Cisco Secure Firewall 1210CE, 1210CP, and 1220CX Hardware Installation Guide

First Published: 2024-10-10

Last Modified: 2025-05-09

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.

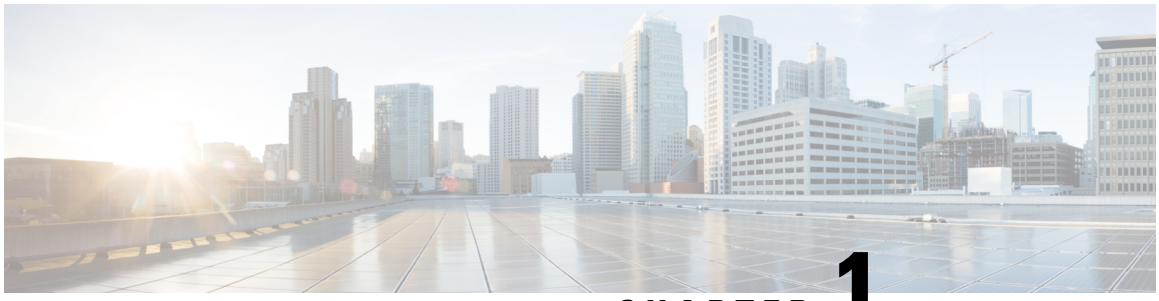
Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual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

CONTENTS



CHAPTER 1

Overview

Features

The Cisco Secure Firewall 1210CE, 1210CP, and 1220CX are a series of compact network security appliances in the Cisco Firewall family. They are first supported in Cisco Secure Firewall Threat Defense Version 7.6 and Cisco Secure ASA Version 9.22.1.

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

The following figure shows the Secure Firewall 1210CE, 1210CP, and 1220CX.

Figure 1: CSF-1210CE, CSF-1210CP, and CSF-1220CX

The following table lists the features for the Secure Firewall 1210CE, 1210CP, and 1220CX.

Table 1: CSF-1210CE, CSF-1210CP, and CSF-1220CX Features

Feature	CSF-1210CE	CSF-1210CP	CSF-1220CX
Form factor	Compact or 1 RU for the rack shelf		
Mounting	• Desktop mount (default) • Wall mount (orderable kit) • Rack shelf (orderable kit) 2-post with rack brackets		
Airflow	Right to left (when viewed from the I/O side) Fan is on the right; pulls in air from the left		
System memory	16 GB		
Management port	One 1-Gbps Gigabit Ethernet RJ-45 10/100/1000 BaseT Restricted to network management access; connect with an RJ-45 cable		
Console ports	One Cisco Serial (RS-232 on RJ-45) One USB Type C 2.0 Provides management access through an external system		
USB port	One USB Type A 3.0 Used to attach an external device such as storage		
Network ports	Eight 1-Gbps copper RJ-45 Gigabit Ethernet ports		
Small form-factor pluggable (SFP)	Not supported		Two 10-Gbps optical Ethernet ports
Supported SFPs	Not supported		See Supported SFP/SFP+/QSFP+ Transceivers , on page 16 for a list of supported 1-Gbps and 10-Gbps SFPs

Feature	CSF-1210CE	CSF-1210CP	CSF-1220CX
PoE+ ports	Not supported	4 (Ethernet 1/5 to Ethernet 1/8) **Note** Supports IEEE 802.3at. In threat defense Version 7.6 and ASA Version 9.22 the total system power is capped at 120 W of PoE with a maximum of 30 W per port. You can divide the total 120 W among the four ports evenly.	Not supported
Reset button	Small recessed button Push and hold with a pin for 5 seconds; resets the chassis to its default state following the next reboot. **Note** Configuration variables are reset to factory default, but the flash is not erased and no files are removed.		
Lock slot	Accepts a Kensington T-bar locking mechanism for securing the chassis		
Power button	Yes Located on the left side of the rear panel		
Power cord socket	IEC320-C14 Supports C13 adapter cables		
AC power supply	External +12 V at 66 W	External +12 V at 110 W and -54 V at 120 W	External +12 V at 66 W
Storage	480-GB M.2 NVMe Internal component only; not field-replaceable. You must return the chassis to Cisco for SSD replacement. See the Cisco Returns Portal for more information.		
Fan	One internal blower fan Internal component only; not field-replaceable. See the Cisco Returns Portal for more information.		
Rubber feet	Yes, for stability		

PoE Power Supply

The Secure Firewall 1210CP supports PoE and ships with a PoE-supported power supply.

Caution Do *not* use the non-PoE power supply with the Secure Firewall 1210CP. If you connect it, the system goes into fail-safe mode, the PoE LEDs blink yellow on the rear panel, and you receive an error message similar to the following:

```
The PoE module failed to come up. This is due to either a faulty or
loose PoE card or an unsupported power supply. Ensure that the supported
power supply is connected to rule out any power supply issues. If the
problem persists, reach out to the Cisco support team.
```

The power supplies have a label near the plug that read "POE" and "NON-POE" for easy identification.

Console Ports

The Secure Firewall 1210CE, 1210CP, and 1220CX have two external console ports, a Cisco RJ-45 serial port and a Type C USB serial port. Only one serial console port can be active at a time. When a cable is plugged into the USB console port, the RJ-45 port becomes inactive. Conversely, when the USB cable is removed from the USB port, the RJ-45 port becomes active. The console ports do not have any hardware flow control. You can use the CLI to configure the chassis through either serial console port by using a terminal server or a terminal emulation program on a computer.

- RJ-45 (8P8C) port—Supports RS-232 signaling to an internal UART controller. The RJ-45 console port does not support a remote dial-in modem. You can use an adapter to convert the RJ45-to-DB9 connection if necessary.
- Type C USB port—Lets you connect to a USB port on an external computer. You can plug and unplug the USB cable from the console port without affecting Windows HyperTerminal operations. We recommend shielded USB cables with properly terminated shields. The default setting is 9600 baud. Use this for the initial connection. Baud rates for the USB console port are 1200, 2400, 4800, 9600, 19200, 38400, 57600, and 115200 bps.

External Flash Storage

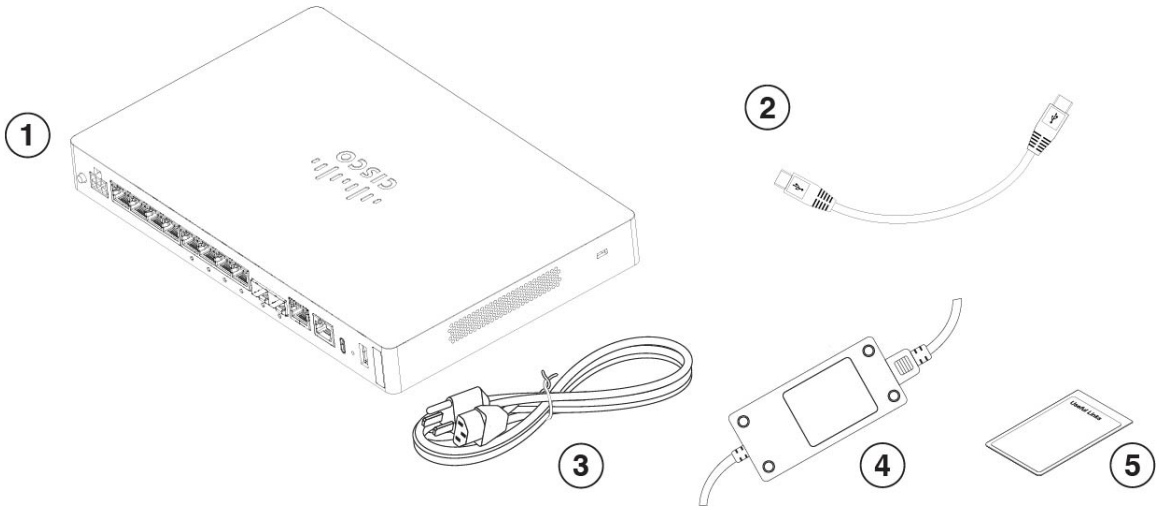
The chassis contains a USB Type A port that you can use to attach an external device. The USB port can provide output power of 5 V and up to a maximum of 1A (5 W of USB power).

