Cisco Secure Firewall 6100 Series Hardware Installation Guide

First Published: 2026-02-10

Last Modified: 2026-02-10

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

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

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

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

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

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

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

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

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

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

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

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

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

CONTENTS

CHAPTER 1

Overview

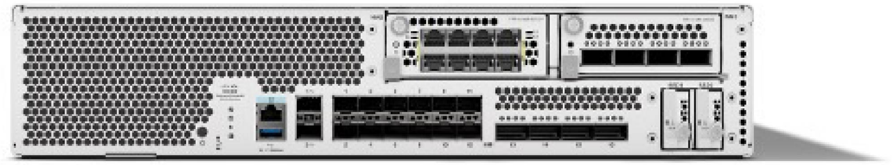
Features

The Cisco Secure Firewall 6100 series is a standalone modular security services platform that includes the 6160 and 6170. See Product ID numbers, on page 33 for a list of the product IDs (PIDs) associated with the 6100 series

The Secure Firewall 6100 series supports Cisco Secure Firewall Threat Defense Version 10.0.0 and Cisco Secure ASA Version 9.24.1 software. See the Cisco Secure Firewall Threat Defense Compatibility Guide and the Cisco Secure Firewall ASA Compatibility guides, 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 6100 series.

Figure 1: CSF-6160 and CSF-6170



The following table lists the features for the Secure Firewall 6100 series.

Table 1: CSF-6160 and CSF-6170 features

Feature	CSF-6160	CSF-6170
Form factor	2 RU Fits a standard 19-inch (48.3-cm) 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	
System memory	24 x 64 GB	24 x 96 GB
Management ports	Two 1/10/25-Gbps SFP28 ports	
Console port	One Cisco Serial (RS-232 on RJ-45)	
USB port	One USB 3.0 with a 5-W Type A port	
Network ports	Twelve fixed 1/10/25/50-Gbps SFP56 fiber ports (named Ethernet 1/1 through 1/12) Four fixed 4x40/100/200 QSFP56 ports (named Ethernet 1/13 to 1/16)	
Network modules	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.	

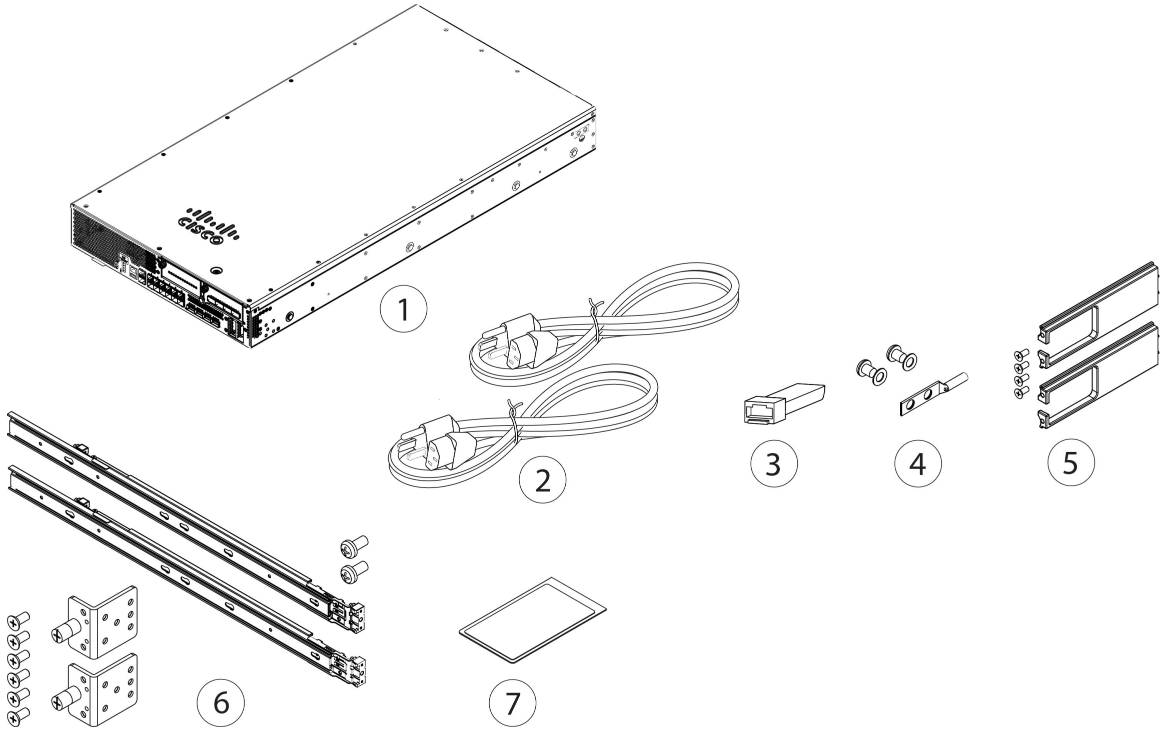
Feature	CSF-6160	CSF-6170
Supported network modules	• 8-port 1/10-Gbps SFP+ (CSF6K-XNM-8X10G) • 8-port 1/10/25-Gbps SFP+ (CSF6K-XNM-8X25G) • 4-port 40-Gbps QSFP/QSFP+ (CSF6K-XNM-4X40G) • 4-port 40/100/200-Gbps QSFP56/QSFP (CSF6K-XNM-4X200G) • 2-port 100-Gbps QSFP56/QSFP28/QSFP (CSF6K-XNM-2X100G) • 6-port 1-Gbps SFP SX multimode hardware bypass (CSF6K-XNM-6X1SXF) • 6-port 10-Gbps SFP SR multimode hardware bypass (CSF6K-XNM-6X10SRF) • 6-port 10-Gbps SFP LR single mode hardware bypass (CSF6K-XNM-6X10LRF) • 6-port 25-Gbps SFP SR multimode hardware bypass (CSF6K-XNM-6X25SRF) • 6-port 25-Gbps SFP LR single mode hardware bypass (CSF6K-XNM-6X25LRF) • 8-port copper 1-Gbps 1000Base-T hardware bypass (CSF6K-XNM-8X1GF) • 2-port 400-Gbps QSFP-DD (CSF6K-XNM-2X400G)	
Power supply	Dual high-voltage AC/DC power supplies Supports HVAC, HVDC and LVDC (-48VDC) • High-line AC: Up to 3000 W per power supply,load-sharing redundancy, hot-swappable • Low-line AC: Up to 1500 W per power supply, load sharing with no redundancy • Both DC inputs connected: Up to 3000 W per power supply, load-sharing redundancy, hot-swappable • One DC input connected: Up to 1500 W per power supply, load sharing with no redundancy	
Redundant power	Yes 1 + 1 redundancy with dual HVAC/HVDC, or dual inputs on LVDC **Note** Ships with two power supplies.	
Fans	Four redundant dual-rotor fan modules; every module has 2 fans (hot-swappable)	

Feature	CSF-6160	CSF-6170
Storage	Two SSD drives Ships with two 3.6-TB SSDs; factory-configured for RAID1.	Two SSD drives Ships with two 7.2-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 facing the rear panel	
Power button	Controls the system's power; on front left panel See Power button and reset button, on page 9 for more information on the power button.	
Reset button	Resets the system to factory default without requiring serial console access; on front left panel. See Power button and reset button, on page 9 for more information on the reset button.	

Package contents

The following figure shows the package contents for the Secure Firewall 6100 series. 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, on page 33 for a list of PIDs associated with the package contents.

Figure 2: CSF-6160 and CSF-6170 package contents



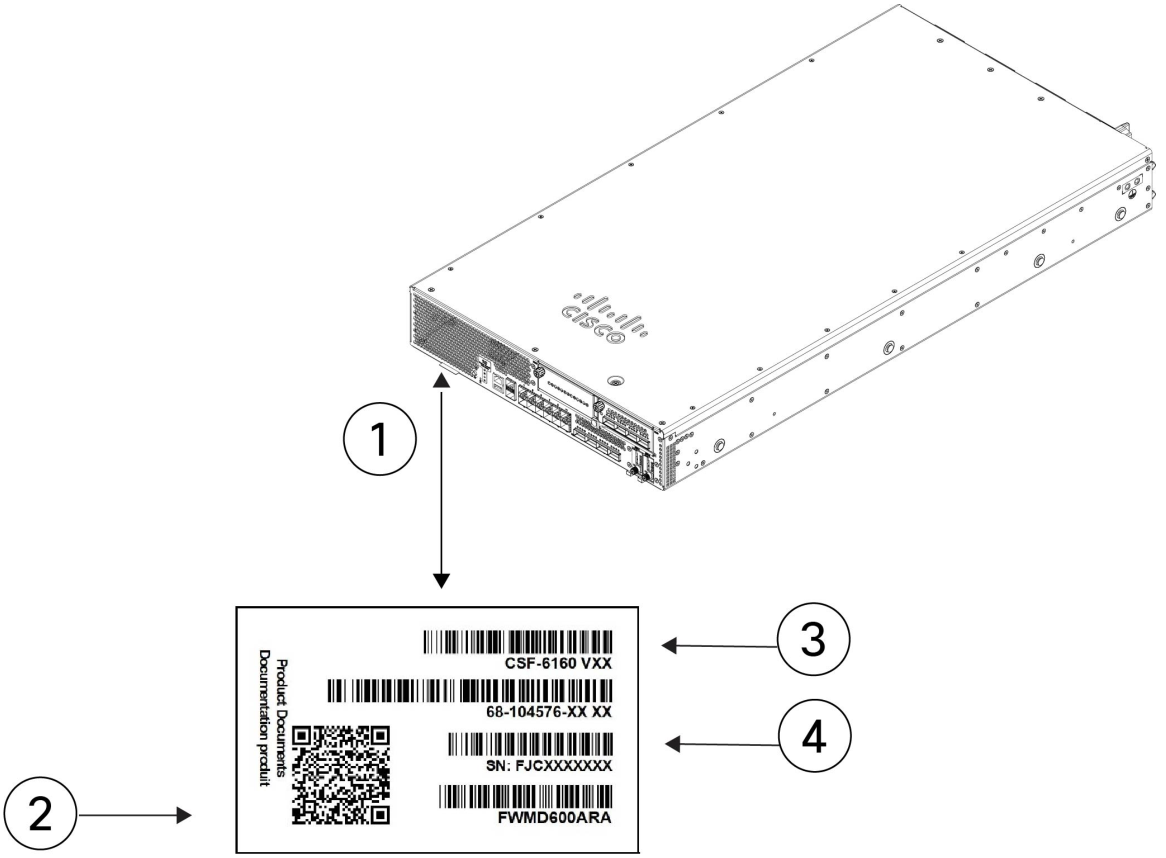
1	Secure Firewall 6100 series chassis	**2**	Two power cords (country-specific) See Power cord specifications, on page 36 for a list of supported power cords.
3	SFP transceiver (Optional; in package if ordered)	**4**	Ground lug, screws, and washers • One ground lug #6AWG 0.25-inch hole • Two ¼-20 x 0.297-inch screws • Two 0.469-inch OD, 0.261-inch ID, 0.025-inch T washers
5	Cable management bracket kit • Two cable management brackets • Four 8-32 x 0.375-inch Phillips screws (Optional; in package if ordered)	**6**	Slide rail accessories kit: • Two slide rails • Two slide rail mounting brackets • Six 8-32 x 0.302-inch slide rail mounting bracket Phillips screws for securing the brackets to the chassis • Two M3 x 0.5 x 6-mm Phillips screws for securing the chassis to your rack

7	*Cisco Secure Firewall 6100* This document has links to the hardware installation guide, regulatory and safety information guide, and warranty and licensing information. It also contains a QR code and URL that point 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 6100 series 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, the hardware installation guide and the zero-touch provisioning guide.

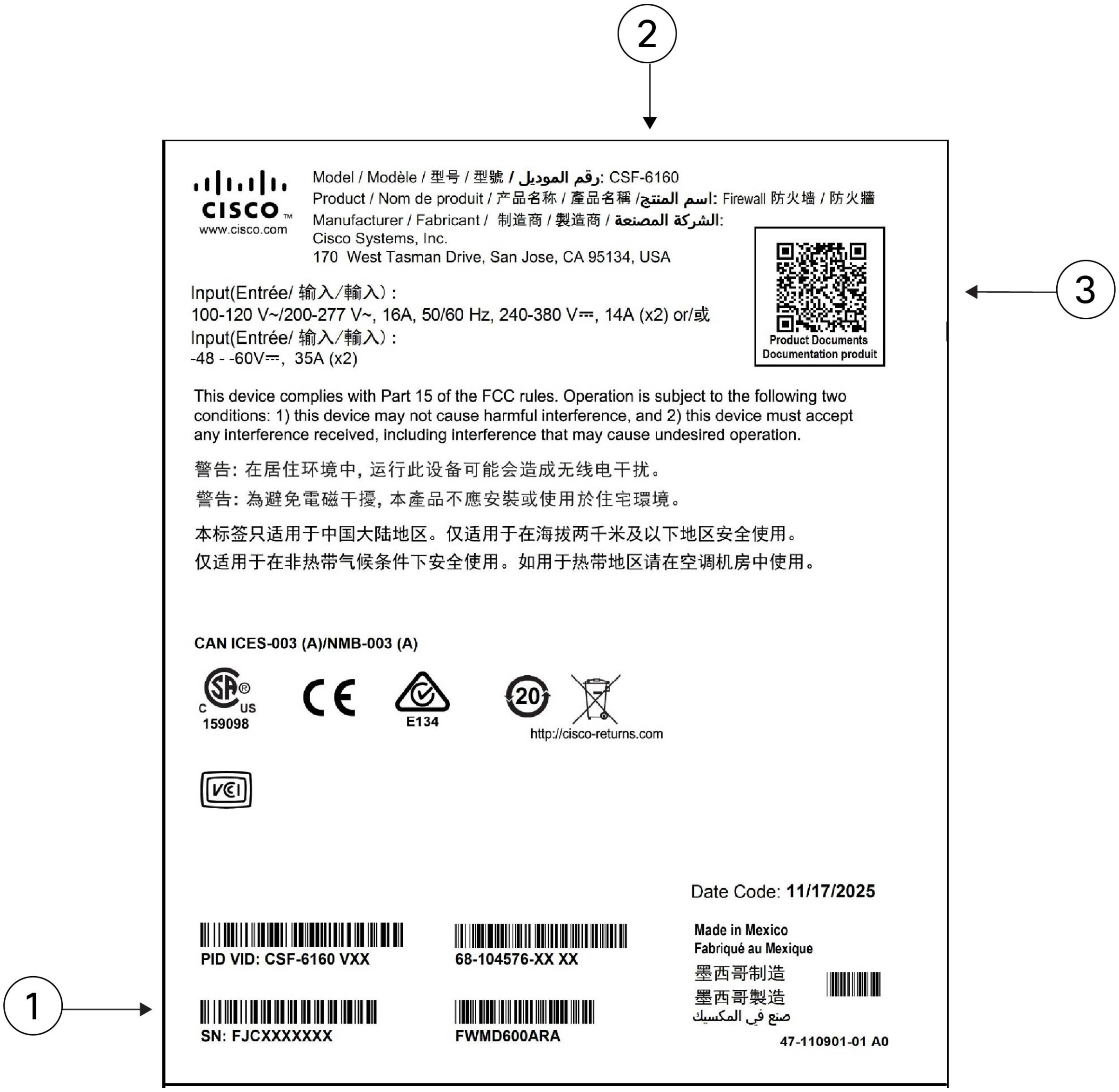
Figure 3: Pullout asset card



1	Pullout asset tag	**2**	Documentation Portal QR code
3	Chassis model number	**4**	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



Model / Modèle / 型号 / 型號 / رقم الموديل: CSF-6160
Product / Nom de produit / 产品名称 / 產品名稱 /اسم المنتج: Firewall 防火墙 / 防火牆
Manufacturer / Fabricant / 制造商 / 製造商 / الشركة المصنعة:
Cisco Systems, Inc.
170 West Tasman Drive, San Jose, CA 95134, USA

Product Documents
Documentation produit

Input(Entrée/ 输入/輸入) :
100-120 V~/200-277 V~, 16A, 50/60 Hz, 240-380 V⎓, 14A (x2) or/或
Input(Entrée/ 输入/輸入) :
-48 - -60V⎓, 35A (x2)

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: 1) this device may not cause harmful interference, and 2) this device must accept any interference received, including interference that may cause undesired operation.

警告: 在居住环境中, 运行此设备可能会造成无线电干扰。

警告: 為避免電磁干擾, 本產品不應安裝或使用於住宅環境。

本标签只适用于中国大陆地区。仅适用于在海拔两千米及以下地区安全使用。
仅适用于在非热带气候条件下安全使用。如用于热带地区请在空调机房中使用。

CAN ICES-003 (A)/NMB-003 (A)

C US
159098

E134

http://cisco-returns.com

Date Code: **11/17/2025**

PID VID: CSF-6160 VXX

68-104576-XX XX

Made in Mexico
Fabriqué au Mexique
墨西哥制造
墨西哥製造
صنع في المكسيك

SN: FJCXXXXXXX

FWMD600ARA

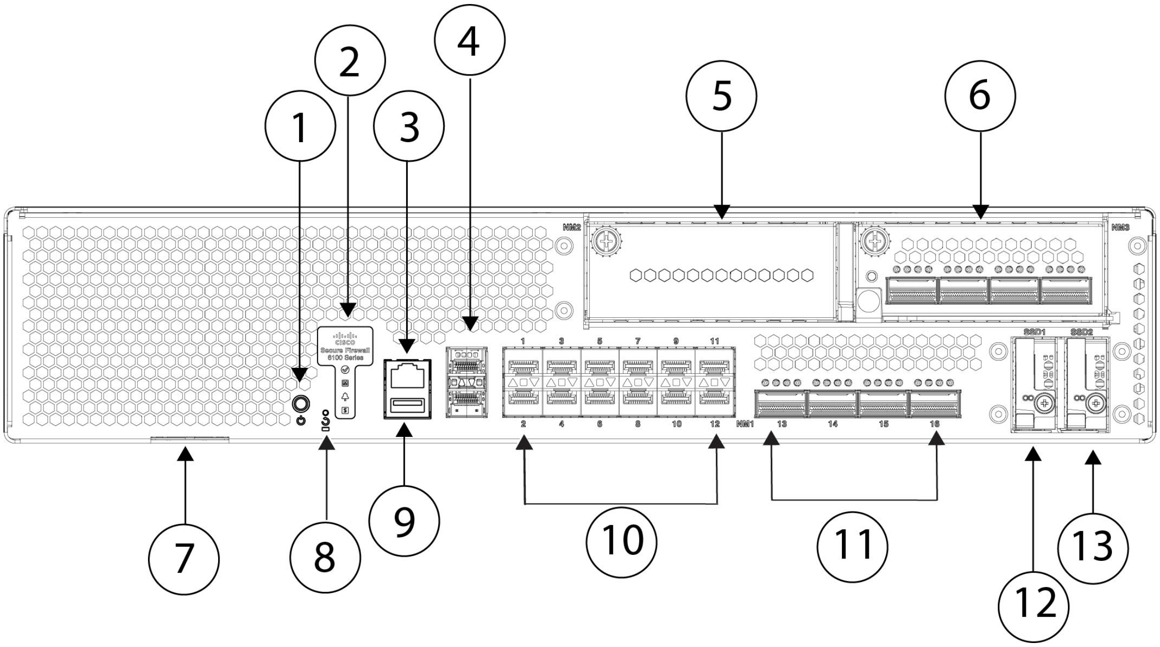
47-110901-01 A0

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

Front panel

The following figure shows the front panel of the Secure Firewall 6100 series. See Front panel LEDs, on page 11 for a description of the LEDs.

