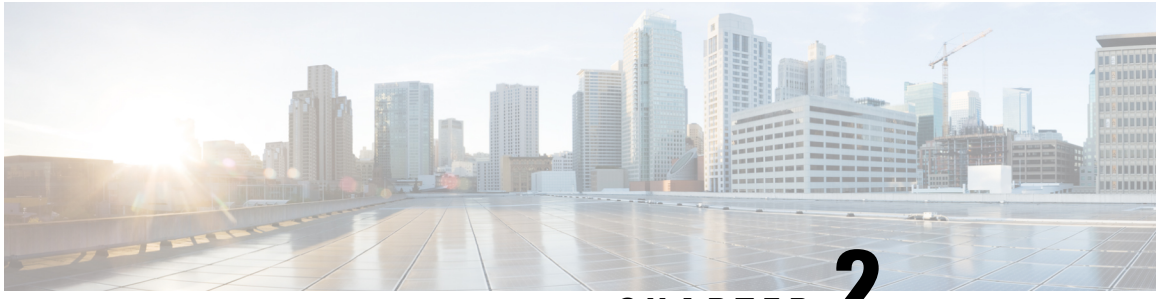


	PID: PWR-CAB-AC-SUI		Part number: 72-5209-01
1	Plug: SEV 1011	**2**	Cord set rating: 16 A, 250 V
3	Connector: IEC 60320/C21		Core length: 14 ft (4.3 m)

Figure 35: United Kingdom



	PID: PWR-AC-UK		Part number: 72-5205-01
1	Plug: IEC309	**2**	Cord set rating: 16 A, 250 V
3	Connector: IEC 60320/C21		Length: 14 ft (4.3 m)



CHAPTER 2

Installation Preparation

Installation Warnings

Read the Regulatory Compliance and Safety Information document before installing the security appliance.

Take note of the following warnings:

Warning

Statement 1071—Warning Definition

IMPORTANT SAFETY INSTRUCTIONS

Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Read the installation instructions before using, installing, or connecting the system to the power source. Use the statement number at the beginning of each warning statement to locate its translation in the translated safety warnings for this device.

SAVE THESE INSTRUCTIONS

Warning **Statement 1005**—Circuit Breaker

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

AC 20 A

Warning **Statement 1015**—Battery Handling

To reduce risk of fire, explosion or leakage of flammable liquid or gas:

- Replace the battery only with the same or equivalent type recommended by the manufacturer.
- Do not dismantle, crush, puncture, use sharp tool to remove, short external contacts, or dispose of in fire.
- Do not use if battery is warped or swollen.
- Do not store or use battery in a temperature > 140°F (60°C).
- Do not store or use battery in low air pressure environment < 69.7 kPa.

Warning **Statement 1017—**Restricted Area

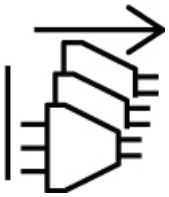
This unit is intended for installation in restricted access areas. Only skilled, instructed, or qualified personnel can access a restricted access area.

Warning **Statement 1024—**Ground Conductor

This equipment must be grounded. To reduce the risk of electric shock, never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.

Warning **Statement 1028—**More Than One Power Supply

This unit might have more than one power supply connection. To reduce risk of electric shock, remove all connections to de-energize the unit.



Warning **Statement 1029—**Blank Faceplates and Cover Panels

Blank faceplates and cover panels serve three important functions: they reduce the risk of electric shock and fire, they contain electromagnetic interference (EMI) that might disrupt other equipment, and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place.

Warning **Statement 1073—**No User-Serviceable Parts

There are no serviceable parts inside. To avoid risk of electric shock, do not open.

Warning **Statement 1074—**Comply with Local and National Electrical Codes

To reduce risk of electric shock or fire, installation of the equipment must comply with local and national electrical codes.

Network Equipment-Building System (NEBS) Statements

NEBS describes the environment of a typical United States Regional Bell Operating Company (RBOC) central office. NEBS is the most common set of safety, spatial, and environmental design standards applied to telecommunications equipment in the United States. It is not a legal or regulatory requirement, but rather an industry requirement.

The following NEBS statements apply to the Secure Firewall 4200 series:

Note **Statement 7001—**ESD Mitigation

This equipment may be ESD sensitive. Always use an ESD ankle or wrist strap before handling equipment. Connect the equipment end of the ESD strap to an unfinished surface of the equipment chassis or to the ESD jack on the equipment if provided.

Warning **Statement 7003**—Shielded Cable Shielded Cable Requirements for Intrabuilding Lightning Surge

The intrabuilding port(s) of the equipment or subassembly must use shielded intrabuilding cabling/wiring that is grounded at both ends.

The following port(s) are considered intrabuilding ports on this equipment:

Copper RJ-45 network ports

Warning **Statement 7005**—Intrabuilding Lightning Surge and AC Power Fault

The intrabuilding port(s) of the equipment or subassembly must not be metallically connected to interfaces that connect to the outside plant (OSP) or its wiring. These interfaces are designed for use as intrabuilding interfaces only (Type 2 or Type 4 ports as described in GR-1089-CORE) and require isolation from the exposed OSP cabling. The addition of primary protectors is not sufficient protection to connect these interfaces metallically to OSP wiring.

This statement applies to the intrabuilding ports listed below:

Copper RJ-45 network ports

Warning **Statement 7012—**Equipment Interfacing with AC Power Ports

Connect this equipment to AC mains that are provided with a surge protective device (SPD) at the service equipment that complies with NFPA 70, the National Electrical Code (NEC).

Note **Statement 7013—**Equipment Grounding Systems—Common Bonding Network (CBN)

This equipment is suitable for installations using the CBN.

Note **Statement 7018—**System Recover Time

The equipment is designed to boot up in less than 30 minutes provided the neighboring devices are fully operational.

Note **Statement 8015—**Installation Location Network Telecommunications Facilities

This equipment is suitable for installation in network telecommunications facilities.

Safety Recommendations

Observe these safety guidelines:

- Keep the area clear and dust free before, during, and after installation.
- Keep tools away from walkways, where you and others might trip over them.
- Do not wear loose clothing or jewelry, such as earrings, bracelets, or chains that could get caught in the chassis.
- Wear safety glasses if you are working under any conditions that might be hazardous to your eyes.
- Do not perform any action that creates a potential hazard to people or makes the equipment unsafe.

- Never attempt to lift an object that is too heavy for one person.

Maintain Safety with Electricity

Warning Before working on a chassis, be sure the power cord is unplugged.

