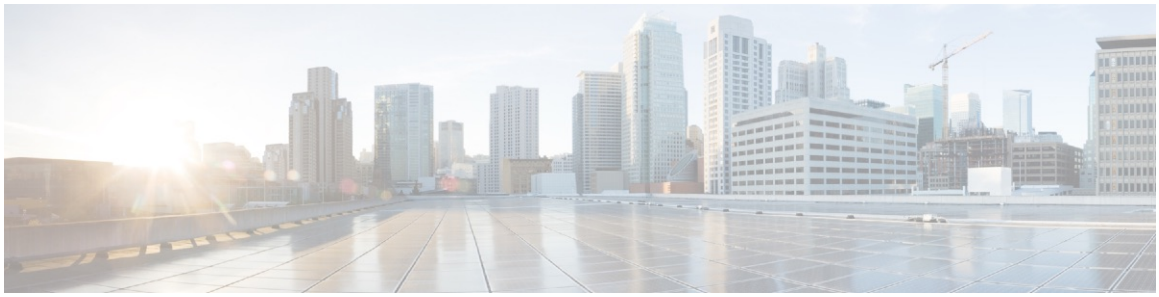
Cisco Secure Firewall 3100 Series Hardware Installation Guide

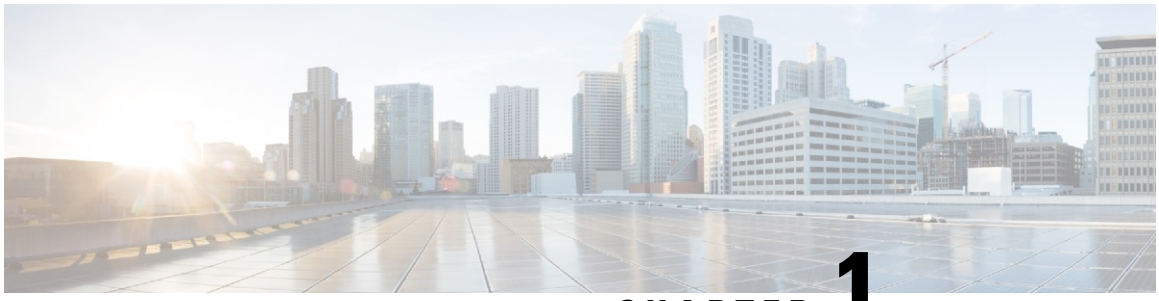
First Published: 2022-04-06

Last Modified: 2023-04-07

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



CONTENTS



CHAPTER 1

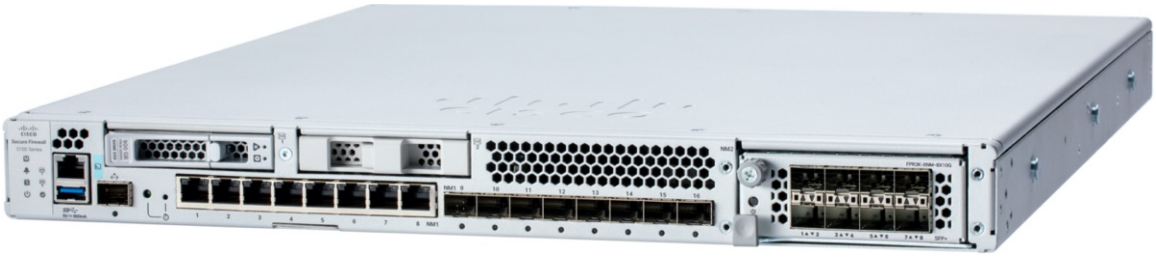
Overview

Features

The Cisco Secure Firewall 3100 is a standalone modular security services platform that includes the Secure Firewall 3110, 3120, 3130, and 3140.

The following figure shows the Secure Firewall 3100.

Figure 1: Secure Firewall 3100



The following table lists the features for the Secure Firewall 3100.

Table 1: Secure Firewall 3100 Features

Feature	3110	3120	3130	3140
Form factor	1 RU Fits a standard 19-inch (48.3-cm) square-hole rack			
Rack mount	(Optional) Two 2-post mount brackets and/or two slide rails 4-post Electronic Industries Association (EIA)-310-D rack **Note** We recommend that you order the slide rails for your Secure Firewall 3100.			
Airflow	Front to rear (I/O side to non-I/O side) Cold aisle to hot aisle			
Processor	AMD 7272	AMD 7282	AMD 7352	AMD 7452
Core count	12	16	24	32
Core clock	2.9 GHz	2.8 GHz	2.3 GHz	2.35 GHz
System memory	2 x 32 GB	2 x 64 GB	4 x 32 GB	4 x 64 GB
Management port	One 1/10-Gb small form-factor pluggable (SFP) port			
Console port	One RJ-45 serial port			
USB port	USB 3.1 Type A (900 mA) port			
Network ports	8 SFP fixed ports and 8 copper RJ-45 ports Named Ethernet 1/1 through 1/16			
Network module ports	Eight 1/10/25-Gb SFP ports Four 40-Gb QSFP ports			

Feature	3110	3120	3130	3140
Network module slots	One (hot-swappable) **Note** Although the hardware supports hot-swapping, the software does not. You must power off the chassis when removing/replacing network modules.			
Network modules	• 8-port 1Gb/10Gb SFP+ (FPR3K-XNM-8X10G)		• 8-port 1Gb/10Gb/25Gb SFP+ (FPR3K-XNM-8X25G) • 8-port 1Gb/10Gb SFP+ (FPR3K-XNM-8X10G) • 4-port 40-Gb QSFP+ (FPR3K-XNM-4X40G)	
AC power supply	Two power supply slots Ships with one 400-W AC power supply module Hot-swappable		Two power supply slots Ships with two 400-W AC power supply modules Hot-swappable	
DC power supply	Yes (optional) Hot-swappable			
Redundant power	No **Note** Yes, if you order an extra power supply.		Yes **Note** Ships with two power supplies.	
Fans	Two dual fan module slots (3 + 1) **Note** The dual fan modules are hot-swappable.			
Storage	Two Nonvolatile Memory Express (NVMe) SSD slots Ships with one 900-GB SSD installed in slot 1. You can order a second RAID1 SSD for slot 2. The RAID1 SSD is preconfigured for RAID1. **Note** Slot 2 is reserved for the optional software RAID1 configuration. **Note** Hot-swapping is supported with 2 SSDs. However, you must enter a CLI command to remove one disk from the RAID before hot swapping. See the CLI configuration guide for your software for the procedure.			
Pullout asset card	Displays the serial number and a QR code that points to the low touch provisioning (LTP) guide.			
Grounding lug	On rear panel			
Power switch	On rear panel			

Feature	3110	3120	3130	3140
Reset button	Resets the system to factory default without requiring serial console access **Note** The reset button is recessed. Press with a pin and hold longer than 5 seconds to set the system back to the factory default.			

Deployment Options

Here are some examples of how you can deploy the Secure Firewall 3100:

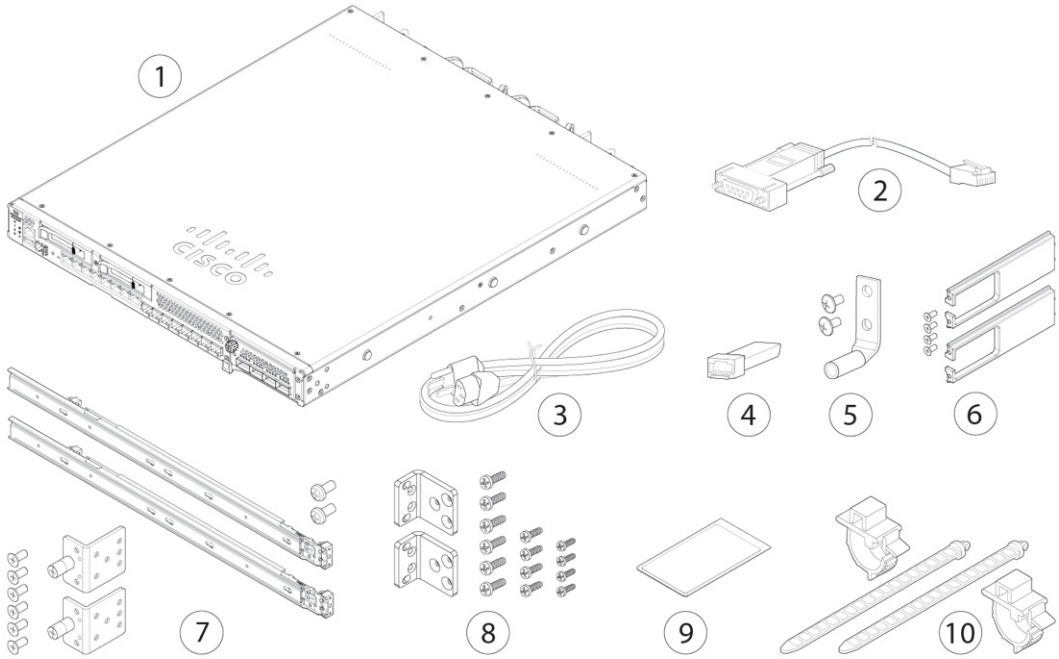
- As a firewall:
  - At the enterprise internet edge in a redundant configuration
  - At branch offices in either a high availability pair or standalone
  - At data centers in a high availability pair or clustered, which serves the needs of smaller enterprises
- As a device that provides additional application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

Package Contents

The following figure shows the package contents for the Secure Firewall 3100. The contents are subject to change and your exact contents contain additional or fewer items depending on whether you order the optional parts. See Product ID Numbers for a list of PIDs associated with the package contents.

Note There are two sets of four screws that you can use to secure the chassis to your rack. Chose the screws that fit your rack.

Figure 2: Secure Firewall 3100 Package Contents



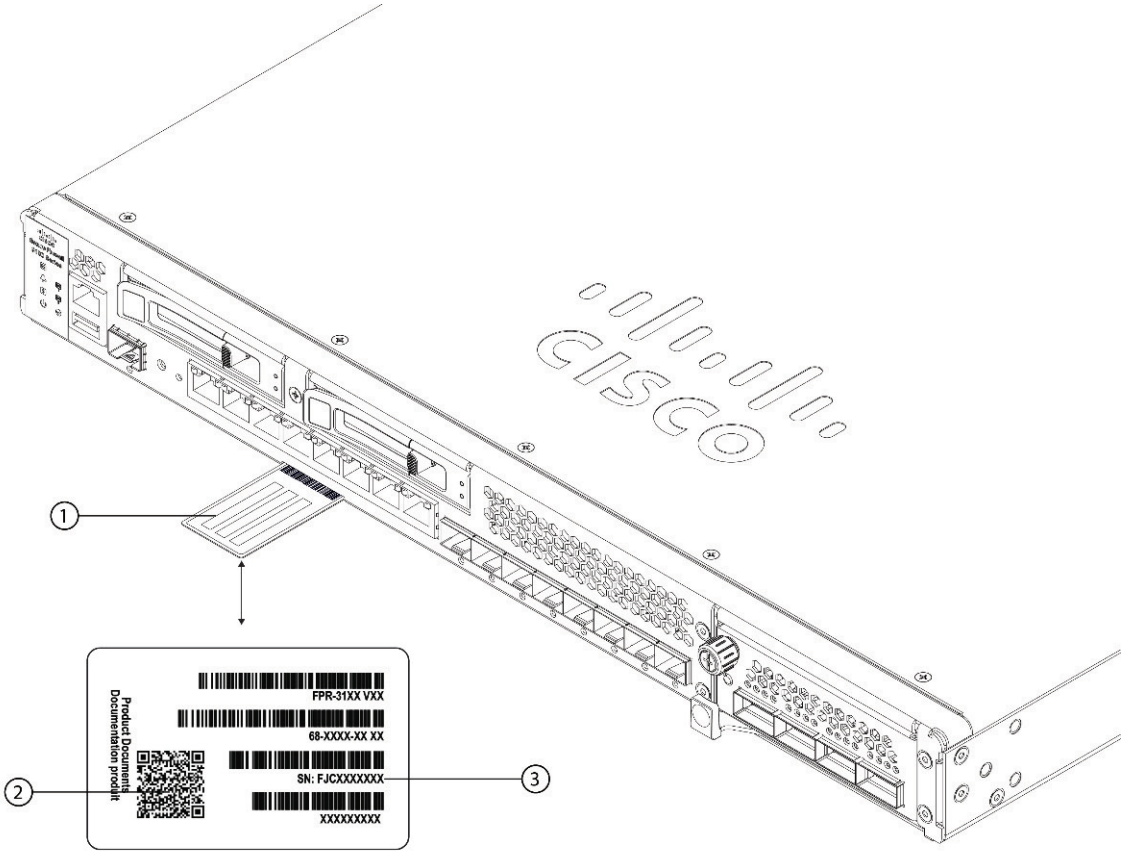
1	Secure Firewall 3100 chassis	**2**	Console cable RJ-45 to DB-9 (part number 72-3383-01)
3	One or two power cords (country-specific) See Power Cord Specifications, on page 34 for a list of supported power cords.	**4**	SFP transceiver (Optional; in package if ordered)
5	One ground lug kit (part number 69-100359-01) • One #6 AWG, 90 degree, #10 post ground lug (part number 32-0608-01) • Two 10-32 x 0.38-inch Phillips screws (part number 48-0700-01)	**6**	Cable management bracket kit (part number 69-100376-01) • Two cable management brackets (part number 700-128334-01) • Four 8-32 x 0.375-inch Phillips screws (part number 48-2696-01) (Optional; in package if ordered)

7	Two slide rails (800-110033-01) Slide rail accessories kit (53-101509-02): • Two slide rail locking brackets (part number 700-121935-01) • Six 8-32 x 0.302-inch slide rail locking bracket Phillips screws (part number 48-102184-01) • Two M3 x 0.5 x 6-mm Phillips screws (part number 48-101144-01) (Optional; in package if ordered)	**8**	Rack-mount bracket kit (53-101510-02): • Two rack-mount brackets (700-127244-01) • Six 8-32 x 0.375-inch Phillips screws (part number 48-2286) for securing the brackets to the chassis • Four 10-32 x 0.75-inch Phillips screws (part number 48-0441-01) for securing the chassis to your rack • Four 12-24 x 0.75-inch Phillips screws (part number 48-0440-01) for securing the chassis to your rack (Optional; in package if ordered)
9	*Cisco Secure Firewall 3100* This document has a URL and QR code 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, the Getting Started Guide, and the Easy Deployment Guide.	**10**	Two power supply module tie wraps and clamps (part number 52-100162-01)

Serial Number and Digital Documentation Portal QR Code

The pullout asset card on the front panel of your Secure Firewall 3100 chassis contains the chassis serial number and the Digital Documentation Portal QR code, which points to the getting started guide, the regulatory and compliance guide, the easy deployment guide, and the hardware installation guide.

Figure 3: Pullout Asset Card



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

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

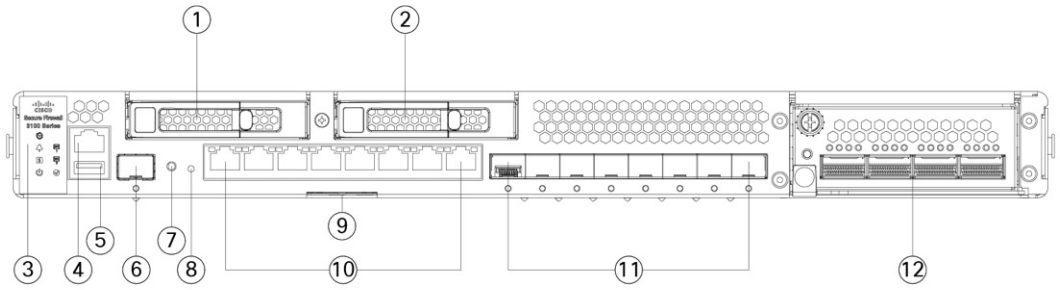
Figure 4: Example Compliance Label

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

Front Panel

The following figure shows the front panel of the Secure Firewall 3100. See Front Panel LEDs, on page 11 for a description of the LEDs.

Figure 5: Secure Firewall 3100 Front Panel



1	SSD-1	**2**	SSD-2
3	System LEDs	**4**	RJ-45 console port
5	Type A USB 3.1 port	**6**	Gigabit Ethernet management port: • Secure Firewall Threat Defense—Management 0 (also referred to as Management 1/1 and Diagnostic 1/1) • ASA—Management 1/1
7	Reset button LED	**8**	Recessed factory reset button
9	Pullout asset card with chassis serial number, getting started guide QR code, and LTP QR code	**10**	Fixed copper ports (NM-1) Copper ports named 1/1 through 1/8 left to right
11	Fixed fiber ports (NM-1) Fiber ports named 1/9 through 1/16 left to right	**12**	Network module (NM-2)

Management Port

The Secure Firewall 3100 chassis management port is a 1/10-Gb fiber SFP port.

RJ-45 Console Port

The Secure Firewall 3100 chassis has a standard RJ-45 console port. You can use the CLI to configure your 3100 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 baud rate is 9600. You can use the standard cable found in your accessory kit to convert the RJ-45 to DB-9 if necessary.

