

Cisco Secure Firewall 3100 Series Hardware Installation Guide

First Published: 2024-10-24

Last Modified: 2026-08-12

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

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

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

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

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

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

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

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

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

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

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

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

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2022-2026 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1 **Overview** 1

- Features 1
- Package contents 4
- Serial number and digital documentation portal QR code 6
- Front panel 8
- Front panel LEDs 9
- Management, console, USB, and network ports 11
- Power switch and reset button 12
- Rear panel 13
- Network modules 15
  - 8-Port 1/10/25-Gbps network module 15
  - 4-Port 40-Gbps network module 17
  - 2-Port 100-Gbps network module 18
- Hardware bypass network modules 20
  - 8-Port 10/100/1000Base-T network module 21
  - 6-Port 1-Gbps SX, 10-Gbps SR/10-Gbps LR/25-Gbps SR/25-Gbps LR network module 22
- Power supply modules 24
- Dual fan modules 26
- SSDs 27
- Supported transceivers 28
- Hardware Specifications 38
- Product ID numbers 39
- Power cord specifications 42

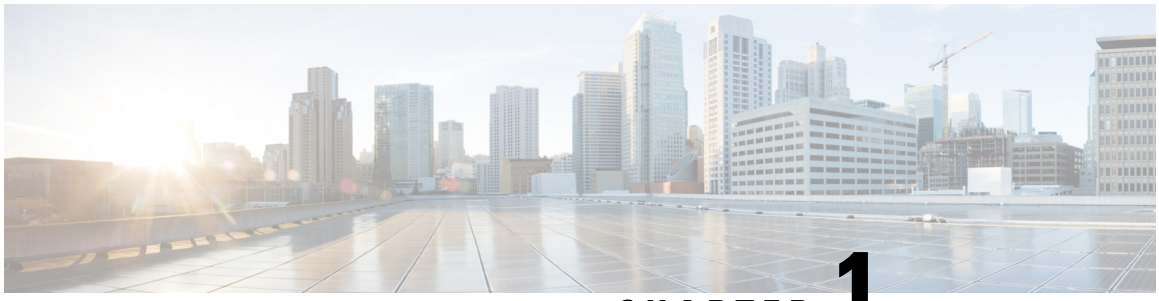
CHAPTER 2 **Installation Preparation** 49

- Installation warnings 49

Network Equipment-Building System (NEBS) statements 51
Safety recommendations 53
Maintain safety with electricity 53
Prevent ESD damage 54
Site environment 54
Site considerations 54
Power supply considerations 55
Rack configuration considerations 55

CHAPTER 3 **Rack-Mount the Chassis 57**
Unpack and inspect the chassis 57
Rack mount the chassis using brackets 58
Rack mount the chassis using slide rails 60
Ground the chassis 67

CHAPTER 4 **Installation, Maintenance, and Upgrade 71**
Install, remove, and replace the network module 71
Remove and replace the SSD 73
Remove and replace the dual fan module 76
Remove and replace the power supply module 77
Connect the DC power supply module 79
Secure the Power Cord on the Power Supply Module 82
Install the FIPS opacity shield 85



CHAPTER 1

Overview

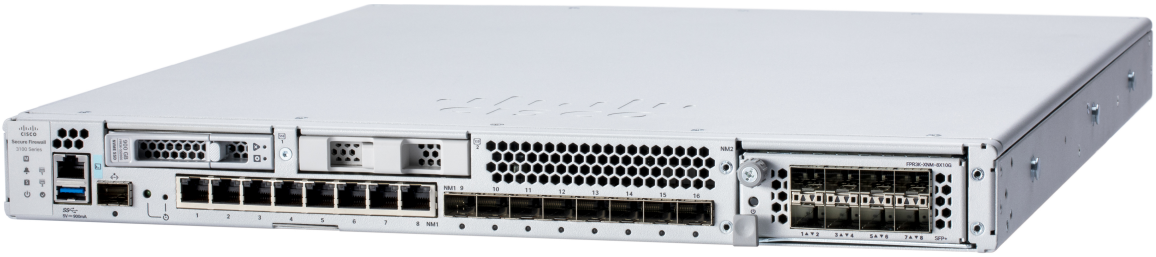
- Features, on page 1
- Package contents, on page 4
- Serial number and digital documentation portal QR code, on page 6
- Front panel, on page 8
- Front panel LEDs, on page 9
- Management, console, USB, and network ports, on page 11
- Power switch and reset button, on page 12
- Rear panel, on page 13
- Network modules, on page 15
- Hardware bypass network modules, on page 20
- Power supply modules, on page 24
- Dual fan modules, on page 26
- SSDs, on page 27
- Supported transceivers, on page 28
- Hardware Specifications, on page 38
- Product ID numbers, on page 39
- Power cord specifications, on page 42

Features

The Cisco Secure Firewall 3100 is a standalone modular security services platform that includes the Secure Firewall 3105, 3110, 3120, 3130, and 3140. The Secure Firewall 3100 supports Cisco Secure Firewall Threat Defense and Cisco Secure ASA software.

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	3105	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				
System memory	64 GB		128 GB	128 GB	256 GB
Management port	One 1/10-Gbps 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 RJ-45 ports and 8 SFP+ fixed ports				
Network module ports	• Eight 1/10/25-Gbps SFP ports • Four 40-Gbps QSFP ports • Two 100-Gbps QSFP ports • Eight 10/100/1000BaseT ports (hardware bypass) • Six 1/10/25-Gbps SFP ports (hardware bypass)				

Feature	3105	3110	3120	3130	3140
Network module slots	One **Note** Hot-swapping of identical modules is supported, but if you replace a network module with another type, you must reboot the system so that the new network module is recognized.				
Network modules	• 8-port 1-Gbps/10-Gbps SFP+ (FPR3K-XNM-8X10G) • 6-port 1-Gbps SFP SX multimode hardware bypass (FPR3K-XNM-6X1SXF) • 6-port 10-Gbps SFP SR multimode hardware bypass (FPR3K-XNM-6X10SRF) • 6-port 10-Gbps SFP LR single mode hardware bypass (FPR3K-XNM-6X10LRF) • 8-port 10/100/1000Base-T hardware bypass (FPR3K-XNM-8X1GF)			• 8-port 1-Gbps/10-Gbps/25-Gbps SFP+ (FPR3K-XNM-8X25G) • 8-port 1-Gbps/10-Gbps SFP+ (FPR3K-XNM-8X10G) • 4-port 40-Gbps QSFP+ (FPR3K-XNM-4X40G) • 6-port 1-Gbps SFP SX multimode hardware bypass(FPR3K-XNM-6X1SXF) • 6-port 10-Gbps SFP SR multimode hardware bypass (FPR3K-XNM-6X10SRF) • 6-port 10-Gbps SFP LR single mode hardware bypass (FPR3K-XNM-6X10LRF) • 6-port 25-Gbps SFP SR multimode hardware bypass (FPR3K-XNM-6X25SRF) • 6-port 25-Gbps SFP LR single mode hardware bypass (FPR3K-XNM-6X25LRF) • 8-port 10/100/1000Base-T hardware bypass (FPR3K-XNM-8X1GF) • 2-port 100-Gbps QSFP+ (FPR3K-XNM-2X1000G)	
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				

Feature	3105	3110	3120	3130	3140
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				
Reset button	Resets the system to factory default without requiring serial console access				

Related Topics

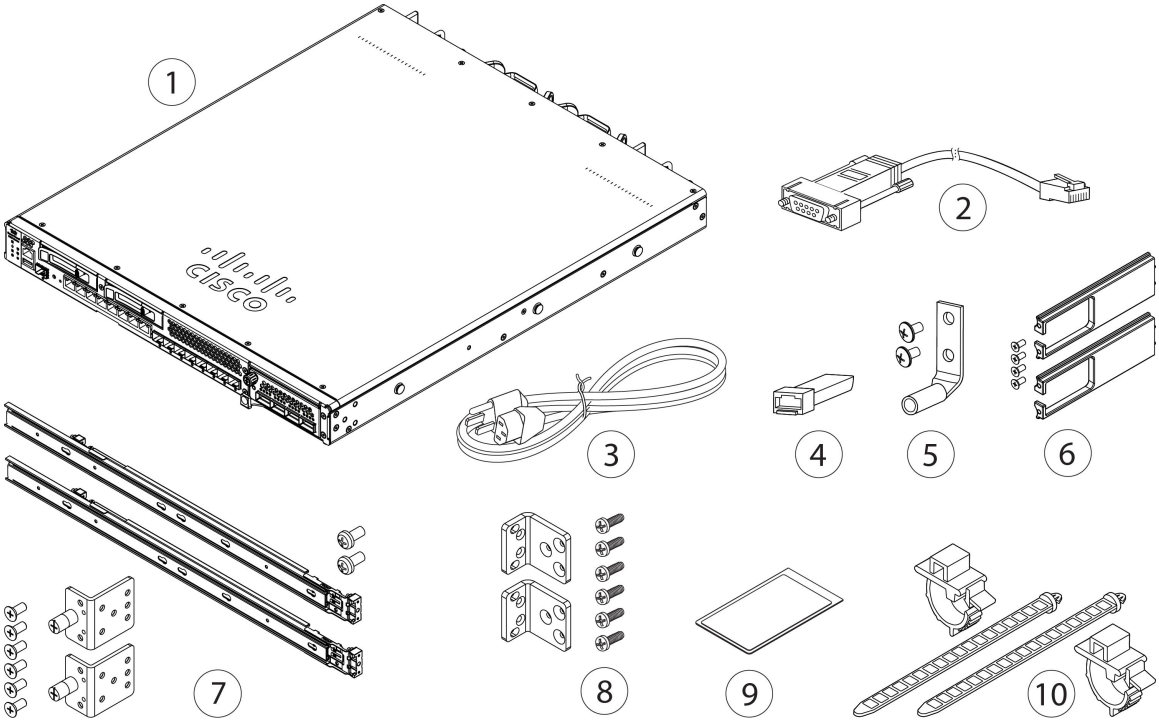
Product ID numbers, on page 39
Supported transceivers, on page 28
Power switch and reset button, on page 12
Management, console, USB, and network ports, on page 11
Cisco Secure Firewall Threat Defense Compatibility Guide
Cisco Secure Firewall ASA Compatibility

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.

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 Optional; in package if ordered
3	One or two country-specific power cords Optional; in package if ordered	**4**	SFP transceiver (Optional; in package if ordered)
5	One ground lug kit • One #6 AWG, 90 degree, #10 post ground lug • Two 10-32 x 0.38-inch Phillips screws	**6**	Cable management bracket kit • Two cable management brackets • Four 8-32 x 0.375-inch Phillips screws (Optional; in package if ordered)

7	Two slide rails Slide rail accessories kit: • Two slide rail locking brackets • Six 8-32 x 0.302-inch slide rail locking bracket Phillips screws • Two M3 x 0.5 x 6-mm Phillips screws (Optional; in package if ordered)	**8**	Rack-mount bracket kit: • Two rack-mount brackets • Six 8-32 x 0.375-inch Phillips screws for securing the brackets to the chassis (Optional; in package if ordered)
9	*Cisco Secure Firewall 3100* This document has links to the hardware installation guide, regulatory and safety information guide, and warranty and licensing information. It also contains a QR code and URL that point to the Digital Documentation Portal. The portal contains links to the product information page, the hardware installation guide, the regulatory and safety information guide, the getting started guide, and the zero-touch provisioning guide.	**10**	Two power supply module tie wraps and clamps

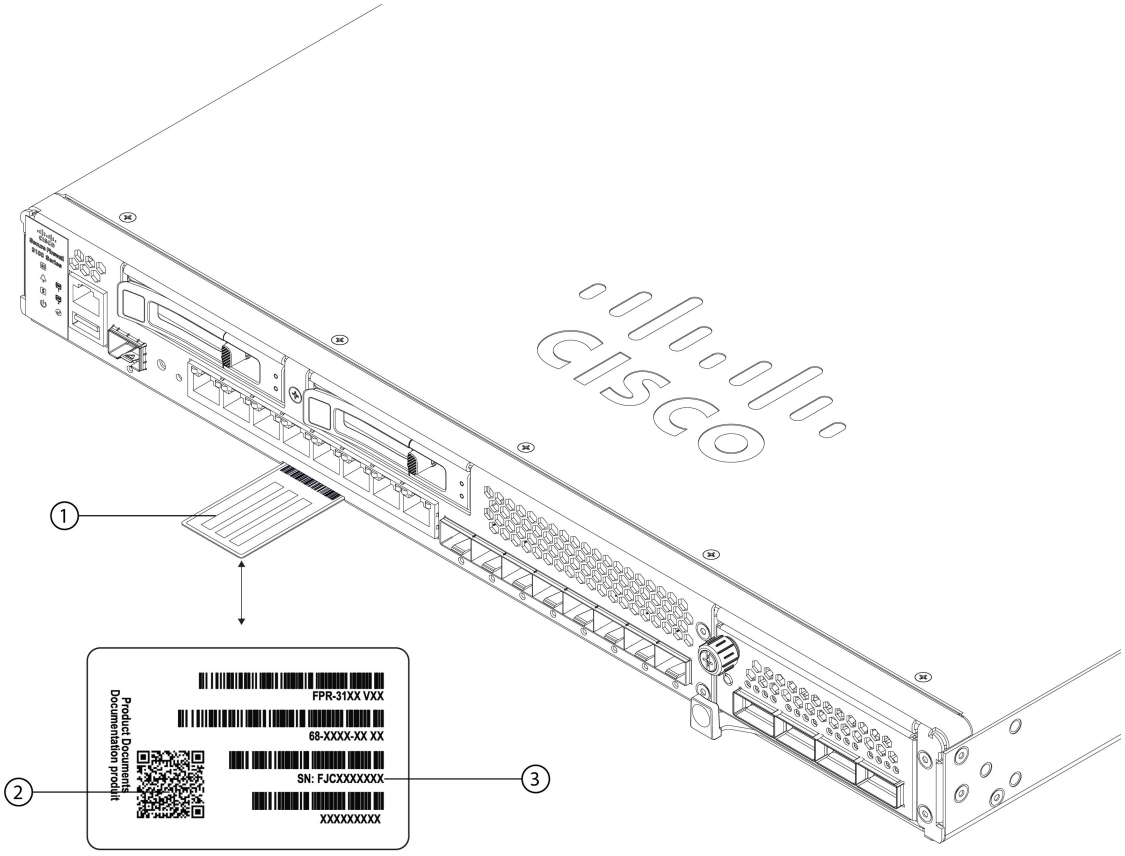
Related Topics

Product ID Numbers, on page 39
Power cord specifications, on page 42

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 zero-touch deployment guide, and the hardware installation guide.

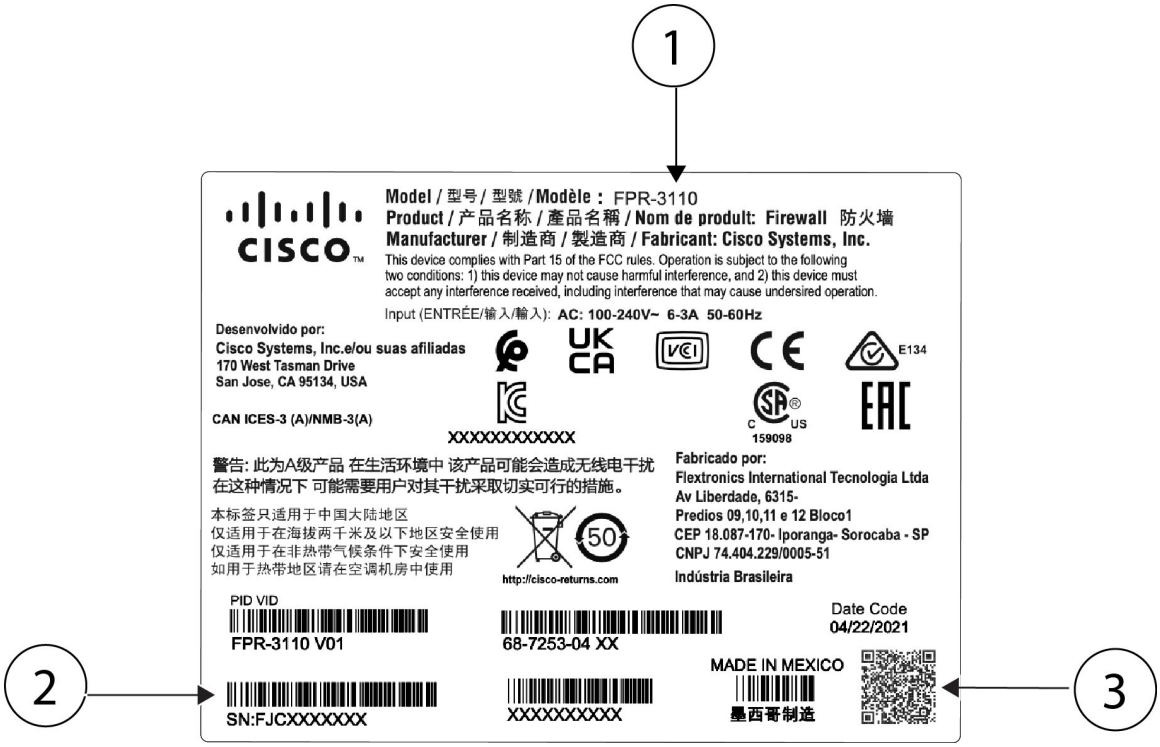
Figure 3: Pullout asset card



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

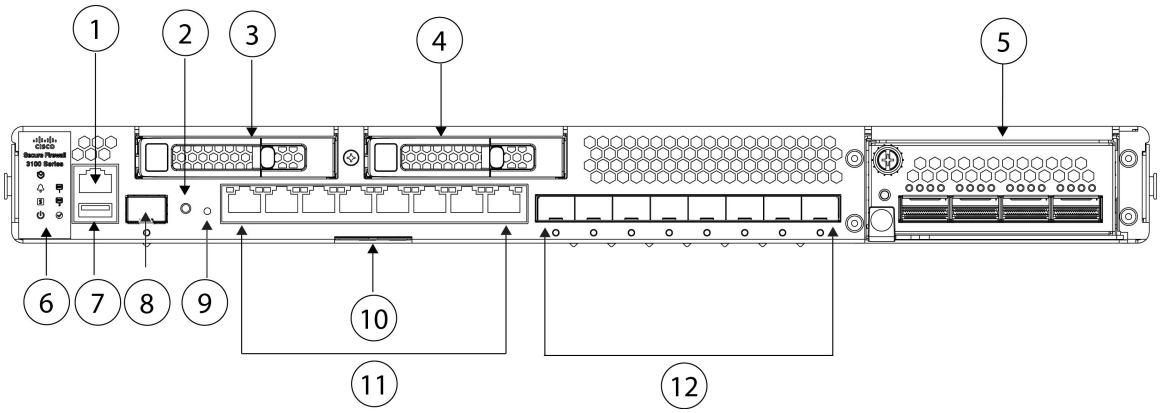


1	Chassis model number	**2**	Chassis serial number
3	Documentation Portal QR code		—

Front panel

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

Figure 5: Secure Firewall 3100 front panel



1	RJ-45 console port	**2**	Recessed factory reset button

3	SSD-1	**4**	SSD-2
5	Network module (NM-2)	**6**	System LEDs
7	Type A USB 3.1 port	**8**	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
9	Reset button LED	**10**	Pullout asset card with chassis serial number, getting started guide QR code, and LTP QR code
11	Eight fixed RJ-45 ports (NM-1) RJ-45 ports named Ethernet 1/1 through 1/8 left to right	**12**	Eight fixed SFP+ ports (NM-1) SFP+ ports named Ethernet 1/9 through 1/16 left to right