Read the Regulatory Compliance and Safety Information document before installing the chassis.

Follow these guidelines when working on equipment powered by electricity:

- Before beginning procedures that require access to the interior of the chassis, locate the emergency power-off switch for the room in which you are working. Then, if an electrical accident occurs, you can act quickly to turn off the power.
- Do not work alone if potentially hazardous conditions exist anywhere in your work space.
- Never assume that power is disconnected; always check.
- Look carefully for possible hazards in your work area, such as moist floors, ungrounded power extension cables, frayed power cords, and missing safety grounds.
- If an electrical accident occurs:
  - Use caution; do not become a victim yourself.
  - Disconnect power from the system.
  - If possible, send another person to get medical aid. Otherwise, assess the condition of the victim, and then call for help.
  - Determine whether the person needs rescue breathing or external cardiac compressions; then take appropriate action.
- Use the chassis within its marked electrical ratings and product usage instructions.
- The chassis is equipped with an AC-input power supply, which is shipped with a three-wire electrical cord with a grounding-type plug that fits into a grounding-type power outlet only. Do not circumvent this safety feature. Equipment grounding should comply with local and national electrical codes.

Prevent ESD Damage

ESD occurs when electronic components are improperly handled, and it can damage equipment and impair electrical circuitry, which can result in intermittent or complete failure of your equipment.

Always follow ESD-prevention procedures when removing and replacing components. Ensure that the chassis is electrically connected to an earth ground. Wear an ESD-preventive wrist strap, ensuring that it makes good skin contact. Connect the grounding clip to an unpainted surface of the chassis frame to safely ground ESD voltages. To properly guard against ESD damage and shocks, the wrist strap and cord must operate effectively. If no wrist strap is available, ground yourself by touching the metal part of the chassis.

For safety, periodically check the resistance value of the antistatic strap, which should be between one and 10 megohms.

Site Environment

See Hardware Specifications, on page 37 for information about physical specifications.

To avoid equipment failures and reduce the possibility of environmentally caused shutdowns, plan the site layout and equipment locations carefully. If you are currently experiencing shutdowns or unusually high error rates with your existing equipment, these considerations may help you isolate the cause of failures and prevent future problems.

Site Considerations

Considering the following helps you plan an acceptable operating environment for the chassis, and avoid environmentally-caused equipment failures.

- Electrical equipment generates heat. Ambient air temperature might not be adequate to cool equipment to acceptable operating temperatures without adequate circulation. Make sure that the room in which you operate your system has adequate air circulation.
- Ensure that the chassis cover is secure. The chassis is designed to allow cooling air to flow effectively within it. An open chassis allows air leaks, which may interrupt and redirect the flow of cooling air from the internal components.
- Always follow ESD prevention procedures to avoid damage to equipment. Damage from static discharge can cause immediate or intermittent equipment failure.

Power Supply Considerations

See Power Supply Module, on page 29 for more detailed information about the power supply in the chassis.

When installing the chassis, consider the following:

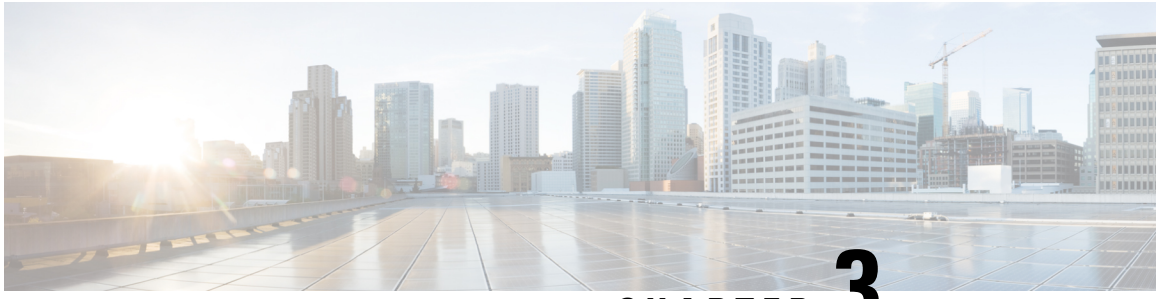
- Check the power at the site before installing the chassis to ensure that it is free of spikes and noise. Install a power conditioner, if necessary, to ensure proper voltages and power levels in the appliance-input voltage.
- Install proper grounding for the site to avoid damage from lightning and power surges.
- The chassis does not have a user-selectable operating range. Refer to the label on the chassis for the correct appliance input-power requirement.
- Several styles of AC-input power supply cords are available for the chassis; make sure that you have the correct style for your site.
- If you are using dual redundant (1+1) power supplies, we recommend that you use independent electrical circuits for each power supply.
- Install an uninterruptible power source for your site, if possible.

Rack Configuration Considerations

See Rack-Mount the Chassis Using Slide Rails, on page 55 for the procedure for rack-mounting the chassis.

Consider the following when planning a rack configuration:

- Standard 19-inch (48.3 cm) 4-post EIA rack with mounting rails that conform to English universal hole spacing according to section 1 of ANSI/EIA-310-D-1992.
- The rack-mounting posts need to be 2 to 3.5 mm thick to work with the slide rail rack mounting.
- If you are mounting a chassis in an open rack, make sure that the rack frame does not block the intake or exhaust ports.
- If your rack includes closing front and rear doors, the doors must have 65 percent open perforated area evenly distributed from top to bottom to permit adequate airflow.
- Be sure enclosed racks have adequate ventilation. Make sure that the rack is not overly congested as each chassis generates heat. An enclosed rack should have louvered sides and a fan to provide cooling air.
- In an enclosed rack with a ventilation fan in the top, heat generated by equipment near the bottom of the rack can be drawn upward and into the intake ports of the equipment above it in the rack. Ensure that you provide adequate ventilation for equipment at the bottom of the rack.
- Baffles can help to isolate exhaust air from intake air, which also helps to draw cooling air through the chassis. The best placement of the baffles depends on the airflow patterns in the rack. Experiment with different arrangements to position the baffles effectively.



CHAPTER 3

Mount the Chassis

Unpack and Inspect the Chassis

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. Keep the shipping container in case you need to send the chassis back due to damage.

See Package Contents, on page 4 for a list of what shipped with the chassis.

Step 1 Remove the chassis 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

Rack-Mount the Chassis Using Slide Rails

This procedure describes how to install the Secure Firewall 4200 in a rack using slide rails. It applies to all models of the 4200 series. You use the pegs on the chassis to secure the slide rail. See Product ID Numbers,

on page 38 for a list of the PIDs associated with racking the chassis. You can install the optional cable management bracket on all models of the Secure Firewall 4200.