Type A USB 3.1 Port

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

- Hot swapping

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

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

Network Ports

The Secure Firewall 3100 chassis has a network module slot that supports the following network modules:

- 8-port 1/10-Gb SFP
- 8-port 1/10/25-Gb SFP
- 6-port 1-Gb SFP SX multimode hardware bypass
- 6-port 10-Gb SFP SR multimode hardware bypass
- 6-port 10-Gb SFP LR single mode hardware bypass
- 6-port 25-Gb SFP SR multimode hardware bypass
- 6-port 25-Gb SFP LR single mode hardware bypass
- 8-port 10/100/1000Base-T hardware bypass

Note First supported on FTD 7.2.1 and ASA 9.18.2.

- 4-port 40-Gb QSFP

Note First supported on FTD 7.2.1 and ASA 9.18.2.

Note The 4-port 40-Gb and 8-port 25-Gb network modules are supported only on the 3130 and 3140.

Factory Reset Button

The Secure Firewall 3100 chassis has a recessed reset button that resets the system to the factory default. All previous configuration is erased after pressing the button down for five seconds. The following occurs:

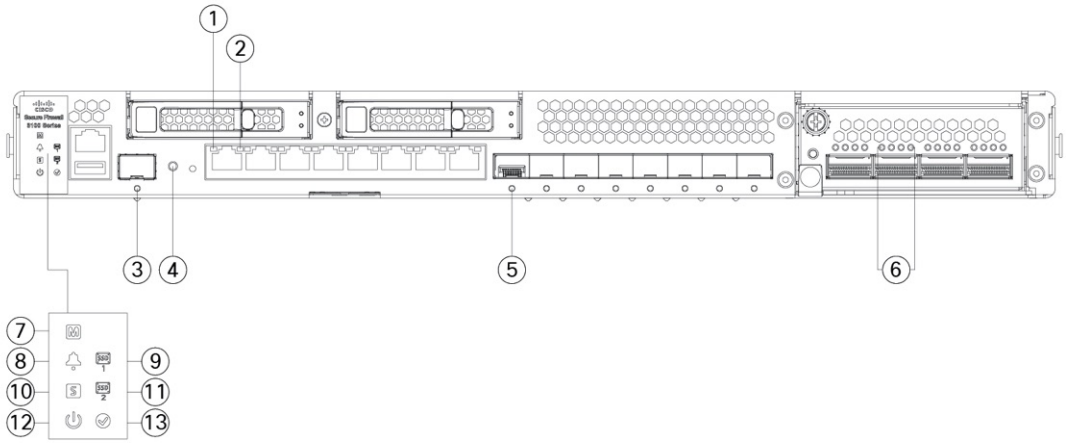
- ROMMON NVRAM is cleared and returned to default.
- All extra images are removed; the current running image remains.
- FXOS logs, core files, SSH keys, certificates, FXOS configuration, and Apache configuration are removed.

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

Front Panel LEDs

The following figure shows the Secure Firewall 3100 front panel LEDs.

Figure 6: Secure Firewall 3100 Front Panel LEDs



1	**RJ-45 Copper Port Link Status** • Off—No link. • Green—Link is up.	2	**RJ-45 Copper Port Activity Status** • Off—No activity • Green, flashing—The number of flashes determines the link speed; 1 flash=10 Mb, 2=100 Mb, 3=1 Gb.

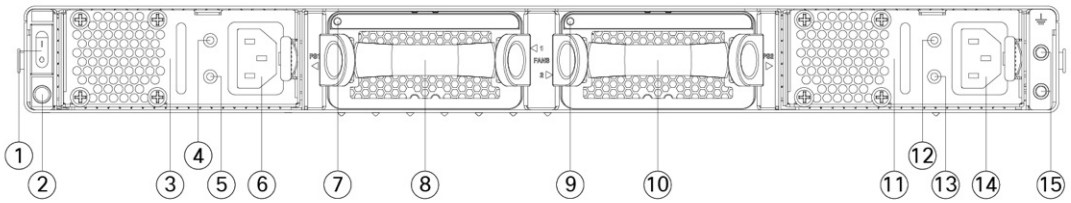
3	**Management Port Status** The 1/10-Gb fiber management port has a bicolor LED under the SFP cage that indicates link/activity/fault: • Off—No SFP. • Green—Link up. • Green, flashing—Network activity. • Amber—SFP present, but no link.	4	**Factory Reset Button Status** • Green, flashing—Flashes 5 seconds after you depress the button. • Off—Reset is complete.
5	**Fiber Port Link/Activity Status** Each fiber port has one dual color LED under the SFP cage. • Off—No SFP. • Green—Link up. • Green, flashing—Network activity at >1G is detected. • Amber—No link or network failure.	6	**Network Module 2 Port Status** • Green—Port is enabled, the link partner is detected. • Amber—Port is enabled, but the link partner is not detected. • Green, flashing—Port is enabled; network activity is detected.
7	**CDO Status** • Green, flashing slowly (twice in 5 seconds)—Cloud is connected. • Green and amber, flashing—Cloud connection failure. • Green—Cloud is disconnected. **Note** See the Easy Deployment Guide for 1000, 2100, or 3100 Series Cisco Secure Firewalls for more information on LTP.	8	**Alarm Status** • Off—No alarms. • Amber—Environmental error. • Green—Status is ok.
9	**SSD 1 Status** • 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.	10	**System Status** • Off—System has not booted up yet. • Green, flashing quickly—System is booting up. • Green—Normal system function. • Amber—System boot up has failed. • Amber, flashing—Alarm condition, system needs service or attention and may not boot properly.

11	**SSD 2 Status** • 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.	**12**	**Power Status** • Off—Input power is not detected. 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 switch toggle event, and initiated the shutdown sequence. If the power switch is in the OFF position, the system powers off after shutdown is completed. Do not remove the AC or DC power source while this LED is blinking so that the system has time to perform a graceful shutdown. • Amber—The system is powering up (before the BIOS boots). This takes one to five seconds at most. • Green—The system is fully powered up.
13	**Activity Status** (Role of a high-availability pair) • Off—The unit is not configured or enabled in a high-availability pair. • Green—The unit is in active mode. • Amber—The unit is in standby mode.		—

Rear Panel

The following figure shows the rear panel of the Secure Firewall 3100.

Figure 7: Secure Firewall 3100 Rear Panel



1	Power on/off switch	**2**	Power LED below **Note** This power LED has the same behavior as the front panel LED. See Front Panel LEDs, on page 11 for more information.
3	Power supply module 1	**4**	Power supply module 1 FAIL LED
5	Power supply module 1 OK LED	**6**	Power supply module 1 connector
7	Dual Fan Module 1 LED	**8**	Dual fan module 1
9	Dual Fan Module 2 LED	**10**	Dual fan module 2
11	Power supply module 2	**12**	Power supply module 2 FAIL LED
13	Power supply module 2 OK LED	**14**	Power supply module 2 connector
15	Two-post grounding pad **Note** The two-post grounding lug and two screws are included in the accessory kit.		—

Power Switch

The power switch is located to the left of power supply module 1 on the rear of the chassis. It is a toggle switch that controls power to the system. If the power switch is off but the power cord is plugged in and the power supply is flashing green, the system is in standby position, and only the 3.3-V standby power is enabled from the power supply module. The 12-V main power is OFF. When the switch is in the ON position, the 12-V main power is turned on and the system boots.

Before you move the power switch to the OFF position, use the **shutdown** commands so that the system can perform a graceful shutdown. This may take several minutes to complete. After the graceful shutdown is complete, the console displays `It is safe to power off now.` Wait until the front panel PWR LED flashes momentarily and is off before removing AC power.

See Front Panel LEDs, on page 11 for the PWR LED description. See the FXOS Configuration Guide for more information on using the **shutdown** commands.

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

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

1/10/25-Gb Network Module

The Secure Firewall 3100 chassis has one network module slot. Network modules are optional, removable I/O modules that provide either additional ports or different interface types. The network module plugs into the chassis on the front panel. See Front Panel, on page 8 for the location of the network module slot on the chassis.

FPR-X-NM-8X10G supports 1 Gb and 10 Gb full-duplex Ethernet traffic per port and is supported on all Secure Firewall 3100s. FPR-X-NM-8X25G supports 1 Gb, 10 Gb, or 25 Gb full-duplex Ethernet traffic per port and is supported *only* on the 3130 and 3140.

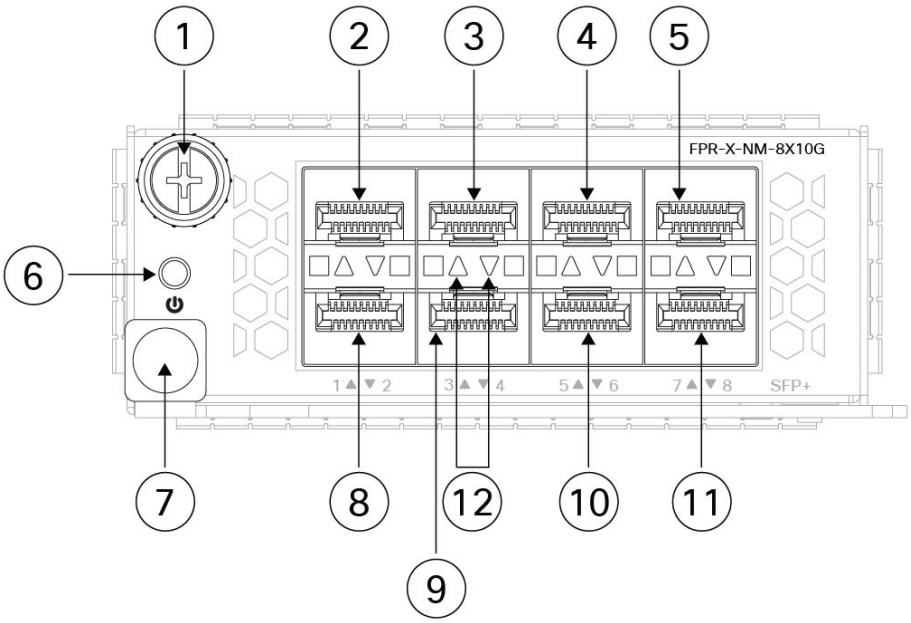
The top ports are numbered from left to right—Ethernet *X*/1, Ethernet *X*/3, Ethernet *X*/5, and Ethernet *X*/7. The bottom ports are numbered from left to right—Ethernet *X*/2, Ethernet *X*/4, Ethernet *X*/6, and Ethernet *X*/8 (see the figure below). Up arrows are the top ports and down arrows are the bottom ports (see the figure below). This network module supports SFP/SFP+/SFP28 transceivers. See Supported SFP/SFP+/QSFP+ Transceivers , on page 27 for the list of Cisco-supported transceivers.

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

Note Although you can install the 8-port 1/10/25-Gb network in the Secure Firewall 3105, 3110, and 3120, the software does not recognize it because it is not supported.

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

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



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

For More Information

- See 40-Gb Network Module, on page 17 for a description of the 40-Gb network module.
- See Install, Remove, and Replace the Network Module, on page 65 for the procedure for removing and replacing network modules.

40-Gb Network Module

The Secure Firewall 3100 chassis has one network module slot. Network modules are optional, removable I/O modules that provide either additional ports or different interface types. The network module plugs into the chassis on the front panel. See Front Panel, on page 8 for the location of the network module slot on the chassis.

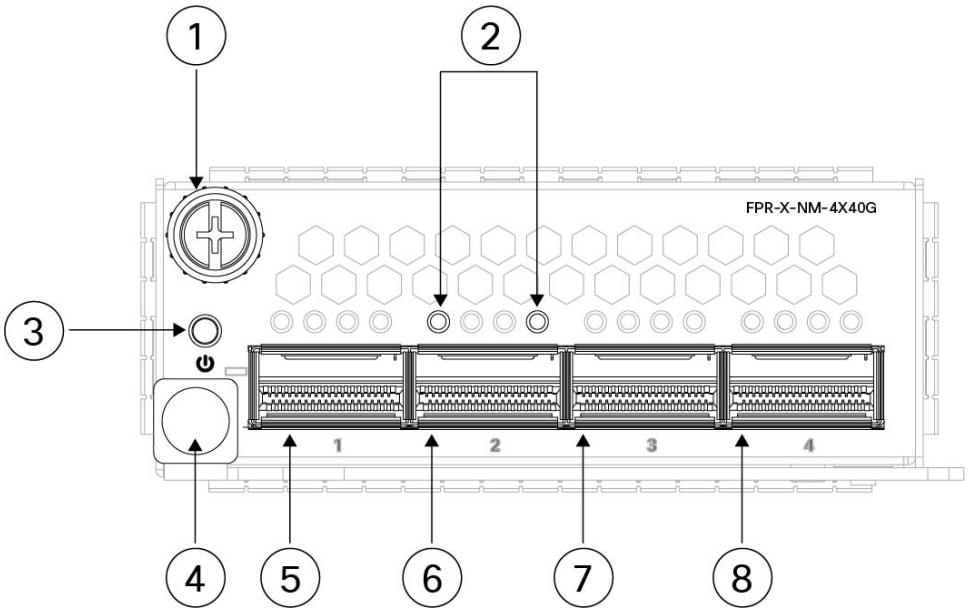
The FPR-X-NM-4X40G supports 40-Gb operation and is supported on the 3130 and 3140. This network module provides full-duplex Ethernet traffic per port. The 40-Gb network module has four QSFP+. The 40-Gb ports are numbered left to right, Ethernet *X*/1 through Ethernet *X*/4. See Supported SFP/SFP+/QSFP+ Transceivers , on page 27 for the list of Cisco-supported transceivers.

Starting with FTD 7.2 and ASA 7.18.1, you can break the four 40-Gb ports into four 10-Gb ports using the supported breakout cables. With the four-port 40-Gb network module, you now have 16 10-Gb interfaces. The added interfaces are Ethernet 2/1/1 through Ethernet 2/1/4.

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 40-Gb network module with another supported network module, you must reboot the chassis so that the new network module is recognized. See the configuration guide for your operating system for the detailed procedures for managing network modules.

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

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



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

For More Information

- See 1/10/25-Gb Network Module, on page 15 for a description of the 1/10/25-Gb network module.
- See Install, Remove, and Replace the Network Module, on page 65 for the procedure for removing and replacing network modules.

Hardware Bypass Network Modules

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 an optical switch that is capable of connecting the two ports when needed. The hardware bypass network modules have built-in SFPs.

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.

Caution When the secure firewall 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 optical 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.

There are three configuration options for hardware bypass network modules:

- Passive interfaces—Connection to a single port.

  For each network segment you want to monitor passively, connect the cables to one interface. This is how the nonhardware bypass network modules operate.

- Inline interfaces—Connection to any two like ports (10 Gb to 10 Gb for example) on one network module, across network modules, or fixed ports.

  For each network segment you want to monitor inline, connect the cables to pairs of interfaces.

- Inline with hardware bypass interfaces—Connection of a hardware bypass paired set.

  For each network segment that you want to configure inline with fail-open, connect the cables to the paired interface set.

  For the 1/10/25-Gb network modules, you connect the top port to the bottom port to form a hardware bypass paired set. This allows traffic to flow even if the secure firewall fails or loses power.

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.

For More Information

- See 1-Gb SX/10-Gb SR/10-Gb LR/25-Gb SR/25-Gb LR Network Module with Hardware Bypass , on page 21 for a description of the 1/10/25-Gb network module.
- See 10/100/1000Base-T Network Module with Hardware Bypass, on page 19 for a description of the 1-Gb network module.
- See Install, Remove, and Replace the Network Module, on page 65 for the procedure for removing and replacing network modules.

10/100/1000Base-T Network Module with Hardware Bypass

The Secure Firewall 3100 chassis has one network module slot. Network modules are optional, removable I/O modules that provide either additional ports or different interface types. The network module plugs into the chassis on the front panel. See Front Panel, on page 8 for the location of the network module slot on the chassis.