Figure 5: CSF-6160 and CSF-6170 front panel



1	Push ON/OFF button Multi-function push button that controls the power cycle, shut down, and power up.	**2**	System LEDs
3	RJ-45 (8P8C) console port	**4**	Dual stacked management ports (supports 1/10/25-Gbps) 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
5	Network module slot (NM-2)	**6**	Network module slot (NM-3)
7	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.	**8**	Recessed factory reset button

9	Type A USB 3.0 port	**10**	Twelve 1/10/25/50-Gbps SFP56 fixed fiber ports (NM-1) Fiber ports named 1/1 through 1/12 left to right
11	Four 40/100/200-Gbps QSFP56 fixed fiber ports (NM-1) Fiber ports named 1/13 through 1/16 left to right	**12**	SSD slot (SSD-1)
13	SSD slot (SSD-2)		—

Power button and reset button

The Secure Firewall 6100 series has a push power button on the front panel that controls system power. The system powers on automatically when AC power is applied. The button is ON when pushed in and OFF when sticking out. For a power cycle, press and hold for 5 seconds; for a graceful shutdown, hold for 15 seconds. Always wait for LEDs to turn off before unplugging power cables to prevent disk corruption.

A recessed factory reset button is also present. Holding it for 5 seconds resets the system to factory defaults, erasing configurations and user files. Use this if credentials are lost and console access is unavailable. If power is lost during the reset, the process must be restarted after power restoration.

Power button

The power button is a nonlatching push button for system power control. It is located on the left side of the front panel. When the AC power is first turned on, you do not have to press the button because the system turns on by default. During the shutdown process the power LED flashes 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 solid amber before unplugging the AC power cables. See Front panel LEDs, on page 11 for a detailed description of the power status LED.

At the ROMMON or FX-OS prompt:

- Press the power button for 5 seconds and release it to initiate a system power cycle. The power LED flashes green at a rate of 2 Hz.
- Press the power button for 15 seconds and release it to initiate a graceful shutdown. The power LED flashes green at a rate of 10 Hz.

Note Threat Defense requires a graceful shutdown. See the Getting Started Guide for the procedure.

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.

Caution If you remove the system power cords before the graceful shutdown is complete, disk corruption can occur.

Factory reset button

The 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.

Management port, console port, and USB port

Management port

The Secure Firewall 6100 series chassis has two management ports. They are 1/10/25-Gbps SFP28 ports that support fiber as well as DAC or GLC-TE.

RJ-45 console port

The Secure Firewall 6100 series 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 Secure Firewall 6100 series 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 BAUD rate
- 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:

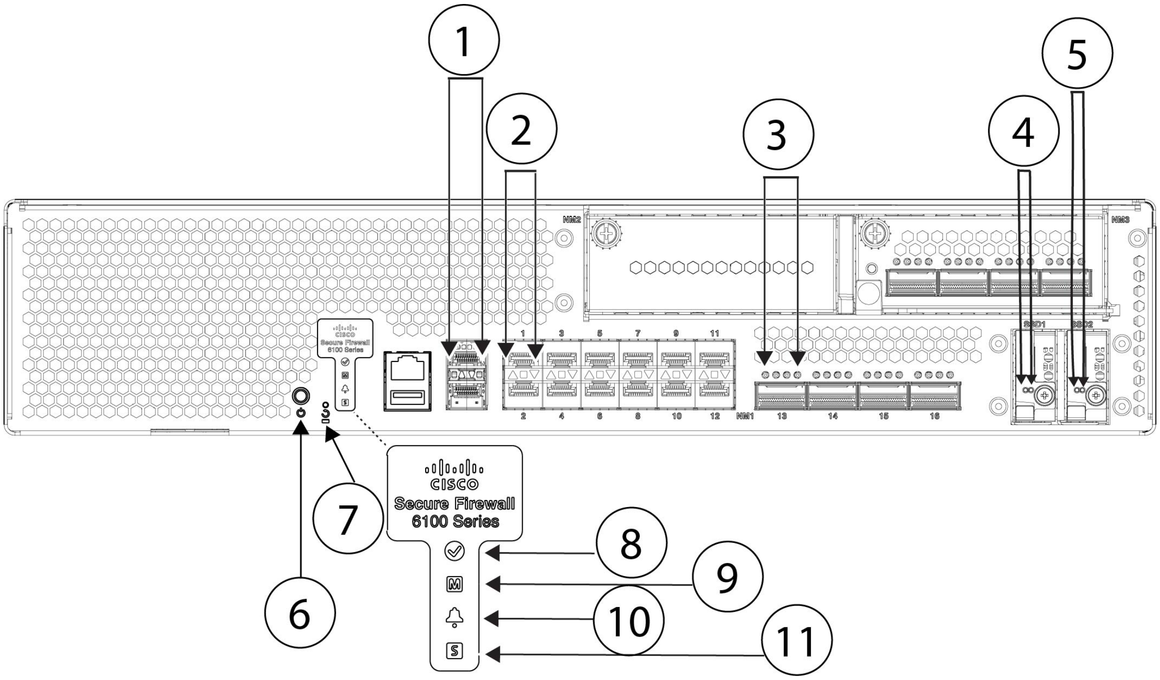
- Hot swapping
- USB drive formatted with FAT32
- Boot kickstart image from ROMMON for discovery recovery purposes
- Copy files to and from workspace:/ and volatile:/ within local-mgmt. The most relevant files are:
  - Core files
  - Ethanalyzer packet captures
  - Tech-support files
  - Security module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

Front panel LEDs

The following figure shows the Secure Firewall 6100 series front panel LEDs.

Figure 6: CSF-6160 and CSF-6170 front panel LEDs



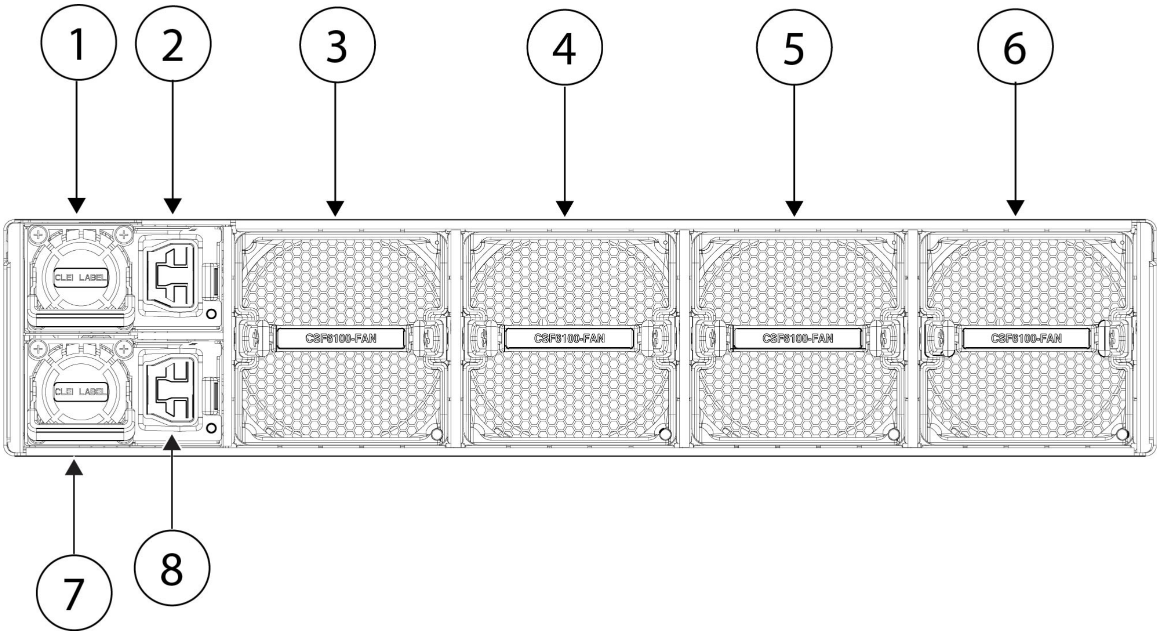
1	**Management port** The 1/10/25-Gbps fiber management port has a bicolor LED under the SFP cage that indicates link/activity/fault: • Off—No SFP. • Green—Link up. • Green, flashing—Network activity. • Amber—SFP present, but no link.	2	**Fixed fiber port link/activity** Each fiber port has one dual color LED under the SFP cage. • Off—No SFP. • Green—Link up and active. • Green, flashing—Network activity. • Amber—No link or network failure.
3	**QSFP fixed port link/activity** Each fiber port has one bicolor LED under the QSFP cage. • Off—No SFP. • Green—Link up and active. • Green, flashing—Network activity. • Amber—No link or network failure. **Note** There are four LEDs for each QSFP socket. When running native 40/100/200 Gbps, only the left LED is active (out of 4 LEDs per port). However, in the 4x10/25G/50G breakout mode, all four LEDs on a port are active and behave depending on the respective channel activity.	4	**SSD-1** **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.
5	**SSD-2** **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.	6	**Power** • 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. • Green, flashing—The system has detected a power button event, and initiated the shutdown sequence. 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. • Green—The system is fully powered up. • Amber—A graceful shutdown has been completed or power failures in the system have been detected.

7	**Factory reset button** • 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.	8	**Active** (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. • Yellow—The unit is in standby mode.
9	**Managed** Reserved for future use.	10	**Alarm** • Off—While system is powering and booting up. • Yellow—Power supply, overtemperature, and/or fan failure. • Green—No alarms.
11	**System** • Off—While system is booting up. • Green, flashing quickly—System is booting up. • Green—Normal system function. • Yellow—System boot up has failed. • Yellow, flashing—Alarm condition, system needs service or attention and may not boot properly.		—

Rear panel

The following figure shows the rear panel of the Secure Firewall 6100 series. See Power supply modules, on page 27 and Fan modules, on page 29 for a description of the power supply and fan LEDs.

Figure 7: CSF-6160 and CSF-6170 rear panel



1	Power supply module (PSU-1)	**2**	Power supply module (PSU-1) connector
3	Dual fan module (FAN-1)	**4**	Dual fan module (FAN-2)
5	Dual fan module (FAN-3)	**6**	Dual fan module (FAN-4)
7	Power supply module (PSU-2)	**8**	Power supply module (PSU-2) connector

For more information

- See Remove and replace the power supply module, on page 76 for the procedure for removing and replacing the power supply module in the Secure Firewall 6100 series.
- See for the procedure for removing and replacing the dual fan module in the Secure Firewall 6100 series.
- See Ground the chassis, on page 67 for the procedure for using the grounding lug to ground the chassis.
- See Power supply modules, on page 27 for a description of the power supply module LEDs.
- See Fan modules, on page 29 for a description of the fan LEDs.

8-Port 1/10/25-Gbps network module (CSF6K-XNM-8X10G)

The Secure Firewall 6100 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 7 for the location of the network module slots on the chassis.

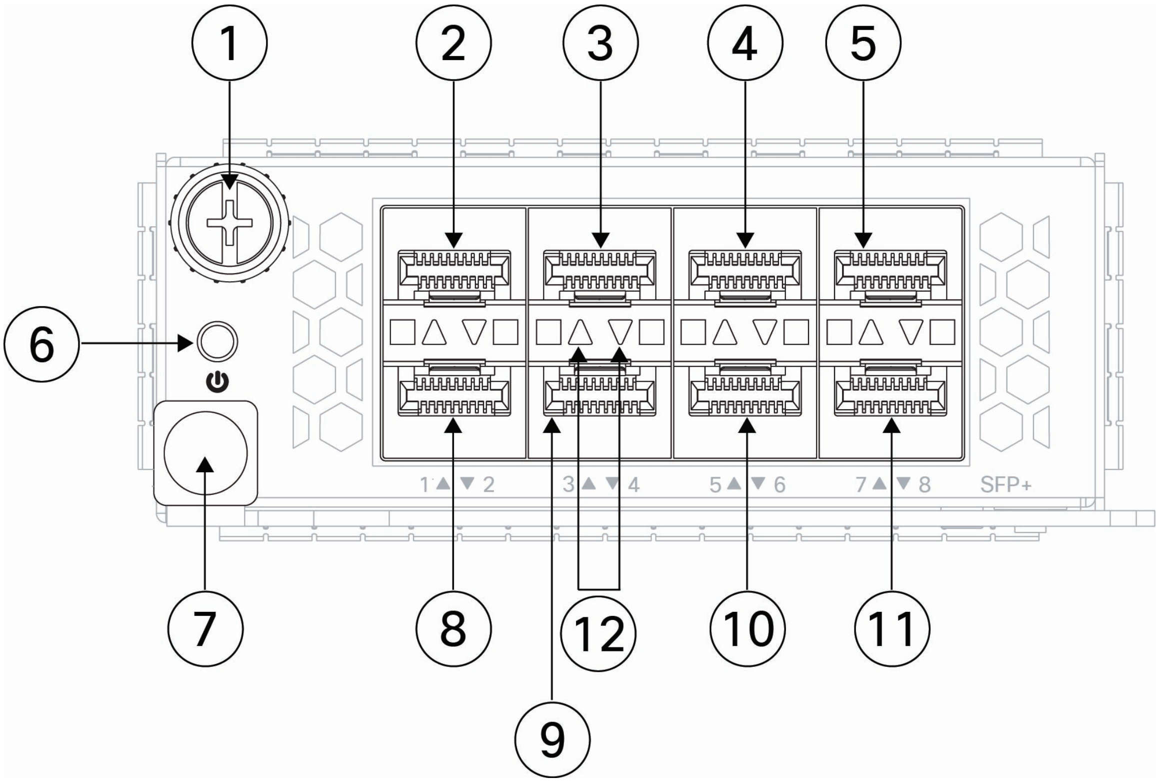
CSF6K-XNM-8X10G supports 1 Gbps and 10 Gbps full-duplex Ethernet traffic per port and is supported on all Secure Firewall 6100s. FPR6K-XNM-8X25G supports 1 Gbps, 10 Gbps, or 25 Gbps full-duplex Ethernet traffic per port and is supported on all Secure Firewall 6100s.

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.

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-Gbps 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-Gbps and 1/10/25-Gbps network module.

Figure 8: CSF6K-XNM-8X10G and 8-Port 1/10/25-GbpsCSF6K-XNM-8X25G



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.

4-Port 40-Gbps network module (CSF6K-XNM-4X40G)

The Secure Firewall 6100 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 7 for the location of the network module slots on the chassis.

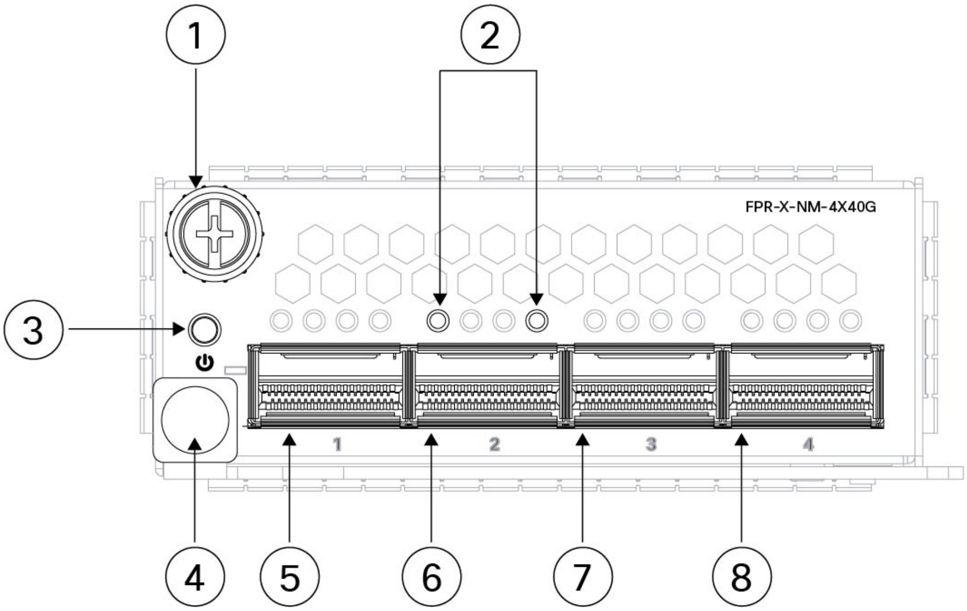
The CSF6K-XNM-4X40G supports 40-Gbps operation. This network module provides full-duplex Ethernet traffic per port. The 40-Gb network module has four QSFP+ ports. The 40-Gb ports are numbered left to right, Ethernet 2/1 or 3/1 through Ethernet 2/4 or 3/4.

You can break each of the four 40-Gbps ports into four 10-Gbps ports using the supported breakout cables. With the four-port 40-Gbps network module, you now have 16 10-Gbps 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-Gbps 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-Gbps network module.

Figure 9: CSF6K-XNM-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

2-Port 100-Gbps network module (CSF6K-XNM-2X100G)

The Secure Firewall 6100 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 7 for the location of the network module slots on the chassis.

The CSF6K-XNM-2X100G supports 40/100-Gbps operation. This network module has two QSFP/QSFP28 ports and provides full-duplex Ethernet traffic per port. The maximum bandwidth supported is 200 Gbps full duplex, where each port operates at 100 Gbps. The 100-Gbps ports are numbered left to right, Ethernet 2/1 or 3/1 through Ethernet 2/2 or 3/2.

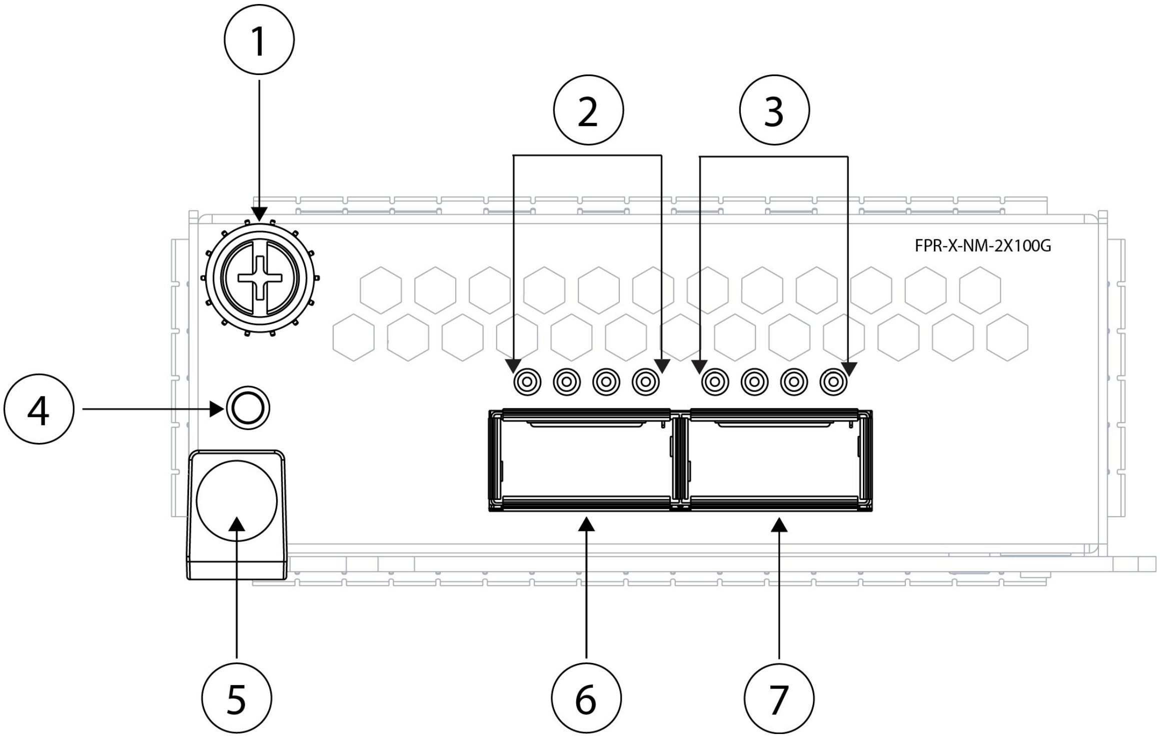
The network module has two 100-Gbps ports named E2/1 and E2/2. You can break each 100-Gbps port into four 10-Gbps or four 25-Gbps ports using the supported breakout cables. For E2/1 the new interfaces are named E2/1/1, E2/1/2, E2/1/3 and E2/1/4. For E2/2 the new interfaces are named E2/1/2, E2/2/2, E2/2/3, and E2/2/4.