The rack is a standard Electronic Industries Association (EIA) rack. It is a 4-post-EIA-310-D, which is the current revision as specified by EIA. The vertical hole spacing alternates at .50 inches (12.70 mm) to .625 inches (15.90 mm) to .625 inches (15.90 mm) and repeats. The start and stop space is in the middle of the .50-inch holes. The horizontal spacing is 18.312 inches (465.1 mm), and the rack opening is specified as a minimum of 17.75 inches (450 mm).

You need the following to install the Secure Firewall 4200 in a rack using slide rails:

- Phillips screwdriver
- Two slide rails (part number 800-109129-01)
- Slide rail accessories kit (part number 53-101561-01):
  - Two slide rail mounting brackets (part number 700-121935-01)
  - Six 8-32 x 0.302-inch slide rail mounting bracket Phillips screws (part number 48-102184-01) for securing the brackets to the chassis
  - Two M3 x 0.5 x 6-mm Phillips screws (part number 48-101144-01) for securing the chassis to your rack
- Cable management bracket kit (optional) (part number 69-101031-01)
  - Two cable management brackets (part number 700-130991-01)
  - Four 8-32 x 0.375-inch Phillips screws (part number 48-2696-01)

Slide rail assemblies work with four-post racks and cabinets with square slots, round 7.1mm holes, #10-32 threaded holes, and #12-24 threaded holes on the rack post front. The slide rail works with front to back spacing of rack posts from 24 to 36 inches. The rack-mounting posts need to be 2 to 3.5 mm thick to work with the slide rail rack mounting.

Safety Warnings

Take note of the following warnings:

Warning **Statement 164**—Lifting Requirement

Two people are required to lift the heavy parts of the product. To prevent injury, keep your back straight and lift with your legs, not your back.

Warning **Statement 1006—**Chassis Warning for Rack-Mounting and Servicing

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.

Warning **Statement 1024—**Ground Conductor

This equipment must be grounded. To reduce the risk of electric shock, never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.

Warning **Statement 1047**—Overheating Prevention

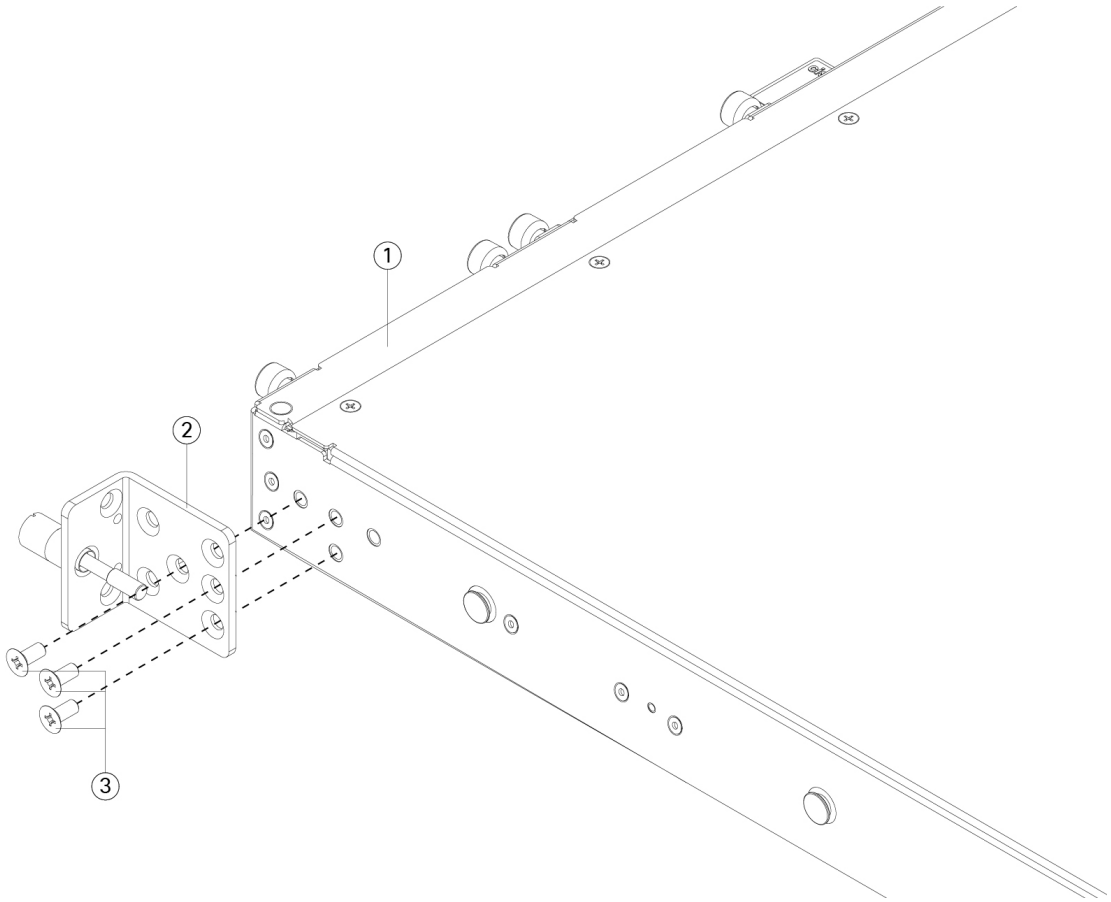
To reduce the risk of fire or bodily injury, do not operate the unit in an area that exceeds the maximum recommended ambient temperature of 104°F (40°C).

Warning **Statement 1073—**No User-Serviceable Parts

There are no serviceable parts inside. To avoid risk of electric shock, do not open.

Step 1 Attach the slide-rail locking brackets to each side of the chassis using the six 8-32 x 0.302-inch Phillips screws (three per side).