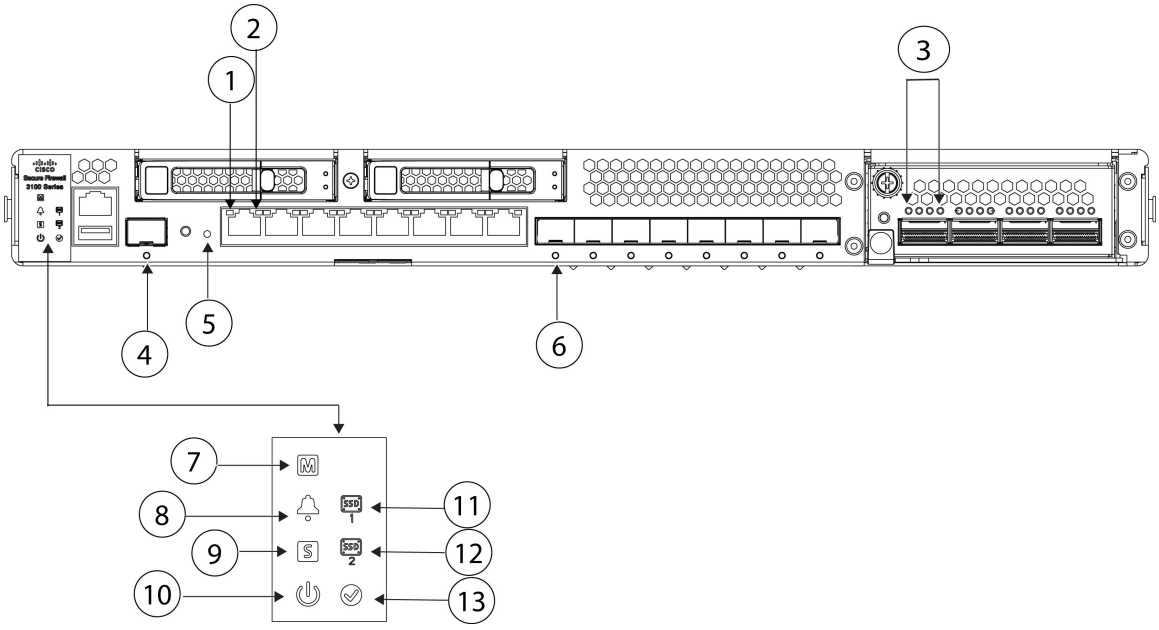
Related Topics

Front panel LEDs, on page 9
Supported transceivers, on page 28

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** • Off—No link. • Green—Link is up.	2	**RJ-45 Copper Port Activity** • Off—No activity • Green, flashing—The number of flashes determines the link speed; 1 flash=10 Mbps, 2=100 Mbps, 3=1 Gbps.
3	**Network Module 2 Port** • 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.	4	**Management Port** The 1/10-Gbps 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.
5	**Factory Reset Button** • Green, flashing—Flashes 5 seconds after you depress the button. • Off—Reset is complete.	6	**Fiber Port Link/Activity** 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.
7	**Managed** • Green, flashing slowly (twice in 5 seconds)—Cloud is connected. • Green and amber, flashing—Cloud connection failure. • Green—Cloud is disconnected.	8	**Alarm** • Off—No alarms. • Amber—Environmental error. • Green—Status is ok.

9	**System** • 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.	**10**	**Power** • 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.
11	**SSD 1** • 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**	**SSD 2** • 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.
13	**Activity** (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.		—

Management, console, USB, and network ports

Management port

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

Console port

The 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.

USB Type A port

The chassis contains a standard USB 3.1 Type A port for an external USB drive that you can use for the startup image, configuration, backup and other standard uses for flash storage.

- Supports EXT2/3/4 or VFAT/FAT32 format
- Identified as the following drive ID depending on the CLI:
  - FxOS local-mgmt—usbdrive:
  - FxOS—usbA:
  - ASA and Firewall Threat Defense—disk1:
  - ROMMON—usb:
- Output power of 5 volts, up to a maximum of 1 A (5 USB power units)

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

Network ports

The chassis has 8 RJ-45 ports and 8 SFP+ fixed ports that are named Ethernet 1/1 through 1/16. Each port includes a pair of LEDs, one each for connection status and link status. The chassis has a network module slot that supports the following ports:

- Eight 1/10/25-Gbps SFP ports
- Four 40-Gbps QSFP ports
- Two 100-Gbps QSFP ports
- Eight 10/100/1000BaseT ports (hardware bypass)
- Six 1/10/25-Gbps SFP ports (hardware bypass)

Related Topics

Supported transceivers, on page 28
Features, on page 1

Power switch and reset button

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.

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.

Reset button

The 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.

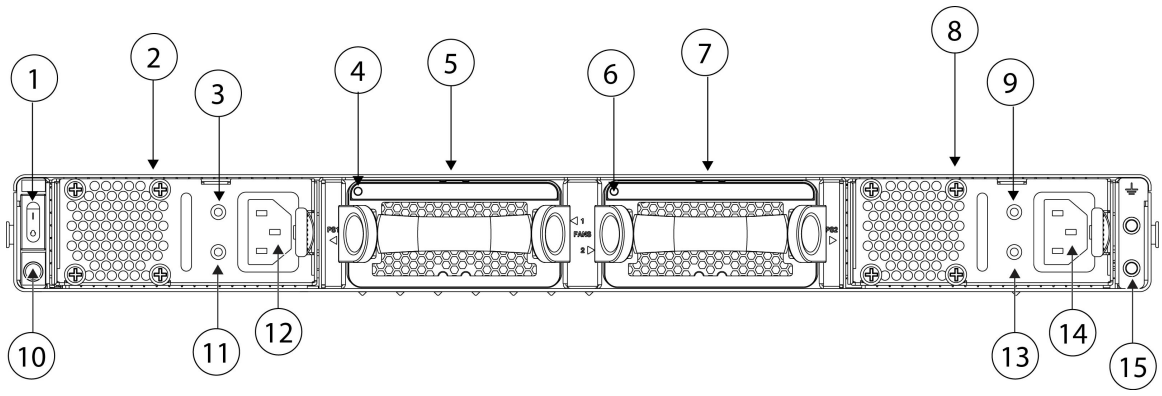
Related Topics

Front panel LEDs, on page 9

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 supply module (PSU-1)
3	Power supply module FAIL LED (PSU-1)	**4**	Fan module LED (FAN-1)
5	Fan module (FAN-1)	**6**	Fan module LED (FAN-2)
7	Fan module (FAN-2)	**8**	Power supply module (PSU-2)
9	Power supply module FAIL LED (PSU-2)	**10**	Chassis power LED **Note** This power LED has the same behavior as the front panel LED.
11	Power supply module OK LED (PSU-1)	**12**	Power supply module connector (PSU-1)
13	Power supply module OK LED (PSU-2)	**14**	Power supply module connector (PSU-2)
15	Two-post grounding pad **Note** The two-post grounding lug and two screws are included in the accessory kit.		—

Related Topics

Front panel LEDs, on page 9
Remove and replace the power supply module, on page 77
Remove and replace the dual fan module, on page 76
Ground the chassis, on page 67
Power supply modules, on page 24
Dual fan modules, on page 26

Network modules

The Secure Firewall 3100 chassis has one network module slot named NM-2. 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.

Make sure you have the correct firmware package and software version installed to support the network modules. See the configuration guide for your software for the procedures for updating the firmware package and verifying the software version.

Related Topics

Front panel, on page 8
Cisco Secure Firewall Threat Defense Compatibility Guide
Cisco Secure Firewall ASA Compatibility

8-Port 1/10/25-Gbps network module

FPR3K-XNM-8X10G supports 1 Gbps and 10 Gbps full-duplex Ethernet traffic per port and is supported on all Secure Firewall 3100s. FPR3K-XNM-8X25G supports 1 Gbps, 10 Gbps, or 25 Gbps full-duplex Ethernet traffic per port and is supported *only* on the 3130 and 3140.

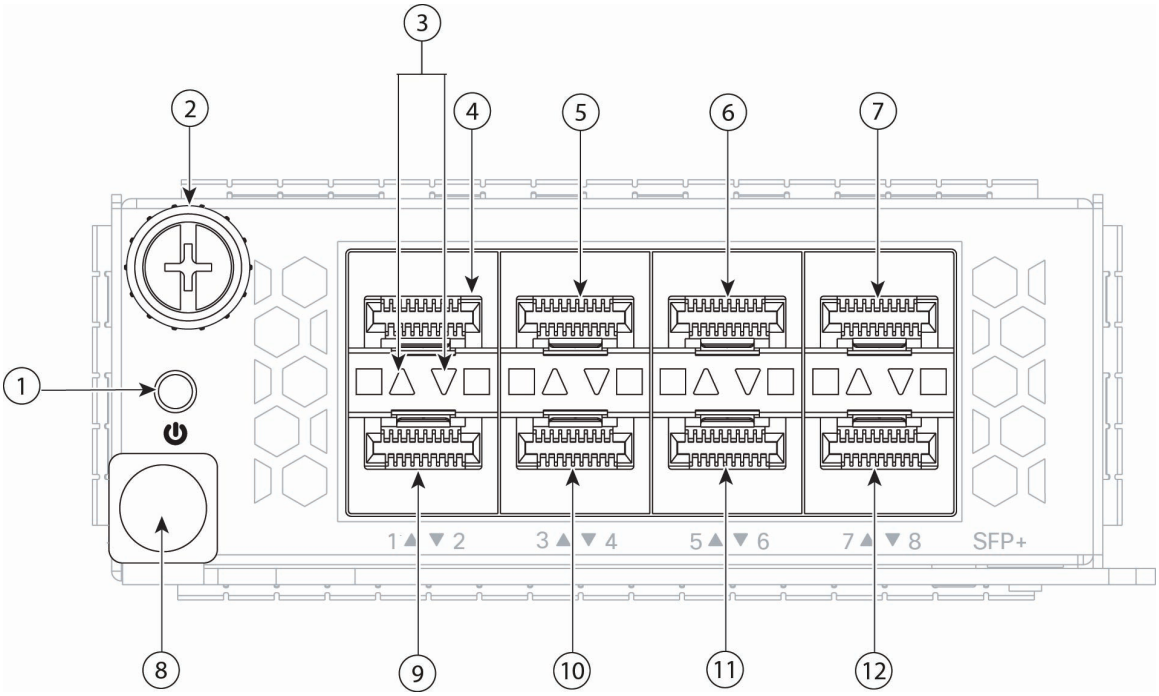
The top ports are numbered from left to right—Ethernet 2/1, Ethernet 2/3, Ethernet 2/5, and Ethernet 2/7. The bottom ports are numbered from left to right—Ethernet 2/2, Ethernet 2/4, Ethernet 2/6, and Ethernet 2/8 (see the figure below). Up arrows are the top ports and down arrows are the bottom ports (see the figure below). This network module supports SFP/SFP+/SFP28 transceivers.

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

Note Although you can install the 8-port 1/10/25-Gbps 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-Gbps and 1/10/25-Gbps network module.

Figure 8: FPR3K-XNM-8X10G and FPR3K-XNM-8X25G



1	Captive screw	**2**	Ethernet 2/1
3	Ethernet 2/3	**4**	Ethernet 2/5
5	Ethernet 2/7	**6**	Power on LED
7	Ejector handle	**8**	Ethernet 2/2
9	Ethernet 2/4	**10**	Ethernet 2/6
11	Ethernet 2/8	**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.

Related Topics

Supported transceivers, on page 28

4-Port 40-Gbps network module

The FPR3K-XNM-4X40G supports 40-Gbps operation and is supported on the 3130 and 3140. This network module provides full-duplex Ethernet traffic per port. The 40-Gbps network module has four QSFP+ ports. The 40-Gbps ports are numbered left to right, Ethernet 2/1 through Ethernet 2/4.

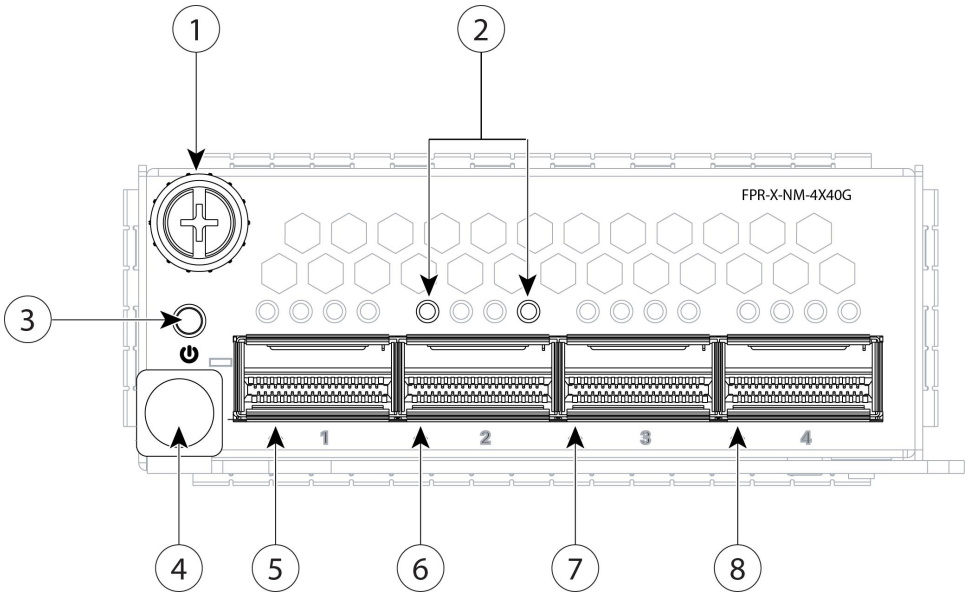
You can break each of the four 40-Gbps ports into four 10-Gbps ports using the supported breakout cables. With the four-port 40-Gbps network module, you now have 16 10-Gbps interfaces. The added interfaces are Ethernet 2/1/1 through Ethernet 2/1/4.

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

Note Although you can install the 4-port 40-Gbps 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 4-port 40-Gbps network module.

Figure 9: FPR3K-XNM-4X40G



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

Related Topics

Supported transceivers, on page 28

2-Port 100-Gbps network module

The FPR3K-XNM-2X100G supports 40/100-Gbps operation and is supported on the 3130 and 3140. This network module has two QSFP/QSFP28 ports and provides full-duplex Ethernet traffic per port. The maximum bandwidth supported is 200 Gbps full duplex, where each port operates at 100 Gbps. The 100-Gbps ports are numbered left to right, Ethernet 2/1 through Ethernet 2/2.

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

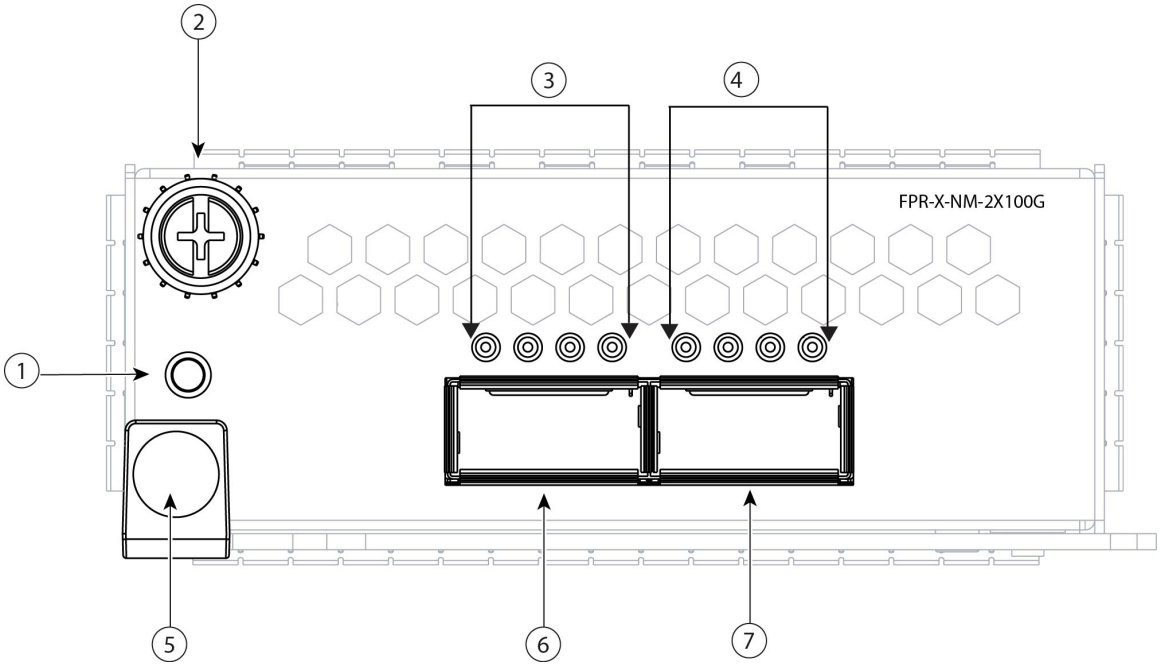
Note The hardware and the system support hot swapping if you are replacing a network module with the same type of network module. If you replace the 100-Gbps network module with another supported network module, you must reboot the chassis so that the new network module is recognized. See the configuration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

Note Although you can install the 2-port 100-Gbps network module 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 2-port 100-Gbps network module.