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 100-Gbps 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-Gbps network module.

Note When a port operates in a 40-Gbps mode, only the left-most LED of the port indicates the link/activity status.

Figure 10: CSF6K-XNM-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		—

4-Port 200-Gbps network module (CSF6K-XNM-4X200G)

The Secure Firewall 6100 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 7 for the location of the network module slots on the chassis.

The CSF6K-XNM-4X200G supports 40/100/200-Gbps operation. This network module provides full-duplex Ethernet traffic per port. The 200-Gbps network module has four QSFP56 ports. The ports are numbered left to right, Ethernet 2/1 or 3/1 through Ethernet 2/4 or 3/4.

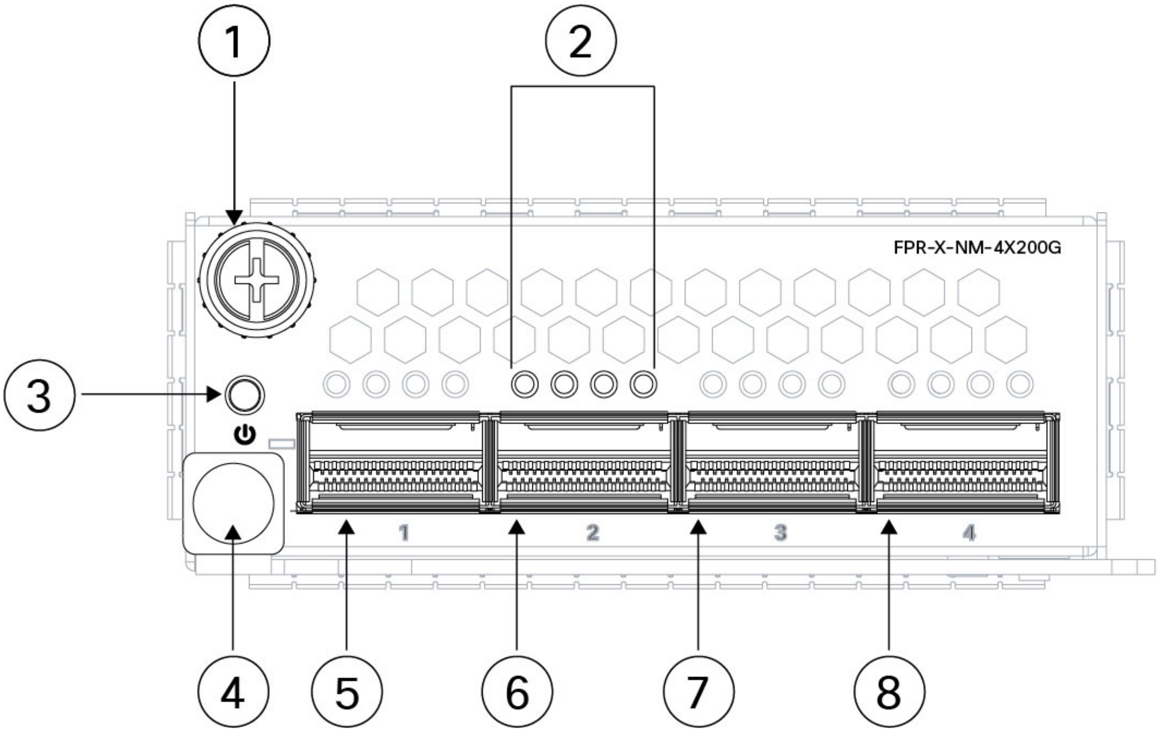
You can break each 100-Gbps port into four 10-Gbps or 25-Gbps ports using the supported breakout cables. With the four-port 200-Gbps network module, you now have 16 10-Gbps or 25-Gbps interfaces. The added interfaces are Ethernet 2/1/1 or 3/1/1 through Ethernet 2/4/4 or 3/4/4.

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-Gbps 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-Gbps network module.

Note When a port operates in 40-Gvps or 100-Gbps mode, only the left-most LED of the port indicates link/activity status.

Figure 11: CSF6K-XNM-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

2-Port 400-Gbps network module (CSF6K-XNM-2X400G)

The Secure Firewall 6100 chassis has two network module slots named NM-2 and NM-3, which are left to right on the front (I/O side) 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 7 for the location of the network module slots on the chassis.

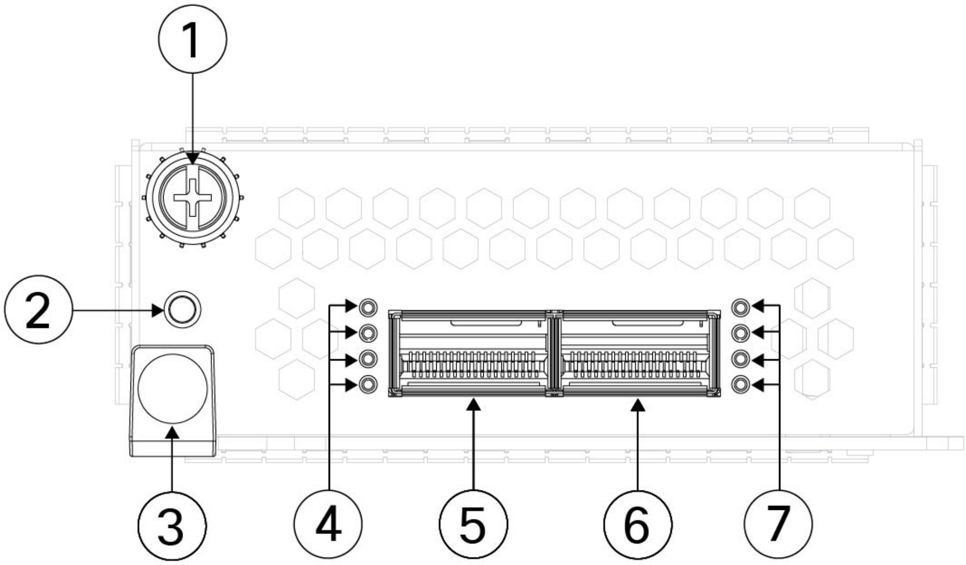
The CSF6K-XNM-2X400G supports 400-Gbps operation, and is also designed to support 200-Gbps, 100-Gbps, and 40-Gbps per port. This network module provides full-duplex Ethernet traffic per port. The 400-Gbps network module supports two QSFP-DD transceivers and is designed to also support 200-Gbps QSFP56, 100-Gbps QSFP28, and 40-Gbps QSFP+ transceivers. The 400-Gbps ports are numbered left to right, Ethernet 2/1 or 3/1 through Ethernet 2/2 or 3/2.

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 200/400-Gbps 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 200/400-Gbps network module.

Note When a port operates in 40-Gbps, 100-Gbps, or 200-Gbps mode, only the left-most LED indicates link/activity status.

Figure 12: CSF6K-XNM-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
7	Network activity LEDs • Off—No SFP. • Amber—No link or a network failure. • Green—Link is up. • Green, flashing—Network activity.		—

8-Port 1000Base-T network module with hardware bypass (CSF6K-XNM-8X1GF)

The Secure Firewall 6100 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 7 for the location of the network module slots on the chassis.

CSF6K-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 6100 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.

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.

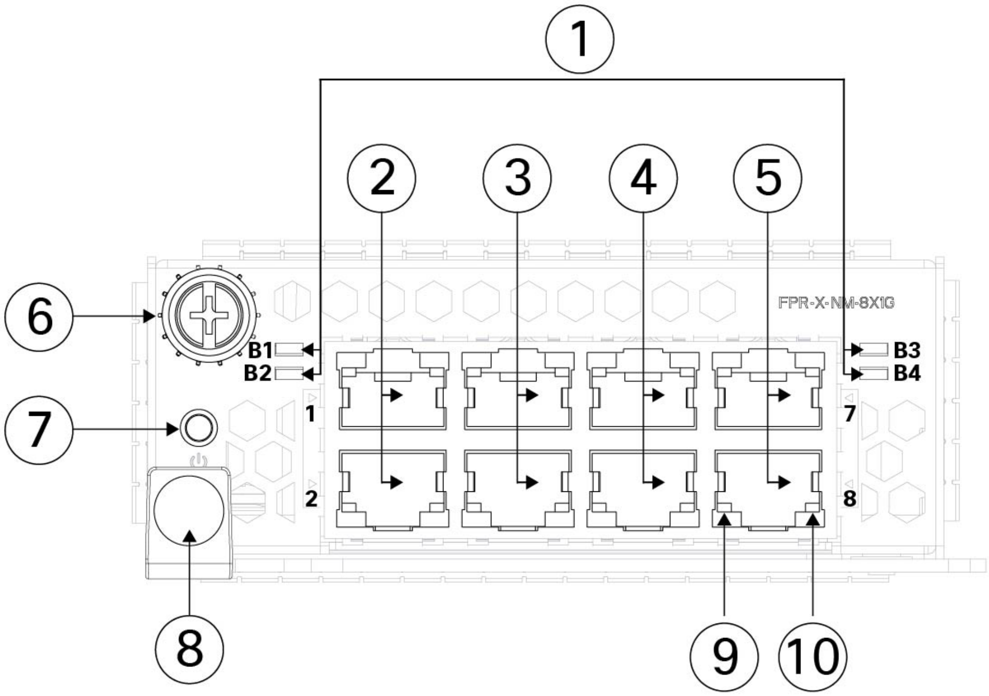
The hardware and the system support hot swapping if you are replacing a network module with the same type of network module. If you replace the 8-port 1000Base-T network module with another supported network module, you must reboot the chassis so that the new network module is recognized. See the configuration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

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.

Note When a port operates in 400-Gbps, 200-Gbps, 100-Gbps, or 40-Gbps mode, only the top LED of the port indicates link/activity status.

Figure 13: CSF6K-XNM-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.

6-Port 1-Gbps SX/10-Gbps SR/10-Gbps LR/25-Gbps SR/25-Gbps LR network module with hardware bypass (CSF6K-XNM-6X10SRF, CSF6K-XNM-6X10LRF, CSF6K-XNM-6X25SRF, and CSF6K-XNM-6X25LRF)

The Secure Firewall 6100 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 7 for the location of the network module slots on the chassis.

The CSF6K-XNM-6X10SRF, CSF6K-XNM-6X10LRF, CSF6K-XNM-6X25SRF, and CSF6K-XNM-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 6100 but is routed to the paired port. This network module has built-in SFP 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.

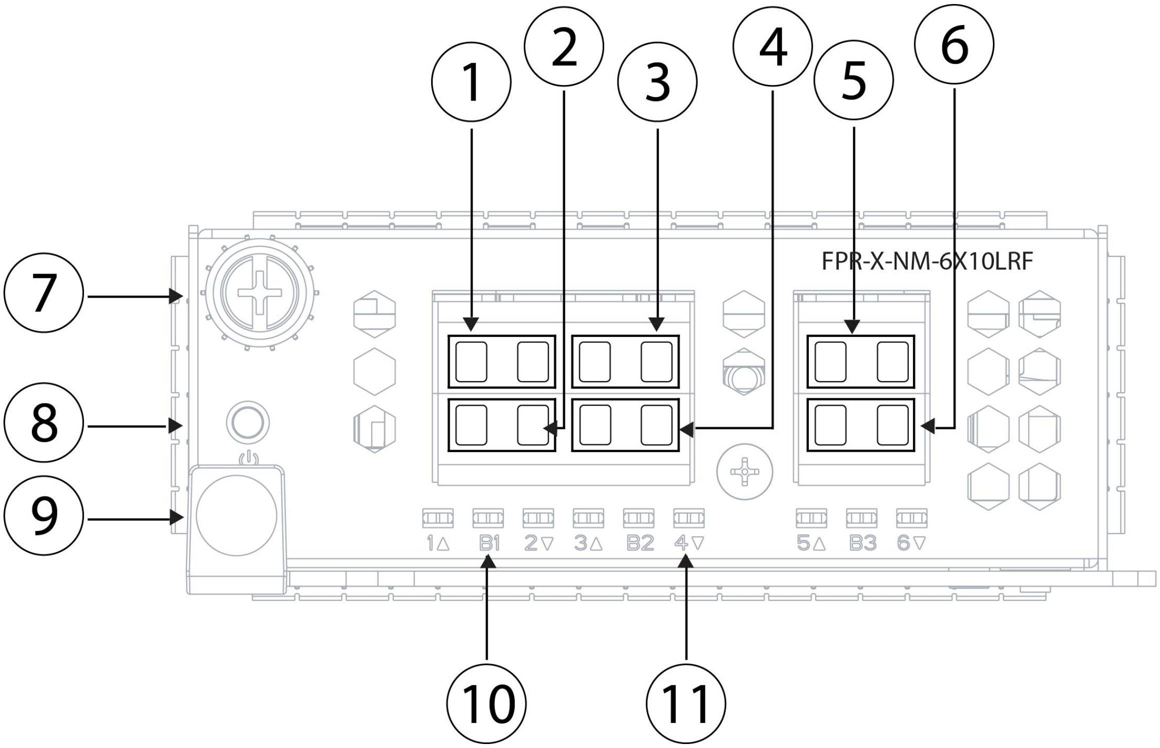
Note If you have an inline interface set with a mix of hardware bypass and nonhardware bypass interfaces, you cannot enable hardware bypass on this inline interface set. You can only enable hardware bypass on an inline interface set if all the pairs in the inline set are valid hardware bypass pairs.

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 10/25-Gbps 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-Gbps network module.

Figure 14: CSF6K-XNM-6X10SRF, CSF6K-XNM-6X10LRF, CSF6K-XNM-6X25SRF, and CSF6K-XNM-6X25LRF



1	Port 1 Ethernet 2/1 or 3/1 Ports 1 and 2 are paired together to form a hardware bypass pair.	**2**	Port 2 Ethernet 2/2 or 3/2 Ports 1 and 2 are paired together to form a hardware bypass pair.
3	Port 3 Ethernet 2/3 or 3/3 Ports 3 and 4 are paired together to form a hardware bypass pair.	**4**	Port 4 Ethernet 2/4or 3/4 Ports 3 and 4 are paired together to form a hardware bypass pair.
5	Port 5 Ethernet 2/5 or 3/5 Ports 5 and 6 are paired together to form a hardware bypass pair.	**6**	Port 6 Ethernet 2/6 or 3/6 Ports 5 and 6 are paired together to form a hardware bypass pair.
7	Captive screw	**8**	Power LED

9	Handle ejector	10	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.
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.		—

Power supply modules

The Secure Firewall 6100 series supports two power supply modules so that dual power supply redundancy protection is available. Facing the back of the chassis, the power supply modules are numbered top to bottom—PSU-1 and PSU-2.

The power supply module is hot-swappable. See Product ID numbers, on page 33 for a list of the PIDs associated with the Secure Firewall 6100 series power supply modules.

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.

The CSF6100-PWR-AC power supply is triple input, AC (low line), HVAC (high line) and HVDC. The dual power supply modules can supply up to 3000-W each of power across the input voltage range (220 VAC). The load is shared when both power supply modules are plugged in and running at the same time.

The HVAC/HVDC power supply module can operate at 110 VAC (low line) input, but output power is cut in half (1500 W each). With two power supply modules installed, the system is capable of 3000 W consumption, but redundancy is not available.

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.

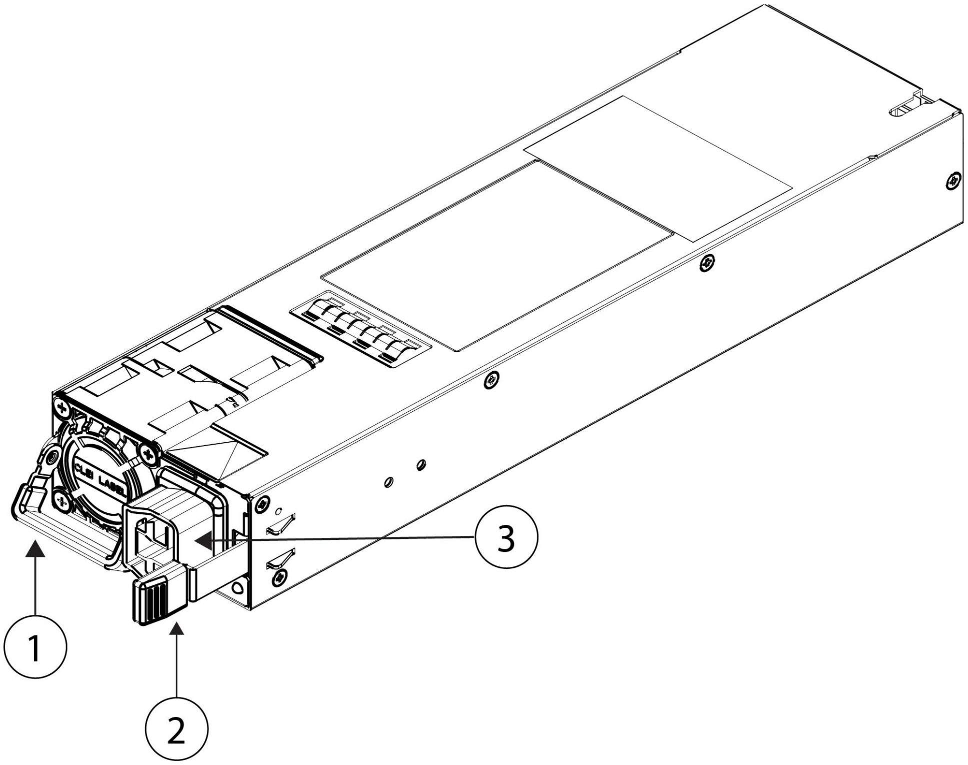
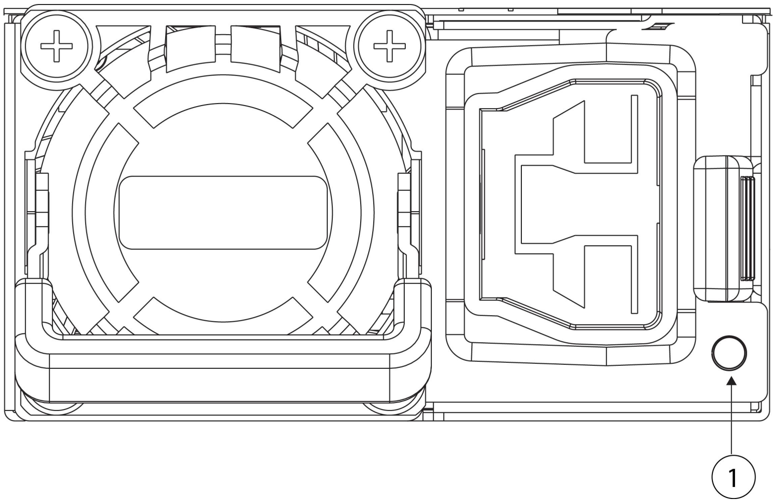


Figure 15: Power supply module

1	Handle	2	Release tab
3	Power cord connector		—

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

Figure 16: Power supply module LED



1	Power supply LED: • Green—Active mode • Green, flashing—Standby mode • Green, flashing—Boot loading process • Amber—No AC power, but the other power supply module in the system is operating • Amber, flashing—Warning event (high temperature or fan fault) • Off—No input power

For more information

- See Remove and replace the power supply module, on page 76 for the procedure for removing and replacing the power supply module in the Secure Firewall 6100.