Figure 36: Attach the Slide-Rail Locking Bracket to the Side of the Chassis

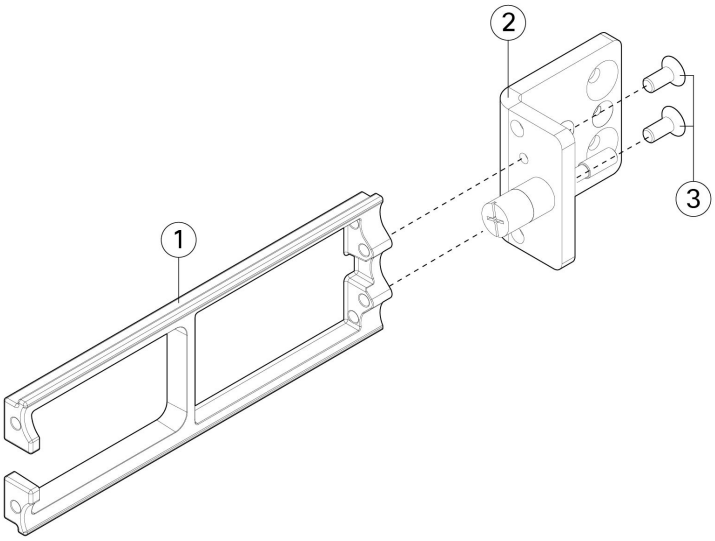


1	Chassis	**2**	Slide-rail locking bracket
3	8-32 x 0.302-inch Phillips screws (three per side)		

Step 2 (Optional) Attach the cable management bracket to the slide-rail locking bracket:

a) Install the cable management screws into the slide-rail locking bracket.

Figure 37: Install the Cable Management Screws into the Slide-Rail Locking Bracket



1	Cable management bracket	**2**	Rack-mount bracket
3	8-32 x 0.375-inch Phillips screws (two per bracket)		—

b) Install two 8-32 x 0.375 inch Phillips screws through the inside of the slide-rail locking bracket to secure the cable management bracket to slide-rail locking bracket.

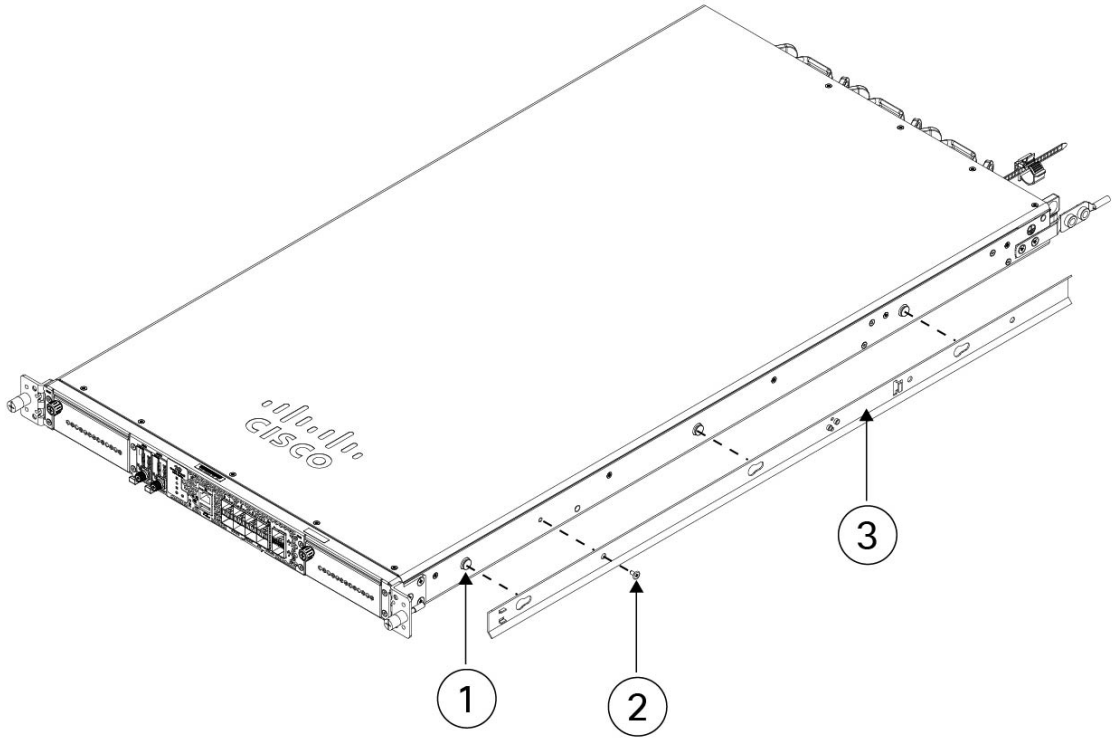
Step 3 Attach the inner rails to the sides of the chassis:

a) Remove the inner rails from the slide rail assemblies.

b) Align an inner rail with each side of the chassis:

- Align the inner rail so that the three slots on the rail line up with the three pegs on the side of the chassis.

Figure 38: Line up the Inner Rail with the Pegs on the Chassis



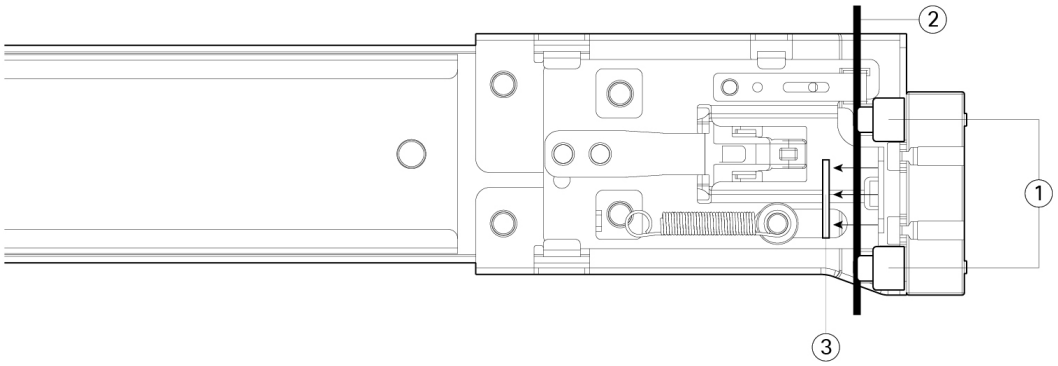
1	Mounting peg on the chassis for the keyed slot	**2**	M3 x 0.5 x 6-mm Phillips screws (one per side)
3	Inner rail		

c) Set the keyed slots over the screws/pegs, and then slide the rail toward the front to lock it in place on the screw/pegs. The rear key slot has a metal clip that locks over the screw/peg.
d) Using one M3 x 0.5 x 6-mm Phillips screw, secure the inner rail to the side of the chassis to prevent sliding.
e) Install the second inner rail to the opposite side of the chassis and secure with the other M3 x 0.5 x 6-mm screw.

Step 4 Open the front securing plate on both slide-rail assemblies. The front end of the slide-rail assembly has a spring-loaded securing plate that must be open before you can insert the mounting pegs into the rack-post holes.