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

Figure 10: FPR3K-XNM-2X100G



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

Related Topics

Supported transceivers

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 Firepower security appliance 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.

Make sure you have the correct firmware package and software version installed to support the network modules. See the configuration guide for your software for the procedures for updating the firmware package and verifying the software version.



Note When the appliance switches from normal operation to hardware bypass or from hardware bypass back to normal operation, traffic may be interrupted for several seconds. A number of factors can affect the length of the interruption; for example, behavior of the 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 40-Gb network module, you connect the two ports to form a paired set. For the 1/10-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 security appliance 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.

Related Topics

Cisco Secure Firewall Threat Defense Compatibility Guide

Cisco Secure Firewall ASA Compatibility

8-Port 10/100/1000Base-T network module

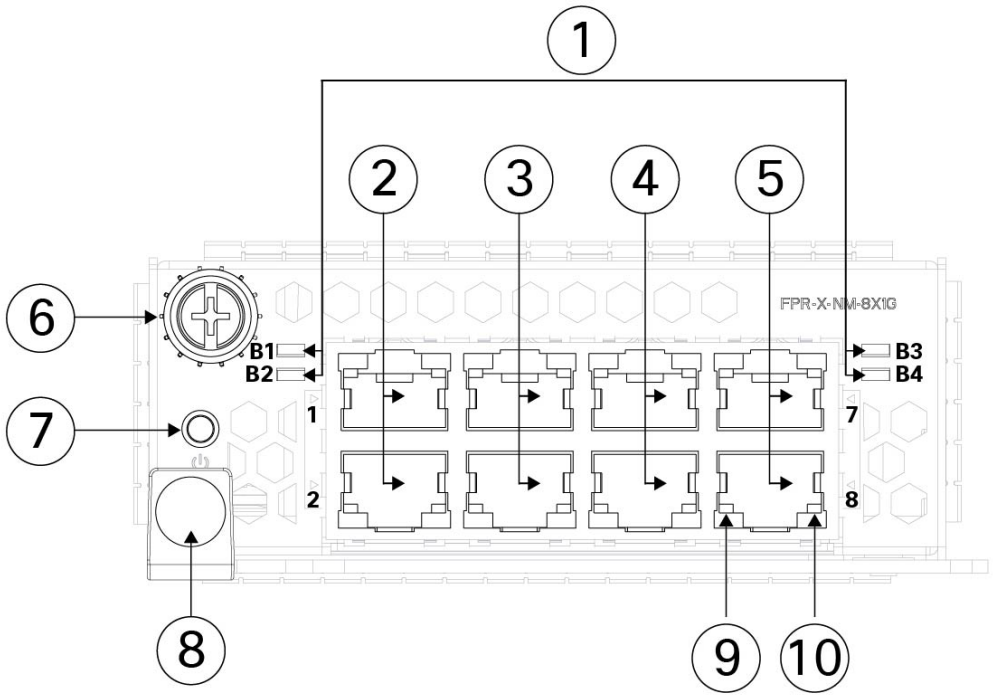
FPR3K-XNM-8X1GF is an 8-port 10/100/1000Base-T hardware bypass network module. The eight ports are numbered from top to bottom, left to right. Ports 1 and 2, 3 and 4, 5 and 6, and 7 and 8 are paired for hardware bypass mode. In hardware bypass mode, data is not processed by the Secure Firewall 3100 but is routed to the paired port.

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

The following figure shows the front panel of the 8-port 10/100/1000Base-Tnetwork module.

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

Figure 11: FPR3K-XNM-8X1GF



1	Bypass LEDs B1 through B4 • Green—In standby mode. • Amber, flashing—Port is in hardware bypass mode, failure event.	**2**	Ethernet 2/1 and Ethernet 2/2 Ports 1 and 2 are paired together to form a hardware bypass pair. LED B1 applies to this paired port.

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

Related Topics

Supported transceivers, on page 28
Hardware bypass network modules, on page 20

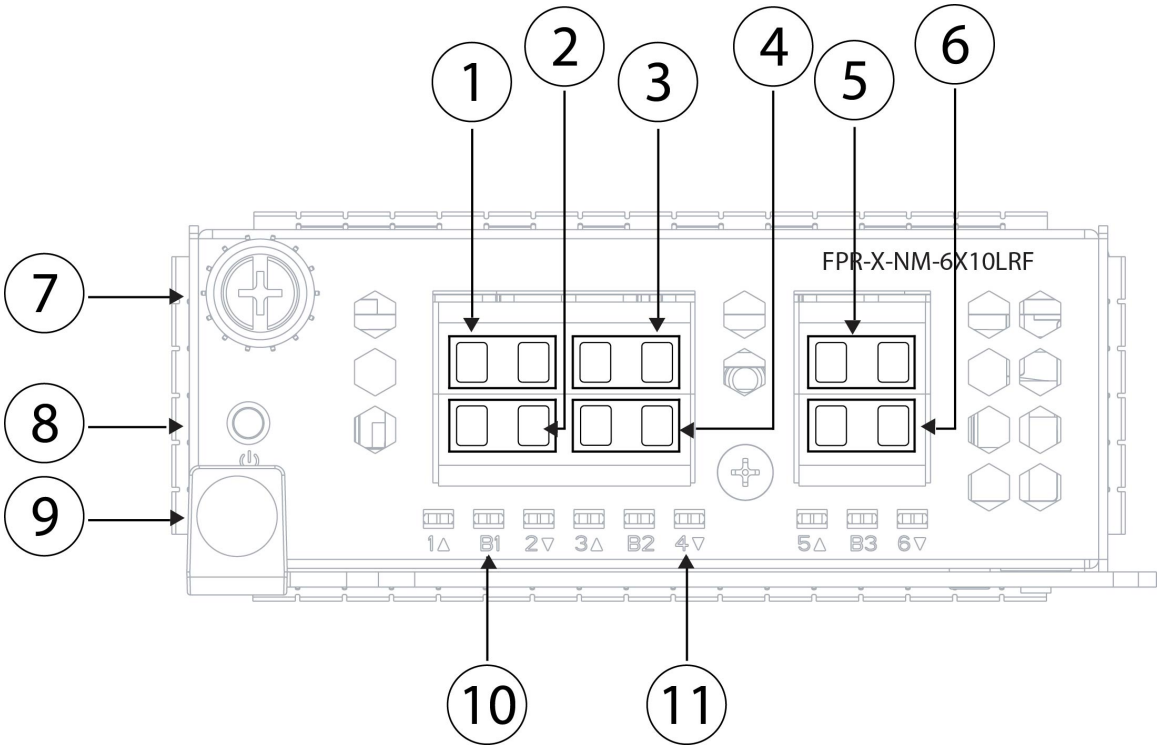
6-Port 1-Gbps SX, 10-Gbps SR/10-Gbps LR/25-Gbps SR/25-Gbps LR network module

The FPR3K-XNM-6X1SXF, FPR3K-XNM-6X10SRF, FPR3K-XNM-6X10LRF, FPR3K-XNM-6X25SRF, and FPR3K-XNM-6X25LRF hardware bypass network modules have six ports that are numbered from top to bottom, left to right. Pair ports 1 and 2, 3 and 4, and 5 and 6 to form hardware bypass paired sets. In hardware bypass mode, data is not processed by the Secure Firewall 3100 but is routed to the paired port. This network module has built-in SFP transceivers. Hot swapping and field replacement of transceivers are not supported.

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

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

Figure 12: FPR3K-XNM-6X1SXF, FPR3K-XNM-6X10SRF, FPR3K-XNM-6X10LRF, FPR3K-XNM-6X25SRF, and FPR3K-XNM-6X25LRF



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

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

Related Topics

Supported transceivers, on page 28
Hardware bypass network modules, on page 20

Power supply modules

The Secure Firewall 3100 supports two AC power supply modules so that dual power supply redundancy protection is available. The 3105, 3110, and 3120 ship with one AC power supply (you can order two) and the 3130 and 3140 ship with two AC power supplies. You can also install DC power supply modules instead of AC power. Facing the back of the chassis, the power supply modules are numbered left to right—PSU1 and PSU2. The power supply module is hot-swappable.

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.

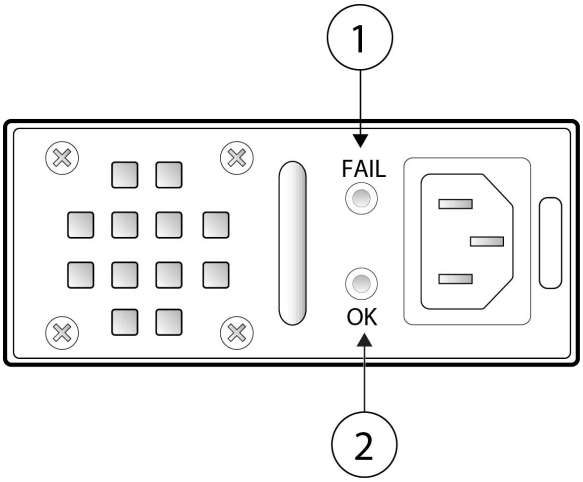
Table 3: DC power supply module hardware specifications

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 13: 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.

Related Topics

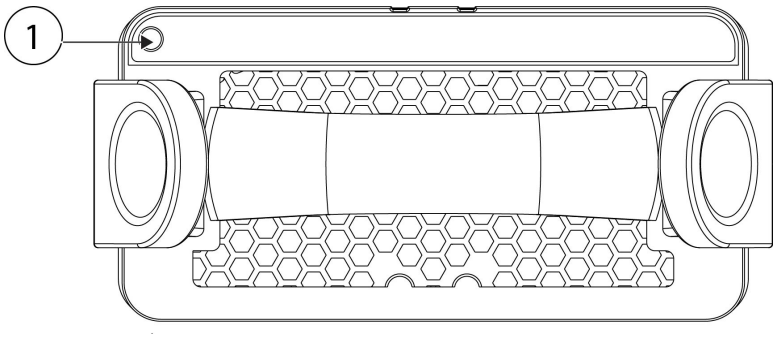
Product ID numbers, on page 39
Remove and replace the power supply module, on page 77

Dual fan modules

The Secure Firewall 3100 has two fan modules that provide 3 + 1 redundancy. Each fan module has two fans and each fan has two independent fan rotors. The fan rotors are monitored individually, and this gives 8 fan rotors per system. When one fan rotor fails, all others 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 14: 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.

Related Topics

Product ID numbers, on page 39
Remove and replace the dual fan module, on page 76

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.

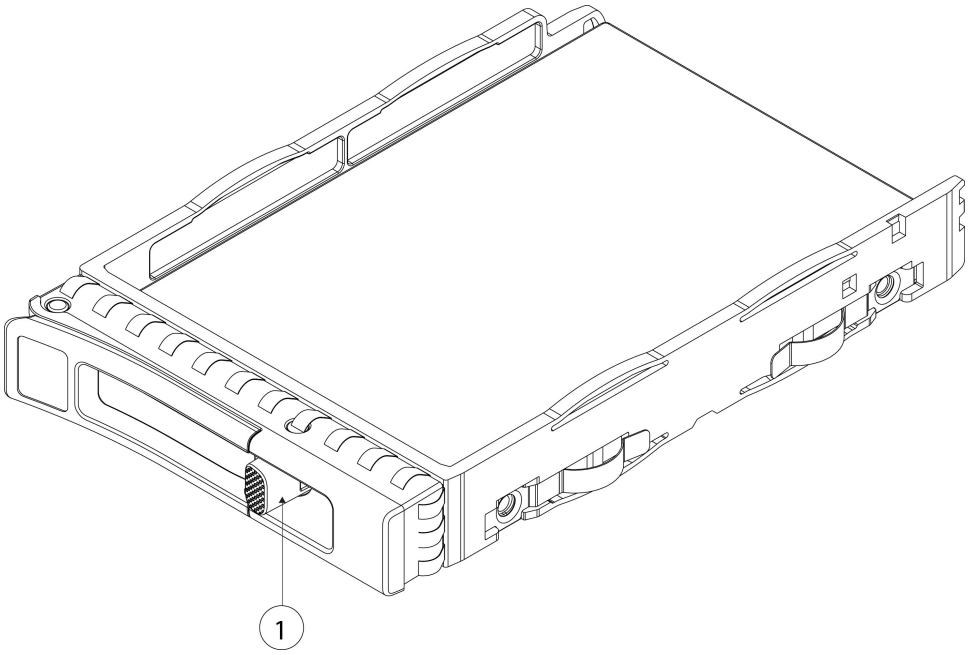
Hot swapping is supported. With two SSDs, you can swap SSD-1 without powering off the chassis. However, you must issue the **raid remove-secure local disk** command to remove SSD-2 from the RAID configuration before hot swapping. Otherwise, you can lose data. If you remove and replace the RAID1 SSD,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

See the configuration guide for your software for the procedures for removing and adding an SSD from the RAID1 configuration.

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. If you are swapping SSDs between two Secure Firewall 3100s, use the **remove-secure local disk** command, otherwise sometimes the SED (self-encrypting drive) gets locked. If you get an error message that the SED is locked, you can enter the PSID and the system clears the SED and creates a new set of keys. To avoid this situation, especially if you do not know what the PSIDs are, always use the **remove-secure local disk** when removing SSDs.

Figure 15: SSD



1	SSD release tab		—

Related Topics

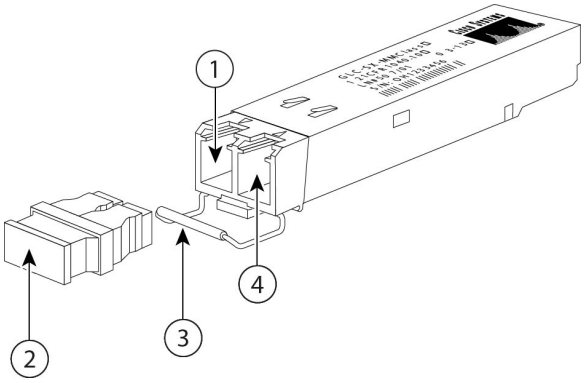
Product ID numbers, on page 39
Front panel LEDs, on page 9
Remove and replace the SSD, on page 73
Cisco Secure Firewall Management Center Device Configuration Guide, 7.4

Supported 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.

Note When using fiber-based optics, make sure that the same SFP type is used on both sides of the cable because speed is not negotiated when using SFP transceivers. This is true for both copper SFPs (the exception being that the GLC-T RJ45-based copper SFPs can negotiate speed) and fiber SFPs. If a port is configured for sfp-detect, then the software configures the port's speed to match the speed capability of the SFP. For dual-rate SFPs, when sfp-detect is configured, the port is always configured for the highest supported speed of the port. For example, a port that has a 10/25-Gbps SFP installed is configured to operate at 25 Gbps when sfp-detect is configured.

Figure 16: 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 transceivers that are supported on the Secure Firewall 3105 fixed ports.

Table 4: FPR3105 fixed ports

Port type	Transceiver PID	First supported release
Fixed SFP/SFP+ ports	• GLC-TE • GLC-SX-MMD • GLC-LH-SMD • GLC-EX-SMD • GLC-ZX-SMD • GLC-GE-100FX • SFP-10G-SR • SFP-10G-SR-S • SFP-10G-LR • SFP-10G-LR-S • SFP-10G-ER • SFP-10G-ER-S • SFP-H10GB-CUxM • SFP-H10GB-ACUxM • SFP-10G-AOCxM	Firewall Threat Defense 7.3/ASA 9.20

The following table lists the transceivers that are supported on the Secure Firewall 3105 management ports.

Table 5: FPR3105 management ports

Port type	Transceiver PID	First supported release
Management SFP/SFP+ ports	• GLC-TE • GLC-SX-MMD • GLC-LH-SMD • GLC-EX-SMD • GLC-ZX-SMD • GLC-GE-100FX • SFP-10G-SR • SFP-10G-SR-S • SFP-10G-LR • SFP-10G-LR-S • SFP-10G-ER • SFP-10G-ER-S • SFP-H10GB-CUxM • SFP-H10GB-ACUxM • SFP-10G-AOCxM	Firewall Threat Defense 7.3/ASA 9.20

The following table lists the transceivers supported on the Secure Firewall 3110, 3120, 3130, and 3140 fixed ports.

Table 6: FPR3110, FPR3120, FPR3130, and FPR3140 fixed ports

Port type	Transceiver PID	First supported release
Fixed SFP/SFP+ ports	• GLC-TE • GLC-SX-MMD • GLC-LH-SMD • GLC-EX-SMD • GLC-ZX-SMD • GLC-GE-100FX • SFP-10G-SR • SFP-10G-SR-S • SFP-10G-LR • SFP-10G-LR-S • SFP-10G-ER • SFP-10G-ER-S • SFP-H10GB-CUxM • SFP-H10GB-ACUxM • SFP-10G-AOCxM	Firewall Threat Defense 7.1/ASA 9.17

The following table lists transceivers that are supported on the Secure Firewall 3130 and 3140 fixed ports.

Table 7: FPR3130 and FPR3140 fixed ports

Port type	Transceiver PID	First supported release
Fixed SFP28 ports	• SFP-25G-SR-S • SFP-10/25G-CSR-S • SFP-10/25G-LR-S • SFP-H25-CUxM • SFP-25G-A0CxM	Firewall Threat Defense 7.1/ASA 9.17

The following table lists the SFPs that are supported on the Secure Firewall 3110, 3120, 3130, and 3140 management ports.

Table 8: FPR3110, FPR3120, FPR3130, and FPR3140 management ports

Port type	Transceiver PID	First supported release
Management SFP/SFP+ ports	• GLC-TE • GLC-SX-MMD • GLC-LH-SMD • GLC-EX-SMD • GLC-ZX-SMD • GLC-GE-100FX • SFP-10G-SR • SFP-10G-SR-S • SFP-10G-LR • SFP-10G-LR-S • SFP-10G-ER • SFP-10G-ER-S • SFP-H10GB-CUxM • SFP-H10GB-ACUxM • SFP-10G-AOCxM	Firewall Threat Defense 7.1/ASA 9.17

The following table lists the transceivers that are supported on the 8-port 10-Gbps network module.