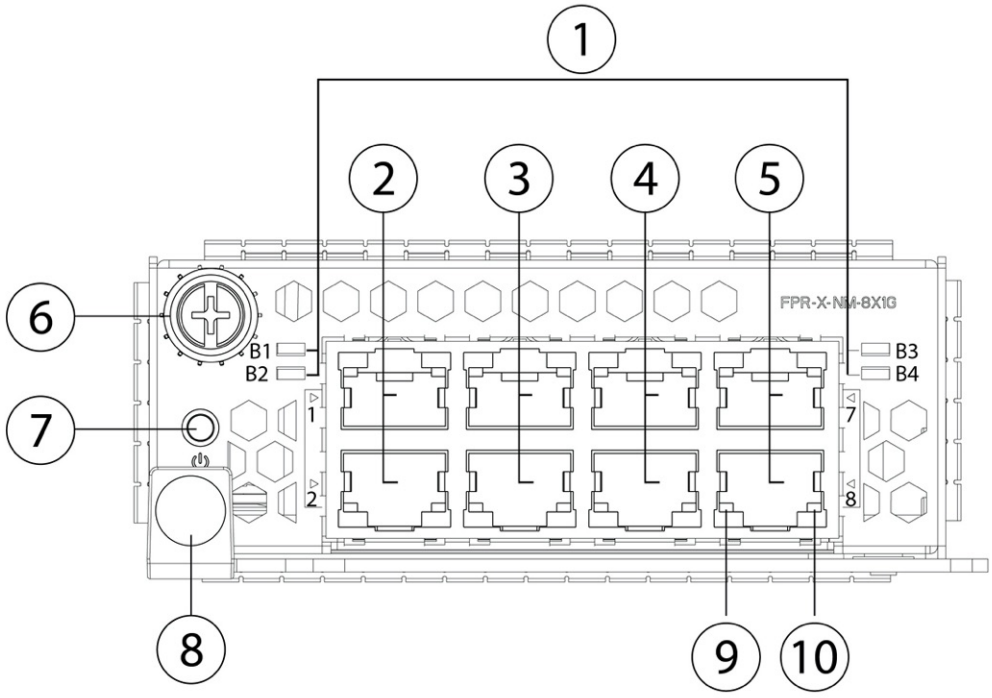
FPR-X-NM-8X1GF is an 8-port 10/100/1000Base-T hardware bypass network module. The eight ports are numbered from top to bottom, left to right. Ports 1 and 2, 3 and 4, 5 and 6, and 7 and 8 are paired for hardware bypass mode. In hardware bypass mode, data is not processed by the Secure Firewall 3100 but is routed to the paired port.

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 10/100/1000Base-T network module with another supported network module, you must reboot the chassis so that the new network module is recognized. See the configuration guide for your operating system for the detailed procedures for managing network modules.

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

The following figure shows the front panel of the 10/100/1000Base-T network module.

Figure 10: 10/100/1000Base-T Network Module (FPR-X-NM-8X1GF)



1	Bypass LEDs B1 through B4 • Green—In standby mode. • Amber, flashing—Port is in hardware bypass mode, failure event.	**2**	Ethernet *X*/1 and Ethernet *X*/2 Ports 1 and 2 are paired together to form a hardware bypass pair. LED B1 applies to this paired port.
3	Ethernet *X*/3 and Ethernet *X*/4 Ports 3 and 4 are paired together to form a hardware bypass pair. LED B2 applies to this paired port.	**4**	Ethernet *X*/5 and Ethernet *X*/6 Ports 5 and 6 are paired together to form a hardware bypass pair. LED B3 applies to this paired port.
5	Ethernet *X*/7 and Ethernet *X*/18 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.	**10**	Right Port LED • Unlit—No connection or port is not in use. • Green—Link up. • Green, flashing—Network activity.

For More Information

- See 1-Gb SX/10-Gb SR/10-Gb LR/25-Gb SR/25-Gb LR Network Module with Hardware Bypass , on page 21 for a description of the 1/10/25-Gb network module.
- See Hardware Bypass Network Modules, on page 18 for a description of hardware bypass.
- See 40-Gb Network Module, on page 17 for a description of the 40-Gb network module.
- See 1/10/25-Gb Network Module, on page 15 for a description of the 1/10/25-Gb network module.
- See Install, Remove, and Replace the Network Module, on page 65 for the procedure for removing and replacing network modules.

1-Gb SX/10-Gb SR/10-Gb LR/25-Gb SR/25-Gb LR Network Module with Hardware Bypass

The Secure Firewall 3100 chassis has one network module slot. Network modules are optional, removable I/O modules that provide either additional ports or different interface types. The network module plugs into the chassis on the front panel. See Front Panel, on page 8 for the location of the network module slot on the chassis.

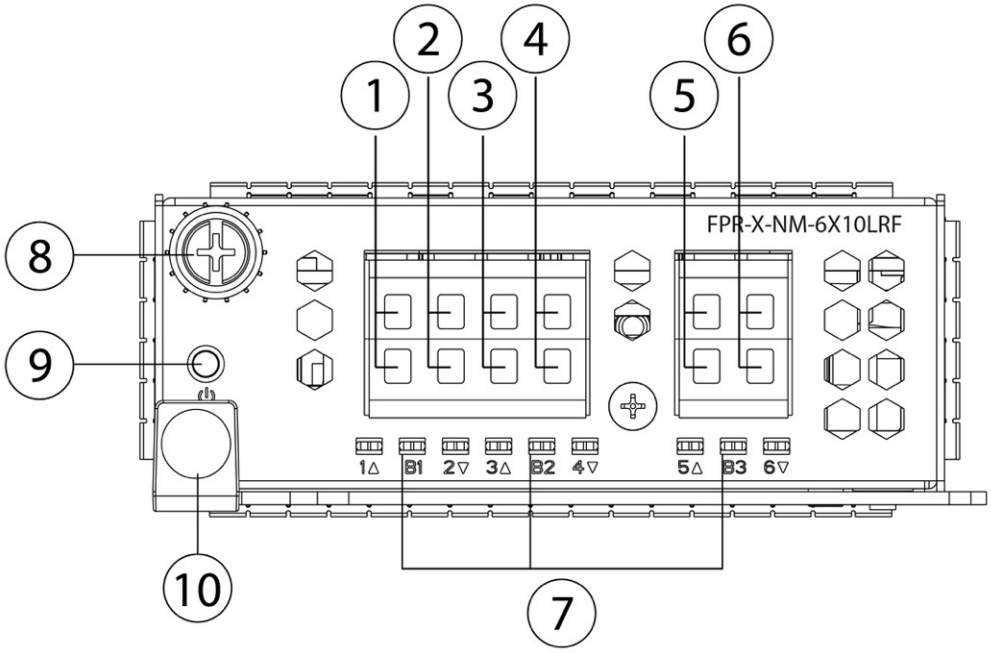
FPR-X-NM-6X1SXF, FPR-X-NM-6X10SRF, FPR-XN-M-6X10LRF, FPR-X-NM-6X25SRF, and FPR-X-NM-6X25LRF hardware bypass network modules have six ports that are numbered from top to bottom, left to right. Pair ports 1 and 2, 3 and 4, and 5 and 6 to form hardware bypass paired sets. In hardware bypass mode, data is not processed by the Secure Firewall 3100 but is routed to the paired port. This network module has built-in SPF transceivers. Hot swapping and field replacement of transceivers are not supported.

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 1/10/25-Gb network module with another supported network module, you must reboot the chassis so that the new network module is recognized. See the configuration guide for your operating system for the detailed procedures for managing network modules.

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

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

Figure 11: 1/10/25-Gb Network Module (FPR-X-NM-6X1SXF, FPR-X-NM-6X10SRF, FPR-XN-M-6X10LRF, FPR-X-NM-6X25SRF, and FPR-X-NM-6X25LRF)



1	Ethernet *X*/1 (top port) Ethernet *X*/2 (bottom port) Ports 1 and 2 are paired together to form a hardware bypass pair.	**2**	Ethernet *X*/3 (top port) Ethernet *X*/4 (bottom port) Ports 3 and 4 are paired together to form a hardware bypass pair.
3	Ethernet *X*/5 (top port) Ethernet *X*/6 (bottom port) Ports 5 and 6 are paired together to form a hardware bypass pair.	**4**	Ethernet *X*/7 (top port) Ethernet *X*/8 (bottom port) Ports 7 and 8 are paired together to form a hardware bypass pair.
5	Ethernet *X*/9 (top port) Ethernet *X*/10 (bottom port) Ports 9 and 10 are paired together to form a hardware bypass pair.	**6**	Ethernet *X*/11 (top port) Ethernet *X*/12 (bottom port) Ports 11 and 12 are paired together to form a hardware bypass pair.

7	Bypass LEDs B1 through B3: • Off—Bypass mode is disabled. • Green—Port is in standby mode. • Amber, flashing—Port is in hardware bypass mode, failure event.	**8**	Captive screw
9	Power LED	**10**	Handle ejector
11	Six network activity LEDs: • Amber—No connection, or port is not in use, or no link or network failure. • Green—Link up, no network activity. • Green, flashing—Network activity.		—

For More Information

- See Hardware Bypass Network Modules, on page 18 for a description of hardware bypass.
- See 10/100/1000Base-T Network Module with Hardware Bypass, on page 19 for a description of the 1-Gb network module.
- See 1/10/25-Gb Network Module, on page 15 for a description of the 1/10/25-Gb network module.
- See 40-Gb Network Module, on page 17 for a description of the 40-Gb network module.
- See Install, Remove, and Replace the Network Module, on page 65 for the procedure for removing and replacing network modules.

Power Supply Module

Note You *cannot* mix AC and DC power supply modules in the chassis.

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.

Note The system power requirements are lower than the power supply module capabilities. See the following table.

AC Power Supply

The dual power supplies can supply up to 800-W power across the input voltage range. The load is shared when both power supply modules are plugged in and running at the same time.

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

Table 2: AC Power Supply Module Hardware Specifications

Input voltage	100 to 240 VAC
Maximum input current	<3 A at 200 VAC <6 A at 100 VAC
Maximum output power	400 W
Frequency	50 to 60 Hz
Efficiency	85% at 50% load
Redundancy	1+1 redundancy with dual power supply modules

DC Power Supply

The power supplies can supply up to 800 W power across the input voltage range. The load is shared when both power supply modules are plugged in and running at the same time.

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

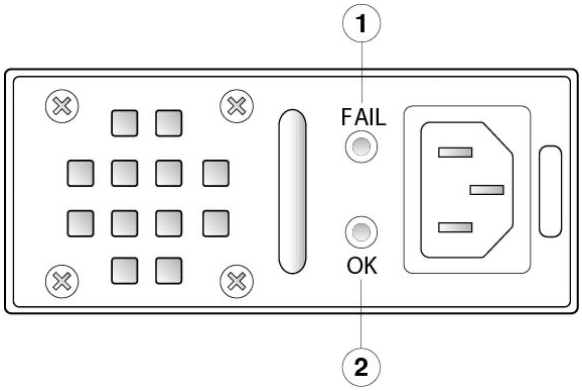
Table 3: DC Power Supply Module Hardware Specifications

Input voltage	-48 to -60 VDC
Maximum input current	< 15 A at -48 V
Redundancy	1+1 redundancy with dual power supply modules
Efficiency	> 88% at 50% load

Power Supply Module LEDs

The following figure shows the bicolor power supply LEDs on the power supply module. The figure shows the AC power supply module. The DC power supply module has the same LEDs.

Figure 12: Power Supply Module LEDs



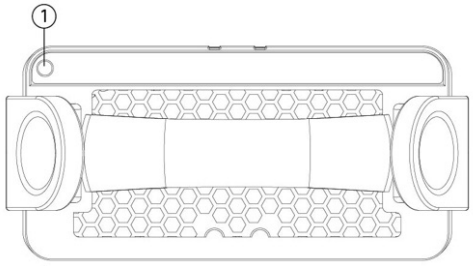
1	**Amber FAIL LED** Fail LED Status: • Off—No fault detected. • Amber, flashing—Fault warning, power supply may still work but could fail due to high temperature, failing fan, or over current. • Amber—Fault detected; power supply not working properly. Includes over voltage, over current, over temperature, and fan failure.	2	**Green OK LED** OK LED Status: • Off—Input power not present. • Green, flashing—Input power present, but system is not powered up (power switch is off). • Green—The power supply module is enabled and running.

Dual Fan Modules

The Secure Firewall 3100 has two dual fan modules that provide 3 + 1 redundancy. When one fan fails, the other three spin at maximum speed so that the system continues to function. The dual fan modules are hot-swappable and installed in the rear of the chassis.

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

Figure 13: Fan LED



1	Two-color LED

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

- Off—The environmental subsystem is not active yet.
- Green—Fan running normally. It may take up to one minute for the LED status to turn green after power is on.
- Amber—One fan has failed. The system can continue to operate normally, but fan service is required.
- Amber, flashing—Two or more fans have failed. Immediate attention is required.

For More Information

- See Product ID Numbers, on page 32 for a list of the PIDs associated with the Secure Firewall 3100 fans.
- See Remove and Replace the Dual Fan Module, on page 70 for the procedure for removing and replacing the dual fan modules.

SSDs

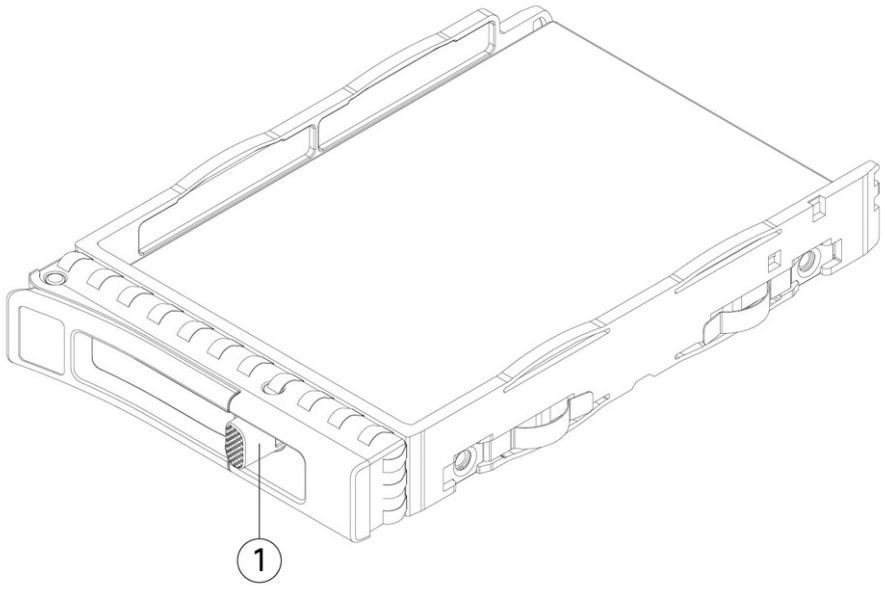
The Secure Firewall 3100 has two SSD slots that each hold one NVMe 900-GB SSD. By default the Secure Firewall 3100 ships with one 900-GB SSD installed in slot 1. The second SSD slot is reserved for software RAID1. The RAID1 SSD is shipped already configured. If you have two SSDs installed, they form a RAID when you boot up.

Hot swapping is supported. With two SSDs, you can swap SSD-1 without powering off the chassis. However, you must issue the **raid remove-secure local disk** command to remove SSD-2 from the RAID configuration before hot swapping. Otherwise, you can lose data. If you remove and replace the RAID1 SSD, you must add it again to the RAID1 configuration using the **raid add local-disk 1|2** command. The SSD drive identifiers are `disk0:` and `disk1:`.

Caution If you have only one SSD, you cannot remove it while the firewall is powered on.

Caution You cannot swap SSDs between different platforms. For example, you cannot use a 2100 series SSD in a 3100 series model.

Figure 14: SSD

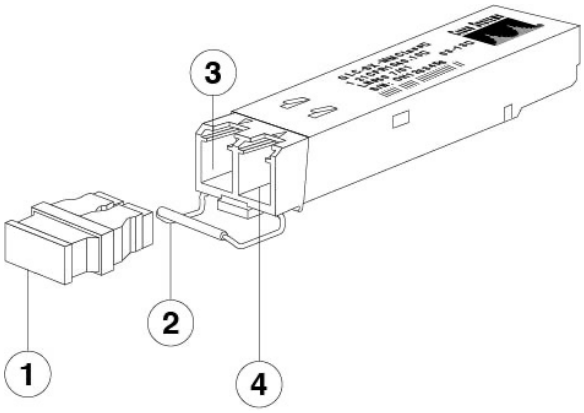


1	SSD release tab		—

Supported SFP/SFP+/QSFP+ Transceivers

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

Figure 15: SFP Transceiver



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

Safety Warnings

Take note of the following warnings:

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

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

Warning **Statement 1056—**Unterminated Fiber Cable

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

Warning **Statement 1057—**Hazardous Radiation Exposure

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

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

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

The following table lists the supported transceivers for the fixed ports on all 3100 models, and the FPR-X-NM-8X10G/FPR-X-NM-8X25G network modules.

Table 4: Supported 1-Gb SFP Transceivers

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

The following table lists the supported transceivers for the fixed ports on all 3100 models and the FPR-X-NM-8X10G/FPR-X-NM-8X25G network modules.

Table 5: Supported 10-Gb SFP Transceivers

Optics Type	PID	Comments
10G-SR	SFP-10G-SR	—
10G-SR	SFP-10G-SR-S	Ethernet only
10G-LR	SFP-10G-LR	—
10G-LR	SFP-10G-LR-S	Ethernet only
10G-ER	SFP-10G-ER-S	—
10G-ZR	SFP-10G-ZR	—
10G-ZR	SFP-10G-ZR-S	—

Optics Type	PID	Comments
10G DAC	SFP-H10GB-CUxM	x = 1, 1.5, 2, 2.5, 3, 4, 5 m **Note** You must set the link partner transmit strength to 400mV or greater.
10G ACU	SFP-H10GB-ACUxM	x = 7 and 10 m
10G AOC	SFP-10G-AOCxM	x = 1, 2, 3, 5, 7, 10 m

The following table lists the supported transceivers for the fixed ports on the Secure Firewall 3130 and 3140, and the FPR-X-NM-8X25G network module.