- External USB drive (optional)—You can use the external USB Type A port to attach a data-storage device. The external USB drive identifier is *disk1*. When the chassis is powered on, a connected USB drive is mounted as disk1 and is available for you to use. Additionally, the file-system commands that are available to disk0 are also available to disk1, including **copy**, **format**, **delete**, **mkdir**, **pwd**, **cd**, and so on.
- FAT-32 File System—The Secure Firewall 1210CE, 1210CP, and 1220CX only support FAT-32-formatted file systems for the external USB drive. If you insert an external USB drive that is not in FAT-32 format, the system mounting process fails, and you receive an error message. You can enter the command **format disk1:** to format the partition to FAT-32 and mount the partition to disk1 again; however, data might be lost.

Package Contents

The following figure shows the package contents for the Secure Firewall 1210CE, 1210CP, and 1220CX. Note that the contents are subject to change and your exact contents might contain additional or fewer items.

Figure 2: CSF-1210CE, CSF-1210CP, and CSF-1220CX Package Contents



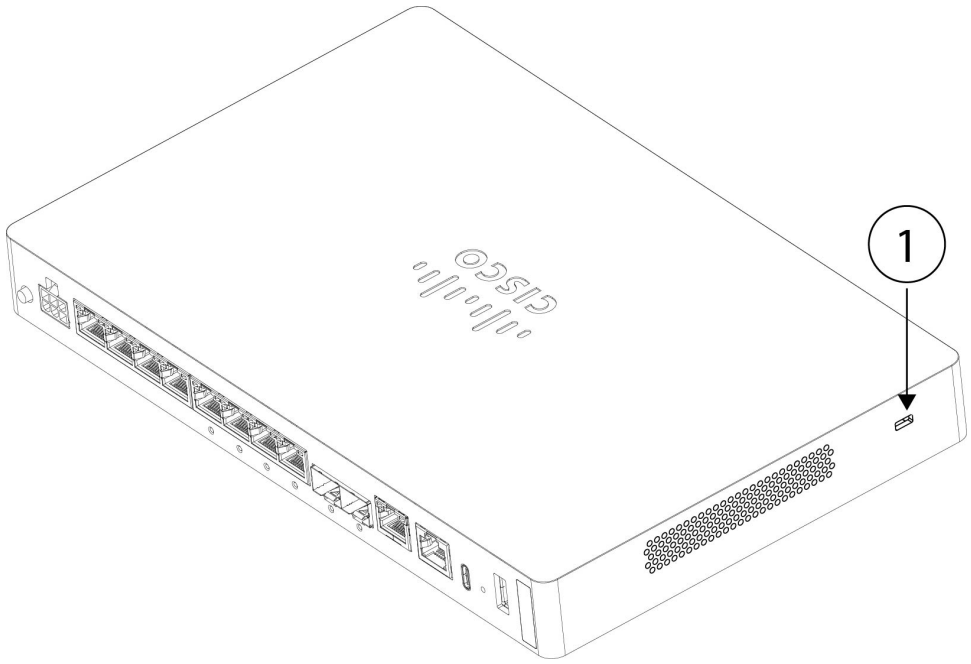
1	Chassis	**2**	USB console cable (Type C) PID: CAB-CONS-USB-C Optional: in package if ordered
3	Power cord See Power Cord Specifications, on page 20 for a list of the approved power cords.	**4**	Power supply
5	*Secure Firewall 1210/1220* This document has links to the hardware installation guide, regulatory 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.		—

Kensington Lock, Serial Number, and Digital Documentation Portal QR Code Locations

Facing the front panel (non-I/O side) you can find the Kensington lock on the left side of the chassis. It accepts a standard Kensington T-bar locking mechanism for securing the chassis.

The following figure shows the location.

Figure 3: Kensington Lock on the Left Side of Chassis

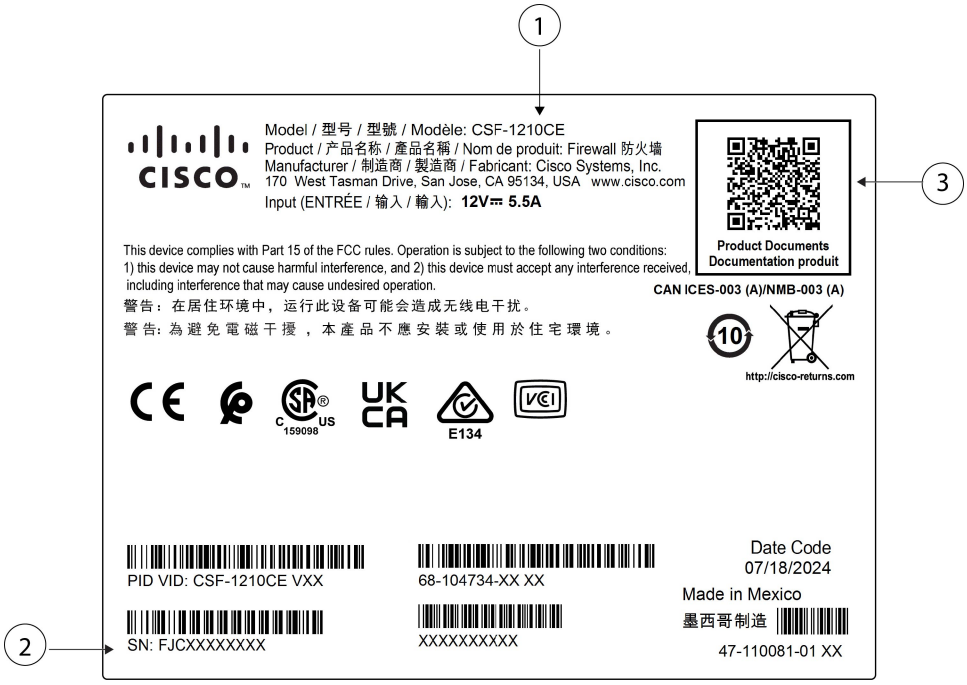


1	Kensington lock on left side of chassis (facing the front panel, non-I/O side)		—

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 getting started guide, the regulatory and compliance guide, the zero-touch provisioning guide, and the hardware installation guide.

The following figure shows an example compliance label found on the bottom of the chassis.

Figure 4: Compliance Label on the Chassis



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

Front Panel

The following figure shows the front panel of the Secure Firewall 1210CE, 1210CP, and 1220CX compact appliances. Note that there are no connectors or LEDs on the front panel.

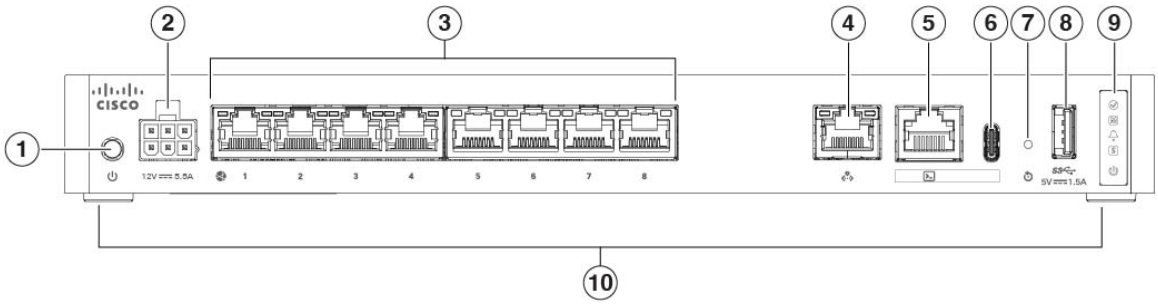
Figure 5: CSF-1210CE, CSF-1210CP, and CSF-1220CX Front Panel

Rear Panel

The following figures show the rear panels of the Secure Firewall 1210CE, 1210CP, and 1220CX compact appliances. See Rear Panel LEDs, on page 9 for a description of the LEDs.