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

Figure 39: Front Securing Mechanism Inside the Front End



1	Front mounting pegs **Note** Works with square slots, 7.1 mm holes, and 10-32 threaded holes	**2**	Securing plate shown pulled back to open position
3	Rack post		—

Step 5 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.

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. Make sure 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.

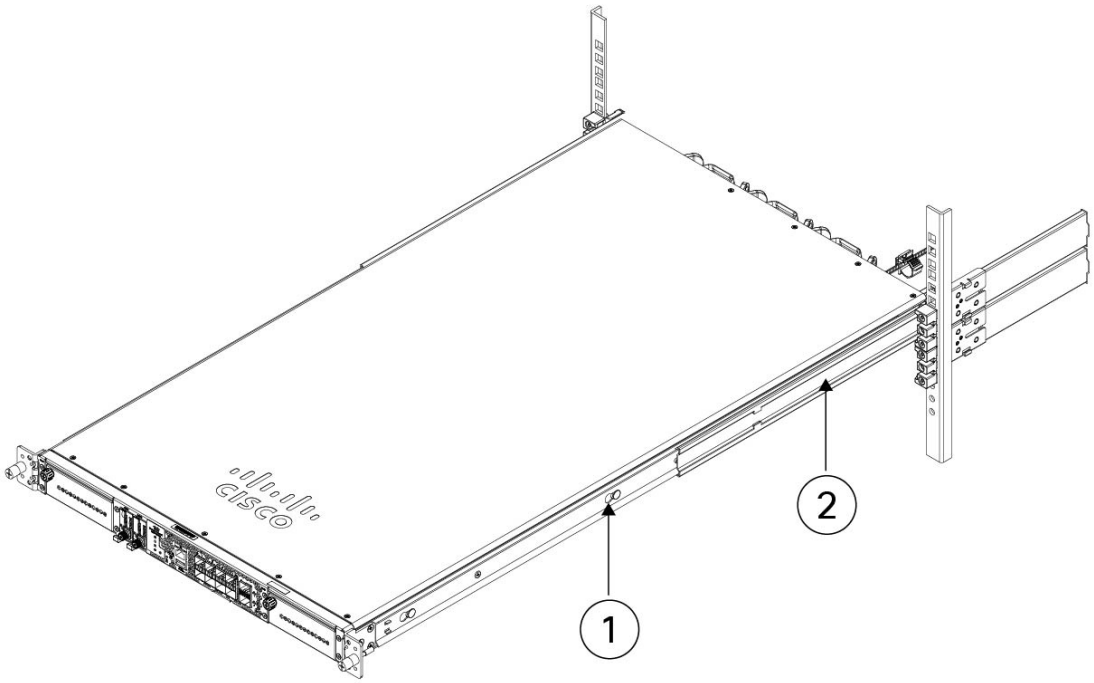
Step 6 Insert the chassis into the slide rails.

a) Align the rear of the inner rails that are attached to the chassis 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 chassis into the rack until the mounting brackets meet the front of the slide rail.

Figure 40: Inner Rail Release Clip



1	Inner rail release clip	**2**	Inner rail attached to chassis

Step 7 Use the captive screws on the front of the mounting brackets to fully secure the chassis to the rack.

What to do next

- See Ground the Chassis, on page 62 for the procedure to ground the Secure Firewall 4200.

Ground the Chassis

Note Grounding the chassis is required, even if the rack is already grounded. A grounding kit is provided for attaching a grounding lug. The grounding lug must be Nationally Recognized Testing Laboratory (NRTL)-listed. In addition, a copper conductor (wires) must be used and the copper conductor must comply with National Electrical Code (NEC) code for ampacity.

You need the following items that you provide:

- Wire-striping tool
- Crimping tool
- Grounding cable

- You need the following items from the accessory kit:
  - One grounding lug (part number 32-100152-01)
  - One grounding lug bracket (part number 700-122528-01)
  - Two M4.0 x 0.6 mm flat-head Phillips screws (part number 48-2030-01)
  - Two ¼-20 x 0.297-inch button-head screws (part number 48-102252-01)
  - Two 0.469-inch OD, 0.261-inch ID, 0.025-inch T washers (part number 49-100464-01)

Safety Warnings

Take note of the following warnings:

Warning **Statement 1024—**Ground Conductor

This equipment must be grounded. To reduce the risk of electric shock, never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.

Warning **Statement 1046—**Installing or Replacing the Unit

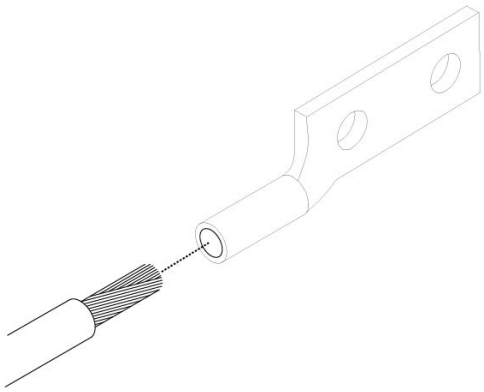
To reduce risk of electric shock, when installing or replacing the unit, the ground connection must always be made first and disconnected last.

If your unit has modules, secure them with the provided screws.

Step 1 Use a wire-stripping tool to remove approximately 0.75 inches (19 mm) of the covering from the end of the grounding cable.

Step 2 Insert the stripped end of the grounding cable into the open end of the grounding lug.

Figure 41: Insert the Cable into the Grounding Lug



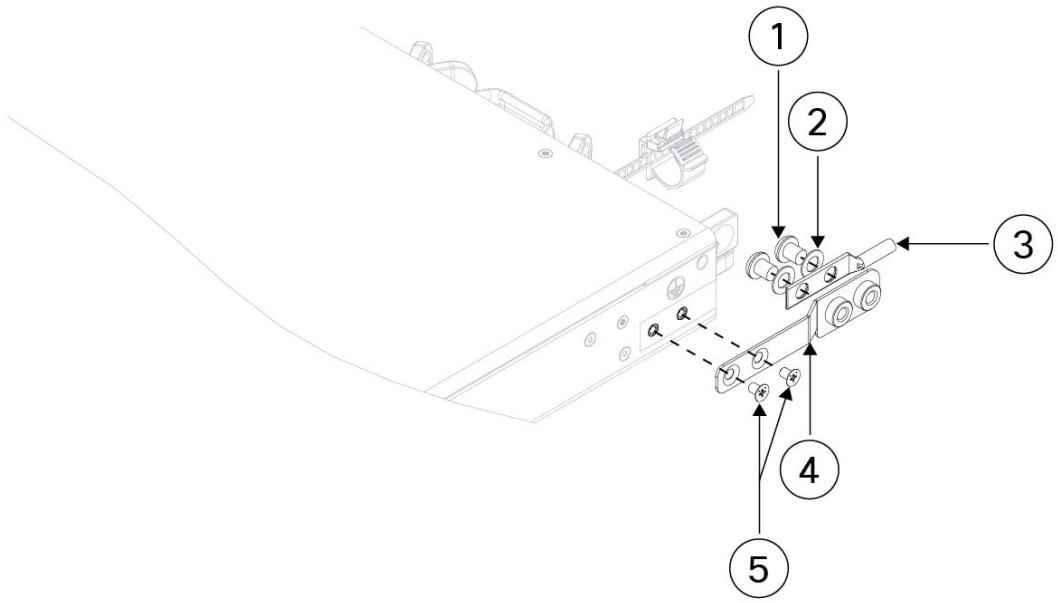
Step 3 Use the crimping tool to secure the grounding cable in the grounding lug.