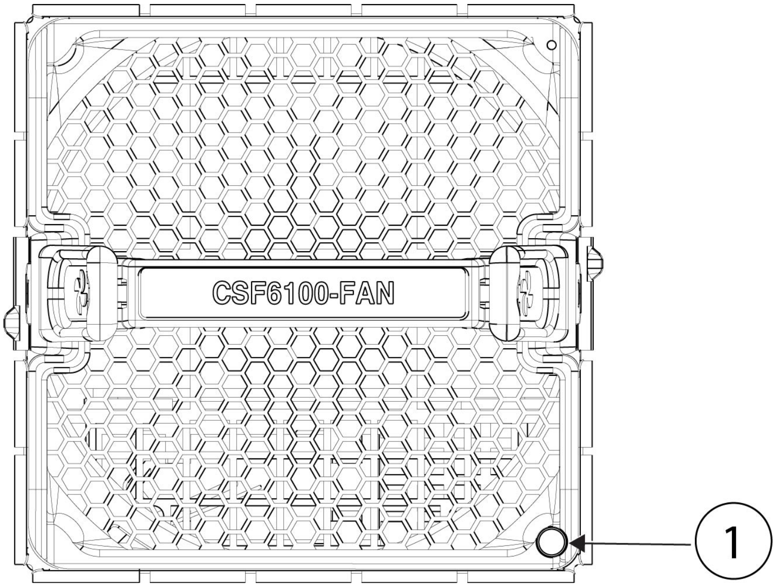
Fan modules

The Secure Firewall 6100 series has four dual-rotor axial fan modules.When one fan fails, the other fan modules spin at maximum speed so that the system continues to function. The fan modules are hot-swappable and installed in the rear of the chassis. They are labeled FAN-1 though FAN-4 from left to right on the rear of the chassis.

⚠ **Caution** If a fan module fails, remove it from the chassis and replace it within 30 seconds. After 30 seconds the CPU temperature can exceed the operating temperature, which can reduce performance. See Remove and replace the fan module, on page 74 for the procedure for removing and replacing the fan module.

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

Figure 17: Fan module LED



1	Two-color LED (green and yellow)

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.
- Yellow, flashing—One or more fan rotor RPMs is not normal. Immediate attention is required.
- Yellow—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 33 for a list of the PIDs associated with the Secure Firewall 6100 series fans.
- See Remove and replace the fan module, on page 74 for the procedure for removing and replacing the fan modules.

SSDs

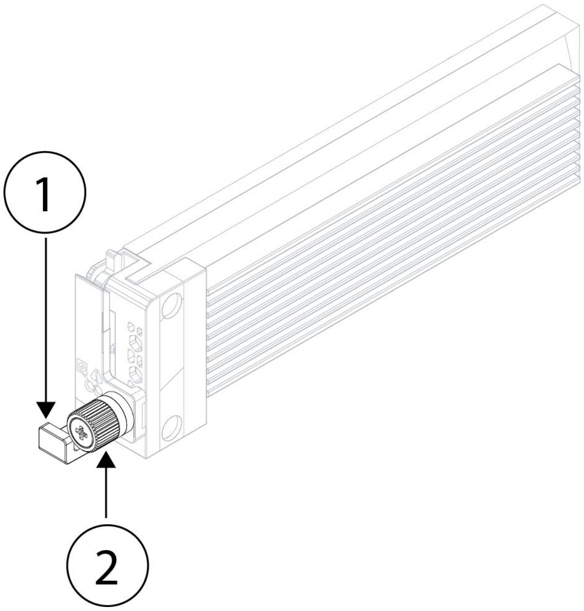
The Secure Firewall 6100 series has two SSD slots that each hold one Non-Volatile Memory Express (NVMe) SSD. By default the Secure Firewall 6160 series ships with two 3.6-TB SSDs installed in slot 1 and slot 2. The Secure Firewall 6170 ships with two 7.2-TB SSDs installed in slot 1 and slot 2. Software 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.

See Product ID numbers, on page 33 for a list of the PIDs associated with the Secure Firewall 6100 series SSDs. The SSD drive identifiers are `disk0:` and `disk1:`.

Figure 18: SSD



1	SSD release tab	**2**	Captive screw

For more information

- See Front panel LEDs, on page 11 for the location and description of the SSD LEDs on the front panel.
- See Remove and replace the SSD, on page 73 for the procedure for removing and replacing the SSD.
- See the configuration guide for your software for the procedures for removing and adding an SSD from the RAID1 configuration.

Hardware specifications

The following table contains hardware specifications for the Secure Firewall 6100 series.

Table 2: CSF-6160 and CSF-6170 hardware specifications

Specification	CSF-6160	CSF-6170
Chassis		
Chassis dimensions (H x W x D)	3.5 x 16.9 x 32.5 inches (8.89 x 42.926 x 82.55 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)	
Chassis weight (fully loaded)	66 lb (29.93 kg)	
Power Supply		
Power supply module dimensions	1.575 x 2.657 x 9.92 inches (40.0 x 67.5 x 252 mm)	
Configuration	2 power supply modules; up to 3000 W each, hot-swappable, load-sharing redundancy	
AC input voltage	100 to 120 VAC (HVAC low line) 200 to 277 VAC (HVAC high line)	
AC input frequency	50 to 60 Hz (nominal)	
HVDC input voltage	240 to 380 VDC	
LVDC input voltage	–48 VDC to –60 VDC	
AC current draw (maximum)	13 A (high line AC)	14 A (high line AC)
System HVDC current draw (maximum)	11 A	12 A
System LVDC current draw (maximum)	29 A	33 A
Input power consumption	1740 W (typical) 2440 W (maximum)	2010 W (typical) 2760 W (maximum)
Environmental		
Temperature	Operating: 32 to 104°F (0 to 40°C) Above 6000 feet, derate the maximum operating temperature by 1°C/1000 ft. Nonoperating: -40 to 85°F (-40 to 65°C)	Operating: 32 to 95°F (0 to 35°C) Above 6000 feet, derate the maximum operating temperature by 1°C/1000 ft. Nonoperating: -40 to 85°F (-40 to 65°C)
Humidity	Operating: 5 to 90% noncondensing Nonoperating: 5 to 95% noncondensing	

Specification	CSF-6160	CSF-6170
Altitude	Operating: 0 to 10,000 ft (0 to 3048 m) Operating: 0 to 6562 ft (0 to 2000 m) in China Derate the maximum operating temperature 1°C/1K-ft above 6000 ft. Nonoperating: 40,000 ft (12,192 m) maximum	
Sound pressure	<=74 dBA (typical) <= 90 dBA (maximum) **Note** This system may exceed 85 dBA when operating in high ambient environments. For environments above 85 dBA, hearing protection for sound pressure is required.	
Sound power	<=81 dB (typical) <=98 dB (maximum)	

Product ID numbers

The following table lists the product IDs (PIDs) associated with the Secure Firewall 6100 series. 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 Secure Firewall Threat Defense Command Reference or the Cisco ASA Series Command Reference to display a list of the PIDs for your Secure Firewall 6100 series.

Table 3: CSF-6160 and CSF-6170 PIDs

PID	Description
Chassis	
CSF6160-A-ASA-K9	Secure Firewall 6160 appliance, ASA
CSF6170-A-ASA-K9	Secure Firewall 6170 appliance, ASA
CSF6160-A-TD-K9	Secure Firewall 6160 appliance, threat defense
CSF6170-A-TD-K9	Secure Firewall 6170 appliance, threat defense
Modular Components	
CSF6100-PWR-AC	AC/HVAC/HVDC power supply
CSF6100-PWR-AC=	AC/HVAC/HVDC power supply (spare)

PID	Description
CSF6100-FAN	Fan module
CSF6100-FAN=	Fan module (spare)
CSF6100-SSD3600	SSD module for the Secure Firewall 6160
CSF6100-SSD3600=	SSD module for the Secure Firewall 6160 (spare)
CSF6100-SSD7200	SSD module for the Secure Firewall 6170
CSF6100-SSD7200=	SSD module for the Secure Firewall 6170 (spare)
Memory	
CSF6100-MEM-C1X64-	Secure Firewall 6160 CPU 1 x 64 GB
CSF6100-MEM-C1X96-	Secure Firewall 6170 CPU 1 x 96 GB
Kits	
CSF6100-ACC-KIT	Hardware accessory kit (rack mounts, cables)
CSF6100-ACC-KIT=	Hardware accessory kit (rack mounts, cables) (spare)
CSF6100-MEM-C1X64=	Secure Firewall 6160 CPU 1 x 64 GB memory kit (spare)
CSF6100-MEM-C1X96=	Secure Firewall 6170 CPU 1 x 96 GB memory kit (spare)
CSF6100-SLD-RAILS	Slide rail kit
CSF6100-SLD-RAILS=	Slide rail kit (spare)
CSF6100-CBL-MGMT	Cable management brackets
CSF6100-CBL-MGMT=	Cable management brackets (spare)
Network modules	
CSF6K-XNM-6X1SXF	6-port 1-Gbps SFP hardware bypass network module, SX multimode
CSF6K-XNM-6X1SXF=	6-port 1-Gbps SFP hardware bypass network module, SX multimode (spare)
CSF6K-XNM-6X10SRF	6-port 10-Gbps SFP hardware bypass network module, SR multimode
CSF6K-XNM-6X10SRF=	6-port 10-Gbps SFP hardware bypass network module, SR multimode (spare)
CSF6K-XNM-6X10LRF	6-port 10-Gbps SFP hardware bypass network module, LR single mode

PID	Description
CSF6K-XNM-6X10LRF=	6-port 10-Gbps SFP hardware bypass network module, LR single mode (spare)
CSF6K-XNM-6X25SRF	6-port 25-Gbps SFP hardware bypass network module, SR multimode
CSF6K-XNM-6X25SRF=	6-port 25-Gbps SFP hardware bypass network module, SR multimode (spare)
CSF6K-XNM-6X25LRF	6-port 25-Gbps SFP hardware bypass network module, LR single mode
CSF6K-XNM-6X25LRF=	6-port 25-Gbps SFP hardware bypass network module, LR single mode (spare)
CSF6K-XNM-8X1GF	8-port 10/100/1000Base-10 hardware bypass network module
CSF6K-XNM-8X1GF=	8-port 10/100/1000Base-10 hardware bypass network module (spare)
CSF6K-XNM-8X10G	8-port 1/10-Gbps SFP+ network module
CSF6K-XNM-8X10G=	8-port 1/10-Gbps SFP+ network module (spare)
CSF6K-XNM-8X25G	8-port 1/10/25-Gbps ZSFP network module
CSF6K-XNM-8X25G=	8-port 1/10/25-Gbps ZSFP network module (spare)
CSF6K-XNM-4X40G	4-port 40-Gbps QSFP+ network module
CSF6K-XNM-4X40G=	4-port 40-Gbps QSFP+ network module
CSF6K-XNM-2X100G	2-port 100-Gbps QSFP+ network module
CSF6K-XNM-2X100G=	2-port 100-Gbps QSFP+ (spare)
CSF6K-XNM-4X200G	4-port 40/100/200-Gbps QSFP+ network module
CSF6K-XNM-4X200G=	4-port 40/100/200-Gbps QSFP+ network module (spare)
CSF6K-XNM-2X400G	2-port 40/100/200/400-Gbps QSFP-DD
CSF6K-XNM-2X400G=	2-port 40/100/200/400-Gbps QSFP-DD (spare)
CSF6100-NM-BLANK	Network module blank slot cover
CSF6100-NM-BLANK=	Network module blank slot cover (spare)

Power cord specifications

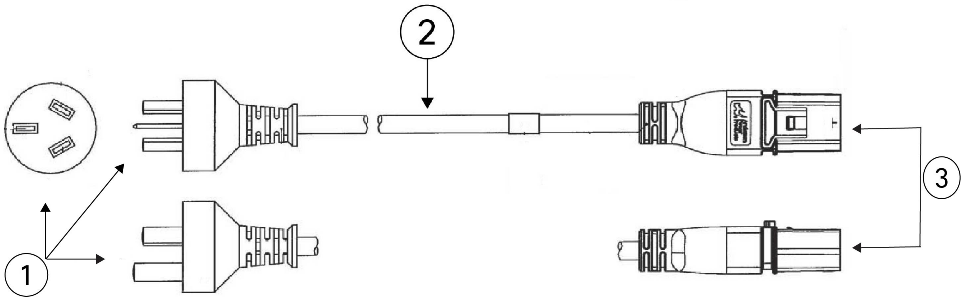
Each power supply has a separate power cord. Standard power cords or jumper power cords are available for connection to the secure firewall. The jumper power cords for use in racks are available as an optional alternative to the standard power cords.

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 Firewall 6100 series are supported.

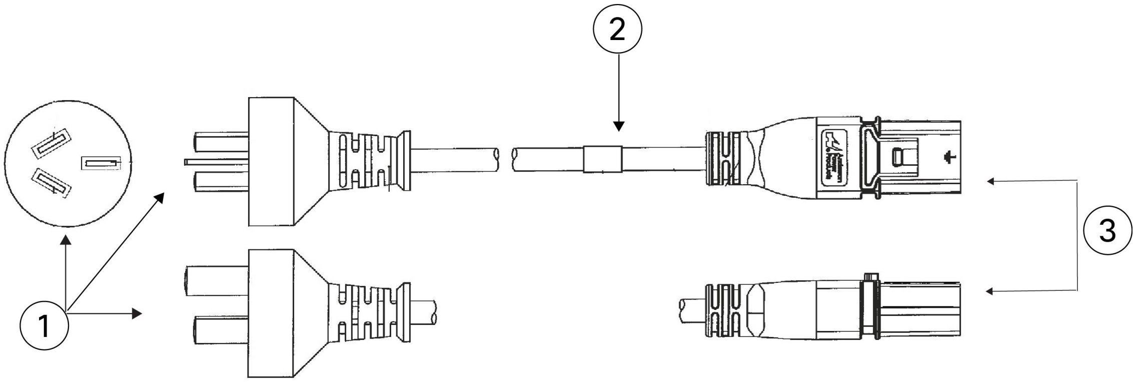
The following HVAC power cords are supported. One end of the cable has the Anderson Saf-D-Grid plug.

Figure 19: Argentina



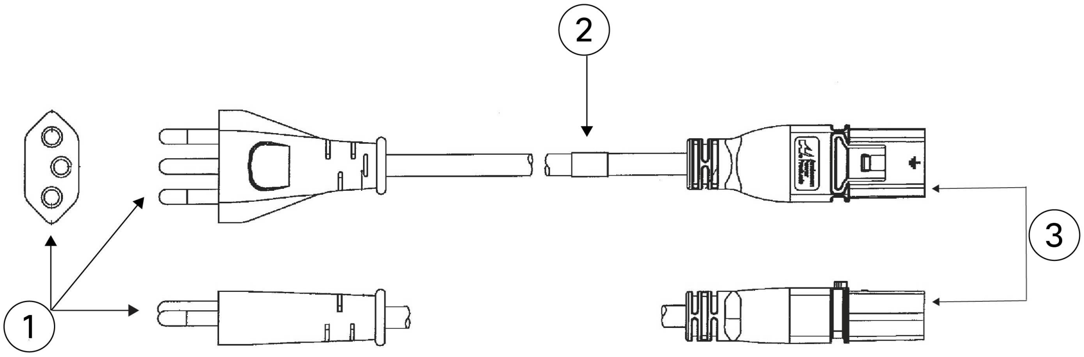
	PID: CAB-AC-16A-SG-AR		Part number: 37-1649-01
1	Plug: IRAM 2073	**2**	Cord set rating: 16 A, 250 V
3	Connector: Saf-D-Grid		Cord length: 14 ft (4.3 m)

Figure 20: Australia/New Zealand



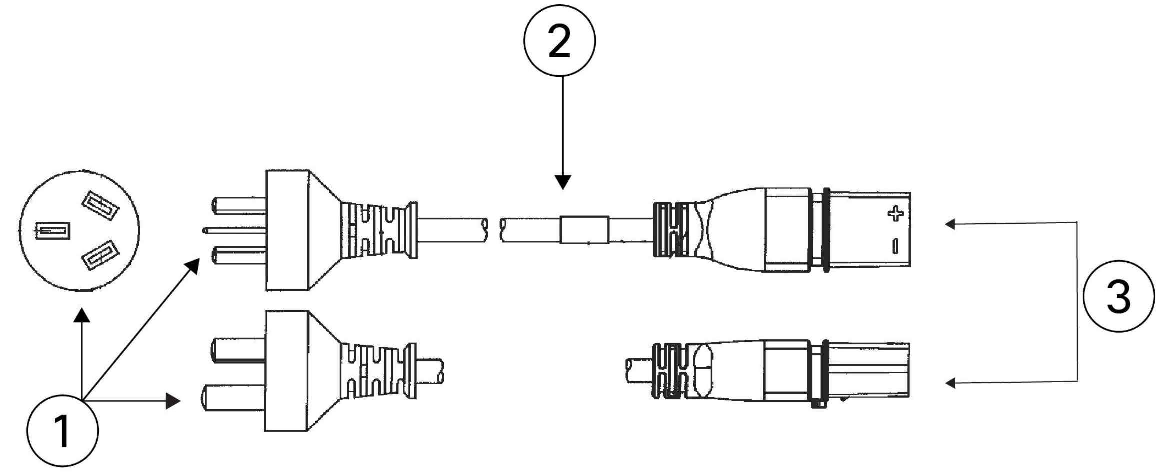
	PID: CAB-AC-16A-SG-AZ		Part number: 37-1661-01
1	Plug: AU20LS3	**2**	Cord set rating: 16 A, 250 V
3	Connector: Saf-D-Grid		Cord length: 14 ft (4.3 m)

Figure 21: Brazil



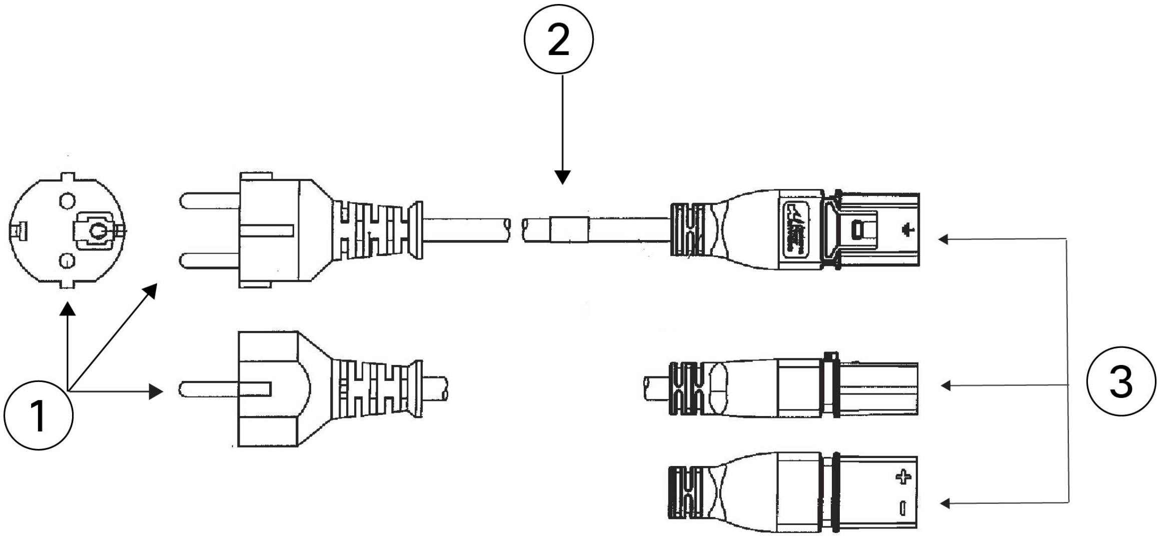
	PID: CAB-AC-16A-SG-BR		Part number: 37-1650-01
1	Plug: EL224	**2**	Cord set rating: 16 A, 250 V
3	Connector: Saf-D-Grid		Cord length: 14 ft (4.3 m)