Table 6: Supported 25-Gb SFP Transceivers

Optics Type	PID	Comments
25G-SR	SFP-25G-SR-S	—
25G-CSR	SFP-10/25G-CSR-S	Dual rate, longer reach
25G-LR	SFP-10/25G-LR-S	Dual rate
25G DAC copper	SFP-H25G-CUxM	1, 1.5, 2, 2.5, 3, 4, 5 m
25G AOC	SFP-25G-AOCxM	1, 2, 3, 4, 5, 7, 10 m

The following table lists the supported transceivers for the fixed ports and the FPR-X-NM-4X40G network module.

Table 7: Supported 40-Gb SFP Transceivers for FPR3K-X-NM-4X40G

Optics Type	PID	Comments
40G-SR4	QSFP-40G-SR4	—
40G-SR4-S	QSFP-40G-SR4-S	Ethernet only
40G-CSR4	QSFP-40G-CSR4	300 m with OM3
40G-SR-BD	QSFP-40G-SR-BD	LC connector
40G-LR4-S	QSFP-40G-LR4-S	Ethernet only
40G-LR4	QSFP-40G-LR4	Ethernet and OTU3
40G-LR4L	WSP-Q40GLR4L	LR4 Lite, up to 2 km
40G-CU	Cisco QSFP-H40G-CU (1M, 3M, 5M)	QSFP to QSFP copper direct-attach cables (passive)

Optics Type	PID	Comments
40G-CU-breakout	QSFP-4SFP10G-CUxM (1M, 2M, 3M, 4M, 5M) **Note** Supported beginning with FTD 7.2 and ASA 7.18.1.	QSFP to 4xSFP copper direct-attach cables
40G-CU-A	Cisco QSFP-H40G-ACU (7M, 10M)	QSFP to QSFP copper direct-attach cables (active)
40G-AOC	QSFP-H40G-AOC (1M, 2M, 3M, 5M, 7M, 10M, 15M, 30M)	QSFP to QSFP active optical cables
40G-AOC-breakout	QSFP-4X10G-AOC (1M, 2M, 3M, 5M, 7M, 10M, 15M, 30M) **Note** Supported beginning with FTD 7.2 and ASA 7.18.1.	QSFP to 4xSFP active optical cables

Hardware Specifications

The following table contains hardware specifications for the Secure Firewall 3100.

Specification	3110	3120	3130	3140
Chassis dimensions (H x W x D)	1.75 x 17 x 20 inches (4.4 x 43.3 x 50.8 cm)			
Network module dimensions (H x W x D)	1.5 x 3.7 x 10.5 inches (4.39 x 9.4 x 26.67 cm)			
Chassis component weights	Network Module: 1.6 lb (.73 kg) SSD: 0.25 lb (.11 kg) Power supply module: 2.01 lb (0.912 kg) Fan module: 0.5 lb (.23)			
Chassis weight	23 lb (10.5 kg) 1 power supply module, 1 network module, 2 dual fan modules, 1 SSD		25 lb (11.4 kg) 2 power supply modules, 1 network module, 2 dual fan modules, 1 SSD	
System power	100/240 VAC 6 A (at 100 VAC), 50 to 60 Hz			
Temperature	Operating: 32 to 104°F (-0 to 40°C) Nonoperating: -4 to 149°F (-20 to 65°C) maximum altitude is 40,000 ft			

Specification	3110	3120	3130	3140
Humidity	Operating and nonoperating: 10 to 85% noncondensing			
Altitude	Operating: 10,000 ft maximum Nonoperating: 40,000 ft maximum			
Sound pressure	65 dB @ 77°F (25°C) typical 80 dB @ 77°F (25°C) maximum			
Sound power	72 (typical) 80 (maximum)			

Product ID Numbers

The following table lists the product IDs (PIDs) associated with the Secure Firewall 3100. All of the PIDs in the table are field-replaceable. If you need to get a return material authorization (RMA) for any component, see Cisco Returns Portal for more information.

Note See the **show inventory** command in the Cisco Firepower Threat Defense Command Reference or the Cisco ASA Series Command Reference to display a list of the PIDs for your Secure Firewall 3100.

Table 8: Secure Firewall 3100 PIDs

PID	Description
Chassis	
FPR3110-ASA-K9	Cisco Secure Firewall 3110 ASA chassis 1 RU
FPR3120-ASA-K9	Cisco Secure Firewall 3120 ASA chassis 1 RU
FPR3130-ASA-K9	Cisco Secure Firewall 3130 ASA chassis 1 RU
FPR3140-ASA-K9	Cisco Secure Firewall 3140 ASA chassis 1 RU
FPR3110-NGFW-K9	Cisco Secure Firewall 3110 next generation firewall chassis 1 RU
FPR3120-NGFW-K9	Cisco Secure Firewall 3120 next generation firewall chassis 1 RU
FPR3130-NGFW-K9	Cisco Secure Firewall 3130 next generation firewall chassis 1 RU
FPR3140-NGFW-K9	Cisco Secure Firewall 3140 next generation firewall chassis 1 RU

PID	Description
Accessories	
FPR3K-ACY-KIT	Accessory kit that ships with the chassis
FPR3K-ACY-KIT=	Accessory kit (spare)
FPR3K-PWR-AC-400	400-W AC power supply
FPR3K-PWR-AC-400=	400-W AC power supply (spare)
PWR-CC1-400WDC	400-W DC power supply
PWR-CC1-400WDC=	400-W DC power supply (spare)
FPR3K-PSU-BLANK	Power supply blank slot cover
FPR3K-PSU-BLANK=	Power supply blank slot cover (spare)
FPR3K-SSD900	900 GB SSD
FPR3K-SSD900=	900 GB SSD (spare)
FPR3K-SSD-BLANK	SSD blank slot carrier
FPR3K-SSD-BLANK=	SSD blank slot carrier (spare)
FPR3K-FAN	Dual fan module
FPR3K-FAN=	Dual fan module (spare)
FPR3K-SLIDE-RAILS	Slide rail kit
FPR3K-SLIDE-RAILS=	Slide rail kit (spare)
FPR3K-CBL-MGMT	Cable management brackets
FPR3K-CBL-MGMT=	Cable management brackets (spare)
FPR3K-BRKT	Rack-mount brackets
FPR3K-BRKT=	Rack-mount brackets (spare)
Network Modules	
FPR3K-XNM-6X1SXF	6-port 1-Gb SFP hardware bypass network module, SX multimode
FPR3K-XNM-6X1SXF=	6-port 1-Gb SFP hardware bypass network module, SX multimode (spare)
FPR3K-XNM-6X10SRF	6-port 10-Gb SFP hardware bypass network module, SR multimode

PID	Description
FPR3K-XNM-6X10SRF=	6-port 10-Gb SFP hardware bypass network module, SR multimode (spare)
FPR3K-XNM-6X10LRF	6-port 10-Gb SFP hardware bypass network module, LR single mode
FPR3K-XNM-6X10LRF=	6-port 10-Gb SFP hardware bypass network module, LR single mode (spare))
FPR3K-XNM-6X25SRF	6-port 25-Gb SFP hardware bypass network module, SR multimode
FPR3K-XNM-6X25SRF=	6-port 25-Gb SFP hardware bypass network module, SR multimode (spare)
FPR3K-XNM-6X25LRF	6-port 25-Gb SFP hardware bypass network module, LR single mode
FPR3K-XNM-6X25LRF=	6-port 25-Gb SFP hardware bypass network module, LR single mode (spare)
FPR3K-XNM-8X1GF	8-port 10/100/1000Base-10 hardware bypass network module
FPR3K-XNM-8X1GF=	8-port 10/100/1000Base-10 hardware bypass network module (spare)
FPR3K-XNM-8X10G	8-port 1/10-Gb SFP+ network module
FPR3K-XNM-8X10G=	8-port 1/10-Gb SFP+ network module (spare)
FPR3K-XNM-8X25G	8-port 1/10/25-Gb QSFP network module
FPR3K-XNM-8X25G=	8-port 1/10/25-Gb QSFP network module (spare)
FPR3K-XNM-4X40G	4-port 40-Gb QSFP+ network module
FPR3K-XNM-4X40G=	4-port 40-Gb QSFP+ network module (spare)
FPR3K-NM-BLANK	Network module blank slot cover
FPR3K-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.

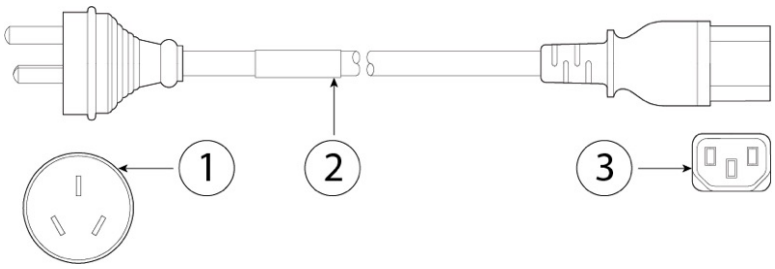
If you do not order the optional power cord with the system, you are responsible for selecting the appropriate power cord for the product. Using a incompatible power cord with this product may result in electrical safety

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 3100 are supported.

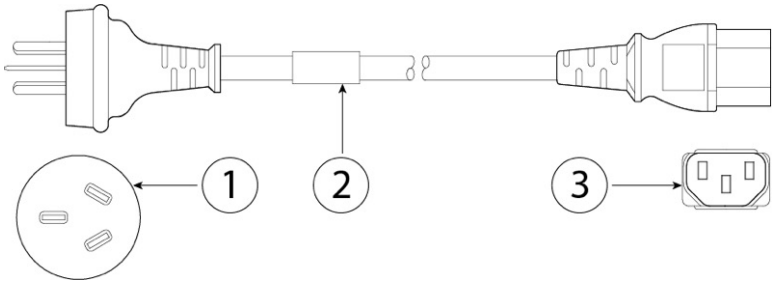
The following power cords are supported.

Figure 16: Argentina (CAB-ACR)



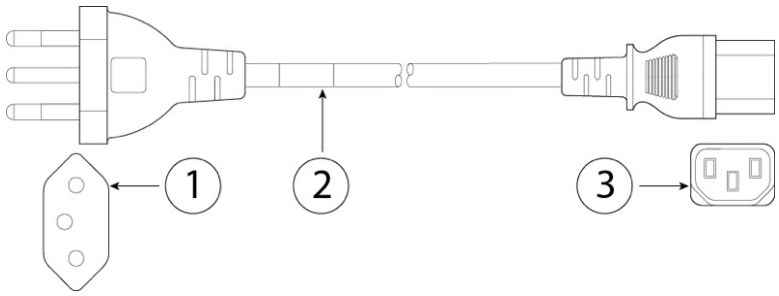
1	Plug: EL 219/IRAM 2073	**2**	Cord set rating: 10 A, 250 V Length: 2.5 m
3	Connector: IEC 60320/C13		—

Figure 17: Australia (CAB-ACA)



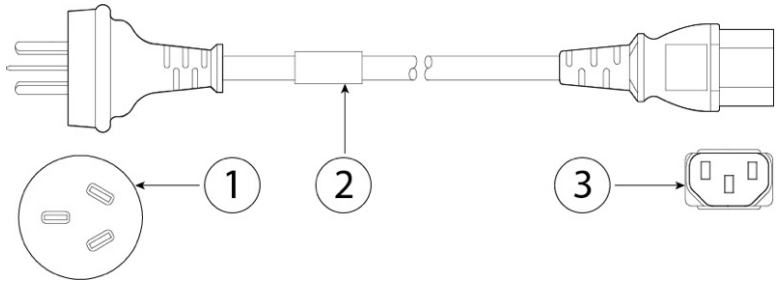
1	Plug: A.S. 3112	**2**	Cord set rating: 10 A, 250 V Length: 2.5 m
3	Connector: IEC 60320/C13		—

Figure 18: Brazil (CAB-C13-ACB)



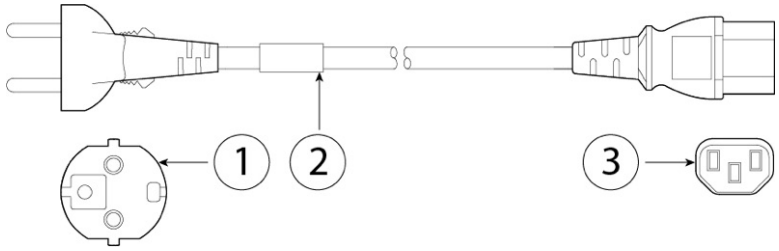
1	Plug: NBR 14136	**2**	Cord set rating: 10 A, 250 V Length: 2.1 m
3	Connector: IEC 60320/C13		—

Figure 19: China (CAB-ACC)



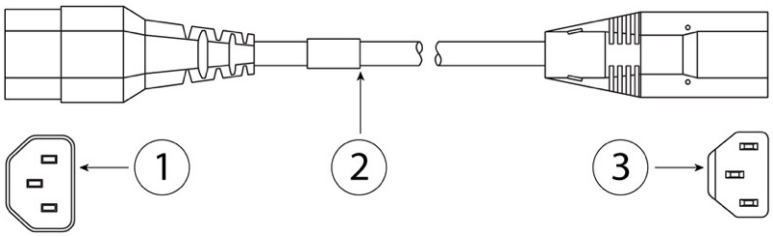
1	Plug: GB2099.1-2008	**2**	Cord set rating: 10 A, 250 V Length: 2.5 m
3	Connector: IEC 60320/C13		—

Figure 20: Europe (CAB-ACE)



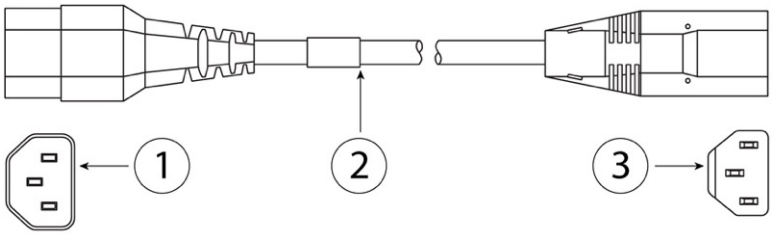
1	Plug: CEE 7 VII	**2**	Cord set rating: 10 A, 250 V Length: 1.5 m
3	Connector: IEC 60320/C13		—

Figure 21: India Jumper (CAB-C13-C14-3M-IN)



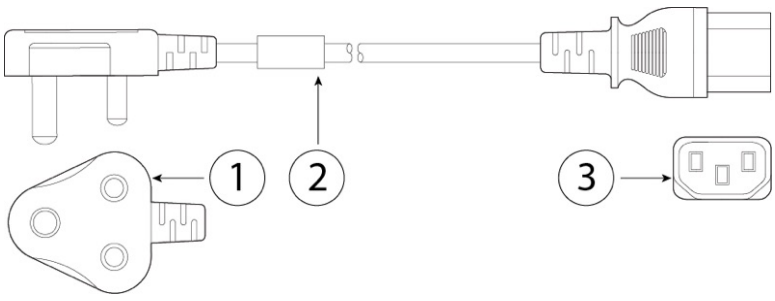
1	IEC 60320/C14G	**2**	Cord set rating: 10 A, 250 V Length: 3 m
3	Connector: IEC 60320/C13		—

Figure 22: India Jumper (CAB-C13-C14-IN)



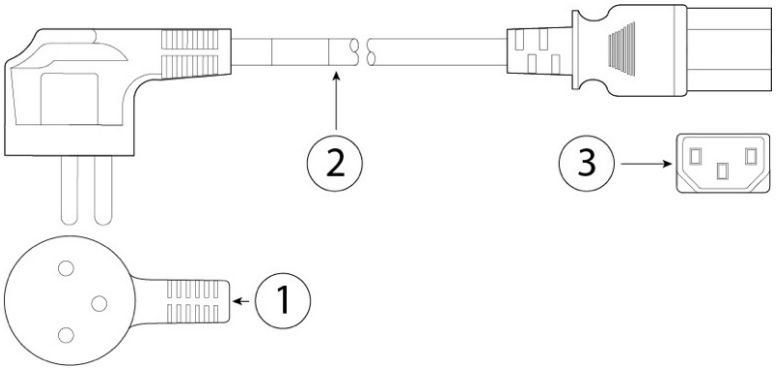
1	IEC 60320/C14G	**2**	Cord set rating: 10 A, 250 V Length: 1.4 m
3	Connector: IEC 60320/C13		—

Figure 23: India (PWR-CORD-IND-D)



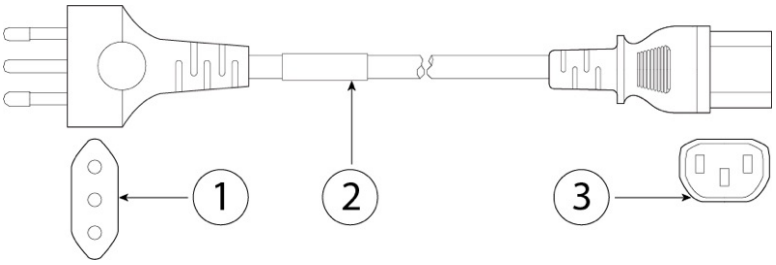
1	Plug: IS 6538-1971	**2**	Cord set rating: 10 A, 250 V Length: 1.8
3	Connector: IEC 60320/C13		—

Figure 24: Israel (CAB-250V-10A-IS)