Step 4 Remove the adhesive label from the grounding pad on the chassis.

Step 5 Insert the grounding lug into the grounding lug bracket using the 2 button-head screws and washers.

Step 6 Attach the grounding lug bracket against the grounding pad on the left side of the chassis so that there is solid metal-to-metal contact, and insert the two M4.0 x 0.6 mm flat-head Phillips screws through the holes in the grounding lug bracket and into the grounding pad.

Figure 42: Attach the Grounding Lug



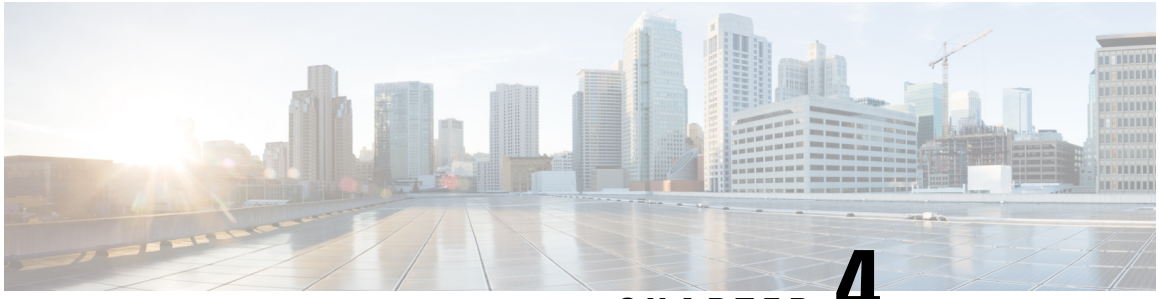
1	Two ¼-20 x .297 inch button-head screws	**2**	Two lock-internal washers
3	Grounding lug	**4**	Grounding lug bracket
5	Two M4.0 x .06 mm flat-head screws		—

Step 7 Make sure that the lug and cable do not interfere with other equipment.

Step 8 Prepare the other end of the grounding cable and connect it to an appropriate grounding point in your site to ensure adequate earth ground.

What to do next

Install the cables according to your default software configuration as described in the Cisco Secure 4200 Getting Started Guide.



CHAPTER 4

Installation, Maintenance, and Upgrade

Install, Remove, and Replace the Network Module

You can remove and replace the network modules (NM-2 and NM-3) in the Secure Firewall 4200. Although the hardware supports removing and replacing the network module while the system is running, the software does not currently support hot swapping. You must power down the chassis or disable the network slot to remove and replace network modules.

See the configuration guide for your operating system for the procedure for managing network modules.

This procedure describes how to install a network module into an empty slot that has never contained a network module, and how to remove an installed network module and replace it with another network module.

Safety Warnings

Take note of the following warning:

Warning **Statement 1073**—No User-Serviceable Parts

There are no serviceable parts inside. To avoid risk of electric shock, do not open.

Step 1 To install a network module for the first time into an empty slot, do the following:

a) Power down the chassis by moving the power switch to the OFF position.

See Rear Panel, on page 14 for more information about the power switch. See the configuration guide for your operating system for the procedure for installing a network module for the first time into an empty slot.

b) Follow Steps 4 through 7 to install the new network module.

c) Power on the chassis by moving the power switch to the ON position.

Step 2 To remove and replace an existing network module, do the following:

a) Save your configuration.

b) To replace an existing network module with the same model network module, disable the network slot. See the configuration guide for your operating system for the procedure to replace an existing network module with the same model.

c) To replace an existing network module with a different model network module, power down the chassis by moving the power switch to the OFF position. See the configuration guide for your operating system for the procedure to replace an existing network module with a new model.

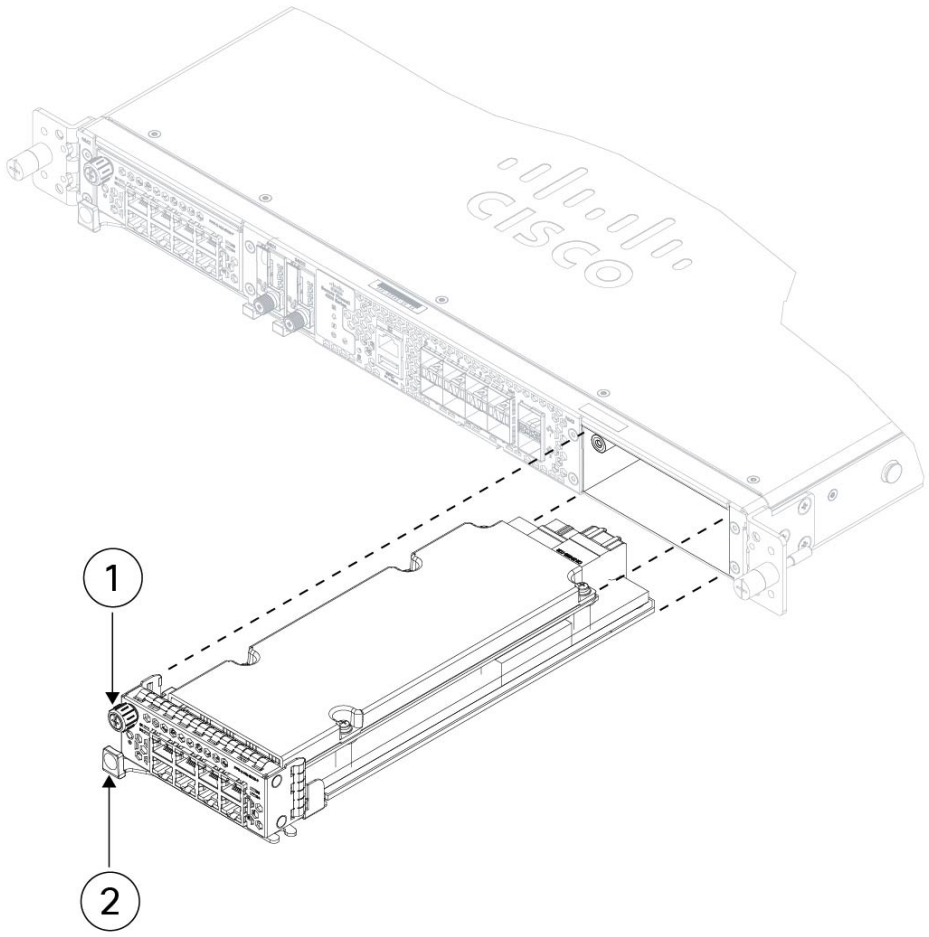
   See Rear Panel, on page 14 for more information about the power switch.