Table 9: FPR3105 8-port 10-Gbps network module

Port type	Transceiver PID	First supported release
FPR3K-XNM-8X10G	• GLC-TE • GLC-SX-MMD • GLC-LH-SMD • GLC-EX-SMD • GLC-ZX-SMD • GLC-GE-100FX • SFP-10G-SR • SFP-10G-SR-S • SFP-10G-LR • SFP-10G-LR-S • SFP-10G-ER • SFP-10G-ER-S • SFP-H10GB-CUxM • SFP-H10GB-ACUxM • SFP-10G-AOCxM	Firewall Threat Defense 7.3/ASA 9.20
	• SFP-10G-T-X	Firewall Threat Defense 7.6/ASA 9.22

The following table lists the transceivers that are supported on the 8-port 10-Gbps network module.

Table 10: FPR3110, FPR3120, FPR3130, and FPR3140 8-port 10-Gbps network module

Port type	Transceiver PID	First supported release
FPR3K-XNM-8X10G	• GLC-TE • GLC-SX-MMD • GLC-LH-SMD • GLC-EX-SMD • GLC-ZX-SMD • GLC-GE-100FX • SFP-10G-SR • SFP-10G-SR-S • SFP-10G-LR • SFP-10G-LR-S • SFP-10G-ER • SFP-10G-ER-S • SFP-H10GB-CUxM • SFP-H10GB-ACUxM • SFP-10G-AOCxM	Firewall Threat Defense 7.1/ASA 9.17
	• SFP-10G-T-X	Firewall Threat Defense 7.6/ASA 9.22

The following table lists the transceivers that are supported on the 8-port 25-Gbps network module.

Table 11: FPR3130 and FPR3140 8-port 25-Gbps network module

Port type	Transceiver PID	First supported release
FPR3K-XNM-8X25G	• GLC-TE • GLC-SX-MMD • GLC-LH-SMD • GLC-EX-SMD • GLC-ZX-SMD • GLC-GE-100FX • SFP-10G-SR • SFP-10G-SR-S • SFP-10G-LR • SFP-10G-LR-S • SFP-10G-ER • SFP-10G-ER-S • SFP-H10GB-CUxM • SFP-H10GB-ACUxM • SFP-10G-AOCxM	Firewall Threat Defense 7.1/ASA 9.17
	• SFP-10G-T-X	Firewall Threat Defense Defense 7.6/ASA 9.22
	• SFP-25G-SR-S • SFP-10/25G-CSR-S • SFP-10/25G-LR-S • SFP-H25-CUxM • SFP-25G-AOCxM	Firewall Threat Defense 7.1/ASA 9.17

The following table lists the transceivers that are supported on the 4-port 40-Gbps network module.

Table 12: FPR3130 and FPR3140 4-port 40-Gbps network module

Port type	Transceiver PID	First supported release
FPR3K-XNM-4X40G	• QSFP-40G-SR4 • QSFP-40G-SR4-S • QSFP-40G-CSR4 • QSFP-40G-SR-BD • QSFP-40G-LR4-S • QSFP-40G-LR4 • WSP-Q40GLR4L • QSFP-H40G-CUxM • QSFP-4SFP10G-CUxM • QSFP-H40G-ACUxM • QSFP-4X10G-ACUxM • QSFP-H40G-AOCxM • QSFP-4X10G-AOCxM	Firewall Threat Defense 7.1/ASA 9.17

The following table lists the transceivers that are supported on the 2-port 100-Gbps network module.

Table 13: FPR3130 and FPR3140 2-port 100-Gbps network module

Port type	Transceiver PID	First supported release
FPR3K-XNM-2X100G	• QSFP-100G-SR4-S • QSFP-100G-LR4-S • QSFP-40/100G-SRBD • QSFP-100G-AOCxM • QSFP-100G-CUxM • QSFP-4SFP25G-CUxM • QSFP-100G-FR-S • QSFP-100G-DR-S • QSFP-40/100-SRBD	Firewall Threat Defense 7.4/ASA 9.20
	• QSFP-100G-LR-S • QSFP-100G-SM-SR • QSFP-100G-SR1.2	Firewall Threat Defense 7.6/ASA 9.22

Related Topics

Cisco SFP Modules for Gigabit Ethernet Applications Data Sheet

Hardware Specifications

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

Specification	3105	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 lb (.91 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				
Humidity	Operating: 5 to 85% noncondensing Nonoperating: 5 to 90% noncondensing				
Altitude	Operating: 10,000 ft maximum Nonoperating: 40,000 ft maximum				
Sound pressure	65 dBA @ 77°F (25°C) typical 74 dBA maximum				
Sound power	72 dB (typical) 80 dB (maximum)				

Specification	3105	3110	3120	3130	3140
NEBS	Operating altitude: 0 to 13,000 ft (3962 m) Operating temperature: • Long Term: 0 to 45°C up to 6000 ft (1829 m) • Long Term: 0 to 35°C 6000-13000 ft (1829-3964 m) • Short Term: -5 to 55°C up to 6000 ft (1829 m) **Note** Firepower 3100 NEBS compliance applies only to the 3130.				

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.

Note Use the **show inventory** command to display a list of the PIDs for your Secure Firewall 3100.

Table 14: Secure Firewall 3100 PIDs

PID	Description
Chassis	
FPR3105-ASA-K9	Cisco Secure Firewall 3105 ASA chassis 1 RU
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
FPR3105-NGFW-K9	Cisco Secure Firewall 3105 next generation firewall 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

PID	Description
FPR3140-NGFW-K9	Cisco Secure Firewall 3140 next generation firewall chassis 1 RU
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)
FPR3K-FIPS-KIT=	FIPS opacity shield kit (spare)
Network Modules	
FPR3K-XNM-6X1SXF	6-port 1-Gbps SFP hardware bypass network module, SX multimode
FPR3K-XNM-6X1SXF=	6-port 1-Gbps SFP hardware bypass network module, SX multimode (spare)

PID	Description
FPR3K-XNM-6X10SRF	6-port 10-Gbps SFP hardware bypass network module, SR multimode
FPR3K-XNM-6X10SRF=	6-port 10-Gbps SFP hardware bypass network module, SR multimode (spare)
FPR3K-XNM-6X10LRF	6-port 10-Gbps SFP hardware bypass network module, LR single mode
FPR3K-XNM-6X10LRF=	6-port 10-Gbps SFP hardware bypass network module, LR single mode (spare))
FPR3K-XNM-6X25SRF	6-port 25-Gbps SFP hardware bypass network module, SR multimode
FPR3K-XNM-6X25SRF=	6-port 25-Gbps SFP hardware bypass network module, SR multimode (spare)
FPR3K-XNM-6X25LRF	6-port 25-Gbps SFP hardware bypass network module, LR single mode
FPR3K-XNM-6X25LRF=	6-port 25-Gbps 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-Gbps SFP+ network module
FPR3K-XNM-8X10G=	8-port 1/10-Gbps SFP+ network module (spare)
FPR3K-XNM-8X25G	8-port 1/10/25-Gbps QSFP network module
FPR3K-XNM-8X25G=	8-port 1/10/25-Gbps QSFP network module (spare)
FPR3K-XNM-4X40G	4-port 40-Gbps QSFP+ network module
FPR3K-XNM-4X40G=	4-port 40-Gbps QSFP+ network module (spare)
FPR3K-X-NM-2X100G	2-port 100-Gbps QSFP/QSFP28 network module
FPR3K-X-NM-2X100G=	2-port 100-Gbps QSFP/QSFP28 network module (spare)
FPR3K-NM-BLANK	Network module blank slot cover
FPR3K-NM-BLANK=	Network module blank slot cover (spare)

Related Topics

Cisco Returns Portal

Cisco Secure Firewall Threat Defense Command Reference
Cisco Secure Firewall ASA Series Command Reference

Power cord specifications

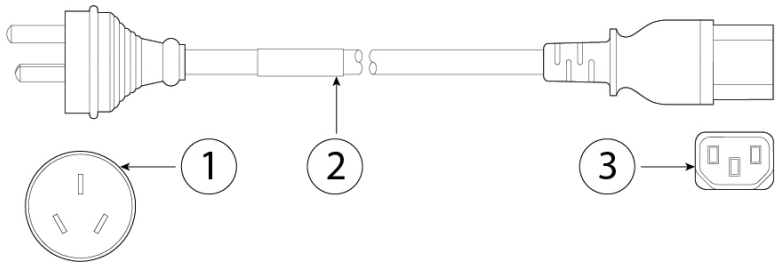
Each power supply has a separate power cord. Standard power cords or jumper power cords are available for connection to the secure firewall. The jumper power cords for use in racks are available as an optional alternative to the standard power cords.

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.

Note Only the approved power cords or jumper power cords provided with the Secure 3100 are supported.

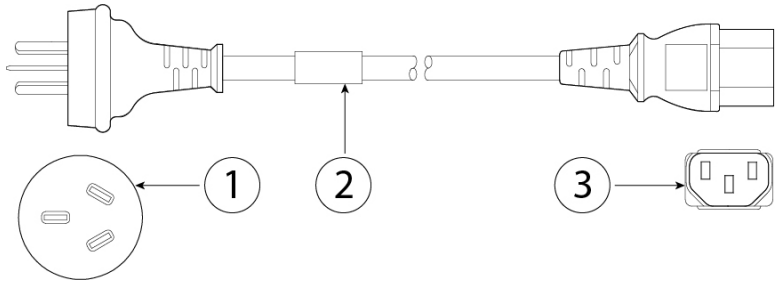
The following power cords are supported.

Figure 17: Argentina (CAB-ACR)



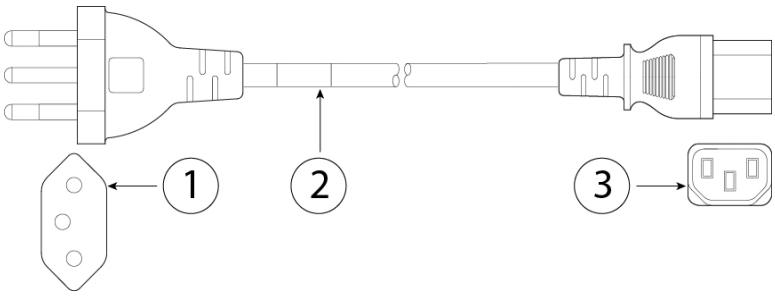
1	Plug: EL 219/IRAM 2073	**2**	Cord set rating: 10 A, 250 V
3	Connector: IEC 60320/C13		Cord length: 2.5 m

Figure 18: Australia (CAB-ACA)



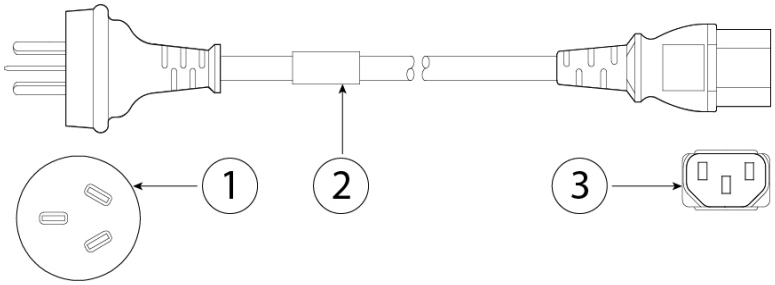
1	Plug: A.S. 3112	**2**	Cord set rating: 10 A, 250 V
3	Connector: IEC 60320/C13		Cord length: 2.5 m

Figure 19: Brazil (CAB-C13-ACB)



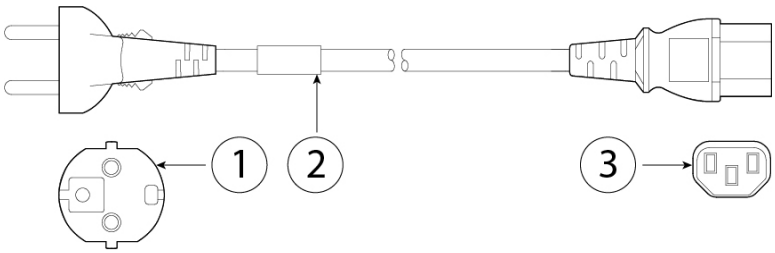
1	Plug: NBR 14136	**2**	Cord set rating: 10 A, 250 V
3	Connector: IEC 60320/C13		Cord length: 2.1 m

Figure 20: China (CAB-ACC)



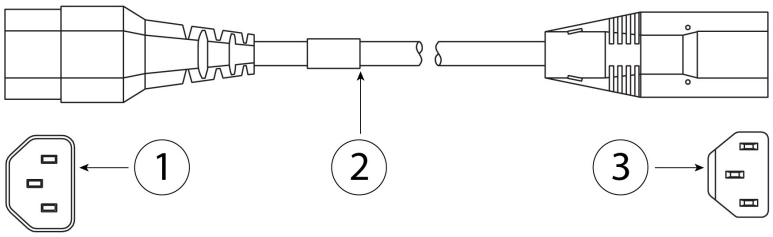
1	Plug: GB2099.1-2008	**2**	Cord set rating: 10 A, 250 V
3	Connector: IEC 60320/C13		Cord length: 2.5 m

Figure 21: Europe (CAB-ACE)



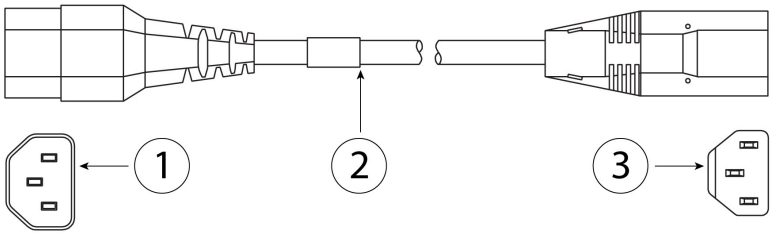
1	Plug: CEE 7 VII	**2**	Cord set rating: 10 A, 250 V
3	Connector: IEC 60320/C13		Cord length: 1.5 m

Figure 22: India jumper (CAB-C13-C14-3M-IN)



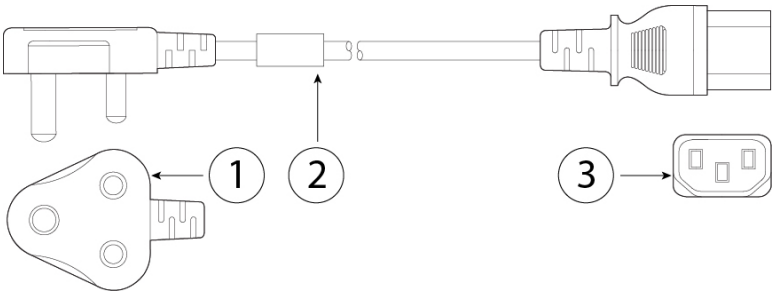
1	IEC 60320/C14G	**2**	Cord set rating: 10 A, 250 V
3	Connector: IEC 60320/C13		Cord length: 3 m

Figure 23: India jumper (CAB-C13-C14-IN)



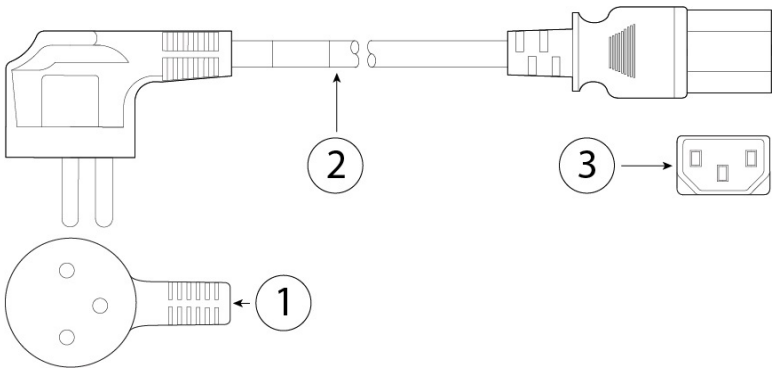
1	IEC 60320/C14G	**2**	Cord set rating: 10 A, 250 V
3	Connector: IEC 60320/C13		Cord length: 1.4 m

Figure 24: India (PWR-CORD-IND-D)



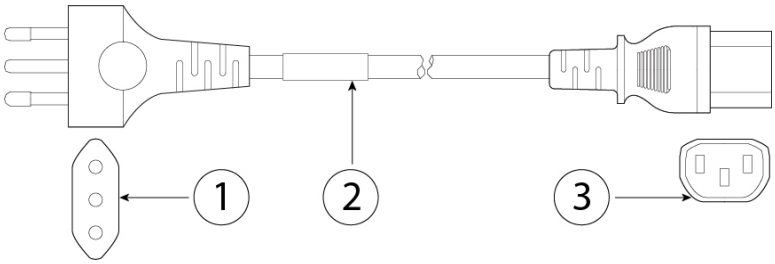
1	Plug: IS 6538-1971	**2**	Cord set rating: 10 A, 250 V
3	Connector: IEC 60320/C13		Cord length: 1.8 m

Figure 25: Israel (CAB-250V-10A-IS)



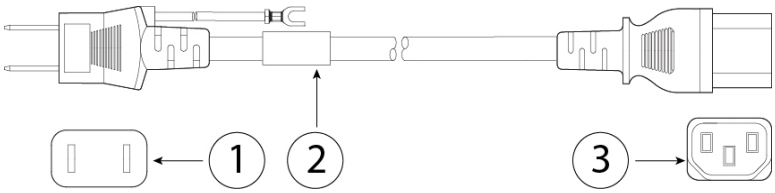
1	Plug: SI-32	**2**	Cord set rating: 10 A, 250 V
3	Connector: IEC 60320/C13		Cord length: 2.5 m

Figure 26: Italy (CAB-ACI)



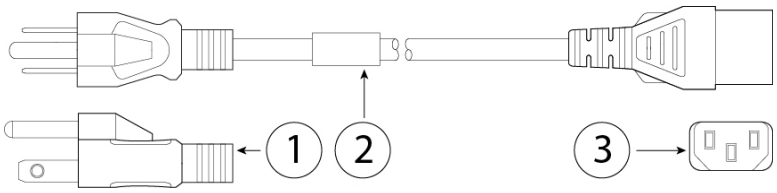
1	Plug: CEI 23-16	**2**	Cord set rating: 10 A, 250 V
3	Connector: IEC 60320/C13		Cord length: 2.5 m

Figure 27: Japan (CAB-JPN)