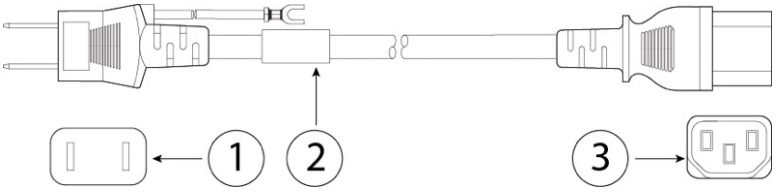
1	Plug: SI-32	**2**	Cord set rating: 10 A, 250 V Length: 2.5 m
3	Connector: IEC 60320/C13		—

Figure 25: Italy (CAB-ACI)



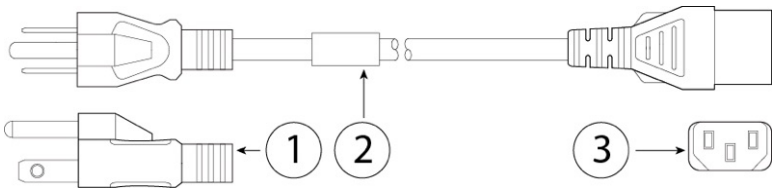
1	Plug: CEI 23-16	**2**	Cord set rating: 10 A, 250 V Length: 2.5 m
3	Connector: IEC 60320/C13		—

Figure 26: Japan (CAB-JPN)



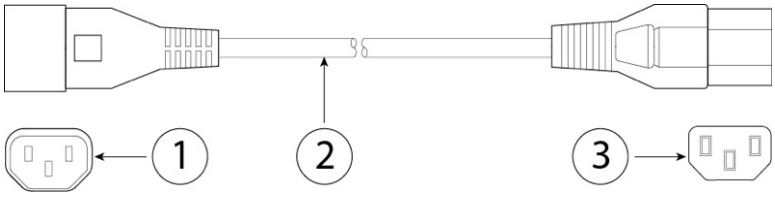
1	Plug: JIS C8303	**2**	Cord set rating: 12 A, 125 V Length: 2.5 m
3	Connector: IEC 60320/C13		—

Figure 27: Japan (CAB-JPN-3PIN)



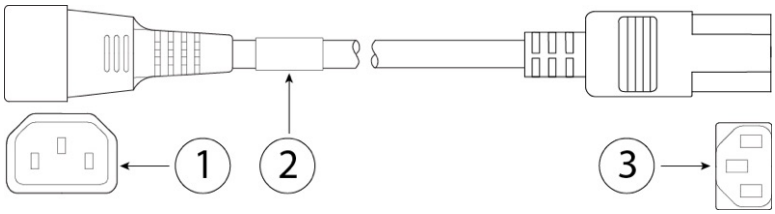
1	Plug: JIS C8303/JIS C8306	**2**	Cord set rating: 12 A, 125 V Length: 2.3 m
3	Connector: IEC 60320/C13		—

Figure 28: Japan (CAB-C13-C14-2M-JP) PSE Mark



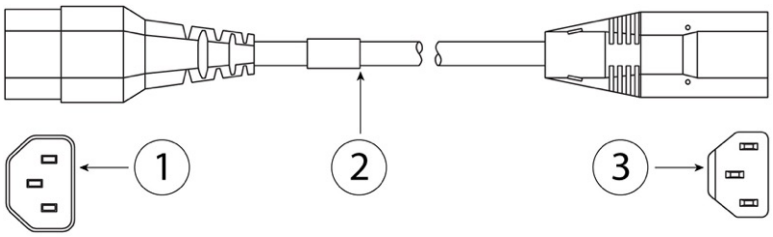
1	IEC 60320-2-2/E	**2**	Cord set rating: 10 A, 250 V Length: 2 m/6.5 ft
3	Connector: IEC 60320/C13		—

Figure 29: Jumper (CAB-C13-C14-2M)



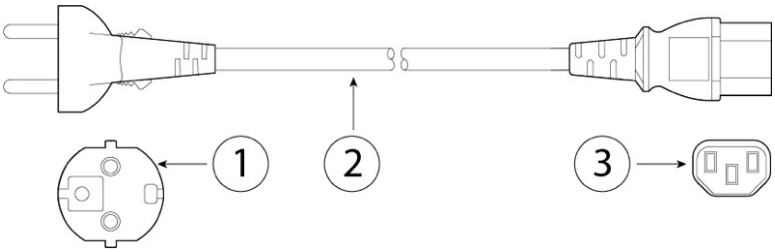
1	IEC 60320/C14G	**2**	Cord set rating: 10 A, 250 V Length: 2 m
3	Connector: IEC 60320/C13		—

Figure 30: Cabinet Jumper (CAB-C13-CBN)



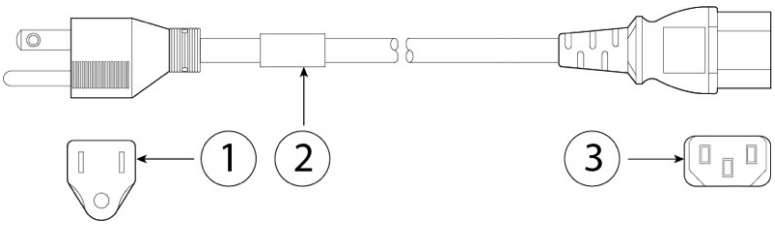
1	IEC 60320-2-2/E	**2**	Cord set rating: 10 A, 250 V Length: 0.7 m
3	Connector: IEC 60320/C13		—

Figure 31: Korea (CAB-AC-C13-KOR)



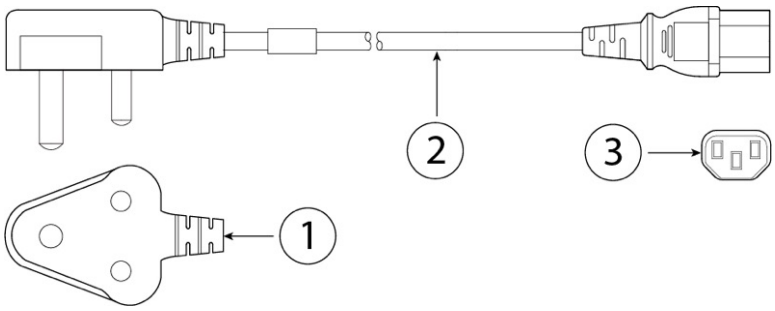
1	Plug: KSC 8305	**2**	Cord set rating: 10 A, 250 V Length: 1.8 m
3	Connector: IEC 60320/C13		—

Figure 32: North America (CAB-AC)



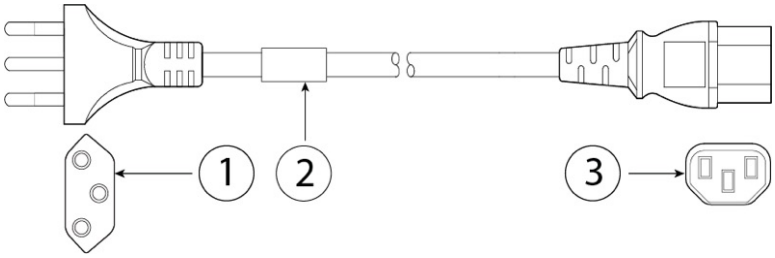
1	Plug: NEMA 5-15P	**2**	Cord set rating: 10 A, 125 V Length: 2.1 m
3	Connector: IEC 60320/C13		—

Figure 33: South Africa (CAB-ACSA)



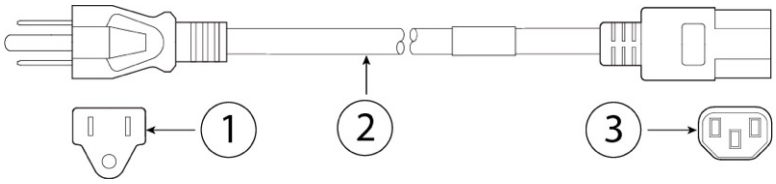
1	Plug: SABS 164/1	**2**	Cord set rating: 16 A, 250 V Length: 1.8 m
3	Connector: IEC 60320/C13		—

Figure 34: Switzerland (CAB-ACS)



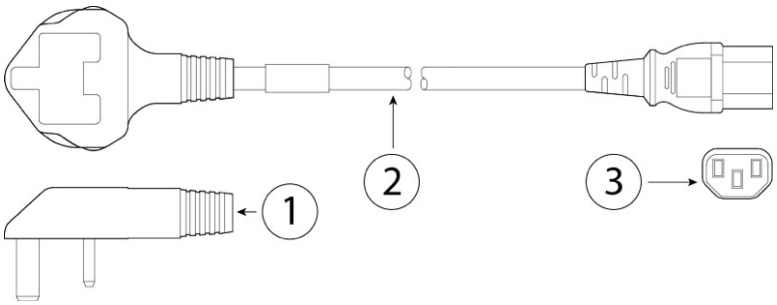
1	Plug: SEV 1011	**2**	Cord set rating: 10 A, 250 V Length: 2.5 m
3	Connector: IEC 60320/C13		—

Figure 35: Taiwan (CAB-ACTW)

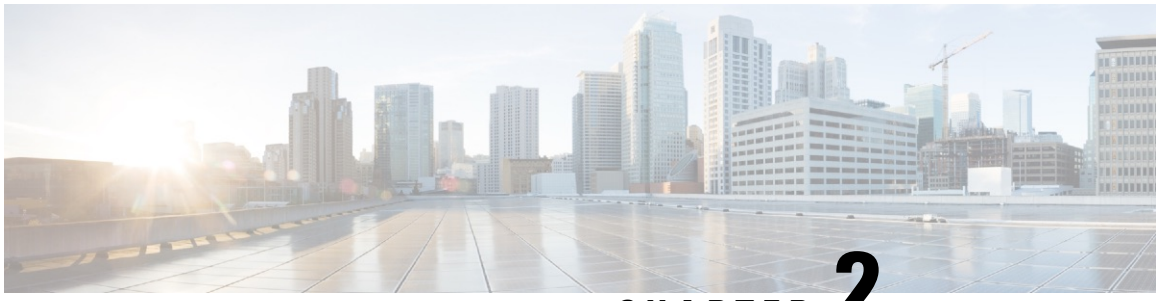


1	Plug: CNS10917	**2**	Cord set rating: 10 A, 125 V Length: 2.29 m
3	Connector: IEC 60320/C13		

Figure 36: United Kingdom (CAB-ACU)



1	Plug: BS1363A/SS145	**2**	Cord set rating: 10 A, 250 V Length: 2.5 m
3	Connector: IEC 60320/C13		—



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 provided at the end of each warning statement to locate its translation in the translated safety warnings for this device.

SAVE THESE INSTRUCTIONS

Warning **Statement 1004**—Installation Instructions

Read the installation instructions before using, installing, or connecting the system to the power source.

Warning **Statement 1005**—Circuit Breaker

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

AC 20 A/DC 40 A

Warning **Statement 1007—**TN and IT Power Systems

This equipment has been designed for connection to TN and IT power systems.

Warning **Statement 1015**—Battery Handling

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

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

Warning **Statement 1017—**Restricted Area

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

Warning **Statement 1021—**SELV Circuit

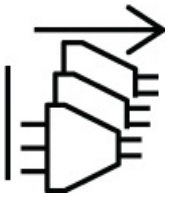
To avoid electric shock, do not connect SELV circuits to telephone-network voltage (TNV) circuits. LAN ports contain SELV circuits, and WAN ports contain TNV circuits. Some LAN and WAN ports both use RJ-45 connectors. Use caution when connecting cables.

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 1030—**Equipment Installation

Only trained and qualified personnel should be allowed to install, replace, or service this equipment.

Warning **Statement 1040—**Product Disposal

Ultimate disposal of this product should be handled according to all national laws and regulations.

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

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

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

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

Network Equipment-Building System (NEBS) Statements

NEBS describes the environment of a typical United States Regional Bell Operating Company (RBOC) central office. NEBS is the most common set of safety, spatial, and environmental design standards applied to

telecommunications equipment in the United States. It is not a legal or regulatory requirement, but rather an industry requirement.

The following NEBS statements apply to the Secure Firewall 3120:

Note **Statement 7001—**ESD Mitigation

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

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

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

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

Copper RJ-45 network ports

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

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

This statement applies to the intrabuilding ports listed below:

Copper RJ-45 network ports

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

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

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

This equipment is suitable for installations using the CBN.

Note **Statement 7018—**System Recover Time

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

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 Module, on page 23 for more detailed information about the power supply in the chassis.

When installing the chassis, consider the following:

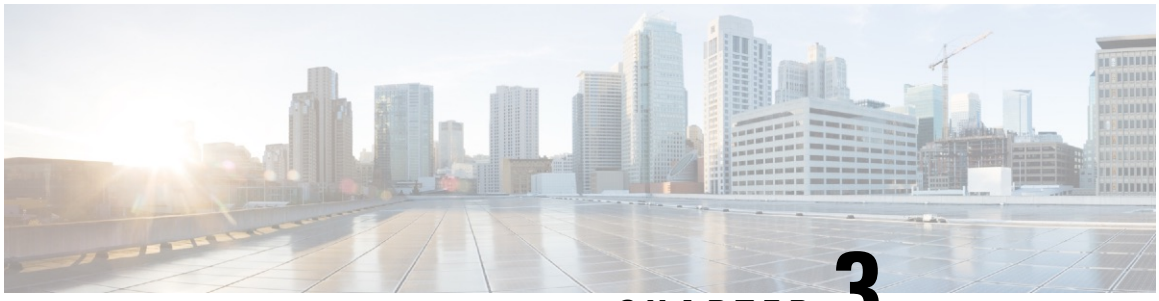
- Check the power at the site before installing the chassis to ensure that it is free of spikes and noise. Install a power conditioner, if necessary, to ensure proper voltages and power levels in the appliance-input voltage.
- Install proper grounding for the site to avoid damage from lightning and power 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 54 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

Rack-Mount the Chassis

Unpack and Inspect the Chassis

Note The chassis is thoroughly inspected before shipment. If any damage occurred during transportation or any items are missing, contact your customer service representative immediately. Keep the shipping container in case you need to send the chassis back due to damage.

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

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

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

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

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

Rack-Mount the Chassis Using Brackets

This procedure describes how to install the Secure Firewall 3100 in a rack using the rack-mount brackets. It also describes how to install the optional cable management brackets. See Product ID Numbers, on page 32 for a list of the PIDs associated with rack-mounting the chassis.

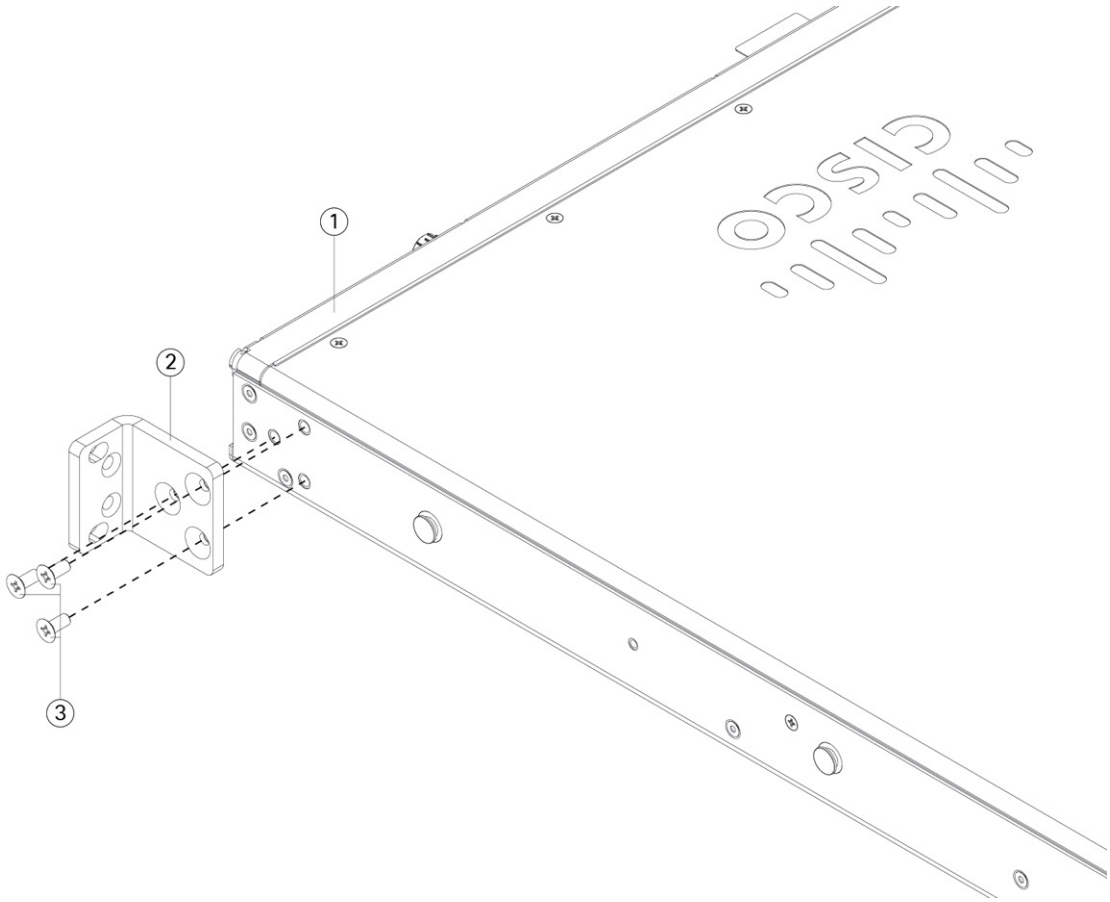
The rack is a standard Electronic Industries Association (EIA) rack. It is a 4-post-EIA-310-D, which is the current revision as specified by EIA. The vertical hole spacing alternates at .50 inches (12.70 mm) to .625 inches (15.90 mm) to .625 inches (15.90 mm) and repeats. The start and stop space is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

You need the following to install the Secure Firewall 3100 in a rack:

- Phillips screwdriver
- Two rack-mount brackets (part number 700-127244-01) with six 8-32 x 0.375 inch screws (part number 48-2286-01)
- Rack-mount screws:
  - Four 12-24 x 0.75 inch Phillips screws (part number 648-0440-01) for securing the chassis to your rack
  - Four 10-32 x 0.75 inch Phillips screws (part number 48-0441-01) for securing the chassis to your rack
- (Optional) Cable management bracket kit (part number 69-100376-01):
  - Two cable management brackets (part number 700-106377-01)
  - Four 8-32 x 0.375 inch Phillips screws (part number 48-2696-01)

Step 1 Attach a rack-mount bracket to each side of the chassis using the six 8-32 x 0.375 inch Phillips screws (three per side).