The following figure shows the rear panel of the Secure Firewall 1210CE.

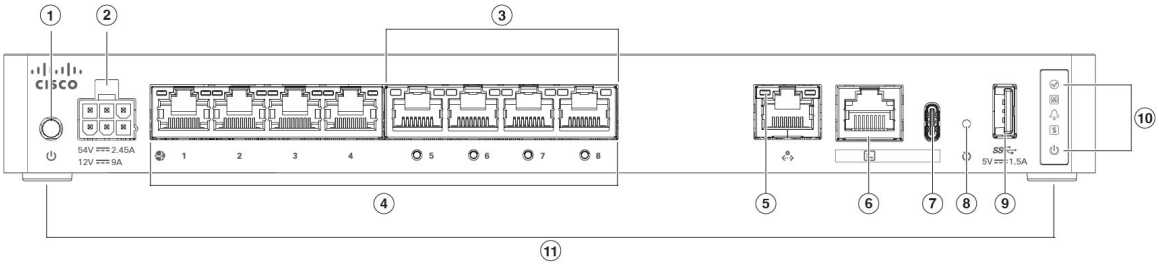
Figure 6: CSF-1210CE Rear Panel



1	Power button The power button is a two-position switch. When the switch is sticking out, it's in OFF state and when it is pushed in, it's in the ON state.	**2**	Power cord socket
3	Ethernet ports 1-8 1G/100M/10M Auto Duplex Auto MDI-X Base-T interfaces	**4**	Management port
5	Console port RJ-45	**6**	Console USB Type C port
7	Reset button	**8**	USB Type A port
9	Status LEDs	**10**	Rubber feet

The following figure shows the rear panel of the Secure Firewall 1210CP. See Rear Panel LEDs, on page 9 for a description of the LEDs.

Figure 7: CSF-1210CP Rear Panel

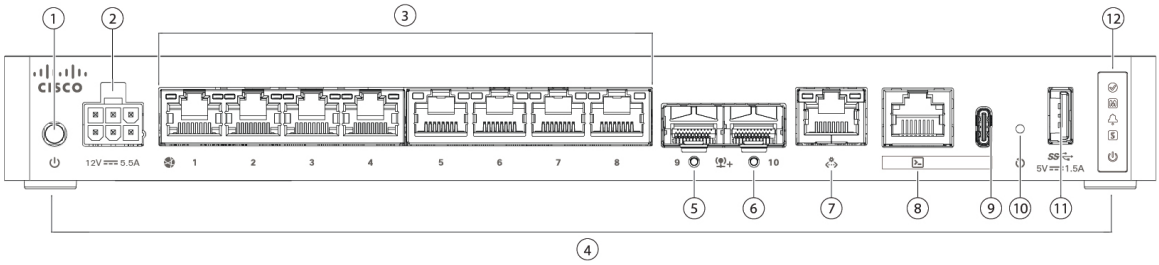


1	Power button The power button is a two-position switch. When the switch is sticking out, it's in OFF state and when it is pushed in, it's in the ON state.	**2**	Power cord socket
3	PoE Ethernet ports 5-8	**4**	Ethernet ports 1-8 1G/100M/10M Auto Duplex Auto MDI-X Base-T interfaces
5	Management port	**6**	Console port RJ-45

7	Console USB Type C port	**8**	Reset button
9	USB Type A port	**10**	Status LEDs
11	Rubber feet		—

The following figure shows the rear panel of the Secure Firewall 1220CX. See Rear Panel LEDs, on page 9 for a description of the LEDs.

Figure 8: CSF-1220CX Rear Panel



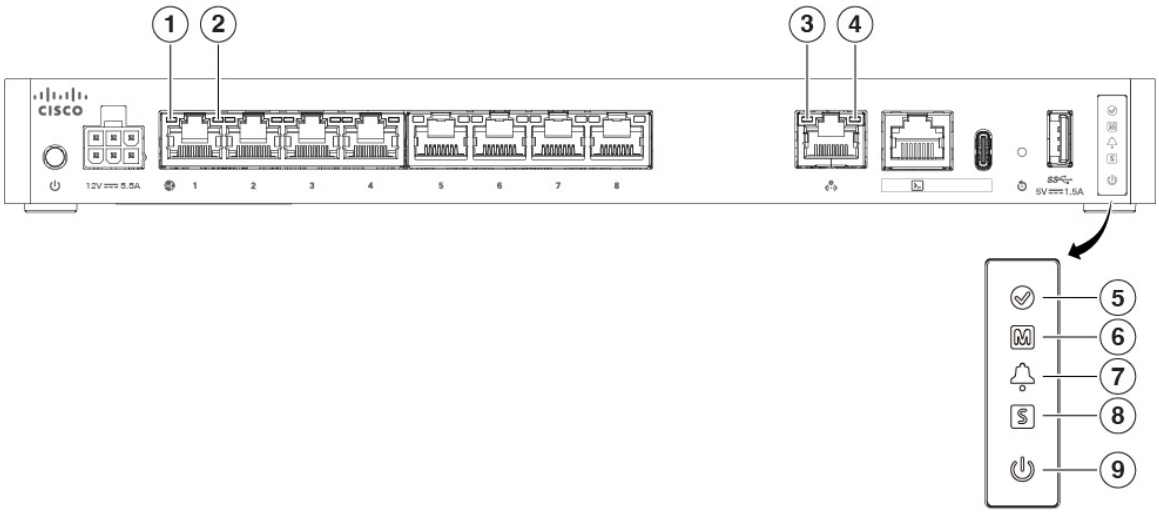
1	Power button The power button is a two-position switch. When the switch is sticking out, it's in OFF state and when it is pushed in, it's in the ON state.	**2**	Power cord socket
3	Ethernet ports 1-8 1G/100M/10M Auto Duplex Auto MDI-X Base-T interfaces	**4**	Rubber feet
5	Ethernet port 9 with SFP interface Supports 1-Gbps/10-Gbps SFPs	**6**	Ethernet port 10 with SFP interface Supports 1-Gbps/10-Gbps SFPs
7	Management port	**8**	Console port RJ-45
9	Console USB Type C port	**10**	Reset button
11	USB Type A port	**12**	Status LEDs

Rear Panel LEDs

The LEDs are found on the rear panel of the Secure Firewall 1210C, 1210CP, and 1220CX.

The following figure shows the LEDs on the rear panel of the Secure Firewall 1210C and describes their states.

Figure 9: CSF-1210C Rear Panel LEDs



1	**Network** Status of the network ports: Link status (L): • Off—No link, or port is not in use. • Green—Link established. • Green, flashing—Link activity.	**2**	**Network** Status of the network ports: Connection-speed status (S): • Green, flashing—One flash every three seconds = 10 Mbps. • Green, flashing—Two rapid flashes = 100 Mbps. • Green, flashing—Three rapid flashes = 1000 Mbps.
3	**Management** Status of the management ports: Link status (L): • Off—No link, or port is not in use. • Green—Link established. • Green, flashing—Link activity.	**4**	**Management** Status of the management ports: Connection-speed status (S): • Green, flashing—One flash every three seconds = 10 Mbps. • Green, flashing—Two rapid flashes = 100 Mbps. • Green, flashing—Three rapid flashes = 1000 Mbps.