Figure 22: China



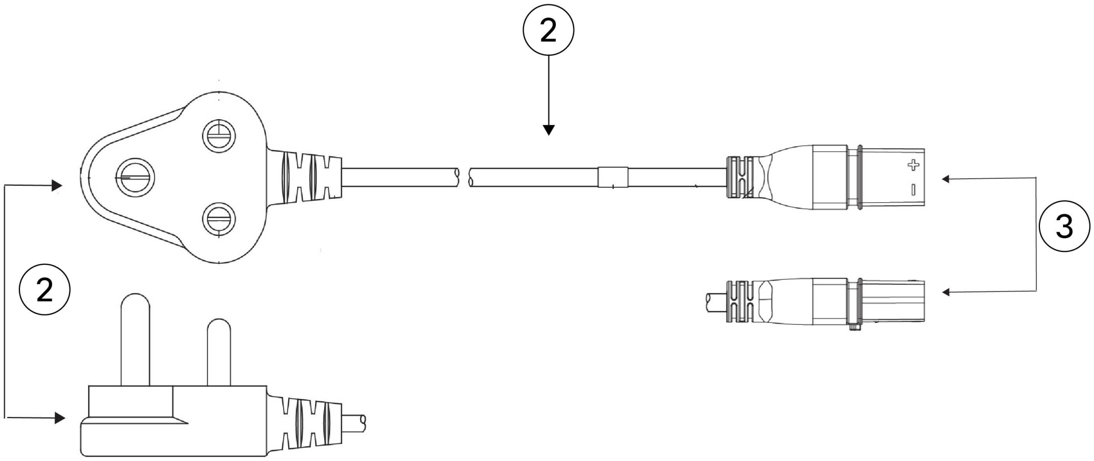
	PID: CAB-AC-16A-SG-CH		Part number: 37-1655-01
1	Plug: GB 16C	**2**	Cord set rating: 16 A, 250 V
3	Connector: Saf-D-Grid		Cord length: 14 ft (4.3 m)

Figure 23: Europe



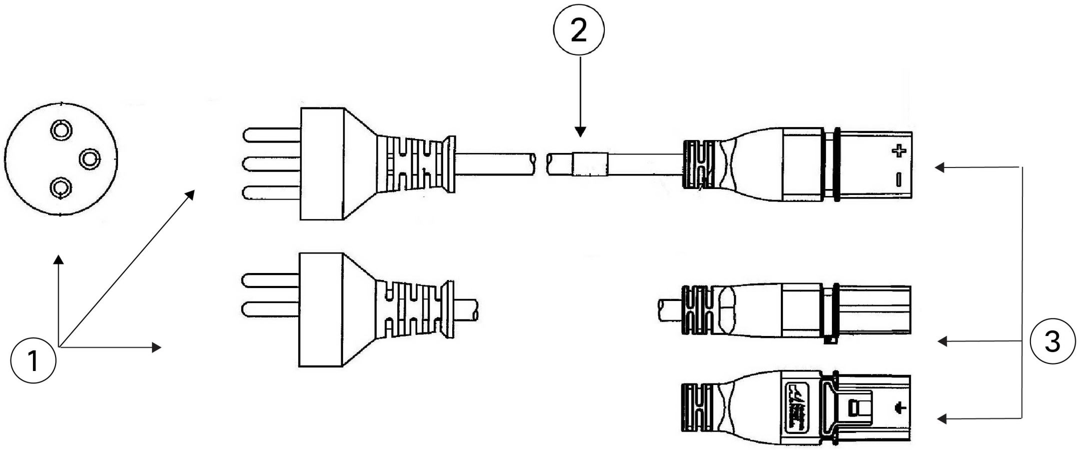
	PID: CAB-AC-16A-SG-EU		Part number: 37-1660-01
1	Plug: CEE 7/7	**2**	Cord set rating: 16 A, 250 V
3	Connector: Saf-D-Grid		Cord length: 14 ft (4.3 m)

Figure 24: India



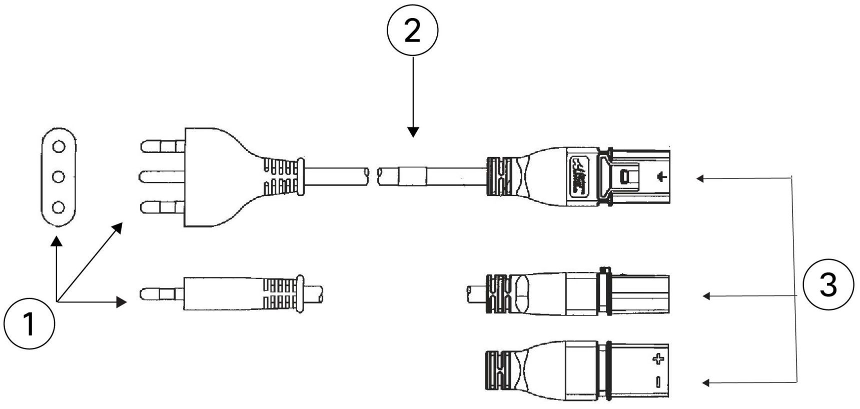
	PID: CAB-AC-16A-SG-IND		Part number: 37-1863-01
1	Plug: SABS 164-1	**2**	Cord set rating: 16 A, 250 V
3	Connector: Saf-D-Grid		Cord length: 14 ft (4.3 m)

Figure 25: Israel



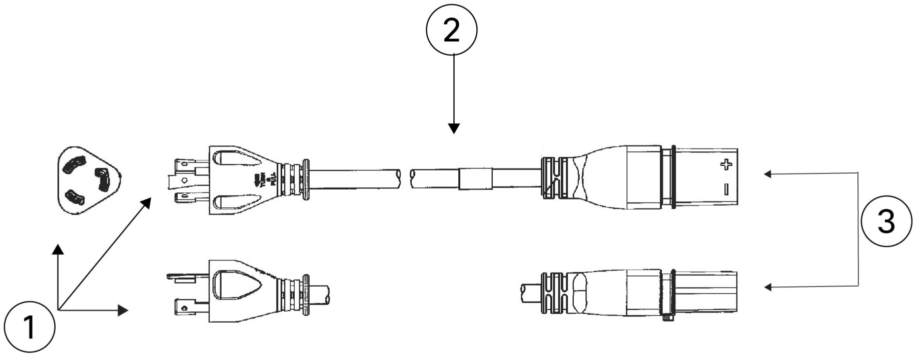
	PID: CAB-AC-16A-SG-IS		Part number: 37-1658-01
1	Plug: SI-16S3	**2**	Cord set rating: 16 A, 250 V
3	Connector: Saf-D-Grid		Cord length: 14 ft (4.3 m)

Figure 26: Italy



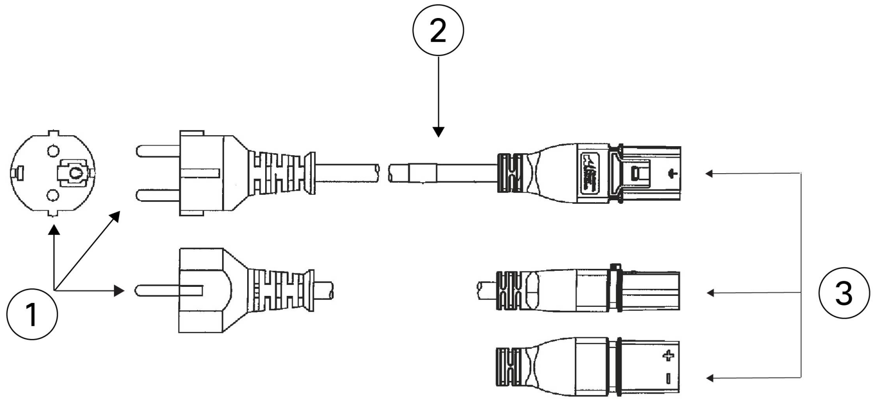
	PID: CAB-AC-16A-SG-IT		Part number: 37-1651-01
1	Plug: CEI 23-50	**2**	Cord set rating: 16 A, 250 V
3	Connector: Saf-D-Grid		Cord length: 14 ft (4.3 m)

Figure 27: Japan



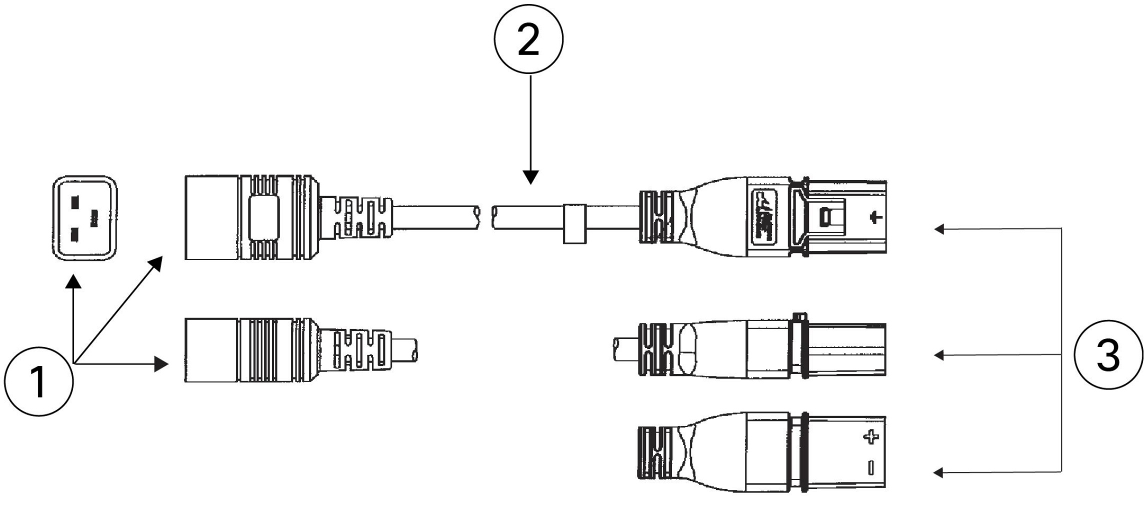
	PID: CAB-AC-16A-SG-JPN		Part number: 37-1656-01
1	Plug: NEMA L6-20	**2**	Cord set rating: 16 A, 250 V
3	Connector: Saf-D-Grid		Cord length: 14 ft (4.3 m)

Figure 28: Korea



	PID: CAB-AC-16A-SG-SK		Part number: 37-1646-01
1	Plug: Src	**2**	Cord set rating: 16 A, 250 V
3	Connector: Saf-D-Grid		Cord length: 14 ft (4.3 m)

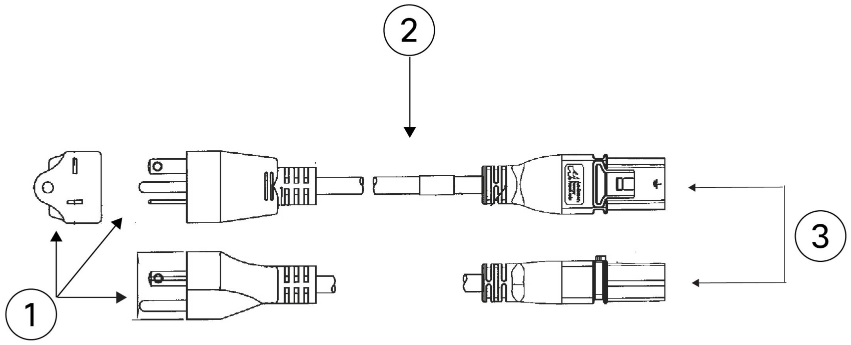
Figure 29: North America cabinet jumper PDU



	PID: CAB-AC-20A-SG-C20		Part number: 37-1653-01

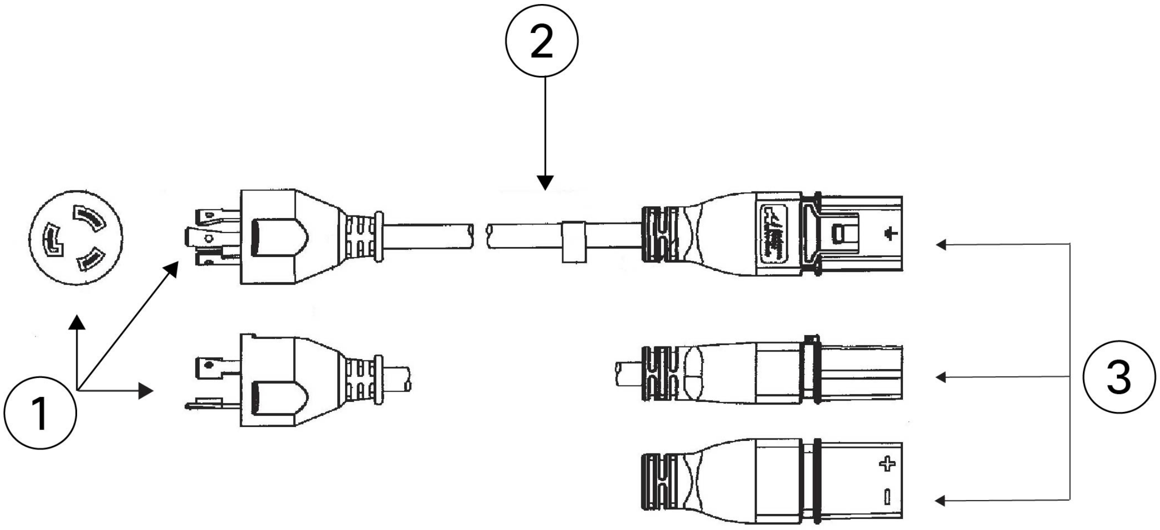
1	Plug: IEC C20	**2**	Cord set rating: 20 A, 250 V
3	Connector: Saf-D-Grid		Cord length: 14 ft (4.3 m)

Figure 30: North America straight blade 125 V



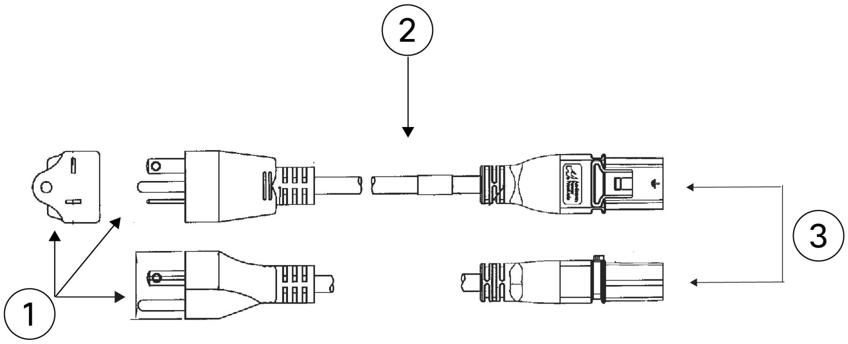
	PID: CAB-AC-20A-SG-US		Part number: 37-1662-01
1	Plug: NEMA 5-20P	**2**	Cord set rating: 20 A, 125 V
3	Connector: Saf-D-Grid		Cord length: 14 ft (4.3 m)

Figure 31: North America twist lock 125 V



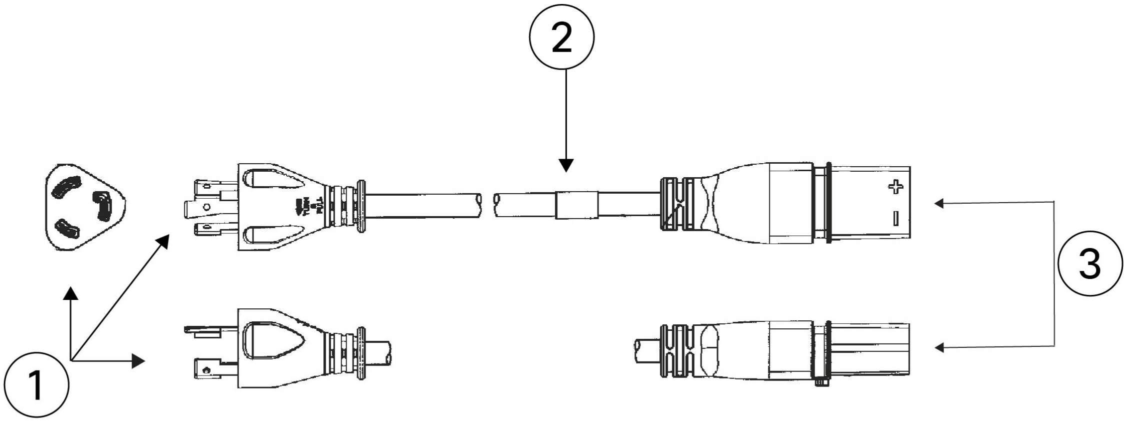
	PID: CAB-AC-20A-SG-US1		Part number: 37-1652-01
1	Plug: NEMA L5-20	**2**	Cord set rating: 20 A, 125 V
3	Connector: Saf-D-Grid		Cord length: 14 ft (4.3 m)

Figure 32: North America straight blade 250 V



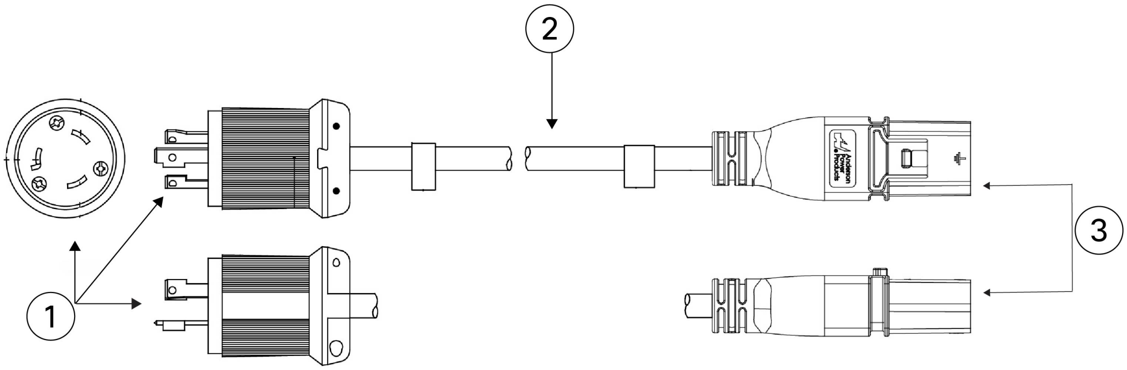
	PID: CAB-AC-20A-SG-US2		Part number: 37-1657-01
1	Plug: NEMA 6-20	**2**	Cord set rating: 20 A, 250 V
3	Connector: Saf-D-Grid		Cord length: 14 ft (4.3 m)