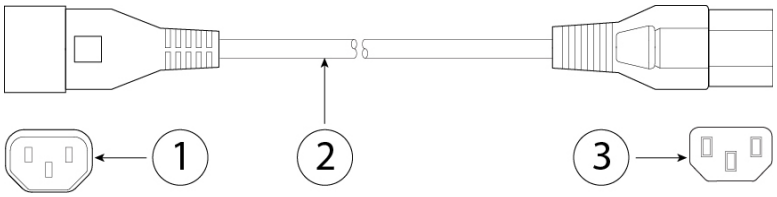
1	Plug: JIS C8303	**2**	Cord set rating: 12 A, 125 V
3	Connector: IEC 60320/C13		Cord length: 2.5 m

Figure 28: Japan (CAB-JPN-3PIN)



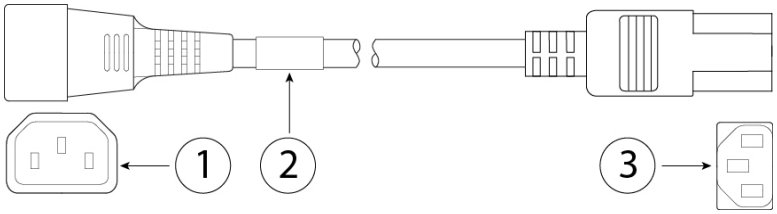
1	Plug: JIS C8303/JIS C8306	**2**	Cord set rating: 12 A, 125 V
3	Connector: IEC 60320/C13		Cord length: 2.3 m

Figure 29: Japan (CAB-C13-C14-2M-JP) PSE Mark



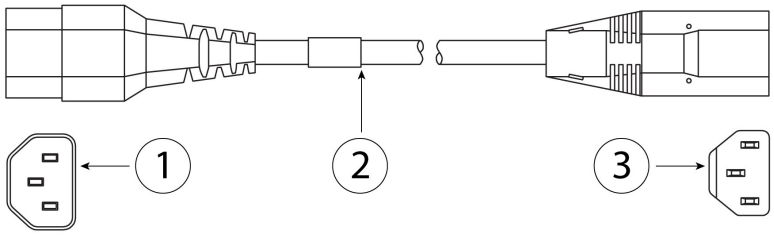
1	IEC 60320-2-2/E	**2**	Cord set rating: 10 A, 250 V
3	Connector: IEC 60320/C13		Cord length: 2 m

Figure 30: Jumper (CAB-C13-C14-2M)



1	IEC 60320/C14G	**2**	Cord set rating: 10 A, 250 V
3	Connector: IEC 60320/C13		Cord length: 2.5 m

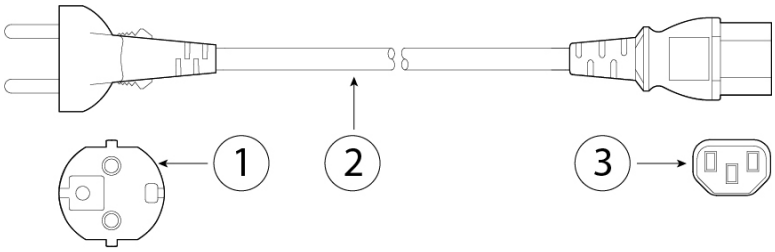
Figure 31: Cabinet jumper (CAB-C13-CBN)



1	IEC 60320-2-2/E	**2**	Cord set rating: 10 A, 250 V

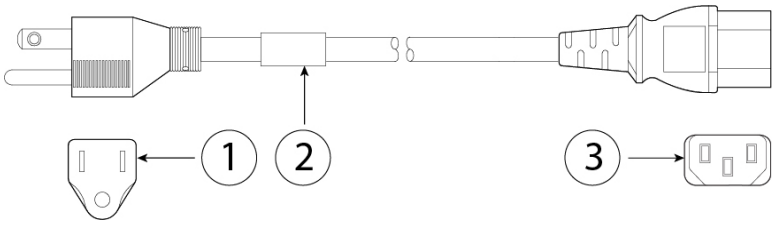
3	Connector: IEC 60320/C13		Cord length: 0.7 m

Figure 32: Korea (CAB-AC-C13-KOR)



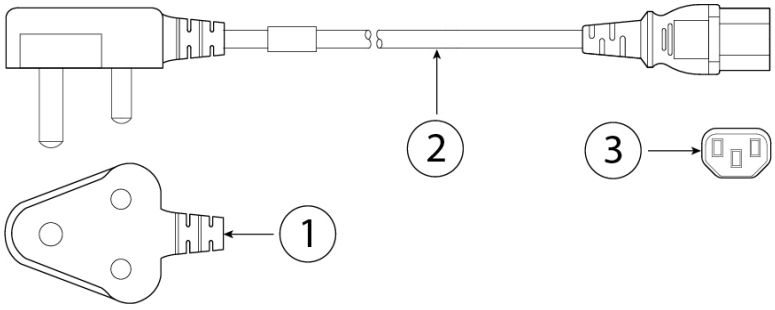
1	Plug: KSC 8305	**2**	Cord set rating: 10 A, 250 V
3	Connector: IEC 60320/C13		Cord length: 1.8 m

Figure 33: North America (CAB-AC)



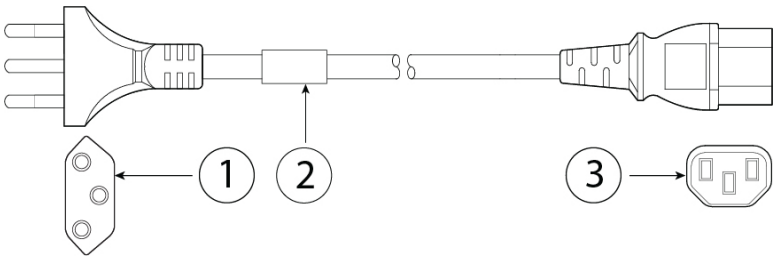
1	Plug: NEMA 5-15P	**2**	Cord set rating: 10 A, 125 V
3	Connector: IEC 60320/C13		Cord length: 2.1 m

Figure 34: South Africa (CAB-ACSA)



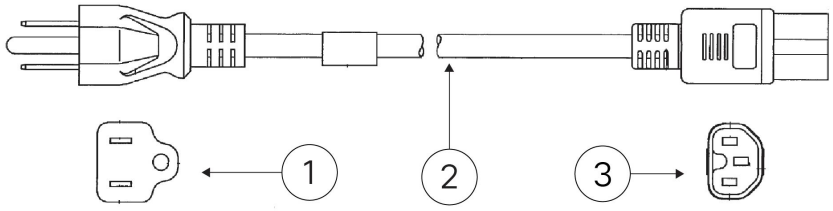
1	Plug: SABS 164/1	**2**	Cord set rating: 16 A, 250 V
3	Connector: IEC 60320/C13		Cord length: 1.8 m

Figure 35: Switzerland (CAB-ACS)



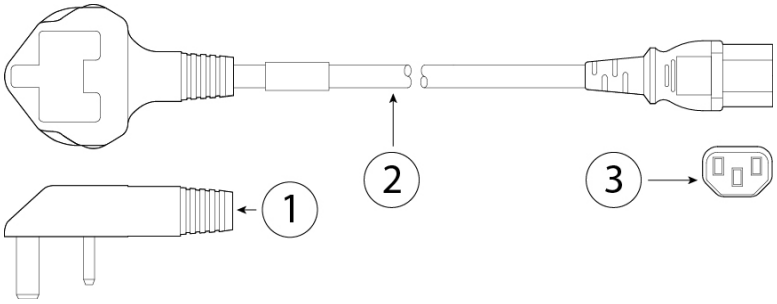
1	Plug: SEV 1011	**2**	Cord set rating: 10 A, 250 V
3	Connector: IEC 60320/C13		Cord length: 2.5 m

Figure 36: Taiwan (CAB-AC-TAI)

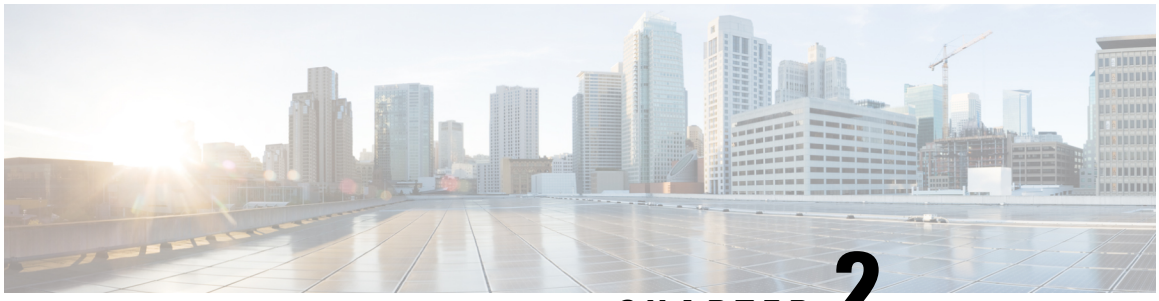


1	Plug: CNS 10917-2	**2**	Cord set rating: 10 A, 125 V
3	Connector: IEC 60320/C15		—

Figure 37: United Kingdom (CAB-ACU)



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



CHAPTER 2

Installation Preparation

- Installation warnings, on page 49
- Network Equipment-Building System (NEBS) statements, on page 51
- Safety recommendations, on page 53
- Maintain safety with electricity, on page 53
- Prevent ESD damage, on page 54
- Site environment, on page 54
- Site considerations, on page 54
- Power supply considerations, on page 55
- Rack configuration considerations, on page 55

Installation warnings

Read the regulatory compliance and safety information document before installing the security appliance.

Take note of the following warnings:



Warning **Statement 1071—**Warning Definition

IMPORTANT SAFETY INSTRUCTIONS

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

SAVE THESE INSTRUCTIONS



Warning **Statement 1005**—Circuit Breaker

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

AC 20 A/DC 40 A

Warning **Statement 1015**—Battery Handling

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

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

Warning **Statement 1017—**Restricted Area

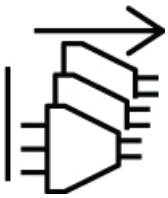
This unit is intended for installation in restricted access areas. Only skilled, instructed, or qualified personnel can access a restricted access area.

Warning **Statement 1024—**Ground Conductor

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

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

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



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

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

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

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

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

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

Warning **Statement 9001—**Product Disposal

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

Related Topics

Regulatory Compliance and Safety Information

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.

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

This equipment is suitable for installation in network telecommunications facilities.

Note **Statement 8016—**Installation Location Where the National Electric Code (NEC) Applies

This equipment is suitable for installation in locations where the NEC applies.

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.

Related Topics

Regulatory Compliance and Safety Information

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

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.

Related Topics

Hardware Specifications, on page 38

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

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.

Related Topics

Power supply modules, on page 24

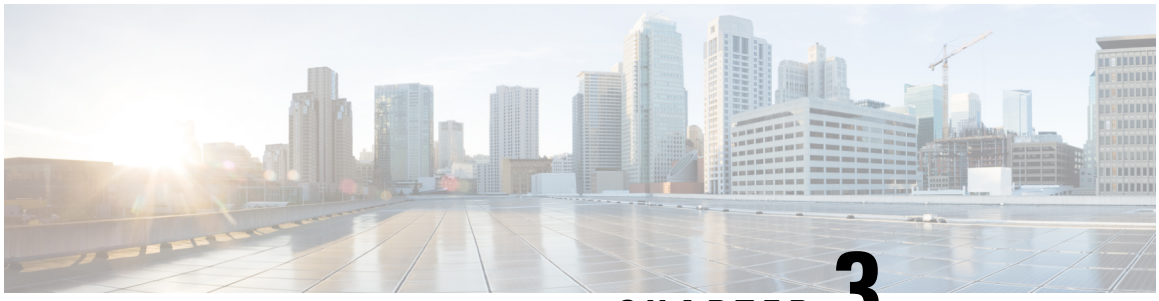
Rack configuration considerations

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.

Related Topics

Rack mount the chassis using slide rails, on page 60
Rack mount the chassis using brackets, on page 58



CHAPTER 3

Rack-Mount the Chassis

- Unpack and inspect the chassis, on page 57
- Rack mount the chassis using brackets, on page 58
- Rack mount the chassis using slide rails, on page 60
- Ground the chassis, on page 67

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.

Procedure

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

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

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

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

Related Topics

Package contents, on page 4

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.

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).

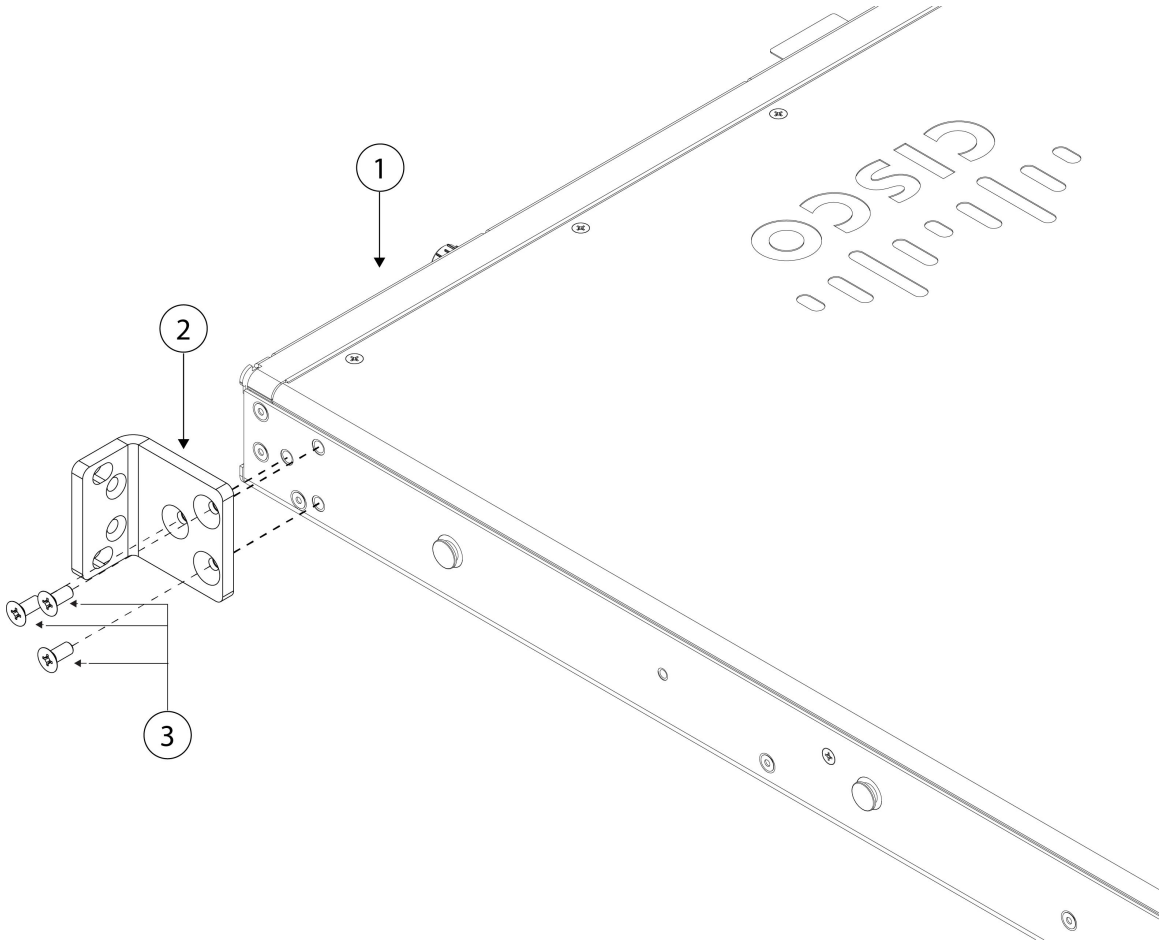
You need the following to install the Secure Firewall 3100 in a rack:

- Phillips screwdriver
- Two rack-mount brackets with six 8-32 x 0.375 inch screws
- Rack-mount screws:
  - Four 12-24 x 0.75 inch Phillips screws for securing the chassis to your rack
  - Four 10-32 x 0.75 inch Phillips screws for securing the chassis to your rack
- (Optional) Cable management bracket kit:
  - Two cable management brackets
  - Four 8-32 x 0.375 inch Phillips screws

Procedure

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 38: Attach the rack-mount bracket to the side of the chassis

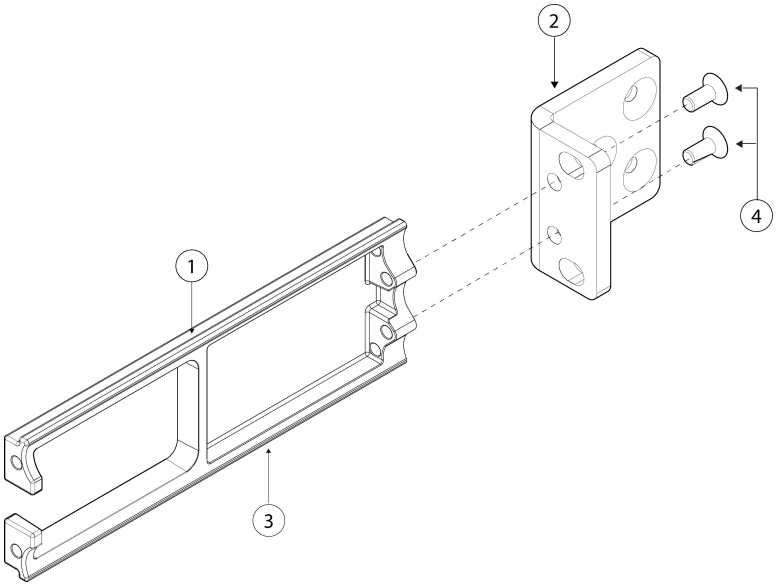


1	Chassis	**2**	Rack-mount bracket
3	8-32 x 0.375-inch Phillips screws (three per side)		—

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 39: Install the cable management screws into the rack-mount bracket



1	Step groove on the cable management bracket	**2**	Rack-mount bracket
3	Cable management bracket	**4**	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

- Install the cables according to your default software configuration as described in the Cisco Secure Firewall 3100 Getting Started Guide.

Related Topics

Product ID numbers, on page 39
Ground the chassis, on page 67

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.