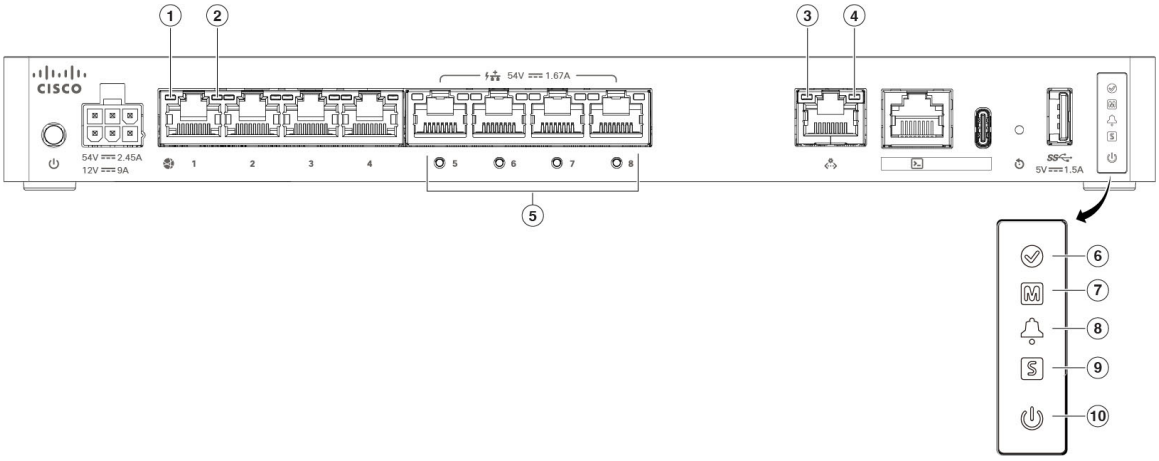
5	**Active** Status of the failover pair: • Off— Failover is not operational. • Green—Failover pair operating normally. The LED is green always unless the chassis in a high availability pair. • Amber—When the chassis is in a high availability pair, the LED is amber for the standby unit.	6	**Managed Status** • Green, flashing slowly (twice in 5 seconds)—Cloud is connected. • Green and amber, flashing—Cloud connection failure. • Green—Cloud is disconnected. **Note** The Security Cloud Control (SCC) LED pattern applies to zero-touch provisioning (ZTP). See the Easy Deployment Guide for Cisco Secure Firewall Threat Defense with Cisco Security Cloud Control for more information.

7	**Alarm Status**
	• Off—No alarms.
	• Amber—Environmental error.
	• Green—Status is ok.
		8	**Status**
			System operating status:
			• Off—System has not booted up yet.
			• Green, flashing quickly—System is booting up.
			• Green—Normal system function.
			• Amber—Critical alarm indicating one or more of the following:
			  • Major failure of a hardware or software component.
			  • Over-temperature condition.
			  • Power voltage outside the tolerance range.

9	**Power** Power supply status: • Off —Power supply off. • Green—Power supply on. • Green, flashing—System is in the process of a graceful shutdown. • Amber—System power is up, system firmware is updating (takes up to 3 minutes), or there is a power fault.		—

The following figure shows the LEDs on the rear panel of the Secure Firewall 1210CP and describes their states.

Figure 10: CSF-1210CP Rear Panel LEDs



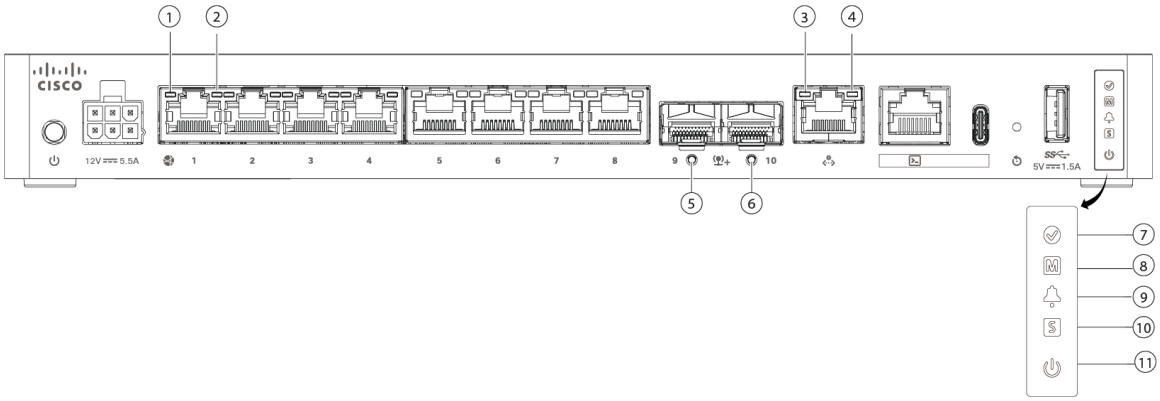
1	**Network** Status of the network ports: Link status (L): • Off—No link, or port is not in use. • Green—Link established. • Green, flashing—Link activity.	2	**Network** Status of the network ports: Connection-speed status (S): • Green, flashing—One flash every three seconds = 10 Mbps. • Green, flashing—Two rapid flashes = 100 Mbps. • Green, flashing—Three rapid flashes = 1000 Mbps.
3	**Management** Status of the management ports: Link status (L): • Off—No link, or port is not in use. • Green—Link established. • Green, flashing—Link activity.	4	**Management** Status of the management ports: Connection-speed status (S): • Green, flashing—One flash every three seconds = 10 Mbps. • Green, flashing—Two rapid flashes = 100 Mbps. • Green, flashing—Three rapid flashes = 1000 Mbps.

5	**PoE** Status of the PoE ports: • Off—No alarms. • Amber—The powered device is in power-deny state. • Amber, flashing —If the chassis is connected to an incompatible power supply, the LEDs of all 4 ports flash to show that the device has gone into fail-safe mode.	6	**Active** Status of the failover pair: • Off— Failover is not operational. • Green—Failover pair operating normally. The LED is green always unless the chassis in a high availability pair. • Amber—When the chassis is in a high availability pair, the LED is amber for the standby unit.
7	**Managed Status** • Green, flashing slowly (twice in 5 seconds)—Cloud is connected. • Green and amber, flashing—Cloud connection failure. • Green—Cloud is disconnected. **Note** The SCC LED pattern applies to ZTP. See the Easy Deployment Guide for Cisco Secure Firewall Threat Defense with Cisco Security Cloud Control for more information.	8	**Alarm Status** • Off—No alarms. • Amber—Environmental error. • Green—Status is ok.

9	**Status**
	System operating status:
	• Off—System has not booted up yet.
	• Green, flashing quickly—System is booting up.
	• Green—Normal system function.
	• Amber—Critical alarm indicating one or more of the following:
	  • Major failure of a hardware or software component.
	  • Over-temperature condition.
	  • Power voltage outside the tolerance range.
		10	**Power**
			Power supply status:
			• Off —Power supply off.
			• Green—Power supply on.
			• Green, flashing—System is in the process of a graceful shutdown.
			• Amber—System power is up, system firemware is updating (takes up to 3 minutes), or there is a power fault.

The following figure shows the LEDs on the rear panel of the Secure Firewall 1220CX and describes their states.

Figure 11: CSF-1220CX Rear Panel LEDs



1	**Network** Status of the network ports: Link status (L): • Off—No link, or port is not in use. • Green—Link established. • Green, flashing—Link activity.	**2**	**Network** Status of the network ports: Connection-speed status (S): • Green, flashing—One flash every three seconds = 10 Mbps. • Green, flashing—Two rapid flashes = 100 Mbps. • Green, flashing—Three rapid flashes = 1000 Mbps.
3	**Management** Status of the management ports: Link status (L): • Off—No link, or port is not in use. • Green—Link established. • Green, flashing—Link activity.	**4**	**Management** Status of the management ports: Connection-speed status (S): • Green, flashing—One flash every three seconds = 10 Mbps. • Green, flashing—Two rapid flashes = 100 Mbps. • Green, flashing—Three rapid flashes = 1000 Mbps.
5	**SFP** Status of the SFP: • Off—No SFP plugged in or no laser. • Green—Link is established. • Green, flashing—Link activity. • Amber—No link or network failure.	**6**	**SFP** Status of the SFP: • Off—No SFP plugged in or no laser. • Green—Link is established. • Green, flashing—Link activity. • Amber—No link or network failure.