Figure 37: Attach the Rack-Mount Bracket to the Side of the Chassis

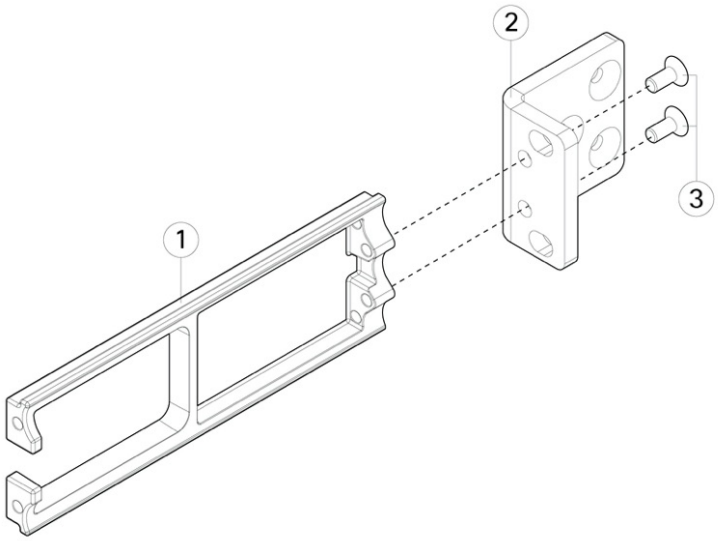


1	Chassis	**2**	Rack-mount bracket
3	8-32 x 0.375-inch Phillips screws (three per side)		

Step 2 (Optional) Attach the cable management bracket to the rack-mount bracket:

a) Install the cable management screws into the rack-mount bracket.

Figure 38: Install the Cable Management Screws into the Rack-Mount Bracket



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

b) Install two 8-32 x 0.375-inch screws through the inside of each rack-mount bracket to secure the cable management bracket to the rack-mount bracket.

Step 3 Attach the chassis with the installed rack-mount bracket to the rack using the screws that work for your rack.

What to do next

- See Ground the Chassis, on page 61 for the procedure to ground the Secure Firewall 3100.
- Install the cables according to your default software configuration as described in the Cisco Secure Firewall 3100 Getting Started Guide.

Rack-Mount the Chassis Using Slide Rails

This procedure describes how to install the Secure Firewall 3100 in a rack using slide rails. It applies to all models of the 3100 series. You use the pegs on the chassis to secure the slide rail. See Product ID Numbers, on page 32 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 3100. The optional cable management bracket kit comes with two cable management brackets and four 8-32 x 0.375-inch screws.

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

.50-inch holes. The horizontal spacing is 18.312 inches (465.1 mm), and the rack opening is specified as a minimum of 17.75 inches (450 mm).

You need the following to install the Secure Firewall 3100 in a rack using slide rails:

- Phillips screwdriver
- Two slide rails (part number 800-110033-01)
- Two slide rail locking brackets (700-121935-01)
- Six 8-32 x 0.302-inch Phillips screws (part number 48-102184-01)
- Two M3 x 0.5 x 6 mm Phillips screws (part number 48-101144-01)
- (Optional) Two cable management brackets (part number 700-106377-01) with four 8-32 x 0.375-inch Phillips screws (part number 48-2696-01)

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

Safety Warnings

Take note of the following warnings:

Warning **Statement 164**—Lifting Requirement

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

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

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

- This unit should be mounted at the bottom of the rack if it is the only unit in the rack.
- When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.
- If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.

Warning **Statement 1018—**Supply Circuit

To reduce risk of electric shock and fire, take care when connecting units to the supply circuit so that wiring is not overloaded.

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 1030—**Equipment Installation

Only trained and qualified personnel should be allowed to install, replace, or service this equipment.

Warning **Statement 1047**—Overheating Prevention

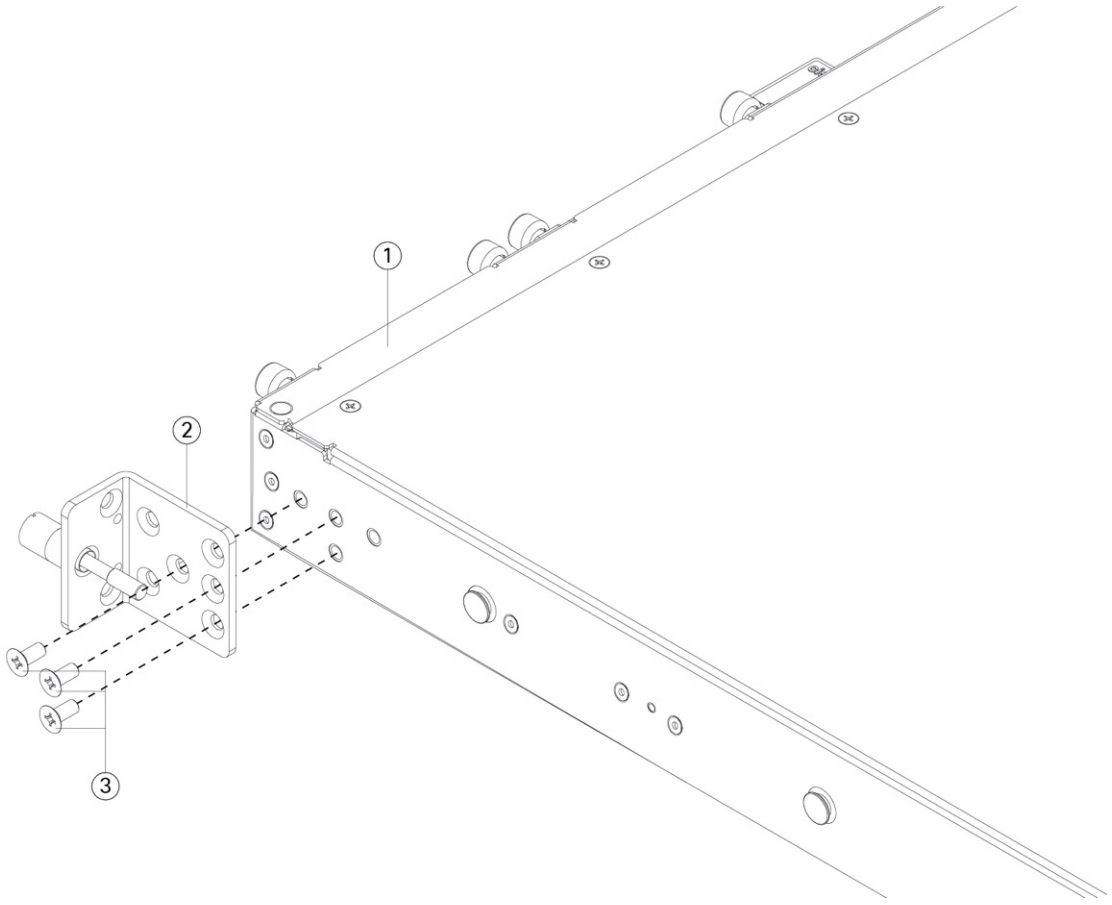
To reduce the risk of fire or bodily injury, do not operate the unit in an area that exceeds the maximum recommended ambient temperature of 104°F (40°C).

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

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

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

Figure 39: Attach the Slide-Rail Locking Bracket to the Side of the Chassis

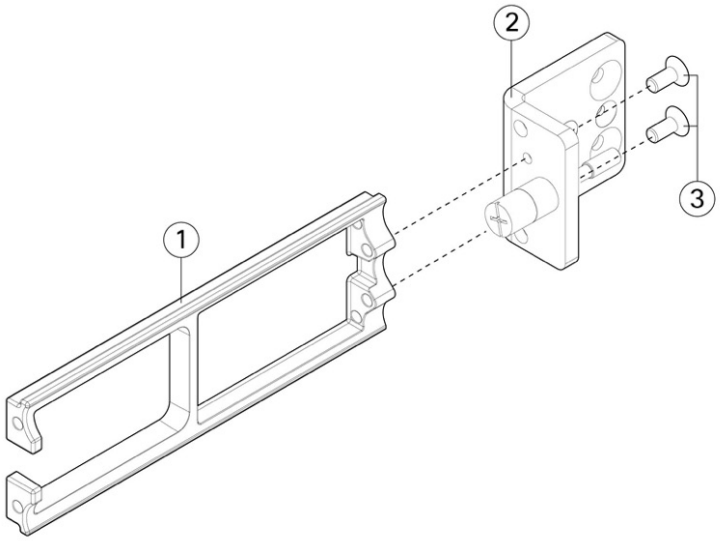


1	Chassis	**2**	Slide-rail locking bracket
3	8-32 x 0.302-inch Phillips screws (three per side)		

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

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

Figure 40: Install the Cable Management Screws into the Slide-Rail Locking Bracket



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

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

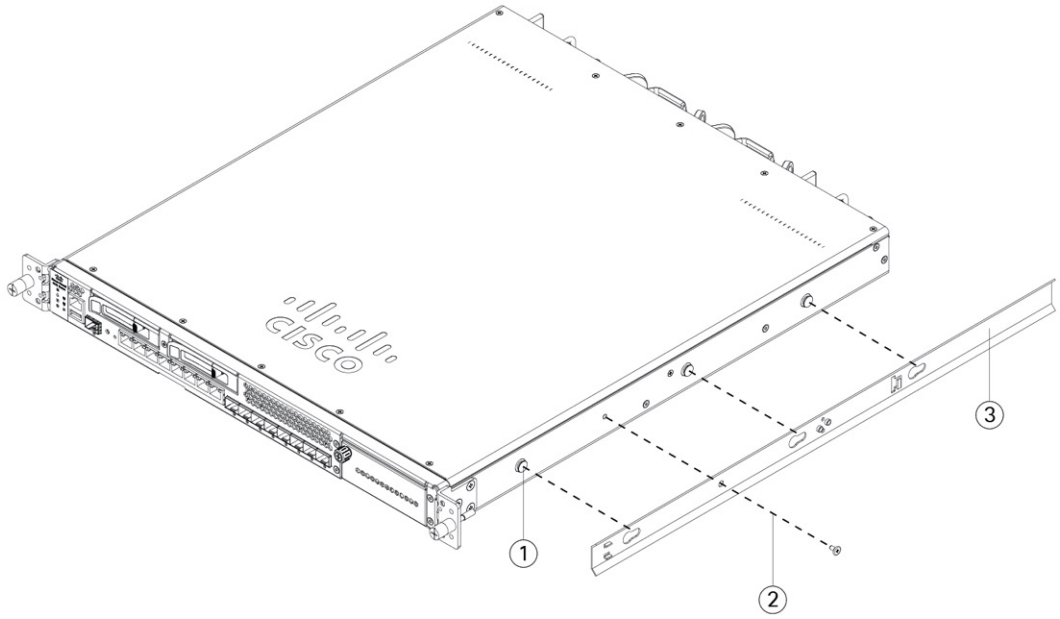
Step 3 Attach the inner rails to the sides of the chassis:

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

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

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

Figure 41: Line up the Inner Rail with the Pegs on the Chassis



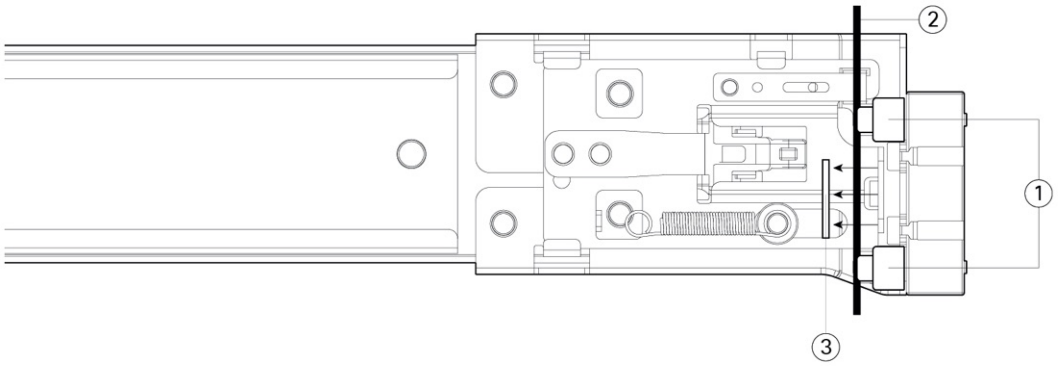
1	Mounting peg on the chassis for the keyed slot	**2**	M3 x 0.5 x 6- mm Phillips screws (one per side)
3	Inner rail		

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

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

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

Figure 42: Front Securing Mechanism Inside the Front End



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

Step 5 Install the slide rails into the rack:

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

The slide rail front-end wraps around the outside of the rack post and the mounting pegs enter the rack-post holes from the outside-front.

Note The rack post must be between the mounting pegs and the open securing plate.

b) Push the mounting pegs into the rack-post holes from the outside-front.

c) Press the securing plate release button marked 'PUSH.' The spring-loaded securing plate closes to lock the pegs in place.

d) Adjust the slide-rail length, and then push the rear mounting pegs into the corresponding rear rack-post holes. The slide rail must be level front-to-rear.

The rear mounting pegs enter the rear rack-post holes from the inside of the rack post.

e) Attach the second slide-rail assembly to the opposite side of the rack. Make sure that the two slide-rail assemblies are at the same height with each other and are level front-to-back.

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

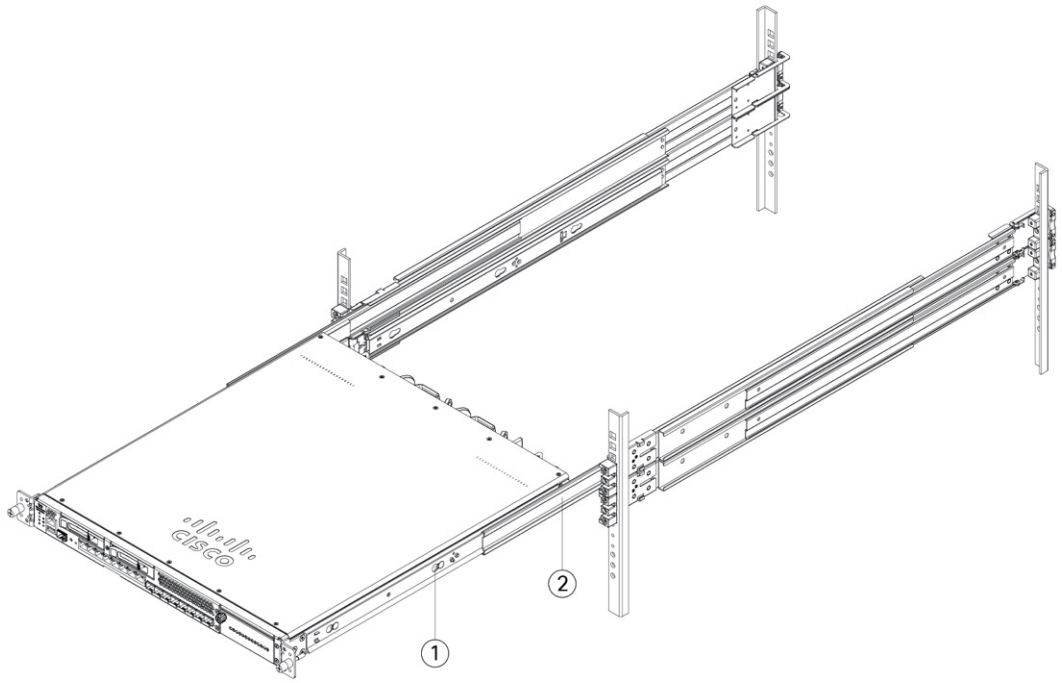
Step 6 Insert the chassis into the slide rails.