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
- Two slide rail locking brackets
- Six 8-32 x 0.302-inch Phillips screws
- Two M3 x 0.5 x 6 mm Phillips screws
- (Optional) Two cable management brackets with four 8-32 x 0.375-inch Phillips screws

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

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

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



Warning **Statement 1024—**Ground Conductor

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



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

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

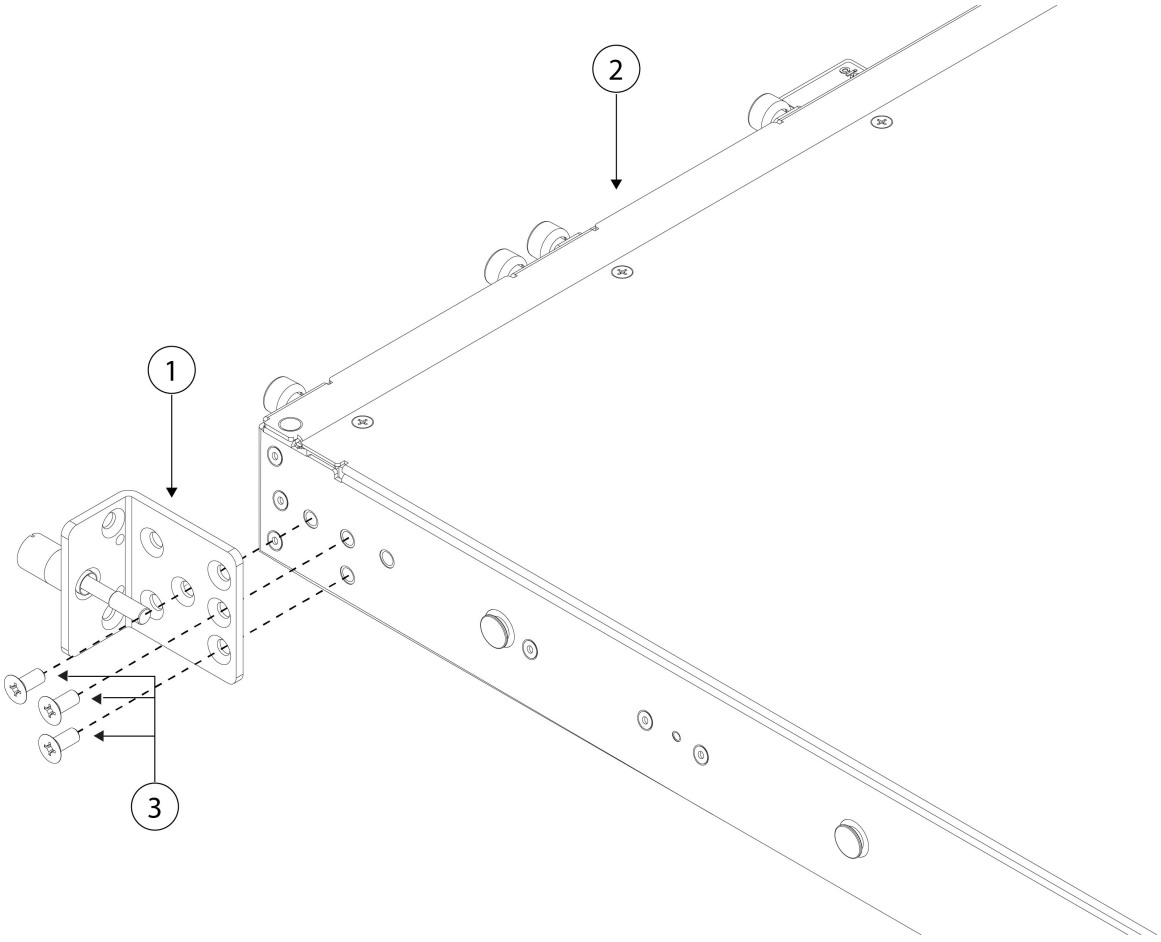
Warning **Statement 1098**—Lifting Requirement

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

Procedure

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

Figure 40: Attach the slide-rail locking bracket to the side of the chassis



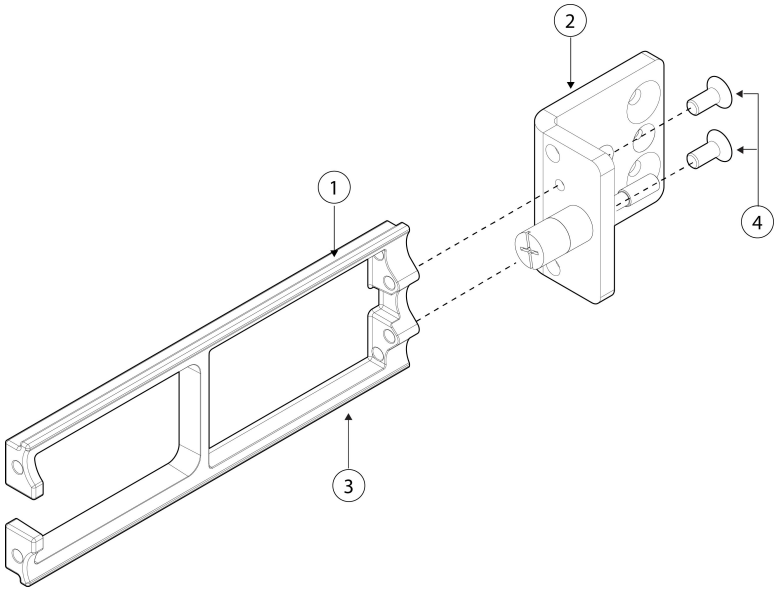
1	Slide-rail locking bracket	**2**	Chassis
3	8-32 x 0.302-inch Phillips screws (three per side)		—

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.

Caution
If you are going to install the FIPS opacity shield, make sure the lower step of the cable management bracket is on the inside in your installation. This allows you to slide the FIPS cover into place more easily.

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



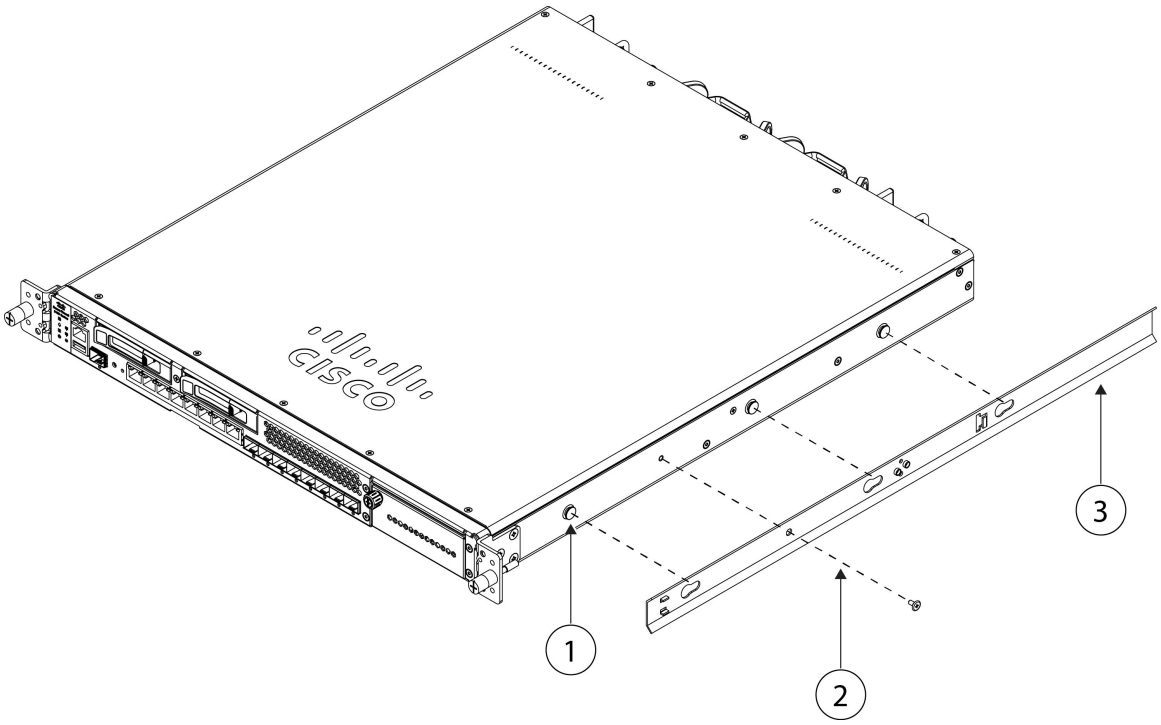
1	Step groove on the cable management bracket	**2**	Rack-mount bracket
3	Cable management bracket	**4**	8-32 x 0.375-inch Phillips screws (two per bracket)

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



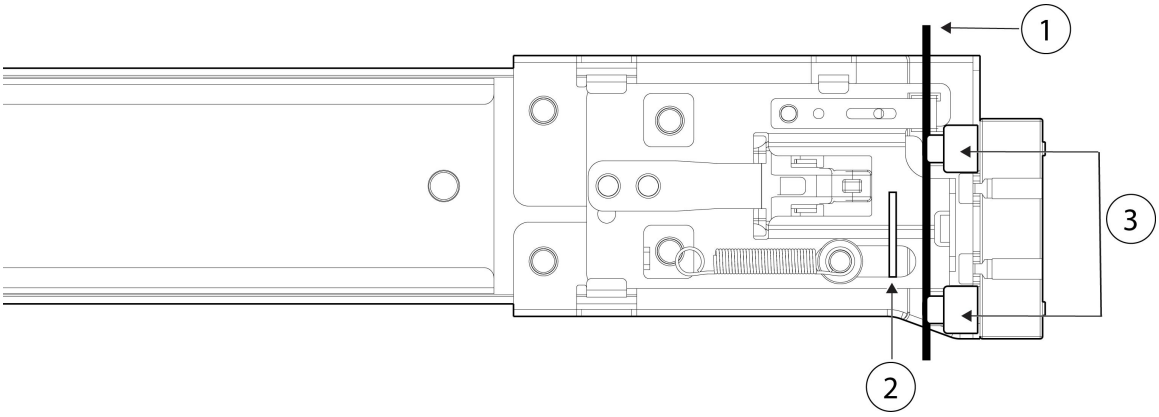
1	Mounting peg on the chassis for the keyed slot	**2**	M3 x 0.5 x 6- mm Phillips screws (one per side)
3	Inner rail		—

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 43: Front securing mechanism inside the front end



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

Step 5 Install the slide rails into the rack:

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

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

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

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

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

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

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

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

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

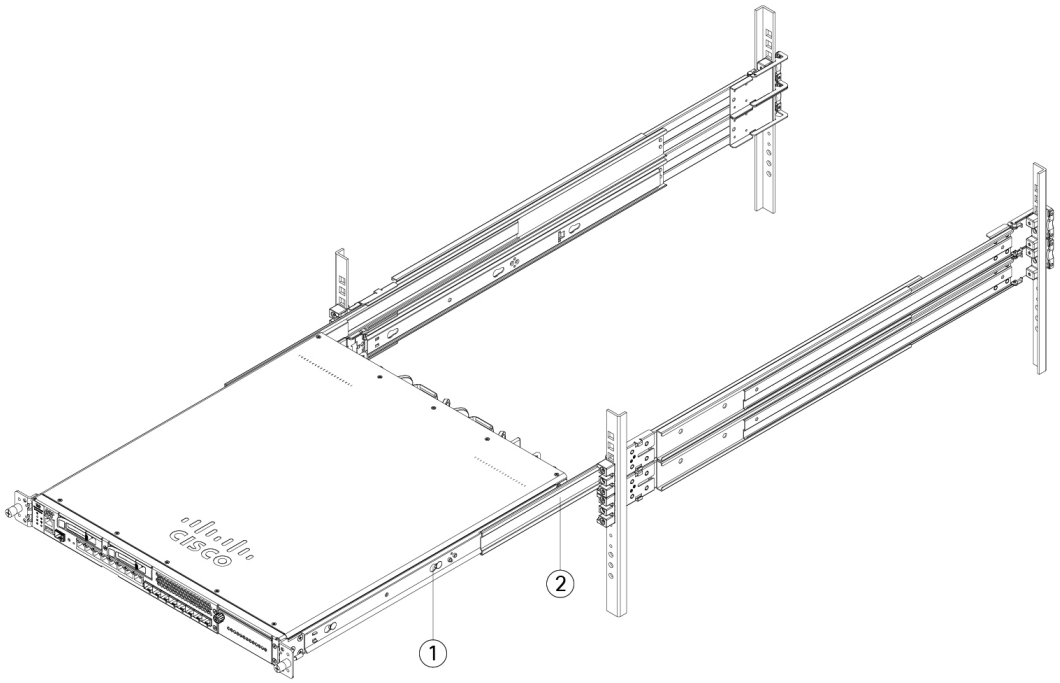
Step 6 Insert the chassis into the slide rails.

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

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

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

Figure 44: 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

- Install the cables according to your software configuration as described in the Cisco Secure Firewall 3100 Getting Started Guide.

Related Topics

Product ID numbers, on page 39
Ground the chassis, on page 67

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
  - Two 10-32 x 0.38-inch screws used to secure the grounding lug

Safety warnings

Take note of the following warnings:

Warning **Statement 1024—**Ground Conductor

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

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

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

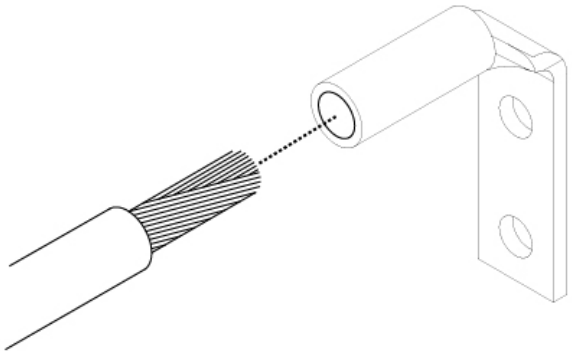
If your unit has modules, secure them with the provided screws.

Procedure

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

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

Figure 45: Insert the cable into the grounding lug

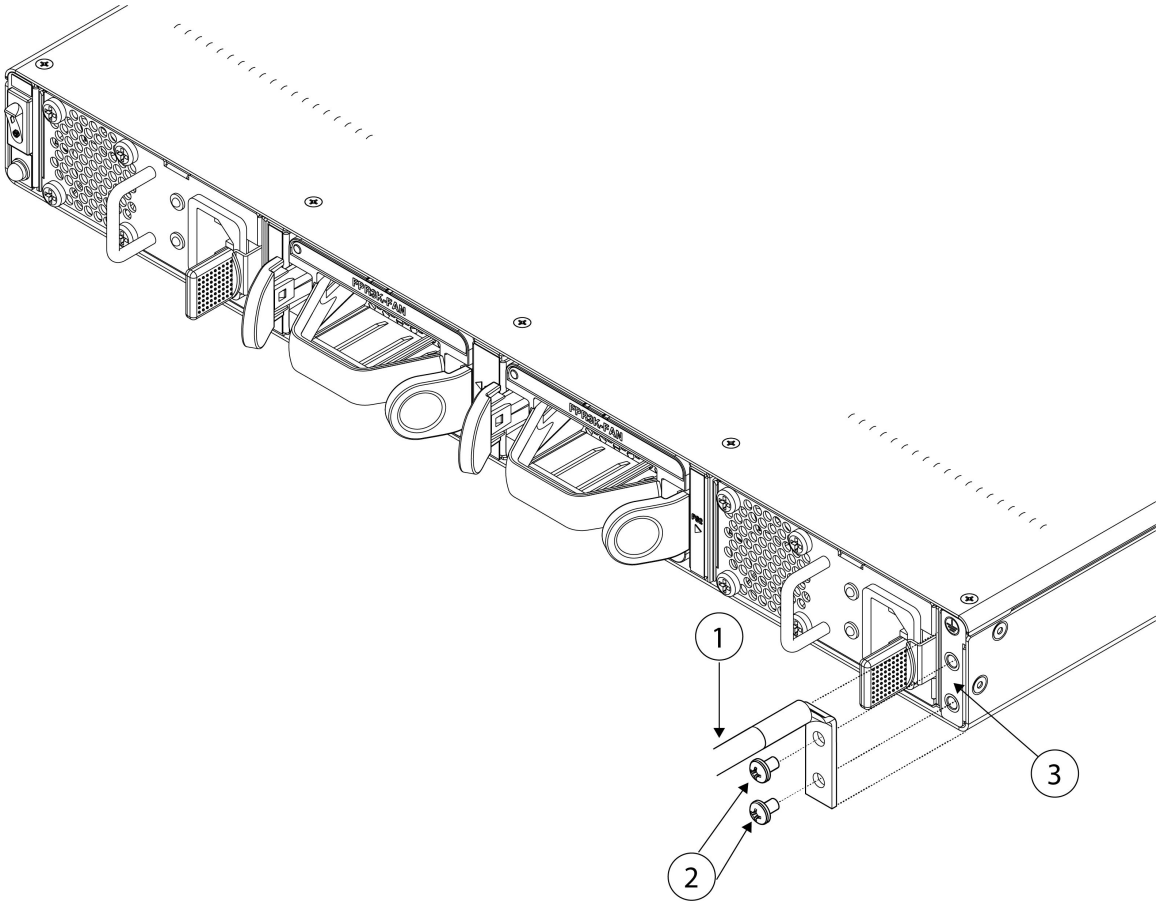


Step 3 Use the crimping tool to secure the grounding cable in the grounding lug.

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

Step 5 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 46: Attach the grounding lug



1	Grounding lug	**2**	Two 10-32 x 0.38-inch screws
3	Ground pad		—

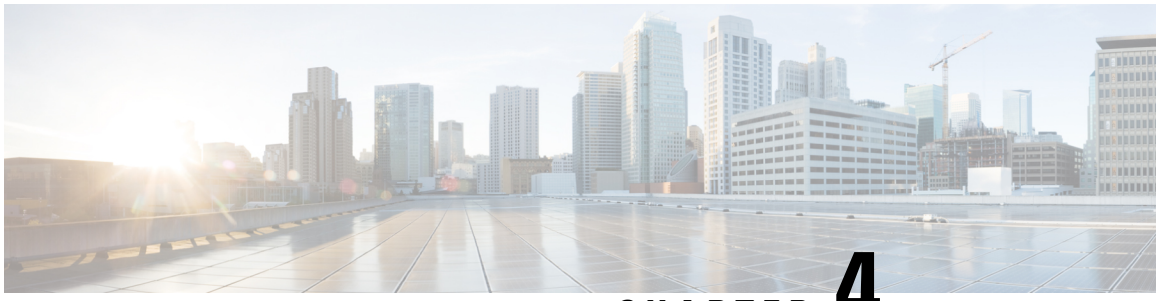
Step 6 Make sure that the lug and cable do not interfere with other equipment.