7	**Active** Status of the failover pair: • Off— Failover pair is in standby mode. • Green—Failover pair is in active mode and operating normally.	8	**Managed Status** • Green, flashing slowly (twice in 5 seconds)—Cloud is connected. • Green and amber, flashing—Cloud connection failure. • Green—Cloud is disconnected. **Note** The SCC LED pattern applies to ZTP. See the Easy Deployment Guide for Cisco Secure Firewall Threat Defense with Cisco Security Cloud Control for more information.

9	**Alarm Status**
	• Off—No alarms.
	• Amber—Power supply, fan, or PoE failure.
		10	**Status**
			System operating status:
			• Off—System is powered off.
			• Green, flashing—System is booting up.
			• Green—Normal system function.
			• Amber—System book issue.
			• Amber, flashing—Alarm or secure book failure.
			  • Major failure of a hardware or software component.
			  • Over-temperature condition.
			  • Power voltage outside the tolerance range.

11	**Power** Power supply status: • Off —Power supply off. • Green—Power supply on. • Green, flashing—System is in the process of a graceful shutdown. • Amber—System power is up, system firmware is updating (takes up to 3 minutes), or there is a power fault.		—

Hardware Specifications

The following table contains hardware specifications for the Secure Firewall 1210CE, 1210CP, and 220CX.

Table 2: CSF-1210CE, CSF-1210CP, and CSF-1220CX Hardware Specifications

Specification	CSF-1210CE	CSF-1210CP	CSF-1220CX
Chassis dimensions (H x W x D)	1.17 x 10.8 x 6.8 inches 2.819 x 27.432 x 17.272 cm **Note** Excludes rubber feet		
Chassis weight	3.04 lb (1.38 kg)	3.17 lb (1.44 kg)	3.09 lb (1.40 kg)
Rack shelf dimensions (H x W x D)	1.7 x 17.3 x 15.7 inches 4.318 x 43.942 x 39.878 cm		
System power	40 W maximum power 32 W typical power		
Temperature	Operating: 32 to 104°F (0 to 40°C) Derate the maximum operating temperature 2.7° F (1.5° C) per 1000 ft (304.8 m) above 6,000 ft (1828.8 m) altitude. Nonoperating: -13 to 158°F (-25 to 70°C) Nonoperating: Maximum altitude is 15,000 ft (4570 m)		
Humidity	Operating: 5 to 85% (noncondensing) Nonoperating:5 to 95% (noncondensing)		
Altitude	Operating: 0 to 10,000 ft (3048 m) Nonoperating: 0 to 15,000 ft (4570 m)		
Acoustic noise	23.5 dBA @ 80.6°F/27°C 42.7 dBA @ maximum fan speed		

Supported SFP/SFP+/QSFP+ Transceivers

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

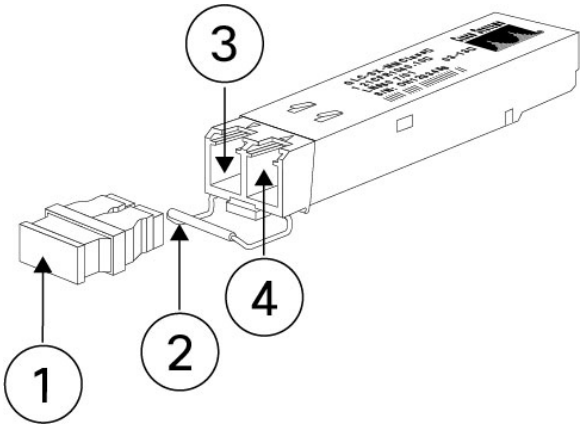
The 1-Gbps and 10-Gbps transceivers are supported on the fixed ports for the following models and software versions:

- CSF-1210CE, CSF-1210CP, CSF-1220CX
- Threat defense Version 7.6 and ASA Version 9.22.1.

See Cisco SFP Modules for Gigabit Ethernet Applications Data Sheet for more information.

The following figure shows the components of a transceiver.

Figure 12: SFP Transceiver



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

Safety Warnings

Take note of the following warnings:

Warning

Statement 1055—Class 1/1M Laser

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

Warning

Statement 1056—Unterminated Fiber Cable

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

Warning **Statement 1057—**Hazardous Radiation Exposure

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

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

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

The following table lists the supported 1-Gbps transceivers for the fixed ports (not supported for management port).

Table 3: Supported 1-Gbps SFP Transceivers

Optics Type	PID	Medium	Operating Wavelength (nm)	Maximum Operating Distance
1000Base-T	GLC-T	Cat 5e	—	328 ft (100 m)
1000Base-T	GLC-TE	Cat 5e	—	328 ft (100 m)
Multimode	GLC-SX-MMD	multimode	850	1804 ft (550 m)[1]
Single mode	GLC-LH-SMD	single mode	1310	32,821 ft (10 km)
SM extended	GLC-EX-SMD	single mode	1310	131, 234 ft (40 km)
SM	GLC-ZX-SMD	single mode	1550	229,659 ft (70 km)[2]

1 Depending on fiber grade and core size, operating distance may vary.
2 Depending on fiber grade and core size, operating distance may vary.

The following table lists the supported transceivers for the fixed ports (not supported for the management port).

Table 4: Supported 10-Gbps SFP Transceivers

Optics Type	PID	Medium	Operating Wavelength (nm)	Maximum Operating Distance
10G-SR	SFP-10G-SR	multimode	850	984 ft (300 m)[3]
10G-SR	SFP-10G-SR-S	multimode	1310	984 ft (300 m)

Optics Type	PID	Medium	Operating Wavelength (nm)	Maximum Operating Distance
10G-LR	SFP-10G-LR	single mode	1310	32,821 ft (10 km)
10G-LR	SFP-10G-LR-S	single mode	850	32,821 ft (10 km)
10G-ER	SFP-10G-ER	single mode	850	131,234 ft (40 km)
10G-ER	SFP-10G-ER-S	single mode	1310	131,234 ft (40 km)
10G-ZR	SFP-10G-ZR	single mode	1550	131,234 ft (40 km)
10G-ZR	SFP-10G-ZR-S	single mode	1550	262,467 ft (80 km)
10G DAC copper	SFP-H10GB-CUxM Length 1, 1.5, 2, 2.5, 3, 4, 5 m	Twinax cable, passive	—	—
10G DAC CU active	SFP-H10GB-ACUxM Length 7, 10 m	Twinax cable, active	—	—
10G AOC	SFP-10G-AOCxM Length 1, 2, 3, 5, 7, 10 m	Active optical cable	—	—

[3] Depending on fiber grade and core size, operating distance may vary.

Product ID Numbers

The following table lists the field-replaceable PIDs associated with the Secure Firewall 1210CE, 1210CP, and 1220CX compact appliances. The spare components are ones that you can order separately from the appliance. If any internal components fail, you must get a return material authorization (RMA) for the entire chassis. See the Cisco Returns Portal for more information.

Note See the **show inventory** command in the Cisco Secure Firewall Threat Defense Command Reference or the Cisco Secure Firewall ASA Series Command Reference to display a list of the PIDs for your Secure Firewall 1210CE, 1210CP, and 1220CX.