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

b) Push the inner rails into the slide rails on the rack until they stop at the internal stops.

c) Slide the release clip toward the rear on both inner rails, and then continue pushing the chassis into the rack until the mounting brackets meet the front of the slide rail.

Figure 43: Inner Rail Release Clip



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

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

What to do next

- See Ground the Chassis, on page 61 for the procedure to ground the Secure Firewall 3100.
- Install the cables according to your software configuration as described in the Cisco Secure Firewall 3100 Getting Started Guide.

Ground the Chassis

Note Grounding the chassis is required, even if the rack is already grounded. A grounding pad with two threaded M4 holes is provided on the chassis for attaching a grounding lug. The grounding lug must be Nationally Recognized Testing Laboratory (NRTL)-listed. In addition, a copper conductor (wires) must be used and the copper conductor must comply with National Electrical Code (NEC) code for ampacity.

You need the following items that you provide:

- Wire-striping tool
- Crimping tool
- Grounding cable
- Two star lock washers for the 10-32 x 0.375 inch-screws used to secure the ground lug
- You need the following items from the accessory kit:
  - Grounding lug #6 AWG, 90 degree, #10 post (part number 332-0608-01)
  - Two 10-32 x 0.38-inch screws used to secure the grounding lug (part number 48-0700-01)

Safety Warnings

Take note of the following warnings:

Warning **Statement 1024—**Ground Conductor

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

Warning **Statement 1025—**Use Copper Conductors Only

To reduce risk of fire, use copper conductors only.

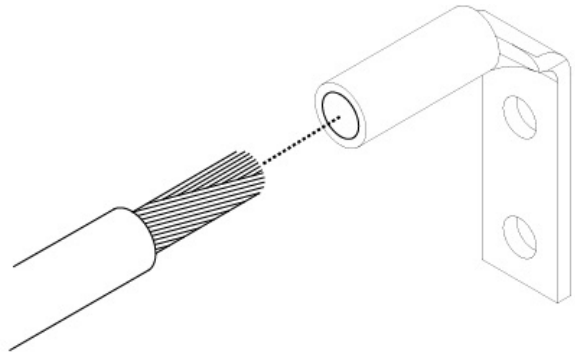
Warning **Statement 1046—**Installing or Replacing the Unit

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

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 44: Insert the Cable into the Grounding Lug

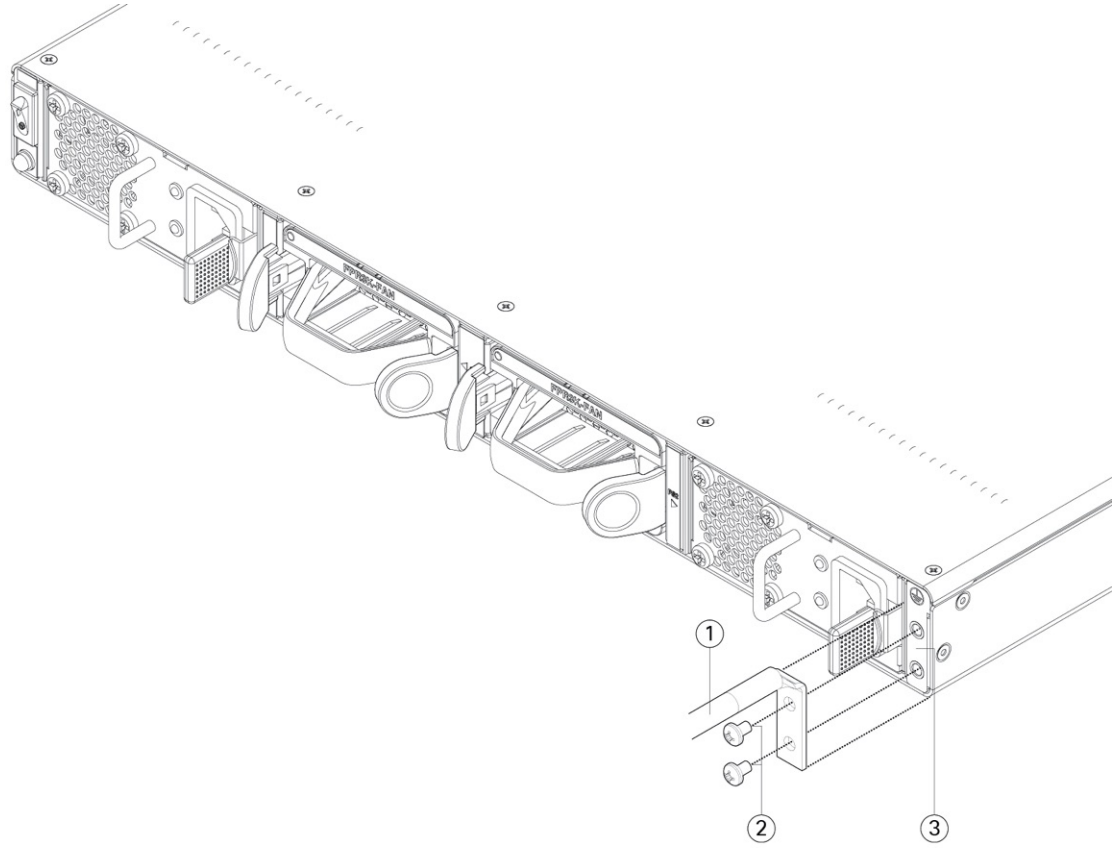


Step 3 Use the crimping tool to secure the grounding cable in the grounding lug.

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

Step 5 Place the grounding lug against the grounding pad so that there is solid metal-to-metal contact, and insert the two screws with washers through the holes in the grounding lug and into the grounding pad.

Figure 45: Attach the Grounding Lug



1	Grounding lug	**2**	Two 10-32 x 0.38-inch screws

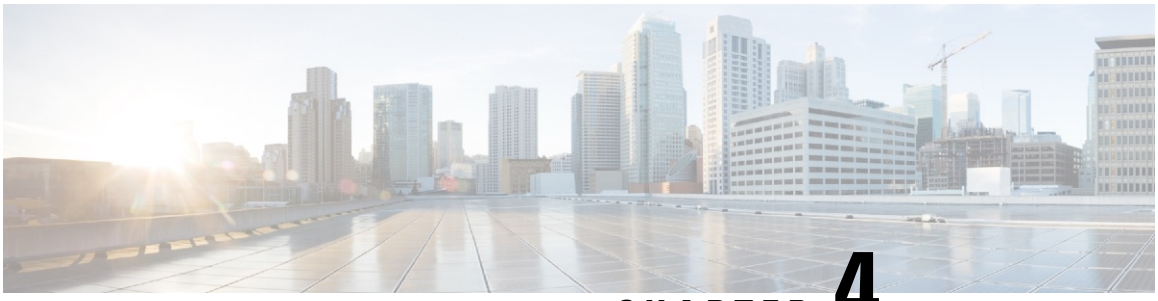
3	Ground pad		—

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 Cisco Secure Firewall 3100 Getting Started Guide.



CHAPTER 4

Installation, Maintenance, and Upgrade

Install, Remove, and Replace the Network Module

You can remove and replace the network module (NM-2) in the Secure Firewall 3100. Although the hardware supports removing and replacing the network module while the system is running, the software does not currently support hot swapping. You must power down the chassis or disable the network slot to remove and replace network modules.

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

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

Safety Warnings

Take note of the following warnings:

Warning **Statement 1030—**Equipment Installation

Only trained and qualified personnel should be allowed to install, replace, or service this equipment.

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

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

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

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

See Rear Panel, on page 13 for more information about the power switch. See the configuration guide for your operating system for the procedure for installing a network module for the first time into an empty slot.

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

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

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

a) Save your configuration.

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

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

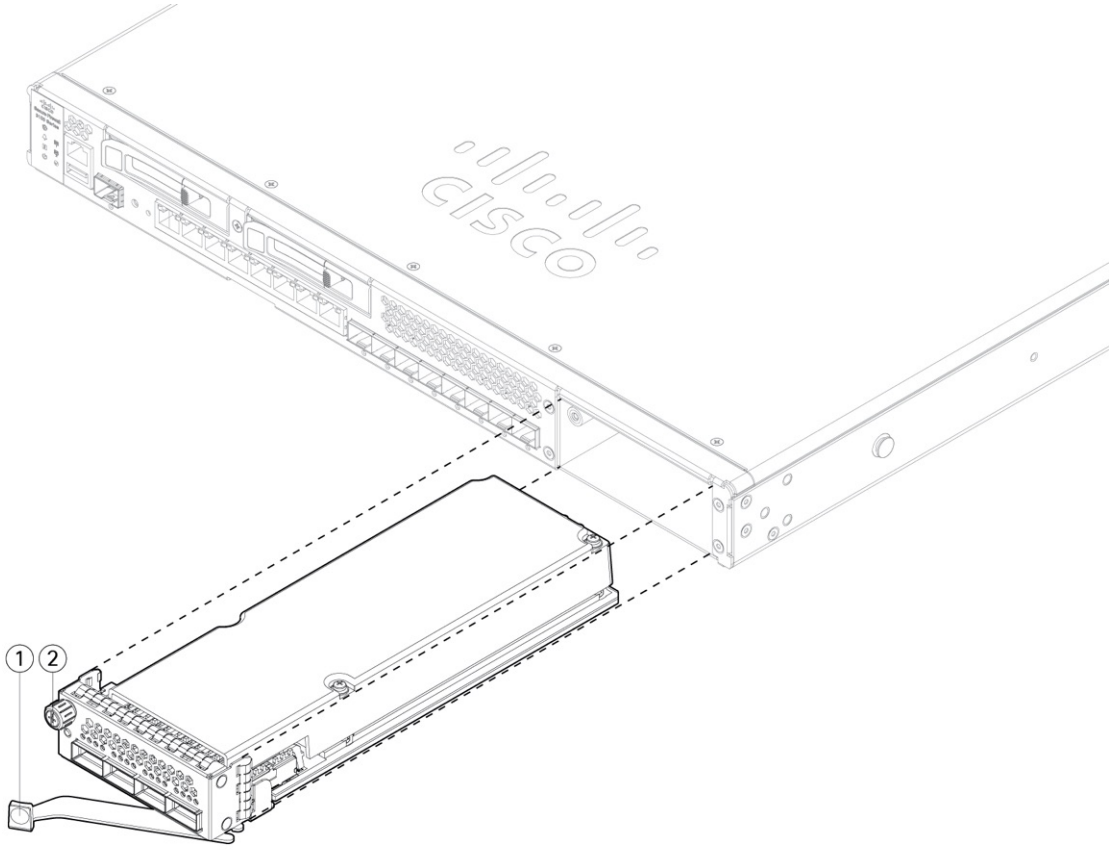
See Rear Panel, on page 13 for more information about the power switch.

d) Continue with Step 3.

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

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

Figure 46: 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 first SSD slot (SSD-1) is for storage. The second slot (SSD-2) is for the optional SW RAID1 support only. See SSDs, on page 26 for more information.

Caution Hot swapping for the RAID configuration is not supported. You can hot-swap SSD-1 if there are two SSDs installed. To hot-swap SSD-2, you must remove it from the RAID configuration using the **raid remove-secure local-disk 1|2** command.

Safety Warnings

Take note of the following warnings:

Warning **Statement 1030—**Equipment Installation

Only trained and qualified personnel should be allowed to install, replace, or service this equipment.

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

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

Step 1 Save your configuration.

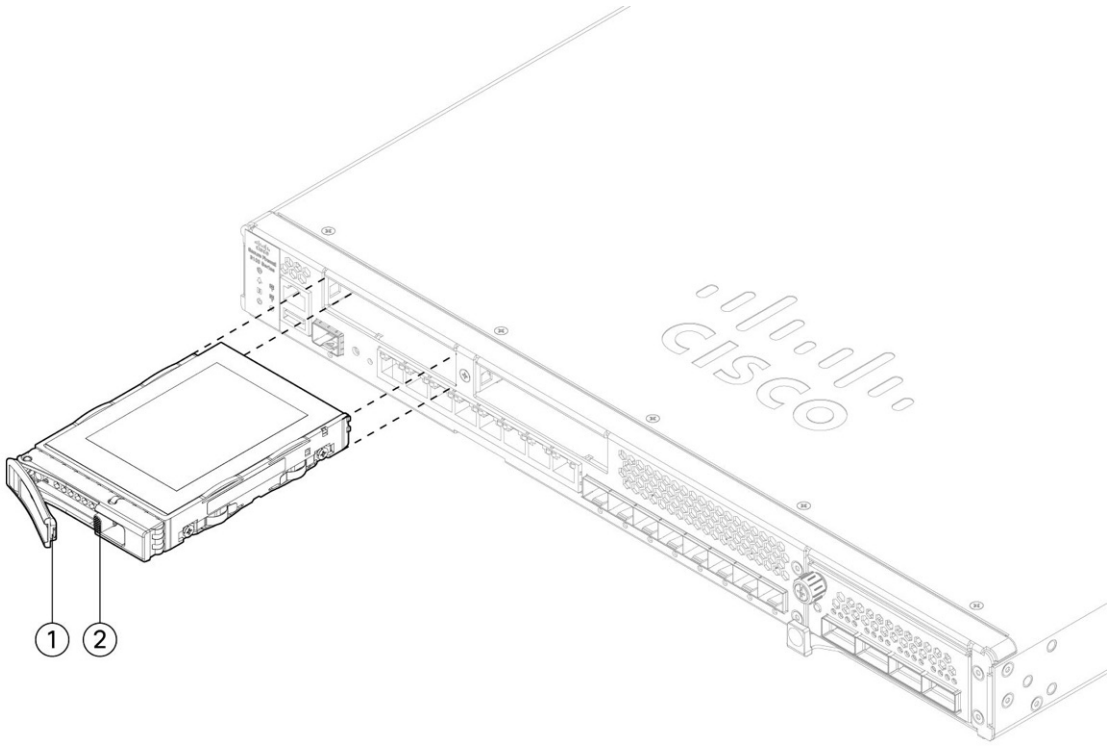
Step 2 If you are removing SSD-1 and there is only one SSD installed in the chassis, power down the chassis by moving the power switch to the OFF position. See Rear Panel, on page 13 for more information on the power switch.

You can only remove the SSD in slot 1 if there are two SSDs installed. If you have only one SSD, you cannot remove it while the chassis is powered on

Step 3 To remove the SSD in slot 1, 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 47: Remove the SSD



1	Ejector handle		SSD release tab

Step 5 To replace the SSD in slot 1, make sure the power switch is still in the OFF position (if you are replacing SSD-1), and then hold the SSD with the ejector handle extended in front of slot 1, push it in gently until it is seated, and close the ejector handle.

Step 6 You can install the RAID1 SSD in slot 2. Make sure the power switch is still in the OFF position, and then remove the blank faceplate in slot 2 by loosening the handle on the faceplate.

Step 7 Hold the RAID1 SSD with the ejector handle extended in front of slot 2, push it in gently until it is seated, and close the ejector handle.

Caution Do not switch the two SSDs. The RAID1 SSD *must* be installed in slot 2.

Step 8 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 9 Add SSD-2 to the RAID configuration using the **raid add local-disk 1|2** command.

Remove and Replace the Dual Fan Module

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

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

Safety Warnings

Take note of the following warnings:

Warning **Statement 1030—**Equipment Installation

Only trained and qualified personnel should be allowed to install, replace, or service this equipment.

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

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

Warning **Statement 1093—**Avoid Sharp Edges

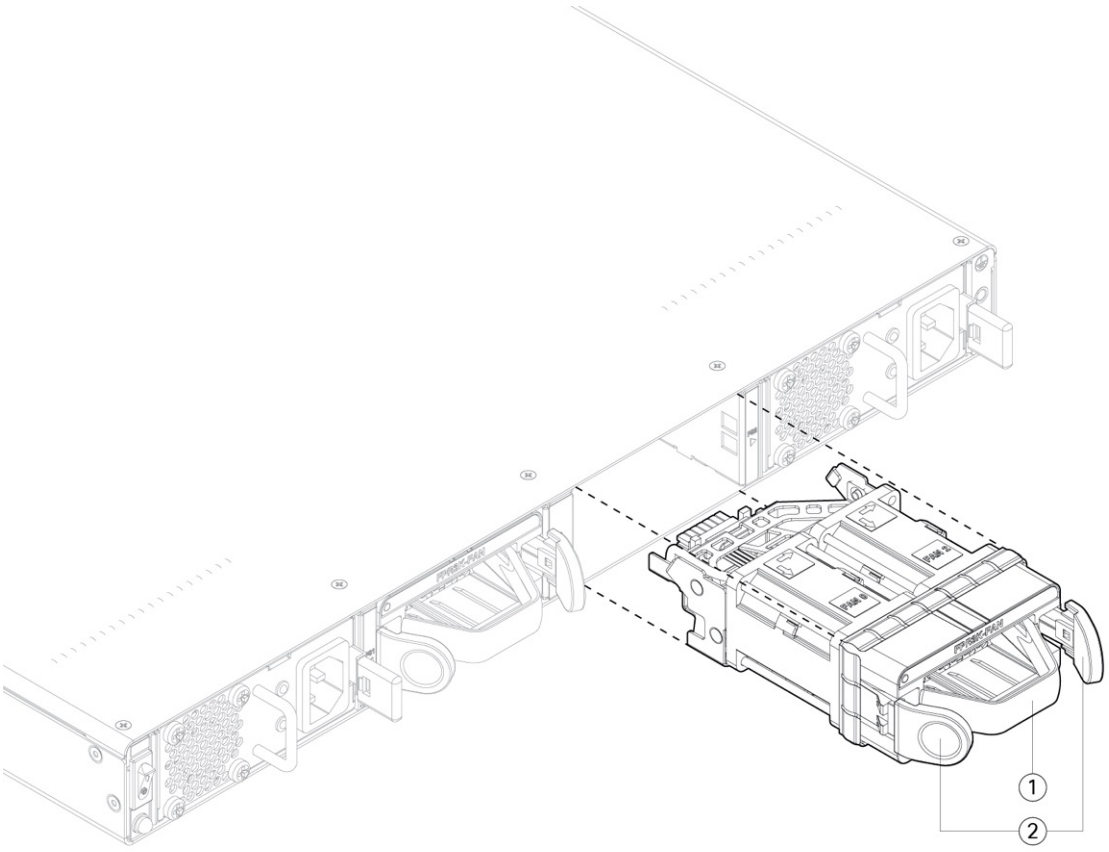
Risk of personal injury. Avoid sharp edges when installing or removing replaceable units.