d) Continue with Step 3.

Step 3 To remove a network module, loosen the captive screw on the upper left side of the network module, press the handle ejector, and pull out the handle. This mechanically ejects the network module from the slot.

Caution The captive screw is not attached to the handle. Be sure the captive screw is completely loosened before pulling the ejector handle out. Otherwise you could damage the ejector handle as the captive screw and handle fight each other.

Figure 43: Remove the Network Module



1	Captive screw	**2**	Ejector handle

If the slot is to remain empty, install a blank faceplate to ensure proper airflow and to keep dust out of the chassis; otherwise, install another network module.

Step 4 To replace a network module, hold the network module in front of the network module slot on the right of the chassis, press the ejector handle, and pull out the handle.

Step 5 Slide the network module into the slot, push it firmly into place, and close the handle on the front of the network module.

Step 6 Tighten the captive screw on the upper left side of the network module.

Step 7 Power on the chassis so that the new network module is recognized.

Remove and Replace the SSD

The chassis supports two NVMe SSDs. The SSDs are configured for SW RAID1 support. See SSDs, on page 32 for more information.

Caution Hot swapping for the RAID configuration is not supported. To remove an SSD, you must remove it from the RAID configuration using the **raid remove-secure local-disk 1|2** command. See Hot Swap an SSD on the Secure Firewall 3100/4200 for the procedures for safely removing an SSD.

Safety Warnings

Take note of the following warning:

Warning **Statement 1073—**No User-Serviceable Parts

There are no serviceable parts inside. To avoid risk of electric shock, do not open.

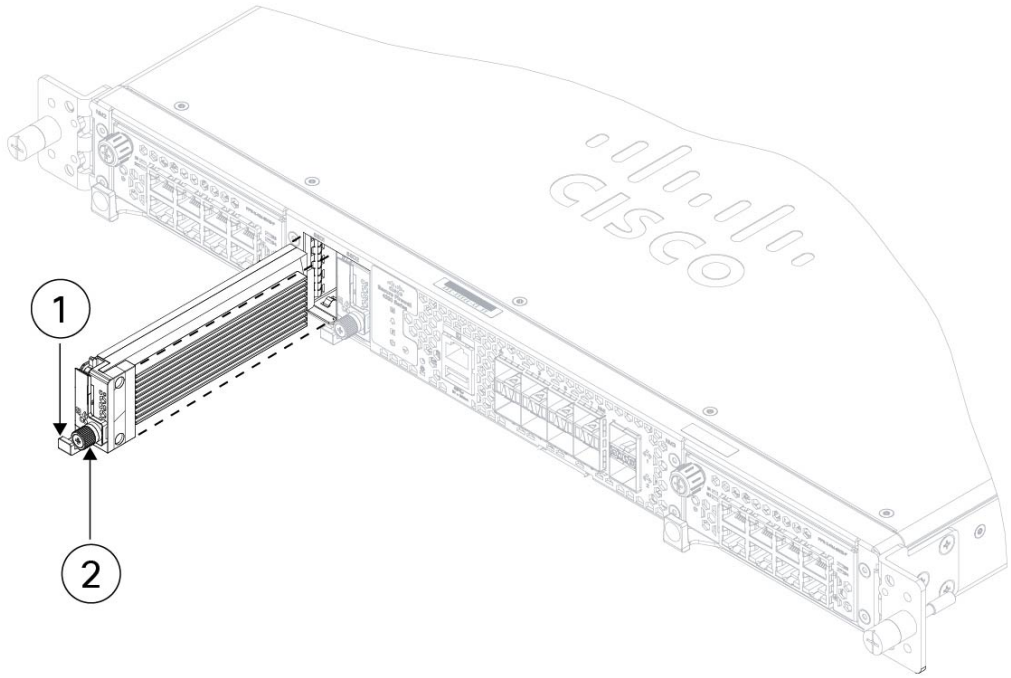
Step 1 Save your configuration.

Step 2 Remove SSD-1 or SSD-2 from the RAID1 configuration by using the **raid remove-secure local-disk 1|2** command.

Step 3 To remove the SSD from the slot, face the front of the chassis, and pinch the release tab on the front of the SSD. This causes the ejector handle to spring open.

Step 4 Grasp the ejector handle to gently pull the SSD out of the chassis.

Figure 44: Remove the SSD



1	Handle		Captive screw

Step 5 To replace SSD-1 or SSD-2, hold the SSD with the ejector handle extended in front of the slot, push it in gently until it is seated, and then close the ejector handle.

Step 6 Check the SSD LED to make sure the SSD is operative. See Front Panel LEDs, on page 11 for a description of the SSD LEDs.

Step 7 Add the new SSD to the RAID configuration using the **raid add local-disk 1|2** command.

Remove and Replace the Dual Fan Module

You can remove and replace the dual fan modules while the chassis is running. There are three dual fan modules in the rear of the chassis. The air flow moves from front to back (I/O side to non-I/0 side).

Caution Removing all of the dual fan modules exposes the chassis to no airflow. Replace the dual fan modules within 30 seconds after removal to avoid overheating the chassis. If you wait longer than 30 seconds, the chassis may power off automatically to prevent damage to components. The chassis does not power up and boot properly if the dual fan modules are missing.

Safety Warnings

Take note of the following warnings:

Warning **Statement 1073—**No User-Serviceable Parts

There are no serviceable parts inside. To avoid risk of electric shock, do not open.