Table 5: CSF-1210CE, CSF-1210CP, and CSF-1220CX PIDs

PID	Description
CSF1210CE-ASA-K9	Secure Firewall 1210CE compact desktop appliance, ASA
CSF1210CP-ASA-K9	Secure Firewall 1210CP PoE compact desktop appliance, ASA

PID	Description
CSF1220CX-ASA-K9	Secure Firewall 1220CX compact desktop appliance, ASA
CSF1210CE-TD-K9	Secure Firewall 1210CE compact desktop appliance, NGFW
CSF1210CP-TD-K9	Secure Firewall 1210CP PoE compact desktop appliance, NGFW
CSF1220CX-TD-K9	Secure Firewall 1220CX compact desktop appliance, NGFW
CSF1200C-PWR-AC	Secure Firewall 1210CE and 220CX 66-W AC (12 V) power supply
CSF1200C-PWR-AC=	Secure Firewall 1210CE and 1220CX 66-W AC (12 V) power supply (spare)
CSF1200CP-PWR-AC	Secure Firewall 1210CP 230-W AC power supply (110 W of 12 V and 120 W of -53.5 V)
CSF1200CP-PWR-AC=	Secure Firewall 1210CP 230-W AC power supply (110 W of 12 V and 120 W of -53.5 V) (spare)
CSF1200C-RACK-MNT=	Secure Firewall 1210CE, 1210CP, 1220CX rack-mount kit (spare)
CSF1200C-WALL-MNT=	Secure Firewall 1210CE, 1210CP, 1220CX wall-mount kit (spare)

Power Cord Specifications

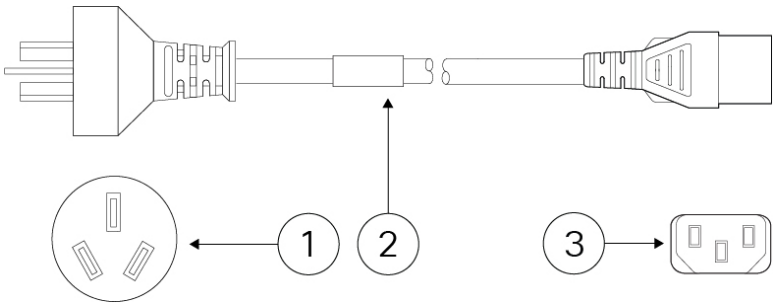
Standard power cords or jumper power cords are available for connection to the security appliance. The jumper power cords for use in racks are available as an optional alternative to the standard power cords.

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

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

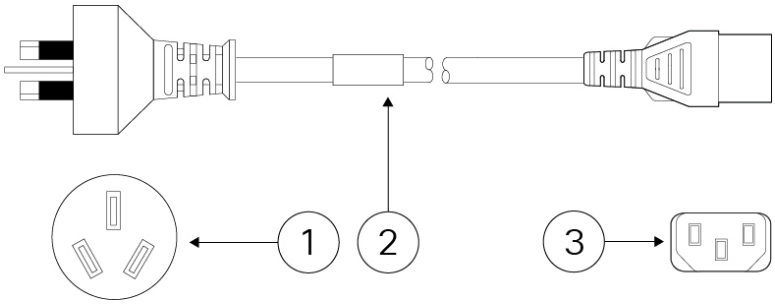
The following power cords are supported.

Figure 13: Argentina (CAB-ACR)



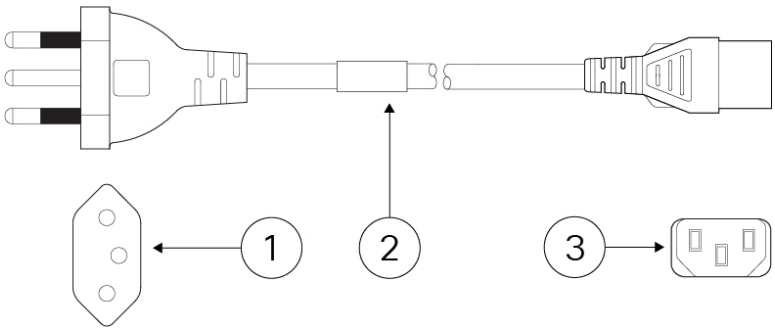
1	Plug: VA2073	**2**	Cord set rating: 10 A, 250 V
3	Connector: V1625		Cord length: 2.5 m

Figure 14: Australia/New Zealand (CAB-ACA)



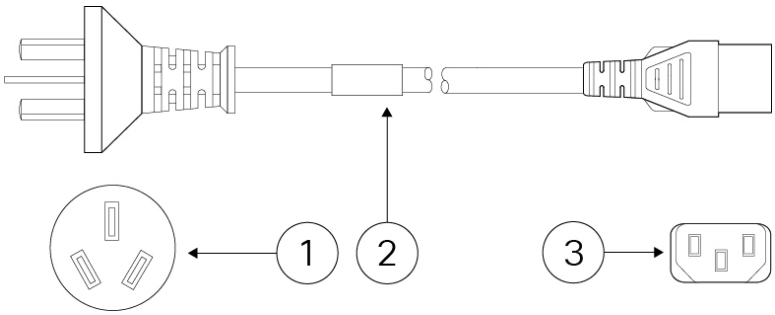
1	Plug: AU10LS3	**2**	Cord set rating: 10 A, 250 V
3	Connector: V1625		Cord length: 2.5 m

Figure 15: Brazil (CAB-C13-ACB)



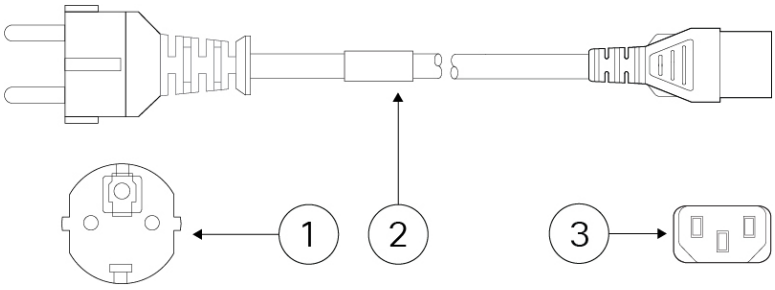
1	Plug: NBR 14136	**2**	Cord set rating: 10 A, 250 V
3	Connector: EL 701B (EN 60320/C13)		Cord length: 2.1 m

Figure 16: China (CAB-ACC)



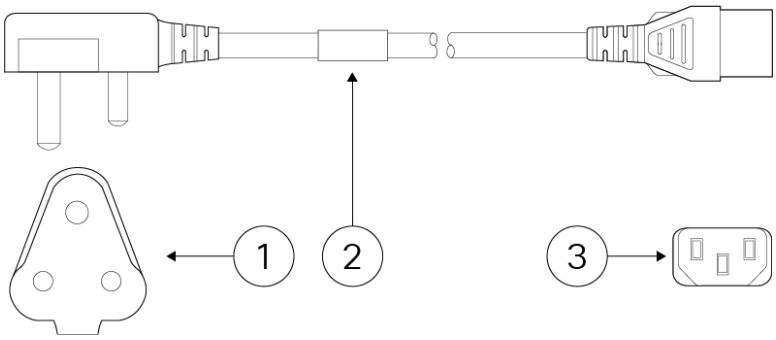
1	Plug: V3203C	**2**	Cord set rating: 10 A, 250 V
3	Connector: V1625		Cord length: 2.5 m

Figure 17: Europe (CAB-ACE)



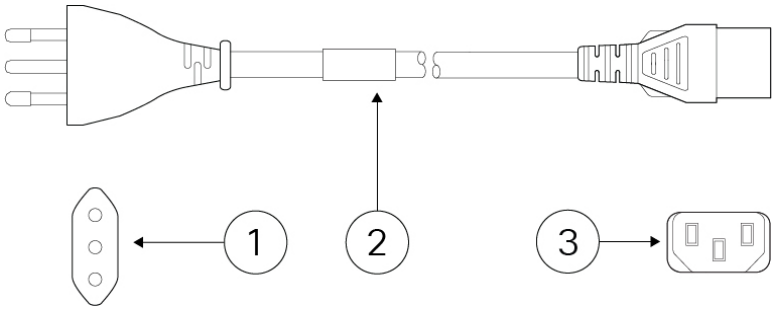
1	Plug: M2511	**2**	Cord set rating: 16 A, 250 V
3	Connector: V1625		Cord length: 1.5 m

Figure 18: India (CAB-IND-10A)