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

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

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

Figure 48: Remove the Dual Fan Module



1	Handle		Squeeze tabs

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

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

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

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

Remove and Replace the Power Supply Module

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

Safety Warnings

Take note of the following warnings:

Warning **Statement 1002—**DC Power Supply

When stranded wiring is required, use approved wiring terminations such as closed-loop or spade-type with upturned lugs. These terminations should be the appropriate size for the wires and should clamp both the insulation and conductor.

Warning **Statement 1003—**DC Power Disconnection

Before performing any of the following procedures, ensure that power is removed from the DC circuit.

Warning **Statement 1015**—Battery Handling

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

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

Warning **Statement 1022—**Disconnect Device

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

Warning **Statement 1025—**Use Copper Conductors Only

To reduce risk of fire, use copper conductors only.

Warning **Statement 1030—**Equipment Installation

Only trained and qualified personnel should be allowed to install, replace, or service this equipment.

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.

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

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

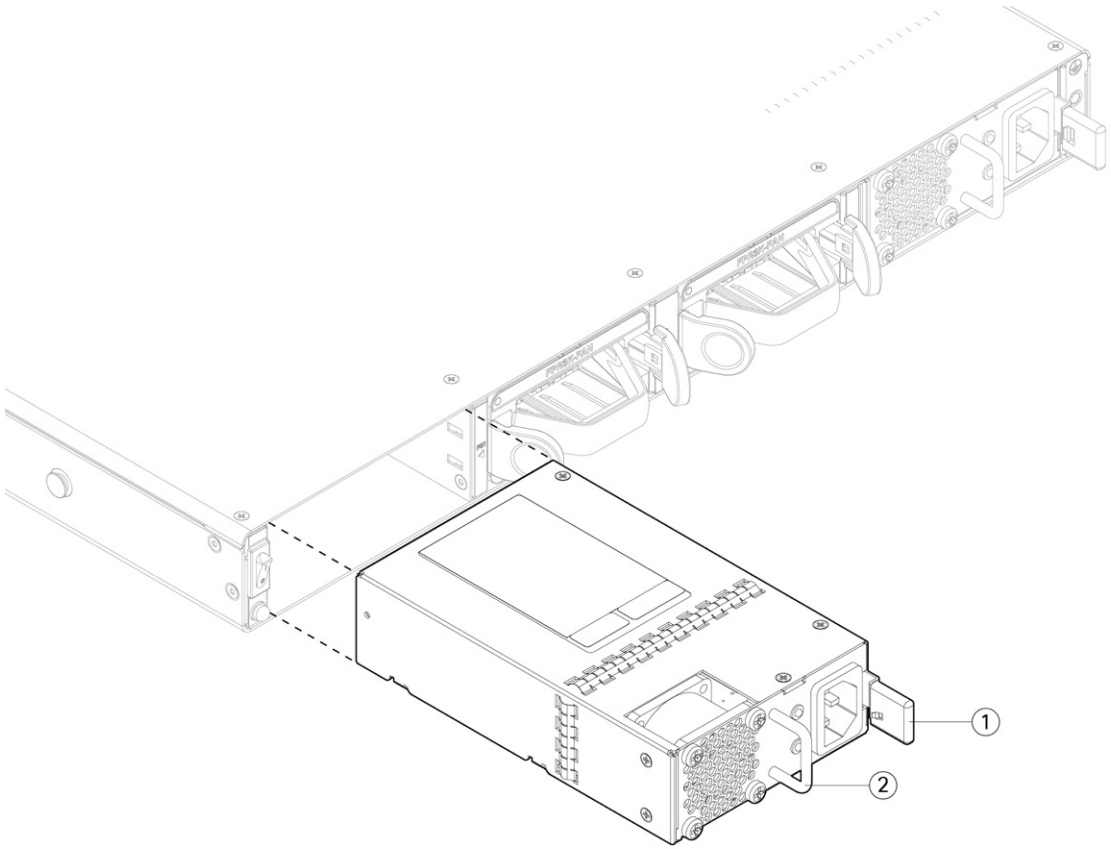
Step 1 Unplug the power supply cable before removing the power supply module. You cannot disengage the power supply module release tab without first removing the cable.

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

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

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

Figure 49: Remove the Power Supply Module



1	Release tab		Handle

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

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

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

Step 7 Plug in the power supply cable.

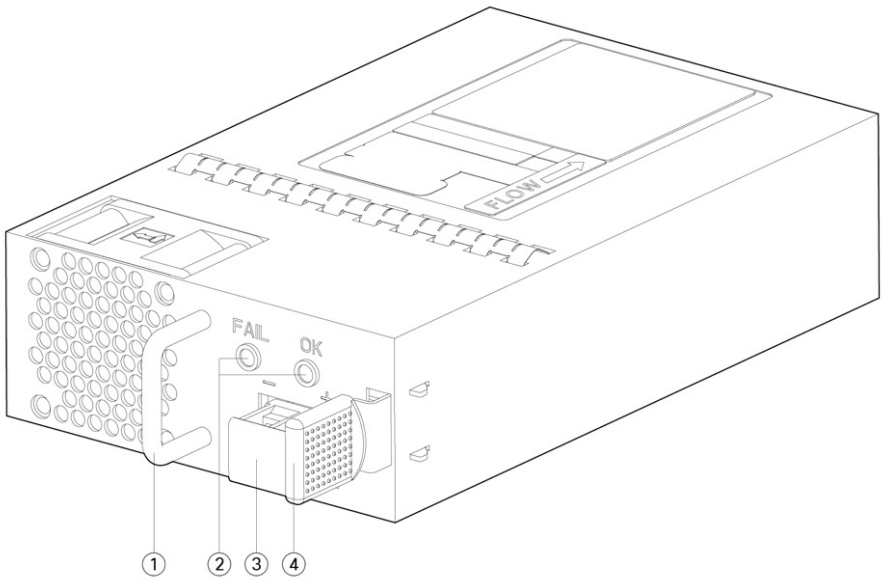
Step 8 Check the LED on the power supply to make sure the power supply is operative. See Power Supply Module, on page 23 for a description of the LEDs.

Connect the DC Power Supply Module

The input connector and plug must be UL recognized under UL 486 for field wiring. The connection polarity is from left to right: negative (–), positive (+), and ground.

Use the handle on the power supply installation and removal. You must support the module with one hand because of its length.

Figure 50: DC Power Supply Module



1	Handle	**2**	FAIL and OK LEDs
3	DC power connector	**4**	Ejector latch

Safety Warnings

Take note of the following warnings:

Warning **Statement 1030—**Equipment Installation

Only trained and qualified personnel should be allowed to install, replace, or service this equipment.

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

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

Before you begin

- The color coding of the DC input power supply leads depends on the color coding of the DC power source at your site. Make sure that the lead color coding you choose for the DC input power supply matches the lead color coding used at the DC power source and verify that the power source is connected to the negative (–) terminal and to the positive (+) terminal on the power supply.
- Make sure that the chassis ground is connected on the chassis before you begin installing the DC power supply. See Ground the Chassis, on page 61 for the procedure.

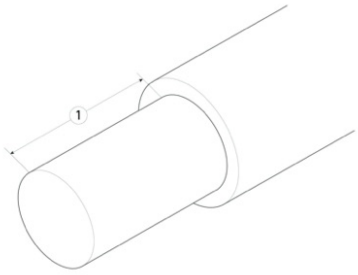
Step 1 Verify that the power is off to the DC circuit on the power supply module that you are installing.

Step 2 While supporting the power supply module with one hand, insert the power supply module into the power supply bay and gently push it in. See the illustration above for the location of the handle.

Step 3 Use a wire-stripping tool to strip each of the two wires coming from the DC input power source. Strip the wires to approximately 0.39 inch (10 mm) + 0.02 inch (0.5 mm). We recommend you use 14 AWG insulated wire.

Note Do not strip more than the recommended length of wire because doing so could leave the wire exposed from the terminal block.

Figure 51: Stripped DC Input Source Wire



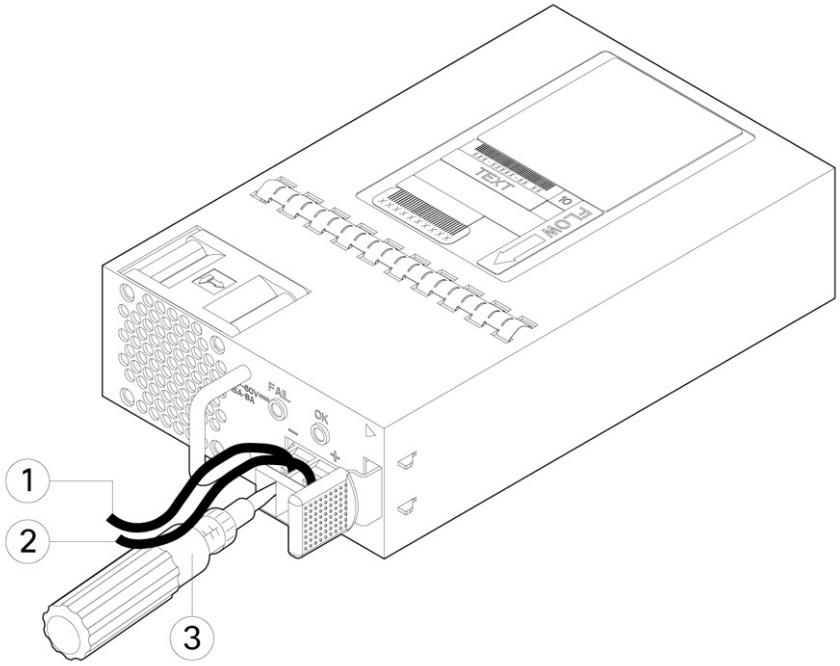
1	Strip the wires to approximately 0.39 inch (10 mm) + 0.02 inch (0.5 mm)		—

Step 4 Insert the exposed wire into the terminal block. Ensure that you cannot see any wire lead outside the plastic cover. Only wires with insulation should extend from the terminal block.

Step 5 Use a screwdriver to tighten the terminal block captive screws.

Caution Do not over torque the terminal block captive screws. Make sure that the connection is snug, but the wire is not crushed. Verify by tugging lightly on each wire to make sure that they do not move.

Figure 52: Tighten the Terminal Block Captive Screws



1	Negative (-) lead wire	**2**	Positive (+) lead wire
3	Screwdriver		—

Step 6 Repeat these steps for the remaining DC input power source wire as applicable.

Step 7 Use a tie wrap so secure the wires to the rack, so that the wires are not pulled from the terminal block.

Step 8 Set the DC disconnect switch in the circuit to ON. In a system with multiple power supplies, connect each power supply to a separate DC power source. In the event of a power source failure, if the second source is still available, it can maintain system operation.

Step 9 Verify power supply operation by checking the power supply LED on the front of the chassis. See Front Panel LEDs, on page 11 for the LED values.

Secure the Power Cord on the Power Supply Module

To secure the power supply module against accidental removal and thus prevent disrupting system performance, use the tie wrap and clamp provided in the accessories kit that ships with your Secure Firewall 3100 series.

Safety Warnings

Take note of the following warnings:

Warning **Statement 1030—**Equipment Installation

Only trained and qualified personnel should be allowed to install, replace, or service this equipment.

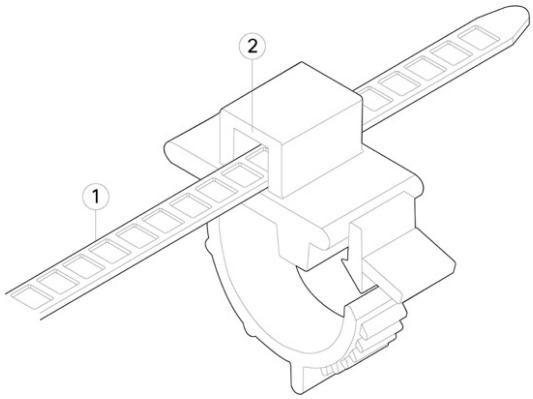
Warning **Statement 1073—**No User-Serviceable Parts

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

Step 1 Attach the clamp to the tie wrap by holding the clamp with the loop side on the bottom and sliding the tie wrap through the box-shaped channel above the clamp (see the following figure).

One side of the tie wrap has evenly spaced ridges and the other is smooth. Be sure the ridged side is face up and that you slide it through the open side of the channel. You hear a click as the tie slides through—it moves in one direction only. To remove the tie wrap from the clamp, push the lever on the closed side of the box-shaped channel and slide out the tie wrap.

Figure 53: Tie Wrap Through the Box Channel of the Clamp



1	Tie wrap	**2**	Box channel

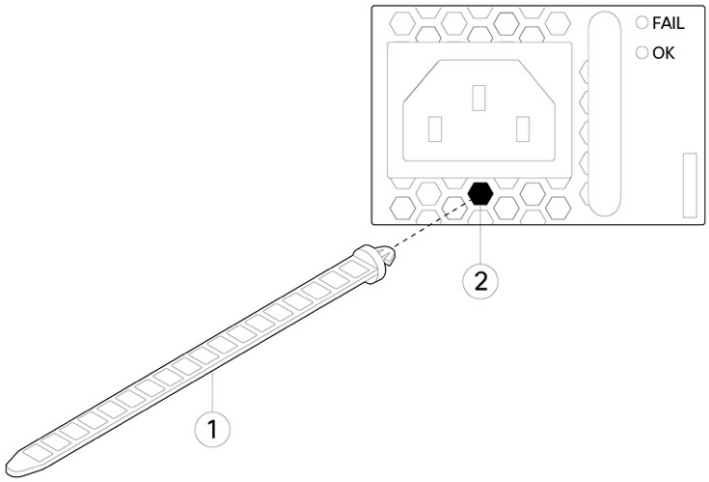
Step 2 Attach the clamp to the power supply module:

a) Locate the hexagonal ventilation hole on the power supply module at the center of the plug just below the power connector body (see the following figures).

b) Plug the snapping portion of the tie wrap into the hexagonal hole.
c) With the clamp side facing up, push the tie wrap in until it is fully engaged.

Caution Make sure you have the correct location because you cannot remove the tie wrap from the power supply module once you have installed it without damaging the tie wrap.

Figure 54: Connect the Tie Wrap

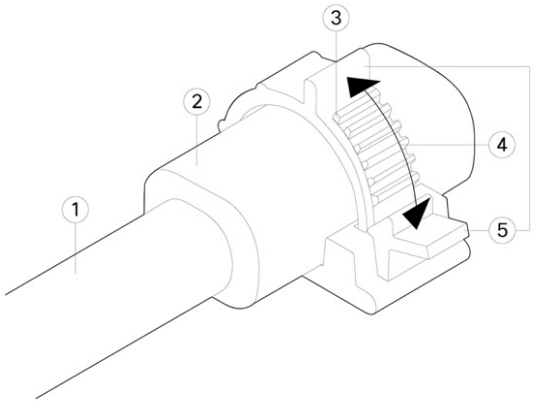


1	Tie wrap	**2**	Hexagonal hole

Step 3 Secure the clamp:

a) Plug in the power cord into the power supply module and wrap the clamp around the over mold portion of the power cord.
b) Squeeze the clamp ends together so that the annular teeth engage with the mate on the clamp.
c) Make sure the clamp fits snugly into the over mold.
d) Adjust the clamp position on the tie wrap so that the clamp is tight against the front of the over mold and the power cord cannot be removed by lightly pulling on it.

Figure 55: Clamp on Over Mold of Power Cord



1	Power cord	**2**	Power cord over mold Clamp release tab
3	Tie clamp annular teeth	**4**	Direction to squeeze the clamp ties
5	Clamp release tabs		—

Step 4 If you need to remove the power cord, push the release tab on the clamp to force the annular clamp teeth to disengage and the clamp opens up. You can then remove the clamp from the power cord.