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 FIPS opacity shield if necessary. See Install the FIPS opacity shield, on page 85 for the procedure.

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, on page 71
- Remove and replace the SSD, on page 73
- Remove and replace the dual fan module, on page 76
- Remove and replace the power supply module, on page 77
- Connect the DC power supply module, on page 79
- Secure the Power Cord on the Power Supply Module, on page 82
- Install the FIPS opacity shield, on page 85

Install, remove, and replace the network module

You can remove and replace the network module (NM-2) in the Secure Firewall 3100. Hot-swapping of identical modules is supported, but if you replace a network module with another type, you must reboot the system so that the new network module is recognized.

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

Caution You can install all supported network modules in all Secure Firewall 3100 models, but the 40-Gb network module (FPR-X-NM-4X40G) and the 1/10/25-Gb network module (FPR-X-NM-8X25G) are only recognized when installed in the 3130 and 3140. The software does not support these network modules for the 3105, 3110, and 3120.

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

Safety warnings

Take note of the following warning:

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

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

Procedure

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

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

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.

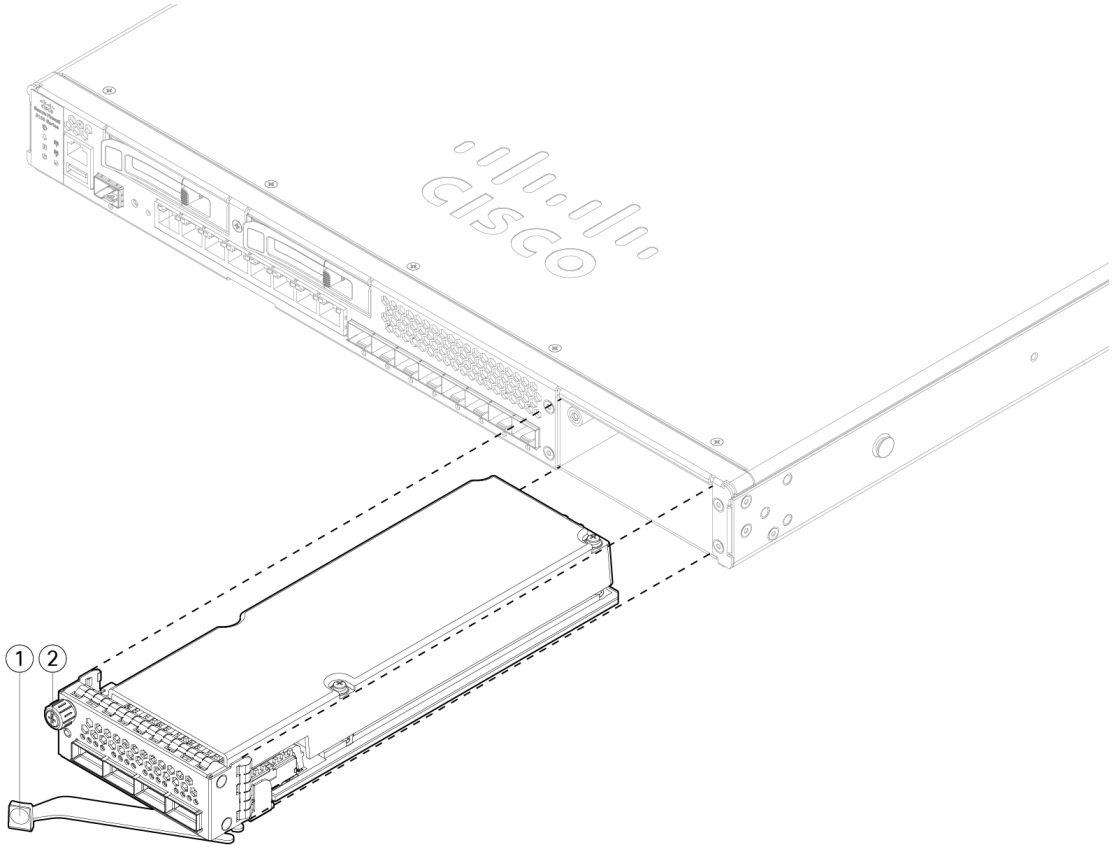
c) To replace an existing network module with a different model network module, power down the chassis by moving the power switch to the OFF position. See the configuration guide for your operating system for the procedure to replace an existing network module with a new model.

d) Continue with Step 3.

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

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

Figure 47: Remove the network module



1	Ejector handle	**2**	Captive screw

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

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

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

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

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

Related Topics

Rear panel, on page 13

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.

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 warning:

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

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

Procedure

Step 1 Save your configuration.

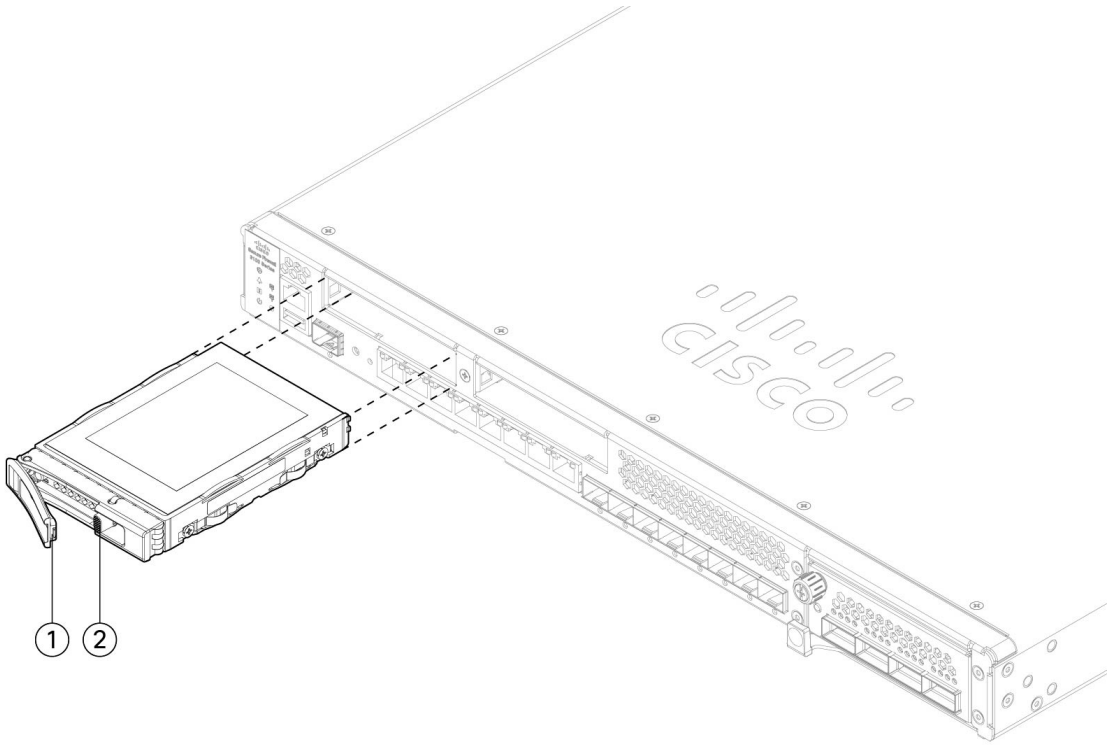
Step 2 If you are removing SSD-1 and there is only one SSD installed in the chassis, power down the chassis by moving the power switch to the OFF position.

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 48: 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.

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

Related Topics

SSDs, on page 27
Front panel LEDs, on page 9

Rear panel, on page 13
Cisco Secure Firewall Management Center Device Configuration Guide, 7.4

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. The chassis operates for 30 seconds after either one or both modules are removed. All modules must be reinserted within 30 seconds to avoid overheating the chassis. If you wait longer than 30 seconds, the chassis may power off automatically to prevent damage to components. The chassis does not power up and boot properly if the dual fan modules are missing.

Safety warnings

Take note of the following warnings:

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

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

Warning **Statement 1093—**Avoid Sharp Edges

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



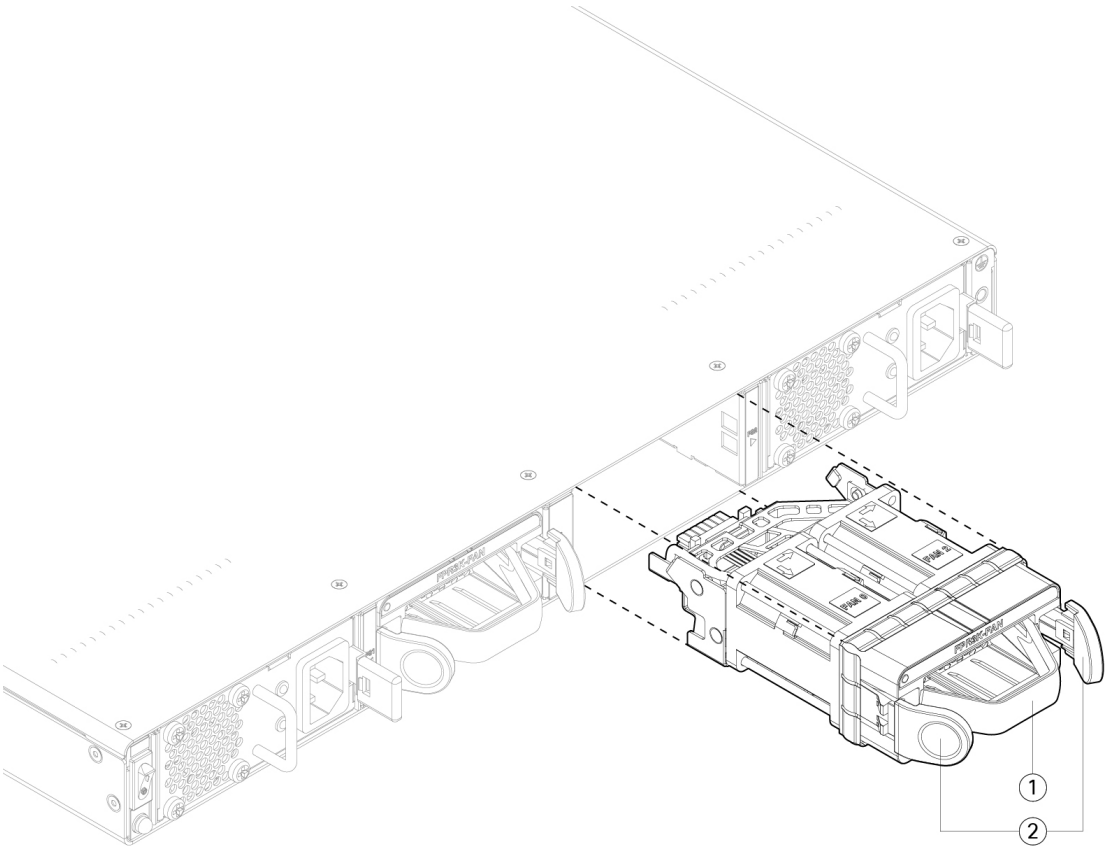
Procedure

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 49: 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.

Related Topics

Front panel LEDs, on page 9

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 1003—**DC Power Disconnection

To reduce risk of electric shock or personal injury, disconnect DC power before removing or replacing components or performing upgrades.



Warning **Statement 1015**—Battery Handling

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

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



Warning **Statement 1022—**Disconnect Device

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



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

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

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



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

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

Procedure

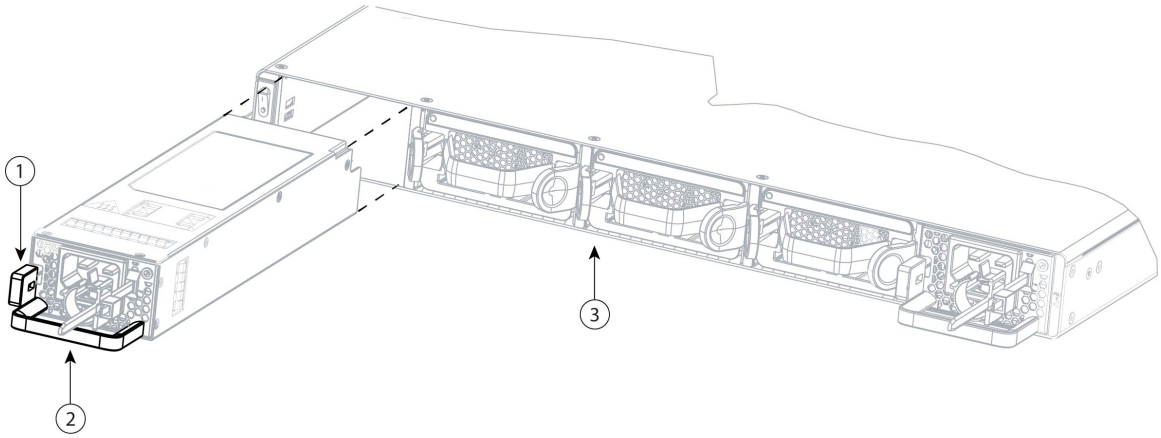
Step 1 Unplug the power supply cable before removing the power supply module. You cannot disengage the power supply module release tab without first removing the cable.

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

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

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

Figure 50: Remove the power supply module



1	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.

Related Topics

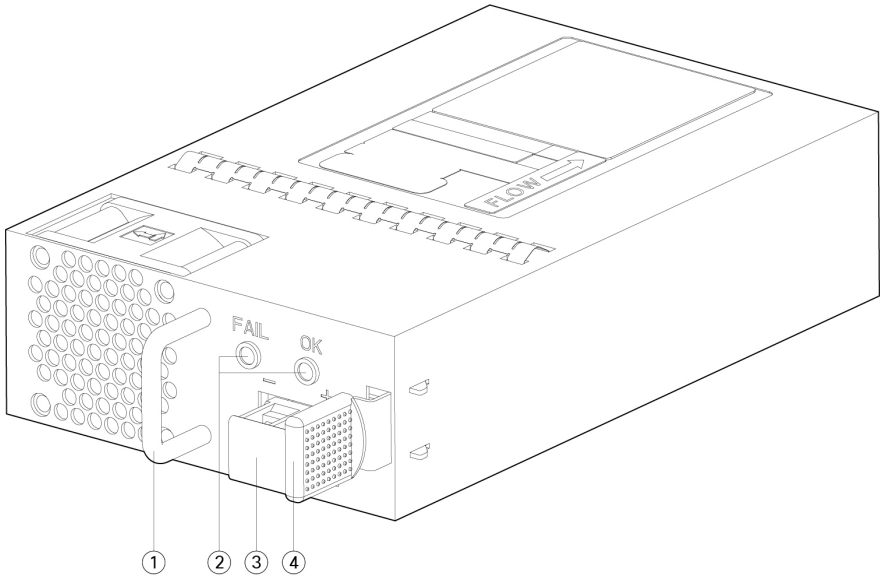
Power supply modules, on page 24

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 51: 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 warning:

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.

Procedure

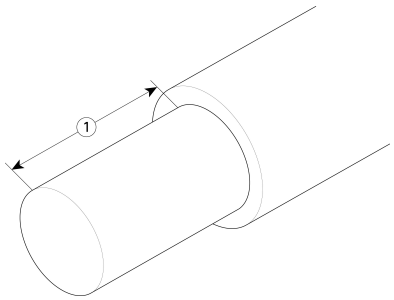
Step 1 Verify that the power is off to the DC circuit on the power supply module that you are installing.

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 52: Stripped DC input source wire



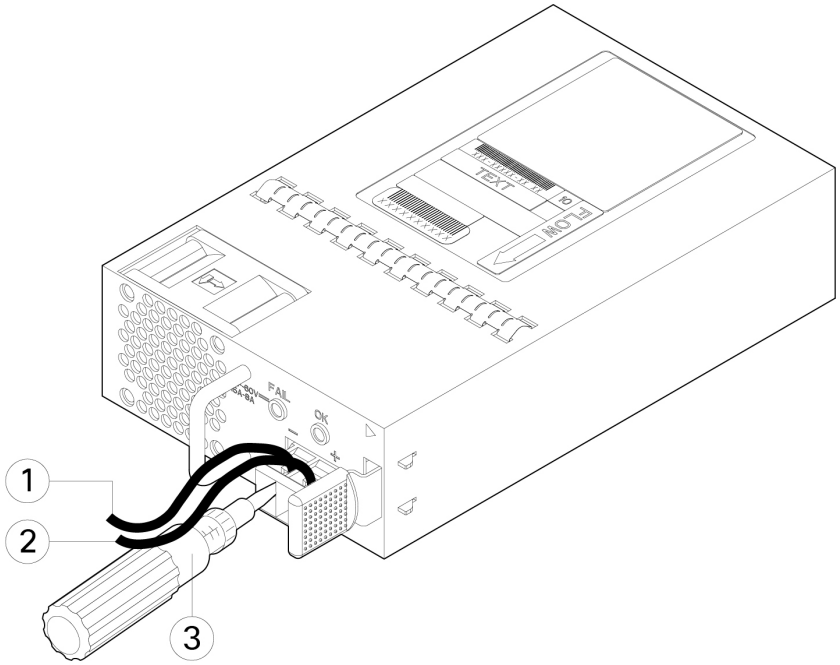
1	Strip the wires to approximately 0.39 inch (10 mm) + 0.02 inch (0.5 mm)		—

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 53: 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.

Related Topics

Ground the chassis, on page 67
Front panel LEDs, on page 9

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 warning:

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

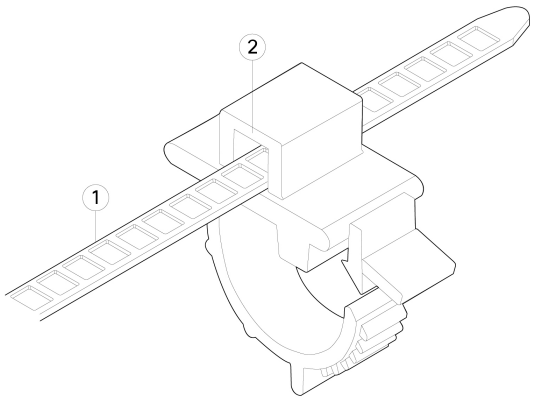
There are no serviceable parts inside. To avoid risk of electric shock, do not open.