Warning **Statement 1093—**Avoid Sharp Edges

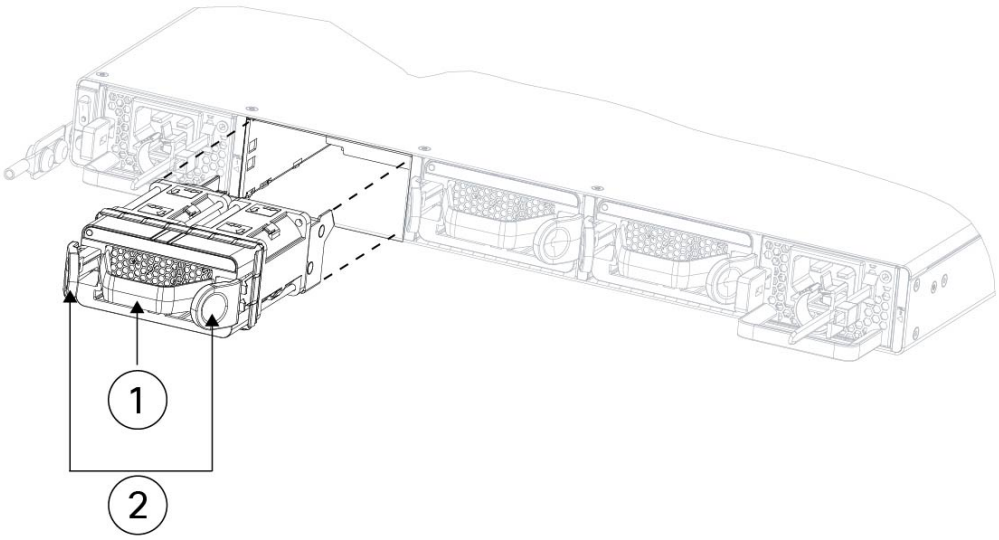
Risk of personal injury. Avoid sharp edges when installing or removing replaceable units.

Step 1 Have the dual fan module ready for immediate insertion and near the chassis so that you can reinstall it within 30 seconds.

Step 2 To remove a fan module, face the rear of the chassis, and press the squeeze tabs on the sides of the fan module to loosen it from the chassis.

Step 3 Grasp the handle and pull the fan module out of the chassis.

Figure 45: Remove the Dual Fan Module



1	Handle		Squeeze tabs

Step 4 To replace a fan module, hold the fan module in front of the fan slot.

Step 5 Press the squeeze tabs on the sides of the fan module and push the it into the chassis.

Step 6 Grasp the handle and push until the fan module is properly seated.
If the system is powered on, listen for the fans. You should immediately hear the fans operating. If you do not hear the fans, make sure the fan module is inserted completely into the chassis and the faceplate is flush with the outside surface of the chassis.

Step 7 Verify that the fan is operational by checking the fan module LED. See Front Panel LEDs, on page 11 for a description of the fan LEDs.

Remove and Replace the Power Supply Module

Power supply modules are hot-swappable. You can remove and replace power supply modules while the system is running.

Safety Warnings

Take note of the following warnings:

Warning **Statement 1015**—Battery Handling

To reduce risk of fire, explosion or leakage of flammable liquid or gas:

- Replace the battery only with the same or equivalent type recommended by the manufacturer.
- Do not dismantle, crush, puncture, use sharp tool to remove, short external contacts, or dispose of in fire.
- Do not use if battery is warped or swollen.
- Do not store or use battery in a temperature > 60° C.
- Do not store or use battery in low air pressure environment < 69.7 kPa.

Warning **Statement 1022**—Disconnect Device

To reduce the risk of electric shock and fire, a readily accessible disconnect device must be incorporated in the fixed wiring.

Warning **Statement 1046**—Installing or Replacing the Unit

To reduce risk of electric shock, when installing or replacing the unit, the ground connection must always be made first and disconnected last.

If your unit has modules, secure them with the provided screws.

Warning **Statement 1073**—No User-Serviceable Parts

There are no serviceable parts inside. To avoid risk of electric shock, do not open.

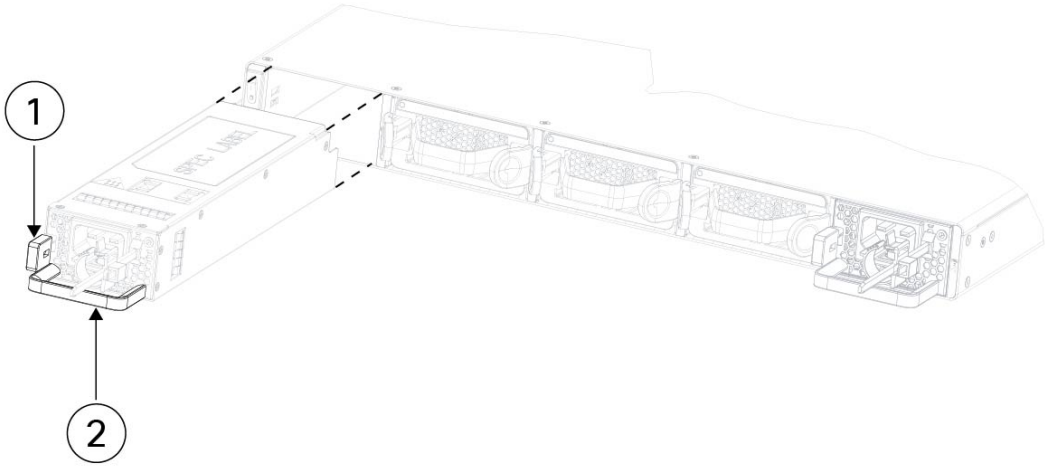
Step 1 Unplug the power supply cable before removing the power supply module. You cannot disengage the power supply module release tab without first removing the cable.

Step 2 To remove a power supply module, face the back of the chassis and grasp the handle.

Step 3 Press the release tab toward the left to disengage the power supply. The release tab is found on the right side of the power supply.

Step 4 Place your other hand under the power supply module to support it while you slide it out of the chassis.

Figure 46: Remove the Power Supply Module



1	Release tab	**2**	Handle

If the slot is to remain empty, install a blank faceplate to ensure proper airflow; otherwise, install another power supply module.

Step 5 To replace a power supply module, hold the power supply module with both hands and slide it into the power supply module bay.

Step 6 Push in the power supply module gently until you hear the release tab engage and the power supply is seated.

Step 7 Plug in the power supply cable.

Step 8 Check the LED on the power supply to make sure the power supply is operative.