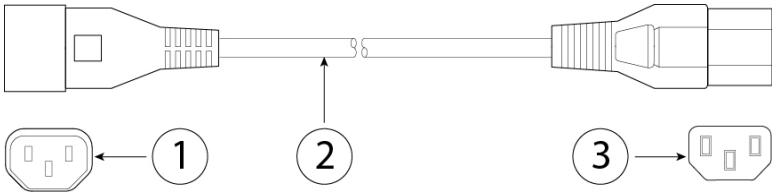
1	Plug: IA16A3-C	**2**	Cord set rating: 16 A, 250 V
3	Connector: V1625BS-E		—

Figure 19: Italy (CAB-ACI)



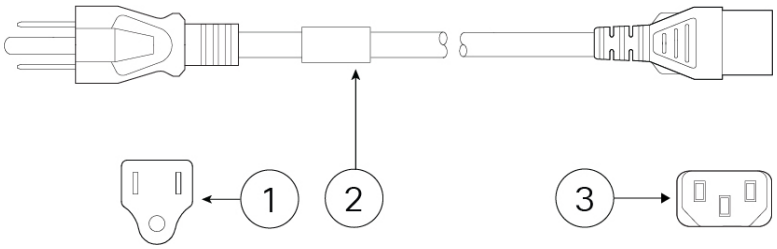
1	Plug: IT10S3	**2**	Cord set rating: 10 A, 250 V
3	Connector: V1625		Cord length: 2.5 m

Figure 20: Japan (CAB-C13-C14-2M-JP) PSE Mark



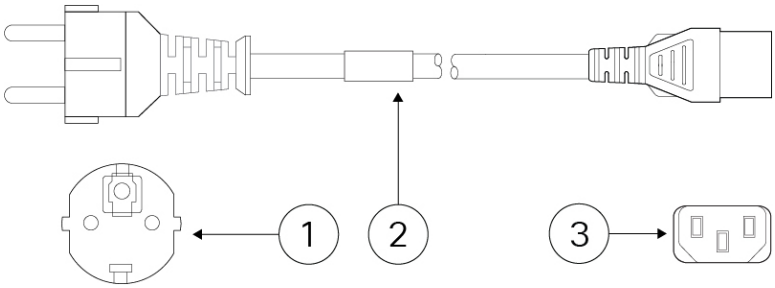
1	IEC 60320-2-2/E	**2**	Cord set rating: 10 A, 250 V
3	Connector: IEC 60320/C13		Cord length: 2 m

Figure 21: Japan (CAB-JPN-3PIN)



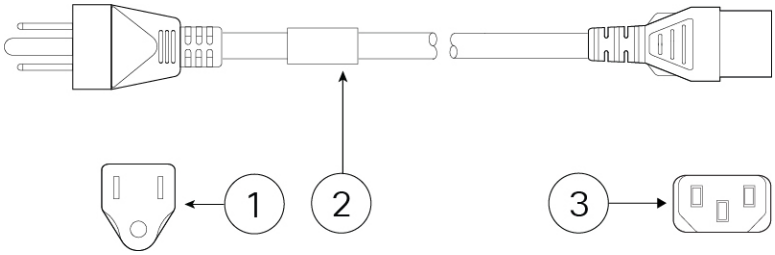
1	Plug: M744	**2**	Cord set rating: 12 A, 125 V
3	Connector: V1625		—

Figure 22: Korea (CAB-AC-C13-KOR)



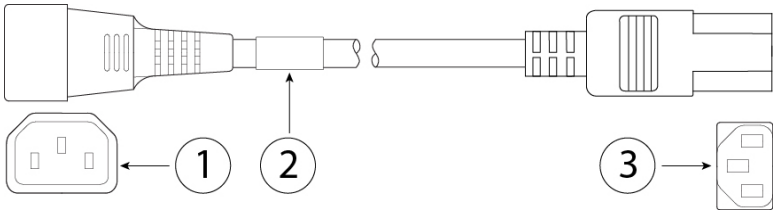
1	Plug: M2511	**2**	Cord set rating: 10 A, 250 V
3	Connector: V1625		—

Figure 23: North America (CAB-AC)



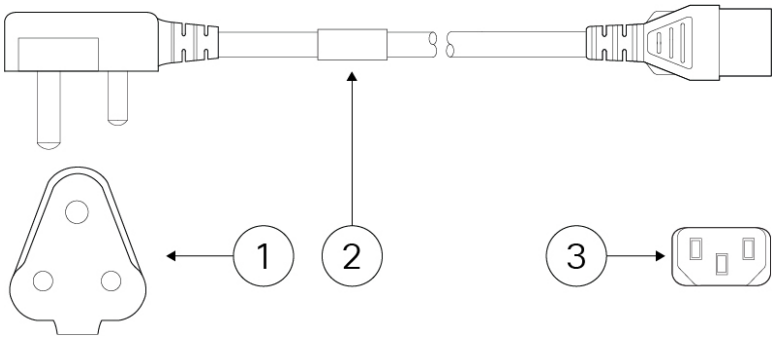
1	Plug: PS204	**2**	Cord set rating: 10 A, 250 V
3	Connector: V1625		—

Figure 24: Jumper (CAB-C13-C14-2M)



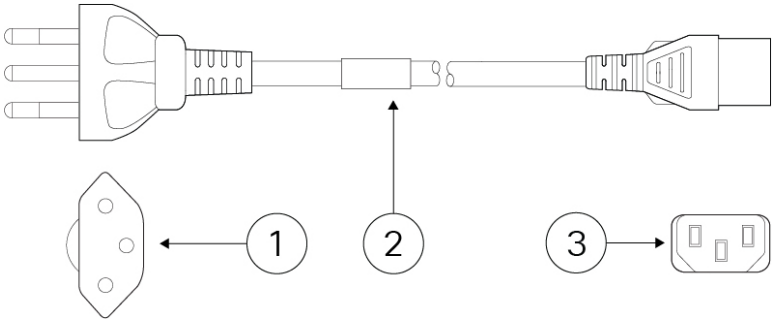
1	IEC 60320/C14G	**2**	Cord set rating: 10 A, 250 V
3	Connector: IEC 60320/C13		Cord length: 2.5 m

Figure 25: South Africa (AIR-PWR-CORD-SA)



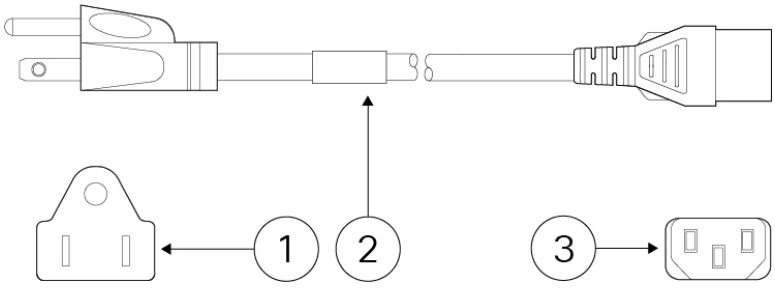
1	Plug: SA16A	**2**	Cord set rating: 10 A, 250 V
3	Connector: V1625		—

Figure 26: Switzerland (CAB-ACS)



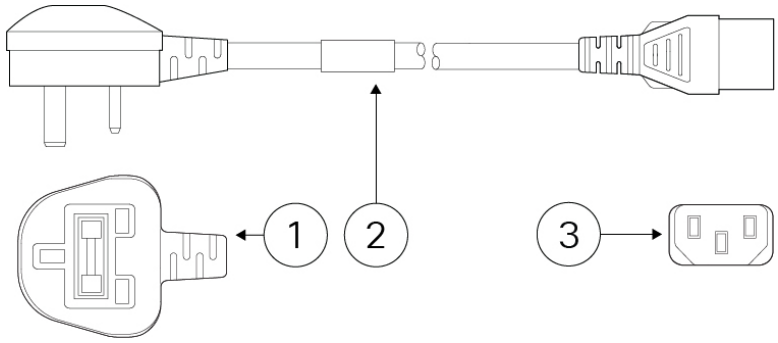
1	Plug: SW10ZS3	**2**	Cord set rating: 10 A, 250 V
3	Connector: V1625		—