Figure 33: North America twist lock 250 V



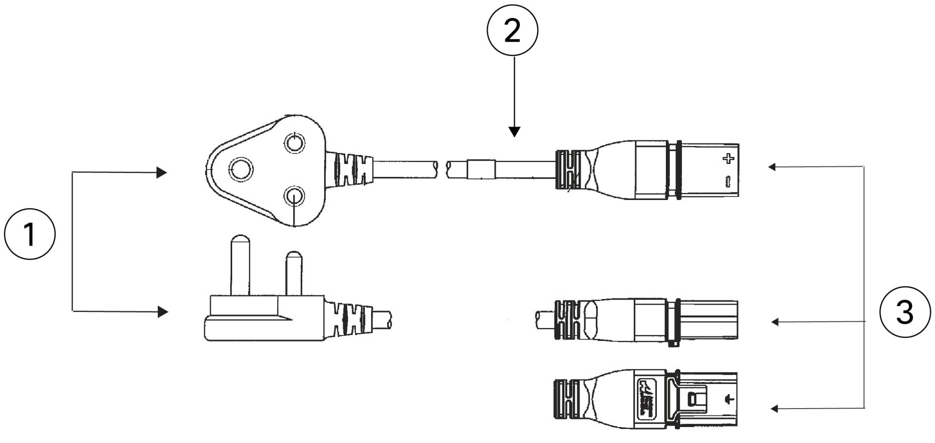
	PID: CAB-AC-20A-SG-US3		Part number: 37-1656-01
1	Plug: NEMA L6-20	**2**	Cord set rating: 20 A, 250 V
3	Connector: Saf-D-Grid		Cord length: 14 ft (4.3 m)

Figure 34: North America Twist Lock 277 V



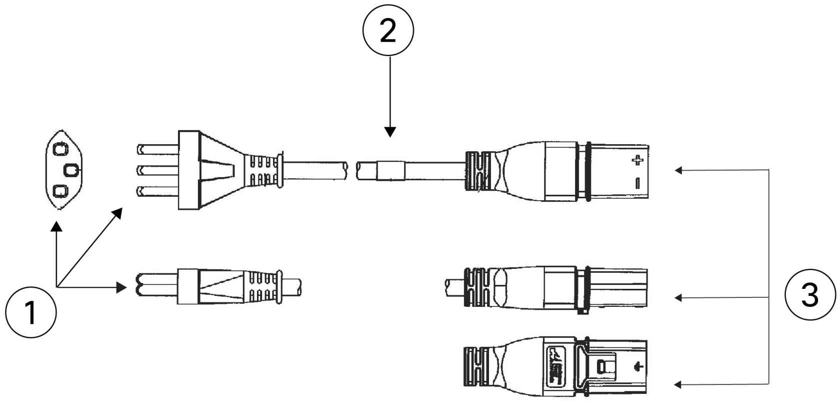
	PID: CAB-AC-20A-SG-US4		Part number: 37-1645-01
1	Plug: NEMA L7-20P	**2**	Cord set rating: 20 A, 277 V
3	Connector: Saf-D-Grid		Cord length: 14 ft (4.3 m)

Figure 35: South Africa



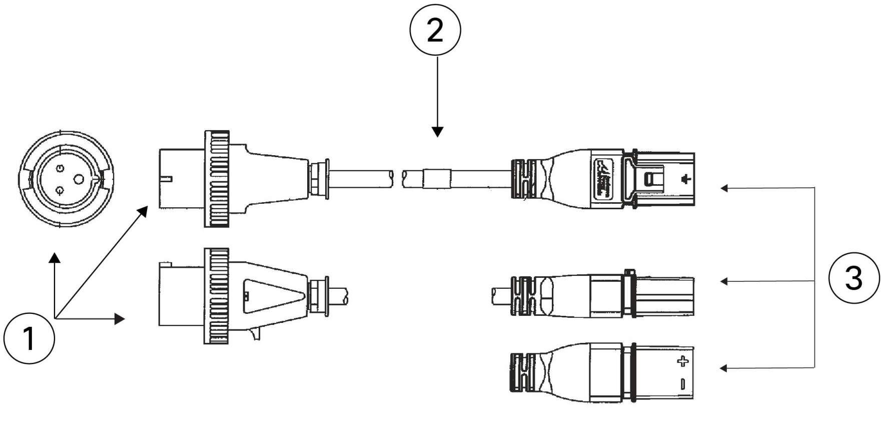
	PID: CAB-AC-16A-SG-SA		Part number: 37-1647-01
1	Plug: EL	**2**	Cord set rating: 16 A, 250 V
3	Connector: Saf-D-Grid		Cord length: 14 ft (4.3 m)

Figure 36: Switzerland



	PID: CAB-AC-16A-SG-SW		Part number: 72-1654-01
1	Plug: SEV 5934-2	**2**	Cord set rating: 16 A, 250 V
3	Connector: Saf-D-Grid		Core length: 14 ft (4.3 m)

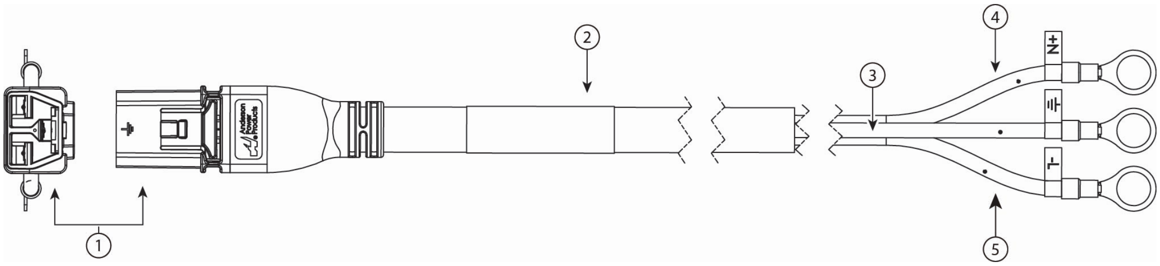
Figure 37: United Kingdom



	PID: CAB-AC-16A-SG-IN		Part number: 37-1659-01
1	Plug: IEC 60309	**2**	Cord set rating: 16 A, 250 V
3	Connector: Saf-D-Grid		Cord length: 14 ft (4.3 m)

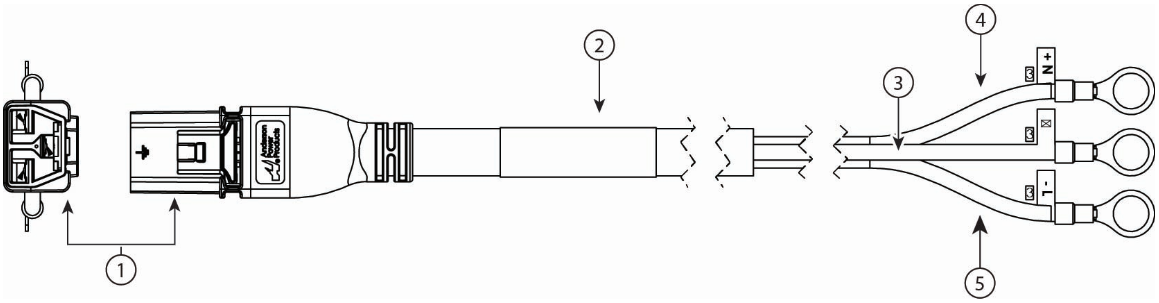
The following HVDC power cords are supported. One end of the cable has the Anderson Saf-D-Grid plug and the other end is three pigtail wires. The pigtail stud size for the insulated ring terminal for both of the following cables is 3/8 inch (9.5 mm).

Figure 38: HVDC North America



	PID: CAB-HVDC-2M		Part number: 72-100766-01
1	Connector: Saf-D-Grid	**2**	Cord set rating: 18 A, 400 VDC
3	Green wire	**4**	White wire
5	Black wire		Cord length: 6.6 ft (2.0 m)

Figure 39: HVDC International and China CCC-compliant



	PID: CAB-HVDC-3T-2M		Part number: 72-100812-01
1	Connector: Saf-D-Grid	**2**	Cord set rating: 25 A, 400 VDC
3	Green/yellow wire	**4**	Blue wire
5	Brown wire		Cord length: 6.6 ft (2.0 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/HVAC/HVDC = 20 A (North America)

AC/HVAC/HVDC = 16 A (International)

Warning **Statement 1017—**Restricted Area

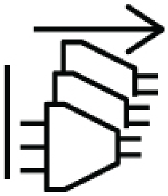
This unit is intended for installation in restricted access areas. Only skilled, instructed, or qualified personnel can access a restricted access area.

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 1051—**Laser Radiation

Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.

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 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.

Note **Statement 1089**—Instructed and Skilled Person Definitions

An instructed person is someone who has been instructed and trained by a skilled person and takes the necessary precautions when working with equipment.

A skilled person or qualified personnel is someone who has training or experience in the equipment technology and understands potential hazards when working with equipment.

Warning **Statement 1091**—Installation by an Instructed Person

Only an instructed person or skilled person should be allowed to install, replace, or service this equipment. See statement 1089 for the definition of an instructed or skilled person.

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 31 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 modules, on page 27 for more detailed information about the power supply in the chassis.

When installing the chassis, consider the following:

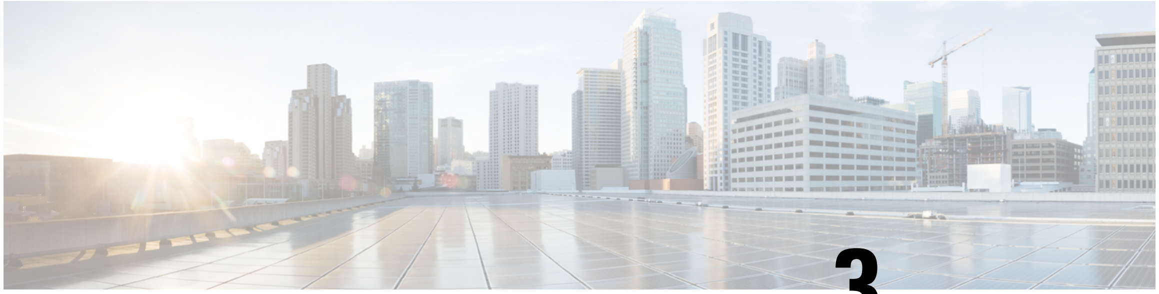
- Check the power at the site before installing the chassis to ensure that it is free of spikes and noise. Install a power conditioner, if necessary, to ensure proper voltages and power levels in the appliance-input voltage.
- Install proper grounding for the site to avoid damage from lightning and power 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 60 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.

Procedure

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 6100 series in a rack using slide rails. It applies to all models of the Secure Firewall 6100 series. You use the pegs on the chassis to secure the slide rail. See Product ID numbers, on page 33 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 6100 series.

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).

Slide rail assemblies work with four-post racks and cabinets with square slots, round 7.1-mm 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.

Slide rail installation requirements

You need the following to install the Secure Firewall 6100 series in a rack using slide rails:

- Phillips screwdriver
- Two slide rails
- Slide rail accessories kit:
  - Two slide-rail mounting brackets
  - Six 8-32 x 0.302-inch slide rail mounting bracket Phillips screws for securing the brackets to the chassis
  - Two M3 x 0.5 x 6-mm Phillips screws for securing the chassis to your rack
- Cable management bracket kit (optional)
  - Two cable management brackets
  - Four 8-32 x 0.375-inch Phillips screws

Safety warnings

Take note of the following warnings:

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.

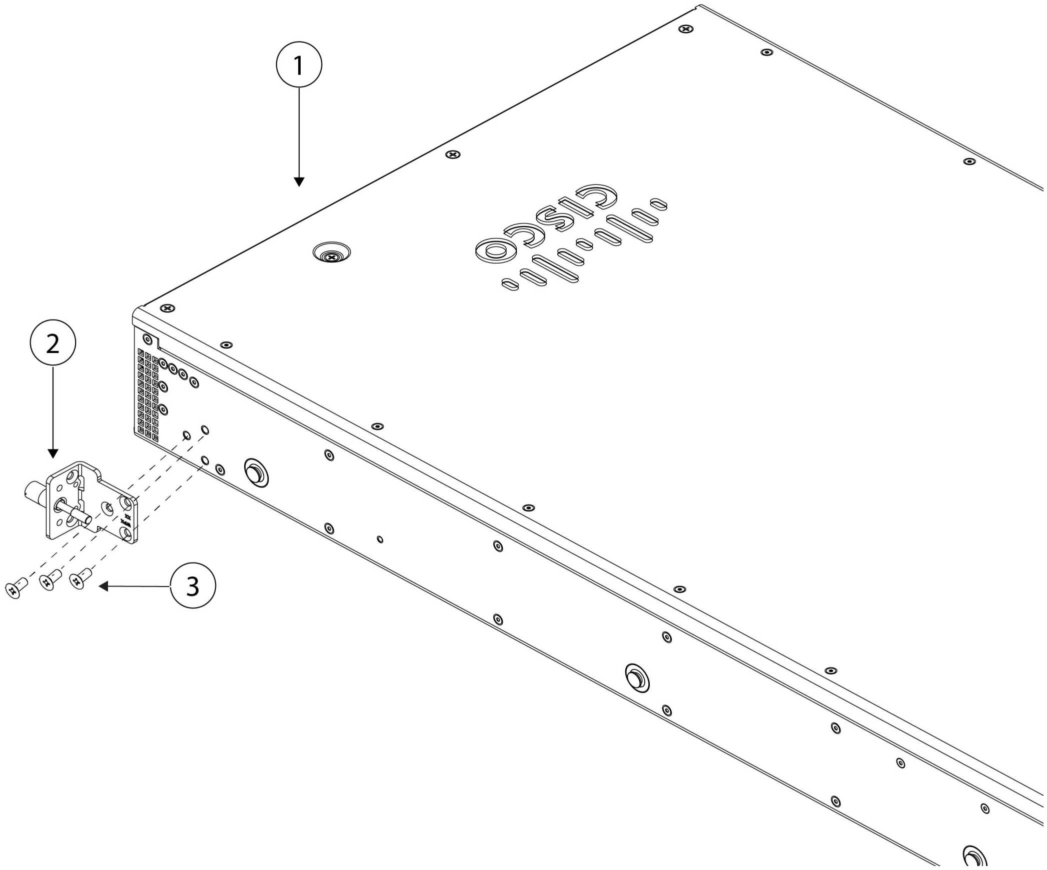
Warning **Statement 1098**—Lifting Requirement

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.

Procedure

Step 1 Facing the front panel, 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 40: Attach the slide-rail locking brackets

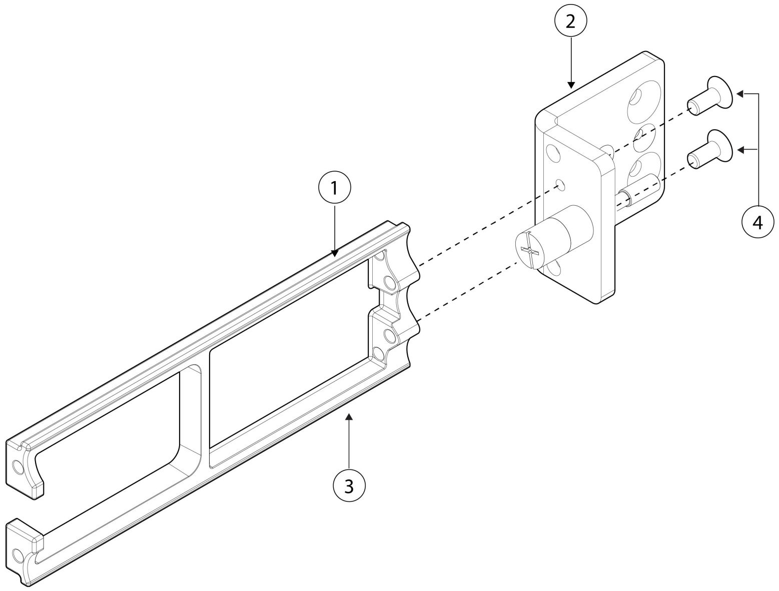


1	Front panel of the chassis	**2**	Slide-rail locking bracket
3	8-32 x 0.302-inch Phillips screws (three per side)		—

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 41: Install the cable management screws into the slide-rail locking bracket



1	Step groove on inside of cable management bracket	**2**	Slide-rail locking bracket
3	Cable management bracket		8-32 x 0.375-inch Phillips screws (two per bracket)

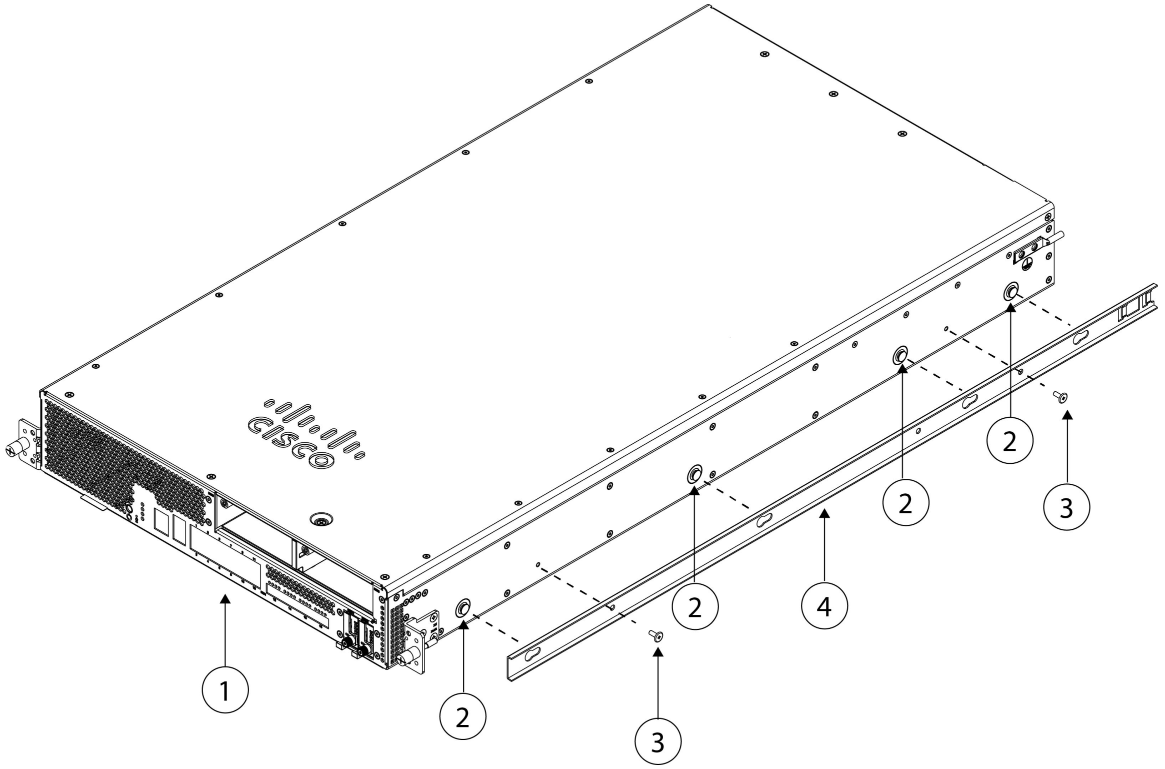
b) Install two 8-32 x 0.375 inch Phillips screws through the inside of the slide-rail locking bracket to secure the cable management bracket to slide-rail locking bracket.

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. Make sure you align the inner rail so that the four slots on the rail line up with the four pegs on the side of the chassis.

Figure 42: Line up the inner rail with the pegs on the chassis



1	Front panel of chassis	**2**	Mounting peg on the chassis for the keyed slot (four per side)
3	M3 x 0.5 x 6-mm Phillips screws (two per side)	**4**	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 two M3 x 0.5 x 6-mm Phillips screws, secure the first inner rail to the side of the chassis to prevent sliding.