Procedure

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 54: Tie Wrap Through the Box Channel of the Clamp



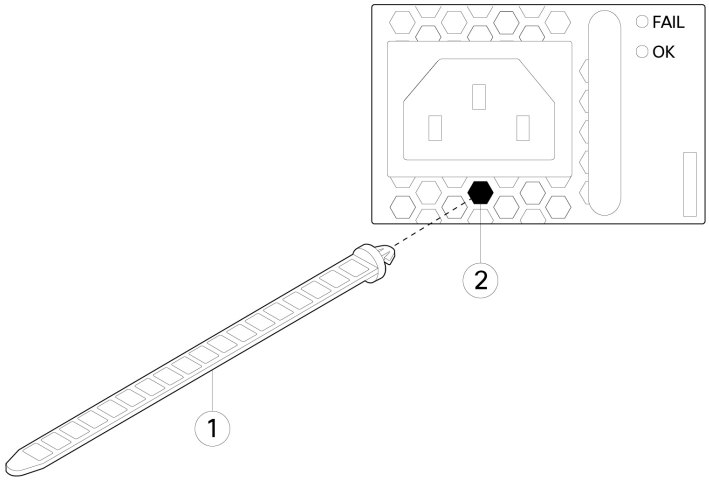
1	Tie wrap	**2**	Box channel

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 55: Connect the Tie Wrap

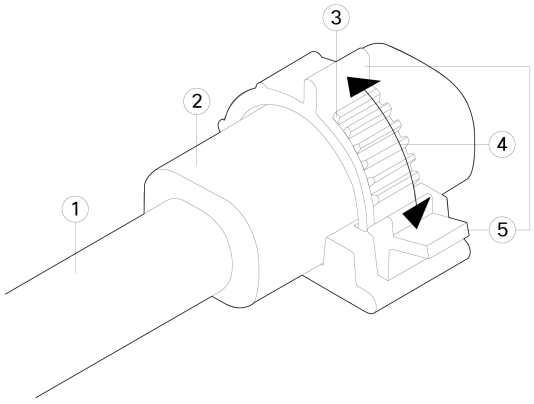


1	Tie wrap	**2**	Hexagonal hole

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 56: 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.

Install the FIPS opacity shield

Caution This procedure should be performed only by the Crypto Officer (CO).

Note Because the FIPS opacity shield covers the serial number on the chassis, the CO should copy the serial number and store it in a secure place. The serial number is needed when you call Cisco TAC.

You need the following to install the FIPS opacity shield:

- #1 Phillips screwdriver
- The following items from the FIPS opacity shield kit (FPR3K-FIPS-KIT):
  - One FIPS opacity shield
  - Six 8-32 x 0.375-inch Phillips screws used to attach the FIPS opacity shield to the cable management brackets
  - Nine Tamper Evidence Labels (TELs)

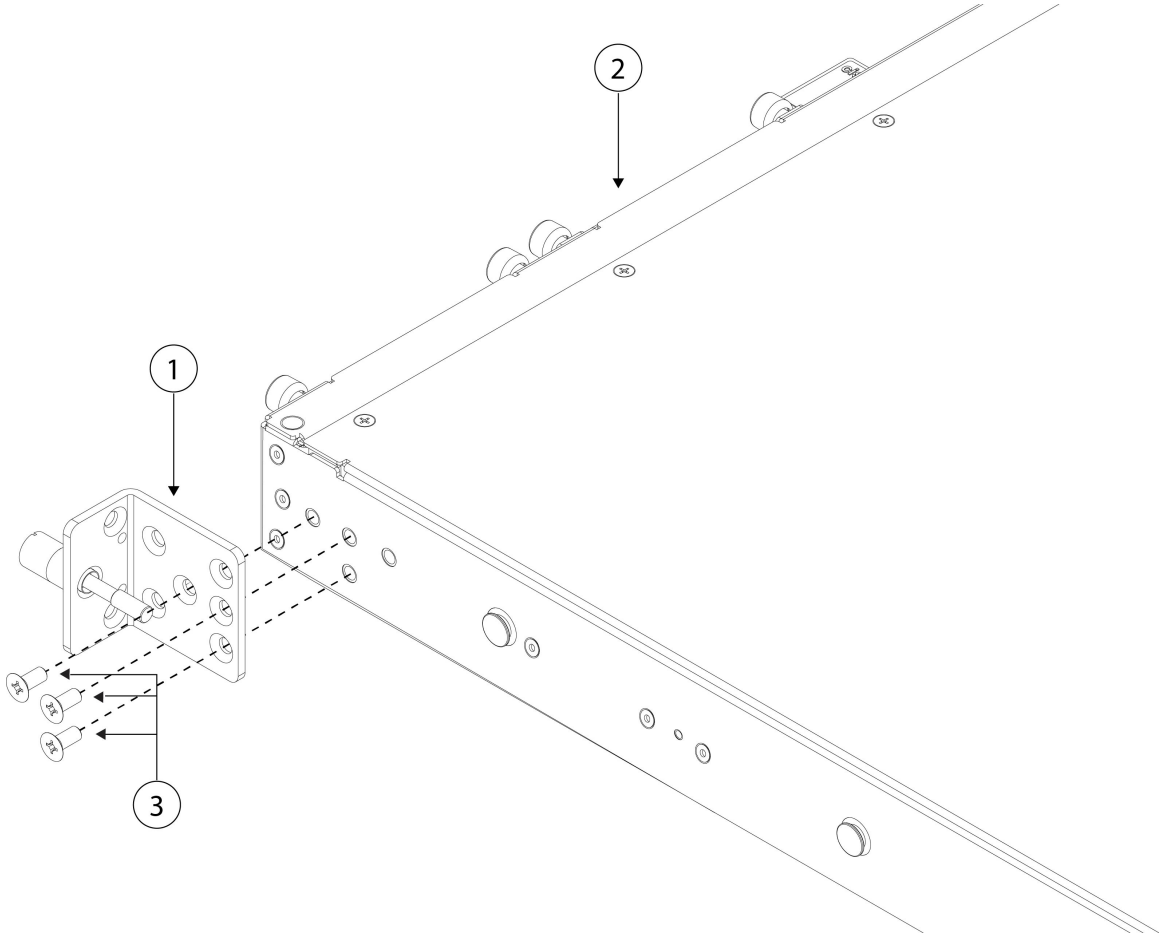
Note The TELs are made of a special thin gauge vinyl with self-adhesive backing. Once the CO attaches them on the chassis, any attempt to open the chassis damages the TELs or the chassis cover. Because the TELs have nonrepeated serial numbers, the CO can inspect them for damage and compare them against the applied serial numbers to verify whether the chassis has been tampered with. TELs with curled corners, rips, and slices indicate tampering. The word “FIPS” or “OPEN” may appear if the label has been peeled back. Cisco recommends that you inspect the TELs for tampering every 30 days.

Procedure

Step 1 Copy the serial number and store it in a secure place.

Step 2 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). See the figure below showing the front panel right side of the chassis.

Figure 57: Attach the slide-rail locking brackets to the side of the chassis



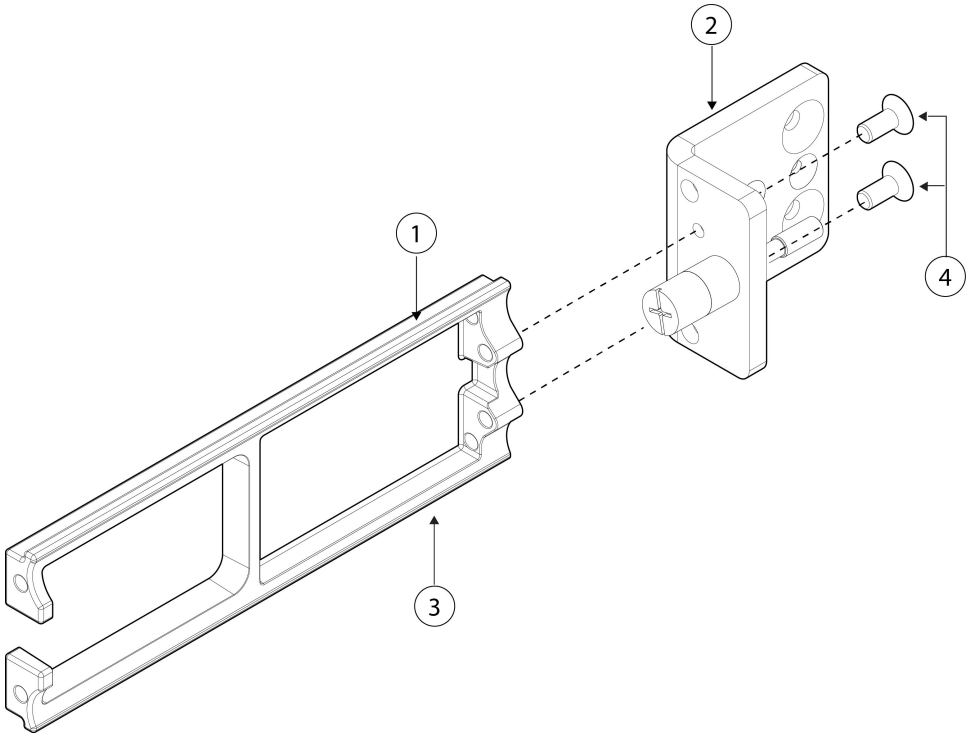
1	Slide-rail locking bracket	**2**	Chassis front panel
3	8-32 x 0.302-inch Phillips screws (three per side)		—

Step 3 Attach the cable management bracket to the slide-rail locking bracket:

a) Install the cable management screws into the slide-rail locking bracket. See the figure below which shows a right-side orientation on the front panel of the chassis.

Caution
Make sure the lower step of the cable management bracket is on the inside in your installation. This allows you to slide the FIPS opacity shield into place more easily.

Figure 58: Install the cable management brackets into the slide-rail locking brackets



1	Step grrove on the cable management bracket	**2**	Rack-mount bracket
3	Cable management bracket	**4**	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 4 Connect the cables to the ports. Make sure the cables have enough slack to route them through the cable mounting brackets.

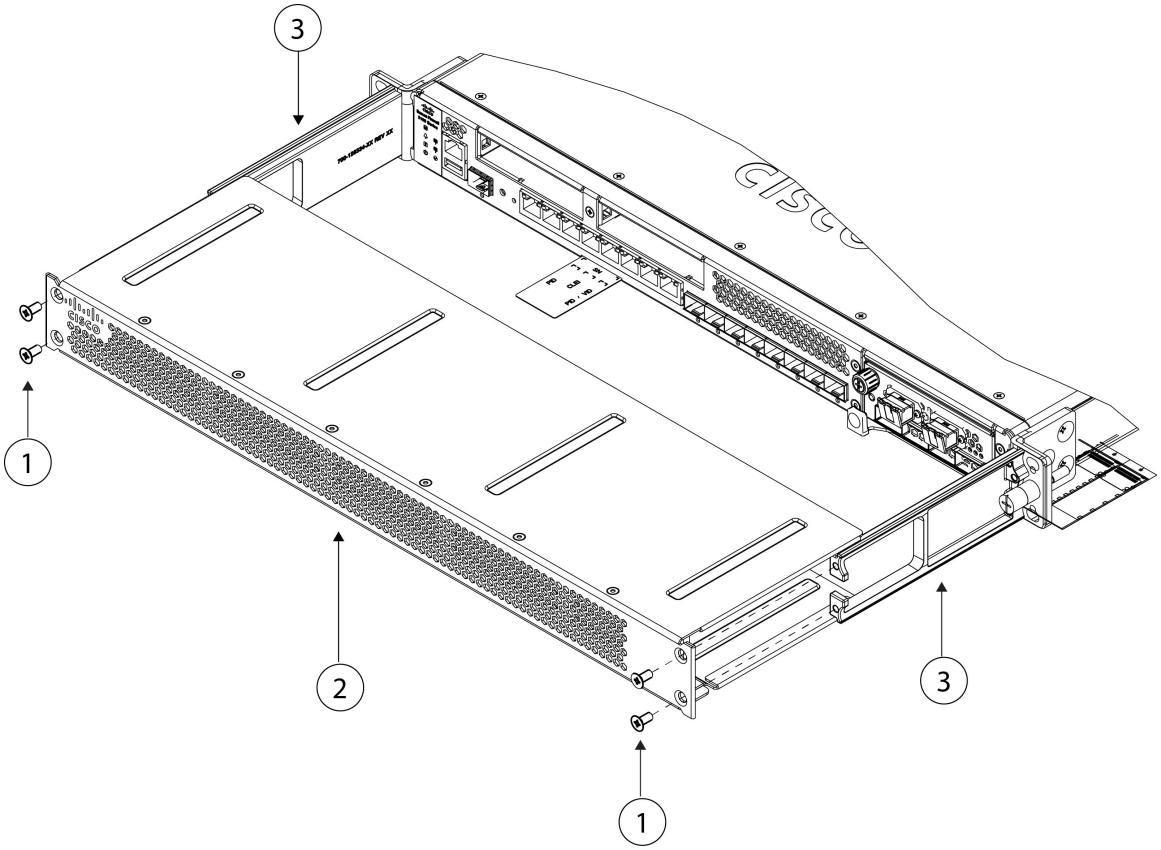
Note
If you are installing the FIPS opacity shield after the initial product installation, the cables are connected. If the attached cables do not have enough slack to route them through the cable mounting brackets, you will have to turn the power off on the appliance, remove the cables, route the cables through the cable mounting brackets, reattach the cables, and continue with Step 5 below.

Note
When you toggle the power switch from ON to OFF, it takes several seconds for the system to power down. Do not remove the power cable until the power LED is off. After removing power from the chassis either by moving the power switch to OFF or unplugging the power cord, wait at least 10 seconds before turning power back ON.

Step 5 Route the cables through the openings in the cable management brackets (see figure below).

Step 6 Slide the FIPS opacity shield toward the cable management brackets and attach it to the cable management brackets using the four 8-32 x 0.375 inch Phillips screws provided in the FIPS opacity shield kit.

Figure 59: Route the cables and attach the FIPS opacity shield to the cable management brackets



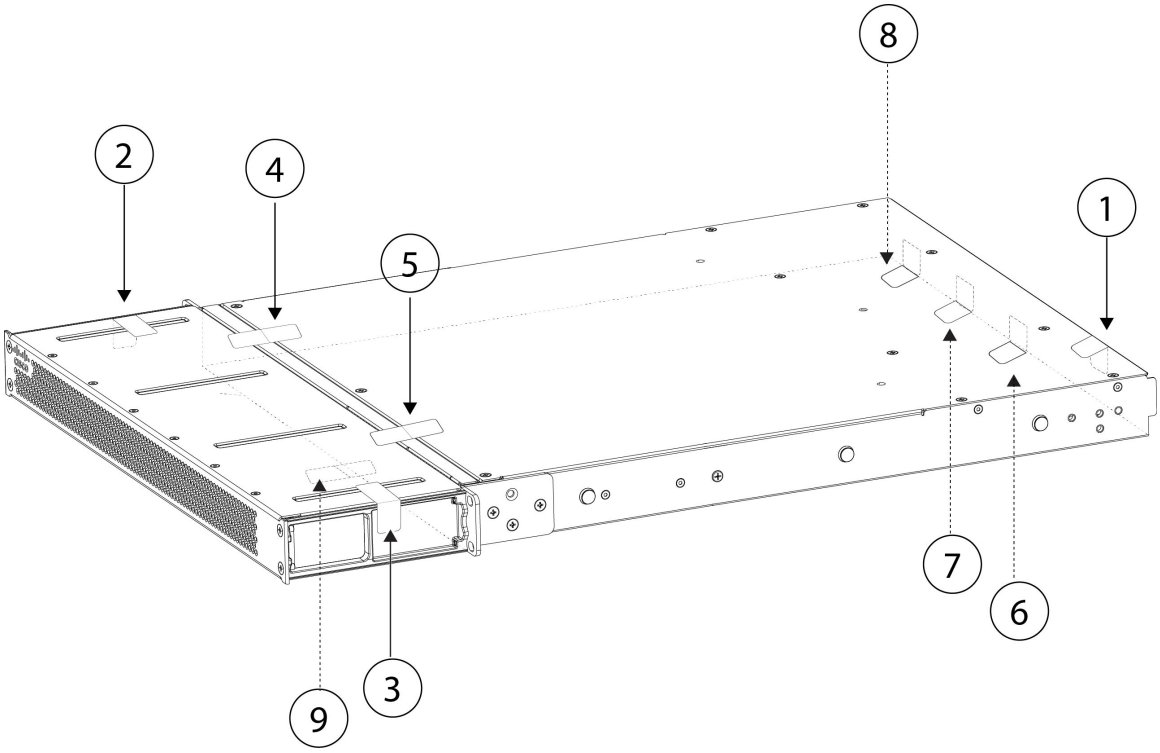
1	8-32 x 0.375 inch-Phillips screws (two per side)	**2**	FIPS opacity shield
3	Cable management brackets to route the cables through		—

Step 7 Before you attach the TELs, clean the chassis of any grease, dirt, or oil with alcohol-based cleaning pads.

Step 8 Attach the nine TELs. See the figure below for the correct placement. Allow the TELs to cure for a minimum of 12 hours.

Caution
Any deviation in the placement of the TELs means the chassis is not in FIPS mode.

Figure 60: TELs placement on the chassis



1	TEL 1 is on the rear and top of the chassis	**2**	TEL 2 on the front and top of chassis
3	TEL 3 on the front on the right side and top of chassis	**4**	TEL 4 is on the top across the FIPS opacity shield and the chassis (on the left of the chassis)
5	TEL 5 is on the top across the FIPS opacity shield and the chassis (on the right of the chassis)	**6**	TEL 6 is on the bottom of the chassis towards the left side of the chassis
7	TEL 7 on the bottom of the chassis in the middle of the chassis	**8**	TEL 8 on the bottom of the chassis towards the right side of the chassis
9	TEL 9 is on the top of the FIPS opacity shield (on the right of the chassis)		—

Step 9 Attach the power cable to the chassis and connect it to an electrical outlet.

Step 10 Press the power switch on the rear panel.

Step 11 Check the power LED on the front panel. Solid green indicates that the chassis is powered on.

Step 12 Place the chassis in FIPS mode.

See the following procedures for how to place the chassis in FIPS mode:

- ASA in Platform Mode
- ASA in Appliance mode

- FTD managed by FMC

What to do next

See the Cisco Secure Firewall 3100 Getting Started Guide for your operating system for further configuration information.

Related Topics

Serial number and digital documentation portal QR code, on page 6
Front panel LEDs, on page 9