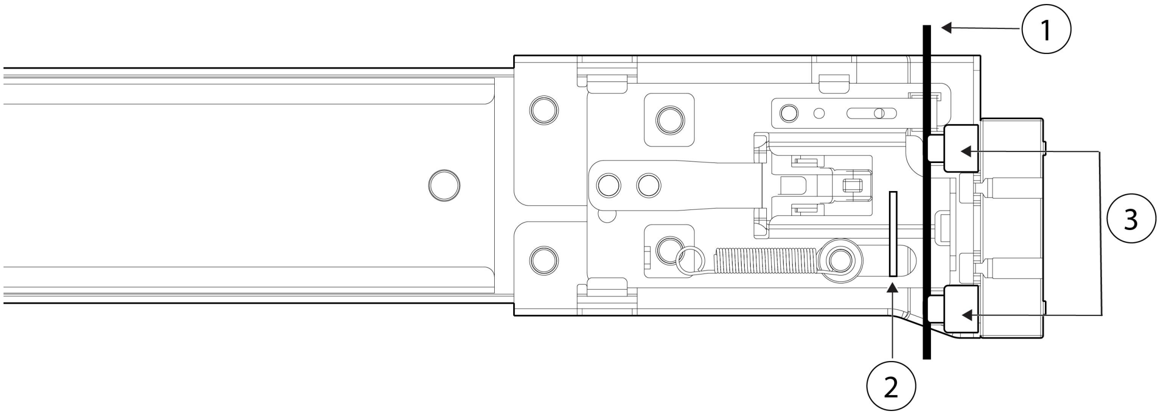
e) Install the second inner rail on the opposite side of the chassis and secure with the other two M3 x 0.5 x 6-mm screws.

Caution
The screws must always be installed to the inner rails for reliability and safety.

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 43: Front securing mechanism inside the front end



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

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.

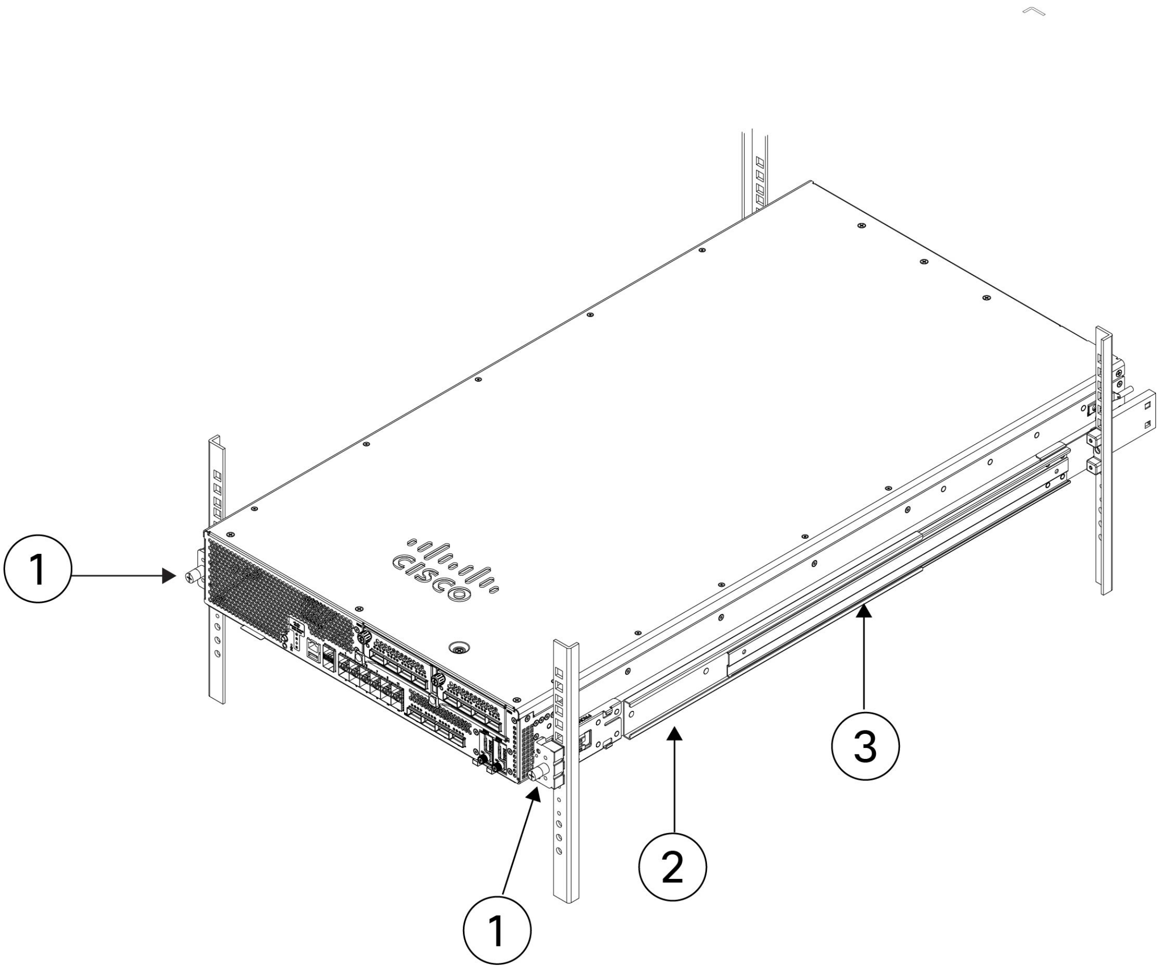
a) Align the rear of the inner rails that are attached to the chassis sides with the front ends of the empty slide rails on the rack.

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 (see figure below).

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

Figure 44: Completed rack mount



1	Captive screws	**2**	Inner rail release clip
3	Inner rail attached to chassis		—

What to do next

- See Ground the chassis, on page 67 for the procedure to ground the Secure Firewall 6100 series.
- Install the cables according to your software configuration as described in the Getting Started Guides.

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 local codes for ampacity.

The grounding pad is found on the left side of the chassis when facing the rear panel with the power supplies and fans) . You can attach a grounding lug using a cable that you supply.

Ground lug installation requirements

You need the following items that you provide:

- Wire tool
- Crimping tool
- Grounding cable

- You need the following items from the accessory kit:
  - One grounding lug (#6AWG 0.25-inch)
  - Two ¼-20 x 0.297-inch button-head screws
  - Two 0.469-inch OD, 0.261-inch ID, 0.025-inch T washers

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.

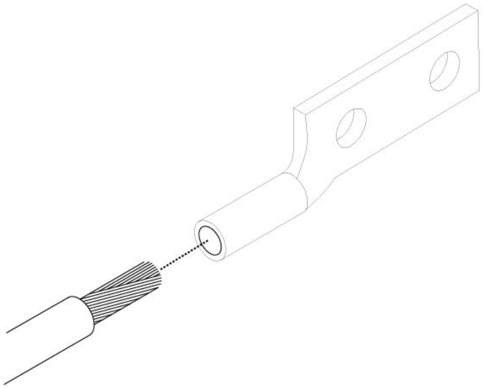
If your unit has modules, secure them with the provided screws.

Procedure

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 45: Insert the cable into the grounding lug

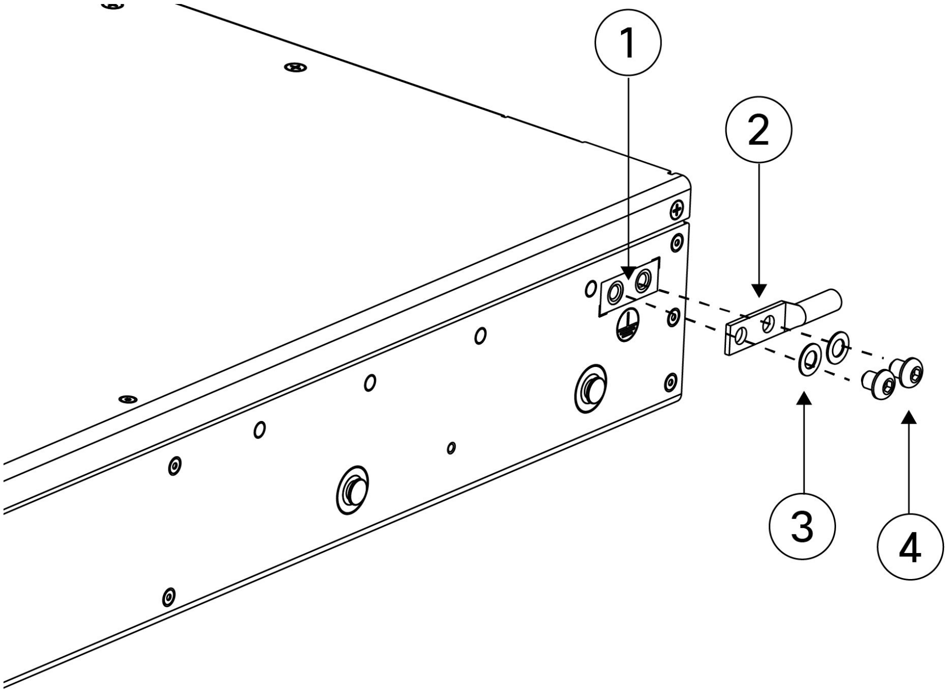


Step 3 Use the crimping tool to secure the grounding cable in the grounding lug.

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

Step 5 Attach the grounding lug against the grounding pad on the left side of the chassis so that there is solid metal-to-metal contact, and insert the two ¼-20 x 0.297-inch button-head screws into the grounding pad.

Figure 46: Attach the grounding lug



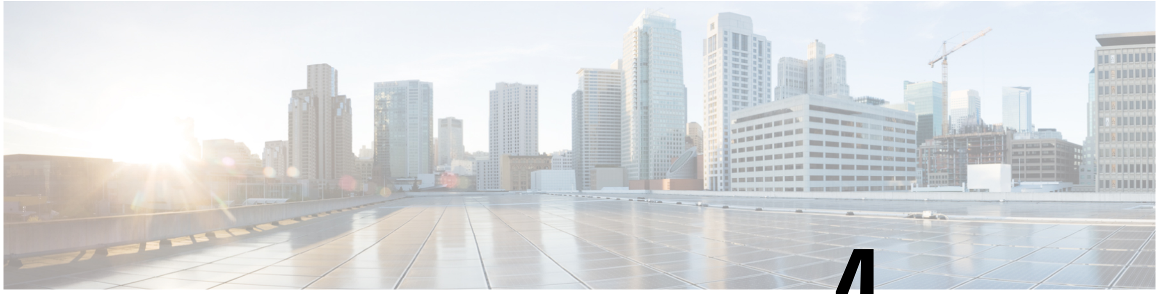
1	Grounding pad	**2**	Two lock-internal washers
3	Left side of the chassis when facing the rear panel	**4**	Two ¼-20 x .297 inch button-head screws
5	Grounding lug		—

Step 6 Make sure that the lug and cable do not interfere with other equipment.

Step 7 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 Getting Started Guides.



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 6100 series. 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.

Procedure

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

a) Power down the chassis by pushing the power button.

   See Front panel, on page 7 for more information about the push power button. 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 pushing the power button.

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 pushing the power button 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.

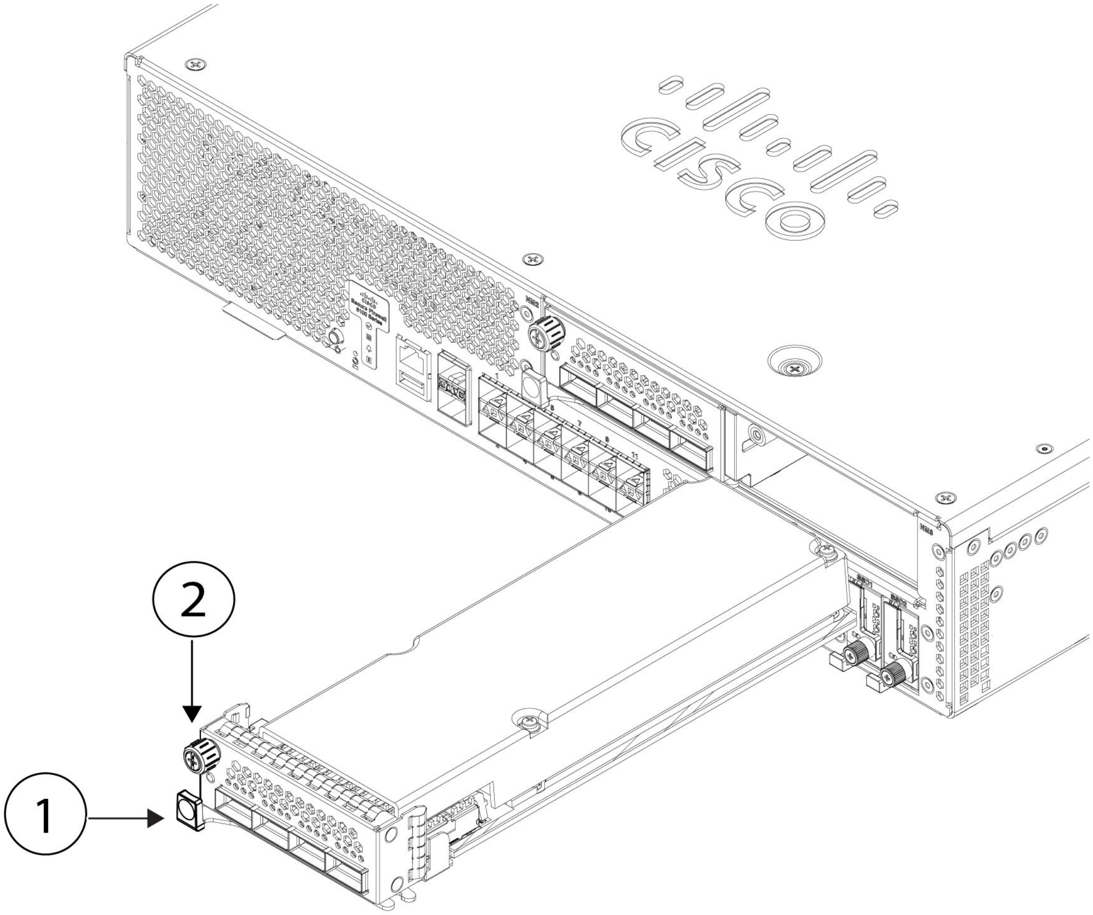
See Front panel, on page 7 for more information about the push power button.

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 47: Remove the network module



1	Ejector handle	2	Captive screw

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 30 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.

Procedure

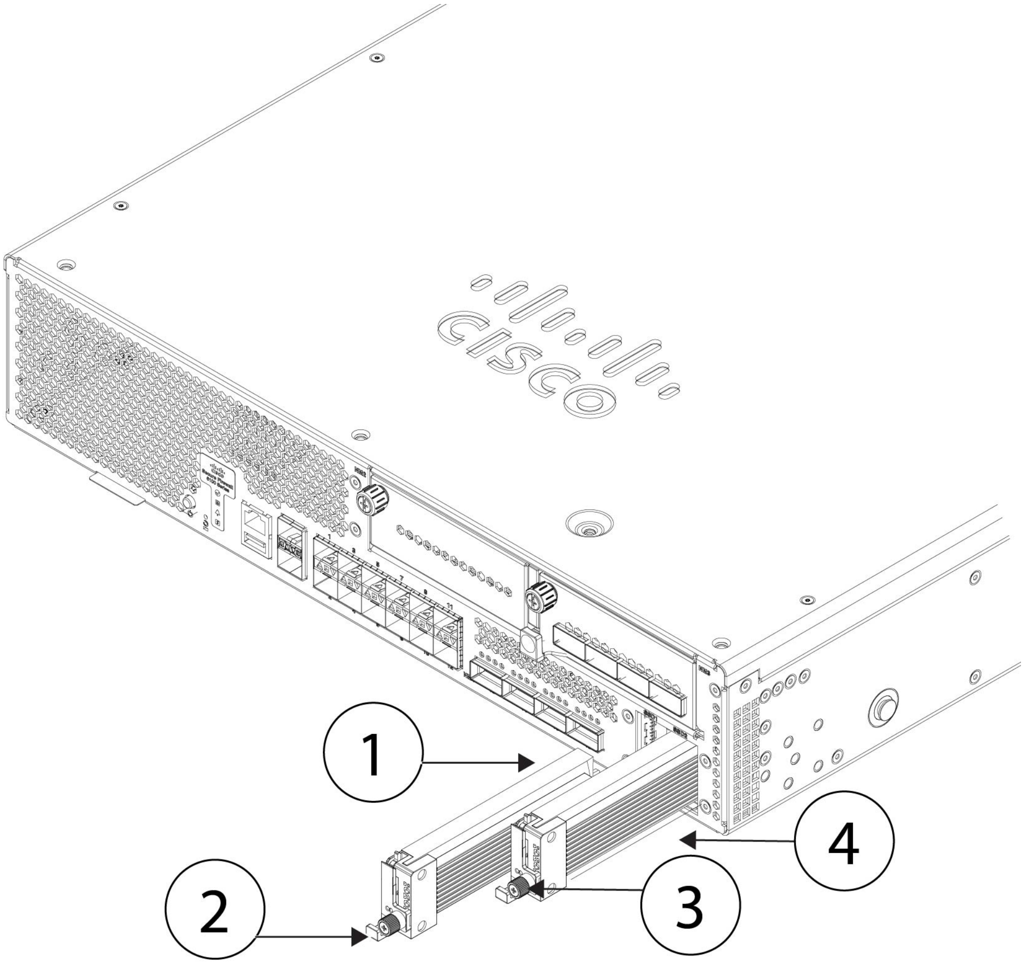
Step 1 Save your configuration.

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 48: Remove the SSD



1	SSD-1 slot	**2**	Handle
3	Captive screw	**4**	SSD-2 slot

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 fan module

You can remove and replace the dual-rotor fan modules while the chassis is running. There are four fan modules in the rear of the chassis. The air flow moves from front to back (I/O side to non-I/0 side). They are labeled FAN-1 though FAN-4 from left to right on the rear of the chassis.

Caution Removing all of the fan modules exposes the chassis to no airflow. The chassis does not power up and boot properly if the fan modules are missing.

Caution If a fan module fails, remove it from the chassis and replace it within 30 seconds. After 30 seconds the CPU temperature can exceed the operating temperature, which can reduce performance.

Safety warnings

Take note of the following warnings:

Warning **Statement 1093—**Avoid Sharp Edges

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

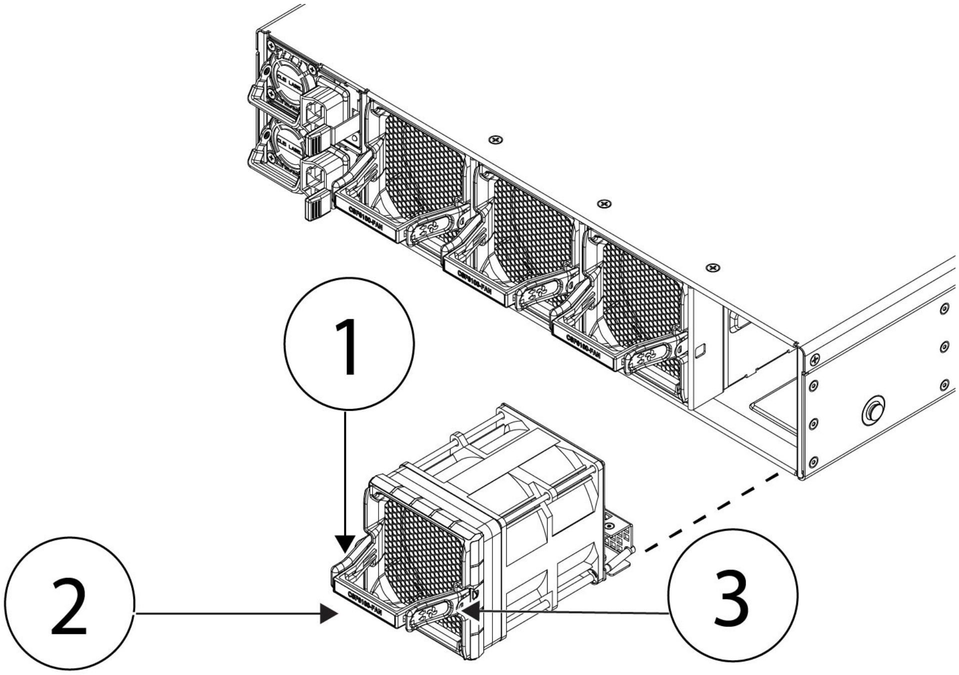
Procedure

Step 1 Have the 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 49: Remove the fan module



1	Squeeze tab	2	Handle
3	Squeeze tab		—

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 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 Fan modules, on page 29 for a description of the fan LED.

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. The SAF-D-GRID connector acts as a disconnect for AC/HVAC/HVDC power supply.

Safety Warnings

Take note of the following warnings:

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.

Procedure

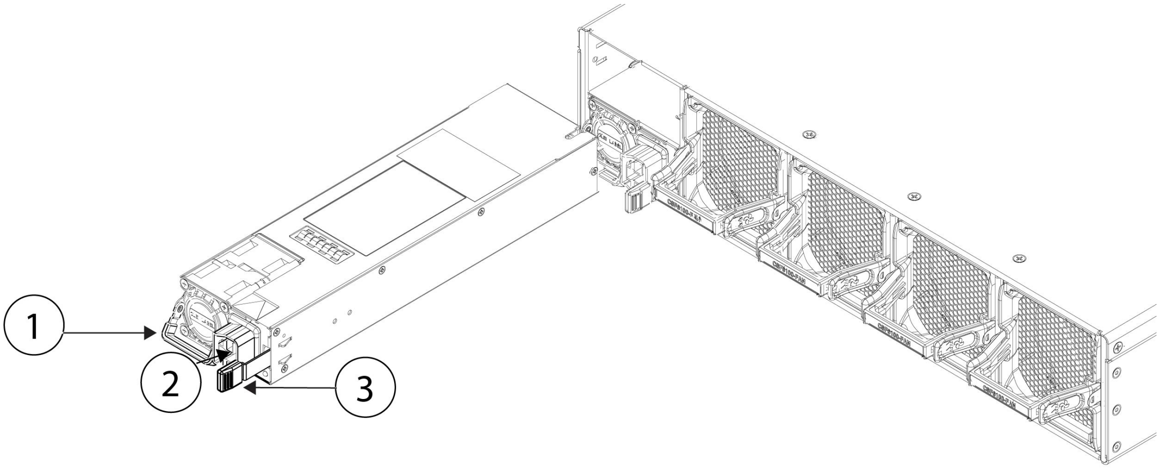
Step 1 Unplug the power supply cable before removing the power supply module. You cannot disengage the power supply module release tab without first removing the cable.

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 50: Remove the power supply module



1	Handle	**2**	Power connector
3	Release tab		—

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 module to make sure the power supply is operative. See Power supply modules, on page 27 for a description of the power supply module LED.

Remove and replace DIMMs

This procedure describes how to remove and replace faulty DIMMs in the Secure Firewall 6100. DIMM-related failures are identified at bootup at which point the system is placed into fail-safe mode and you can use the CLI to identify fault DIMMs as seen below.

Note You cannot directly order the DIMM replacements. You must work with TAC to get the new DIMMs so that you do not void your warranty.

Caution To prevent ESD damage, wear grounding wrist straps during this procedure and handle the DIMMs by the carrier edges only.

Identify faulty DIMMs

Use the **show dimm detail** CLI command to determine which DIMMs are faulty. Also, at bootup, if a DIMM failure is detected, you will see that it is missing from the DIMM list. The following example shows that no DIMMs have failed. All 24 DIMMs are listed in both CPUs.

This example output is only seen on the serial console when ROMMON is booting.

```
firepower-6160# scope server
firepower-6160 /chassis/server # scope memory-array 1
firepower-6160 /chassis/server/memory-array # show dimm detail
DIMMs installed:
CPU1 CHANNEL A CPU1 CHANNEL B CPU1 CHANNEL C CPU1 CHANNEL D CPU1 CHANNEL E CPU1 CHANNEL
 F
CPU1 CHANNEL G CPU1 CHANNEL H CPU1 CHANNEL I CPU1 CHANNEL J CPU1 CHANNEL K CPU1 CHANNEL
 L
CPU2 CHANNEL A CPU2 CHANNEL B CPU2 CHANNEL C CPU2 CHANNEL D CPU2 CHANNEL E CPU2 CHANNEL
 F
CPU2 CHANNEL G CPU2 CHANNEL H CPU2 CHANNEL I CPU2 CHANNEL J CPU2 CHANNEL K CPU2 CHANNEL
 L
```

The following example shows that there is a DIMM failure. CPU1 CHANNEL L is missing.

```
DIMMs installed:
CPU1 CHANNEL A CPU1 CHANNEL B CPU1 CHANNEL C CPU1 CHANNEL D CPU1 CHANNEL E CPU1 CHANNEL
 F
CPU1 CHANNEL G CPU1 CHANNEL H CPU1 CHANNEL I CPU1 CHANNEL J CPU1 CHANNEL K
CPU2 CHANNEL A CPU2 CHANNEL B CPU2 CHANNEL C CPU2 CHANNEL D CPU2 CHANNEL E CPU2 CHANNEL
 F
CPU2 CHANNEL G CPU2 CHANNEL H CPU2 CHANNEL I CPU2 CHANNEL J CPU2 CHANNEL K CPU2 CHANNEL
 L
WARNING: This system needs more memory device(s). Expected 24, installed 23
%WARNING% - Please correct the memory issue to assure best performance.
```

Safety Warnings

Take note of the following warnings:

Warning **Statement 1093—**Avoid Sharp Edges

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

Follow these steps to remove and replace a faulty DIMM in the Secure Firewall 6100 chassis:

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

Caution Cisco does not support third-party DIMMs. Using non-Cisco DIMMs can result in system problems or damage to the internal board.

Before you begin

- Contact TAC to verify DIMM failure and to obtain replacement DIMM(s).
- Schedule a maintenance window for the affected Secure Firewall 6100 after receiving the replacement DIMM(s).
- Have an ESD strap and mat ready to use during the procedure.
- Remove all sources of power from the chassis.

Note See Power button and reset button, on page 9 for the procedure to power off the chassis.

- Remove the chassis from the rack.

Procedure

Step 1 Record the CPU and Channel designation for the faulty DIMM(s).

Step 2 Remove all sources of power from the chassis.

For AC systems, disconnect the AC inlet from the power supply module.

For DC systems, turn off the disconnect switch or circuit breaker and remove the power supply module from the chassis.

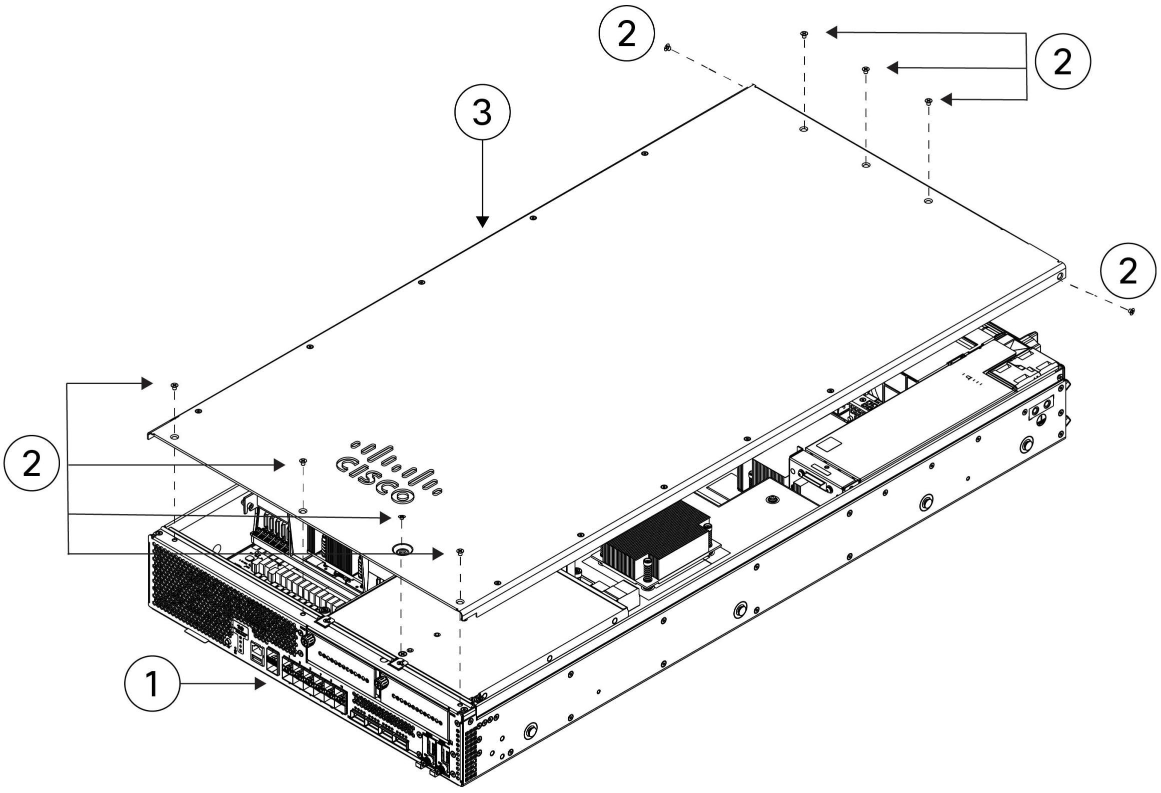
Step 3 Remove the chassis from the rack.

See Rack-mount the chassis using slide rails, on page 60 for the procedure to remove the chassis from the rack.

Step 4 Place the chassis on an antistatic mat.

Step 5 Remove the seven screws from the top of the chassis cover and the two screws on the sides. Pull the cover up and off the chassis.

Figure 51: Remove the chassis cover

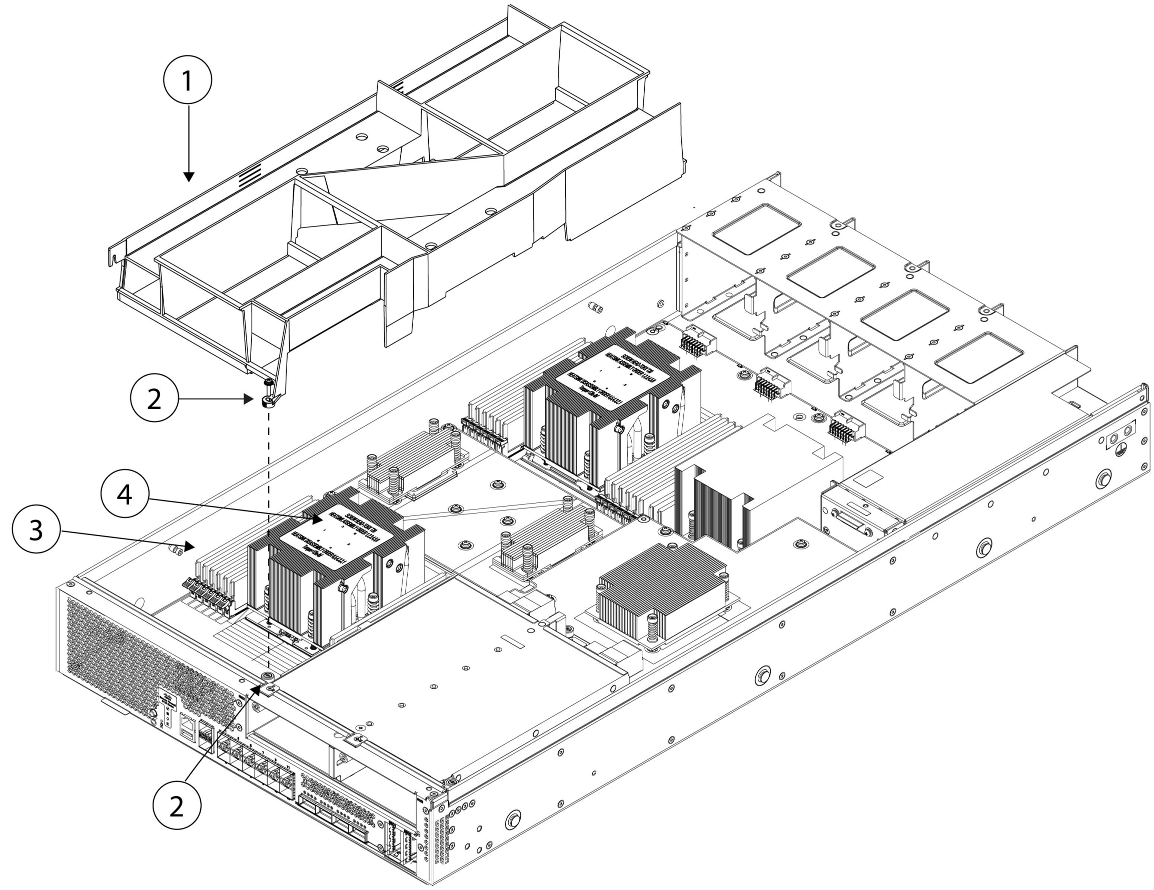


1	Front panel (I/O side)	**2**	Chassis cover screws (9)
3	Chassis cover		—

Step 6 Remove the screw on the air baffle and then lift it up and out.

The air baffle covers the top DIMM banks and the two CPUs.

Figure 52: Remove the air baffle from the internal board

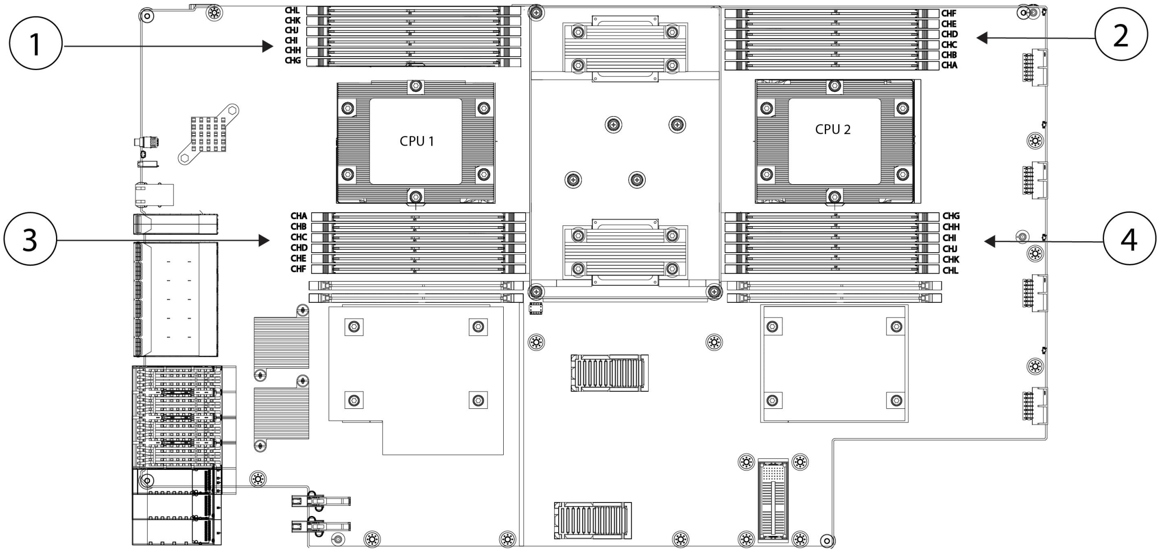


1	Air baffle	**2**	Air baffle screw
3	DIMM bank	4	CPU 1

Step 7 Locate the DIMM you are removing on the internal board.

There are four DIMM banks with six DIMM slots per bank.

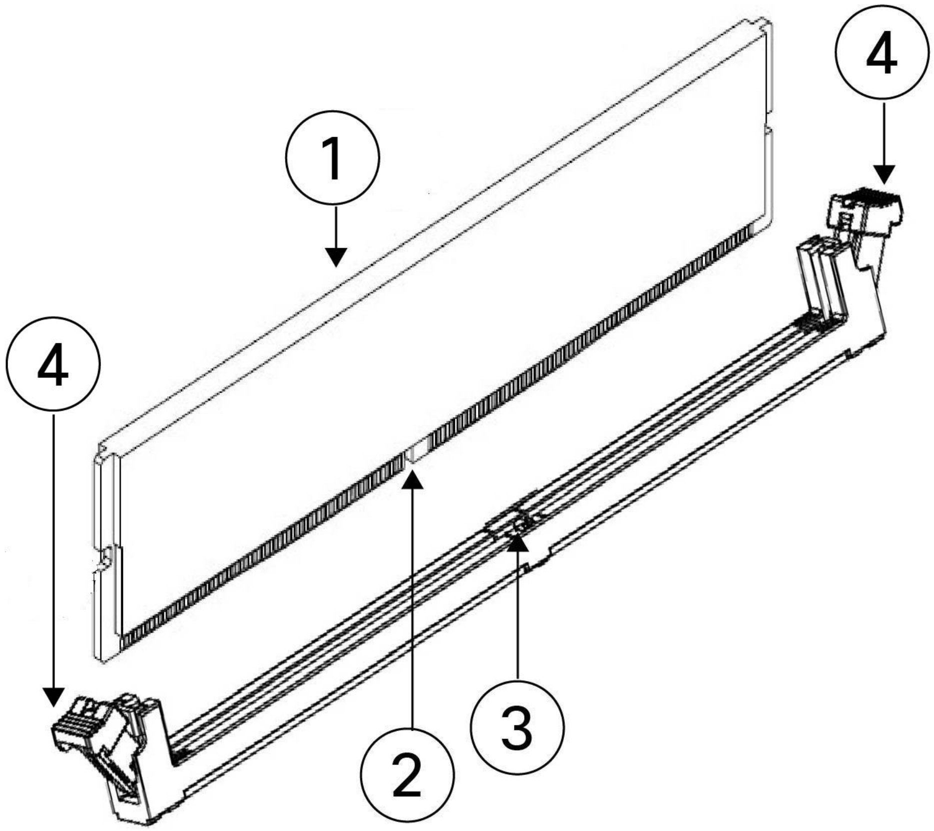
Figure 53: DIMM banks on the internal board



1	DIMM bank with channels L, K, J, I, H, G	**2**	DIMM bank with channels F, E, D, C, B, A
3	DIMM bank with channels A, B, C, D, E, F	4	DIMM bank with channels G, H, I, J, K, L

Step 8 Open the DIMM slot latches by pressing down on the ejectors at both ends of the slot; pull the DIMM up and out.

Figure 54: Open DIMM connector latches



1	DIMM	**2**	DIMM notch
3	DIMM slot notch	**4**	Open DIMM connector latches

Step 9 Align the new DIMM with the empty slot on the internal board of the chassis. Use the alignment feature in the DIMM slot to correctly orient the DIMM.

Note
Make sure the notch in the DIMM lines up with the slot. If the slot is misaligned, you can damage the DIMM or slot.

Step 10 Push down evenly on the top two corners of the DIMM until it is fully seated and the ejector levers on both ends of the DIMM lock into place.

Step 11 Lower the air baffle back in place and tighten the screw (see the *Remove the air baffle from the internal board* figure above).

Step 12 Replace the chassis cover and tighten the nine screws (see the *Remove the chassis cover* Figure above).

Step 13 Install the chassis in the rack.

See Rack-mount the chassis using slide rails, on page 60 for the procedure to remove the chassis from the rack.

Step 14 Connect the power supply modules.

Step 15 Bring the Secure Firewall 6100 back online.

See the FXOS Configuration Guide for your software version for the instructions to bring the chassis back online.