Figure 27: Taiwan (CAB-ACTW)

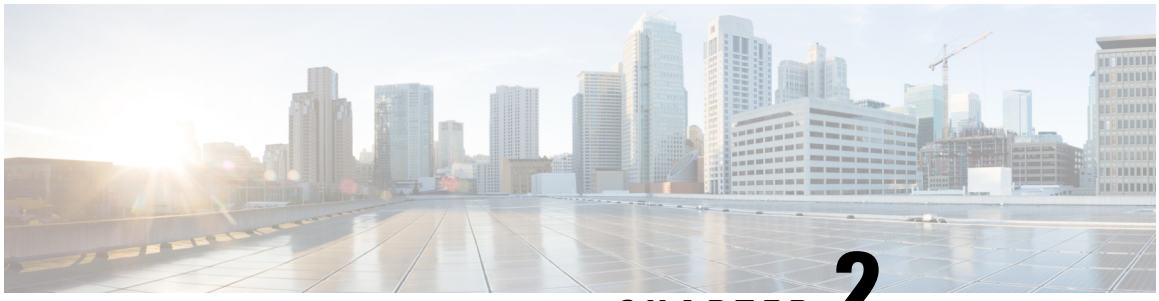


1	Plug: EL 302 (CNS10917)	**2**	Cord set rating: 10 A, 125 V
3	Connector: EL 701 (EN 60320/C13)		—

Figure 28: United Kingdom (CAB-ACU)



1	Plug: 3P BS 1363	**2**	Cord set rating: 10 A, 250 V
3	Connector: IEC 60320/C13		—



CHAPTER 2

Installation Preparation

Installation Warnings

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

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: 20 A, 120 V, and 16 A, 250 V

Warning **Statement 1008—**Class 1 Laser Product

This product is a Class 1 laser product.

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 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 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 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.

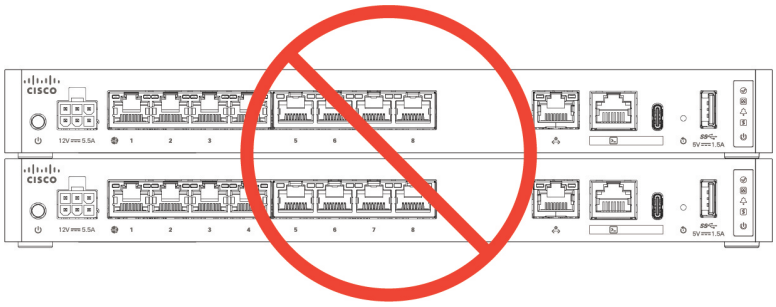
Warning **Statement 9001**—Product Disposal

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

Position the Chassis

See Desktop-Mount the Chassis, on page 34 for information on desktop-mounting the chassis.

Figure 29: Do Not Stack the Chassis



Caution Do not stack the chassis on top of another chassis. If you stack the units, they will overheat, which causes the units to power cycle.

Whether positioning the chassis on a desktop, on a closet shelf, or mounting it on a wall, consider the following:

- Be sure to choose an area where the chassis is out of the way to make sure it is not bumped or accidentally dislodged. The chassis has feet on the bottom so it does not sit flush where placed, thus allowing proper air circulation through and around it. Make sure that the chassis is not tightly enclosed or crowded by other objects that might impede proper circulation.
- Choose a location that lets you easily bring the power cord and Ethernet and console cables to the chassis, with plenty of slack and yet tucked away, so they cannot be inadvertently unplugged.

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 and Compliance Information document before installing the chassis.

Follow these guidelines when working on equipment powered by electricity:

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

Prevent ESD Damage

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

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

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

Site Environment

See Hardware Specifications, on page 16 for information about physical specifications.

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

Site Considerations

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

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

Power Supply Considerations

When installing the chassis, consider the following:

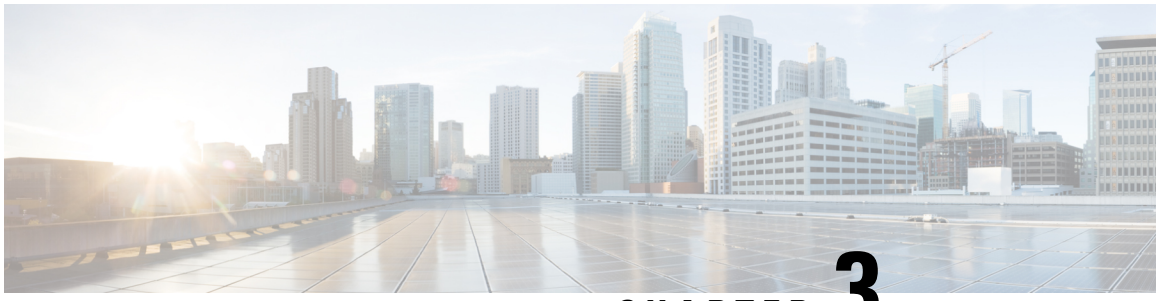
- Check the power at the site before installing the chassis to ensure that it is free of spikes and noise. Install a power conditioner, if necessary, to ensure proper voltages and power levels in the appliance-input voltage.
- Install proper grounding for the site to avoid damage from lightning and power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

Rack Configuration Considerations

See Rack-Mount the Chassis, on page 37 for the procedure for rack-mounting the chassis.

Consider the following when planning a rack configuration:

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



CHAPTER 3

Mount the Chassis

Unpack and Inspect the Chassis

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

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

Procedure

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

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

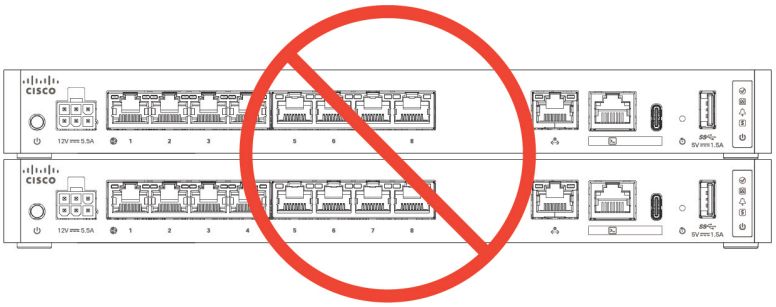
Step 3 Check for damage and report any discrepancies or damage to your customer service representative. Have the following information ready:

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

Desktop-Mount the Chassis

You can mount the chassis on a desktop by placing it on a desk in a horizontal position. To prevent interference with the airflow through the system, make sure there are no blockages or obstructions within 2 inches of the intake and exhaust sides. Do not remove the rubber feet included with the chassis. They are also needed for proper cooling.

Figure 30: Desk-Top Mount the Chassis



Caution Do not stack one chassis on top of another chassis. If you stack the units, they overheat, which causes the units to power cycle.

What to do next

Install the cables according to your default software configuration as described in the Cisco Secure Firewall 1210/20 Threat Defense Getting Started Guide.

Wall-Mount the Chassis

You can purchase an optional wall-mount kit. You can wall-mount the chassis left-, or rear panel-side up. You can use the wall-mount bracket to mark the holes for mounting it on the wall. The wall-mount bracket is 8.9 x 6.5 x 0.378 inches (22.672 x 16.512 x .96 cm). You need to make two level marks on the wall where you want to hang the chassis. For vertical orientation (rear panel up), the holes should be 5.575 inches (14.160 cm) inches apart. For horizontal orientation, the holes should be 8 inches (20.32 cm) apart.

The wall-mount kit contains the following items:

- Wall-mount bracket
- Three Phillips M3 x 0.5 x 5.2-mm screws
- Two Phillips #6 x 1¼-inch screws
- One #8 wall anchor kit with screws

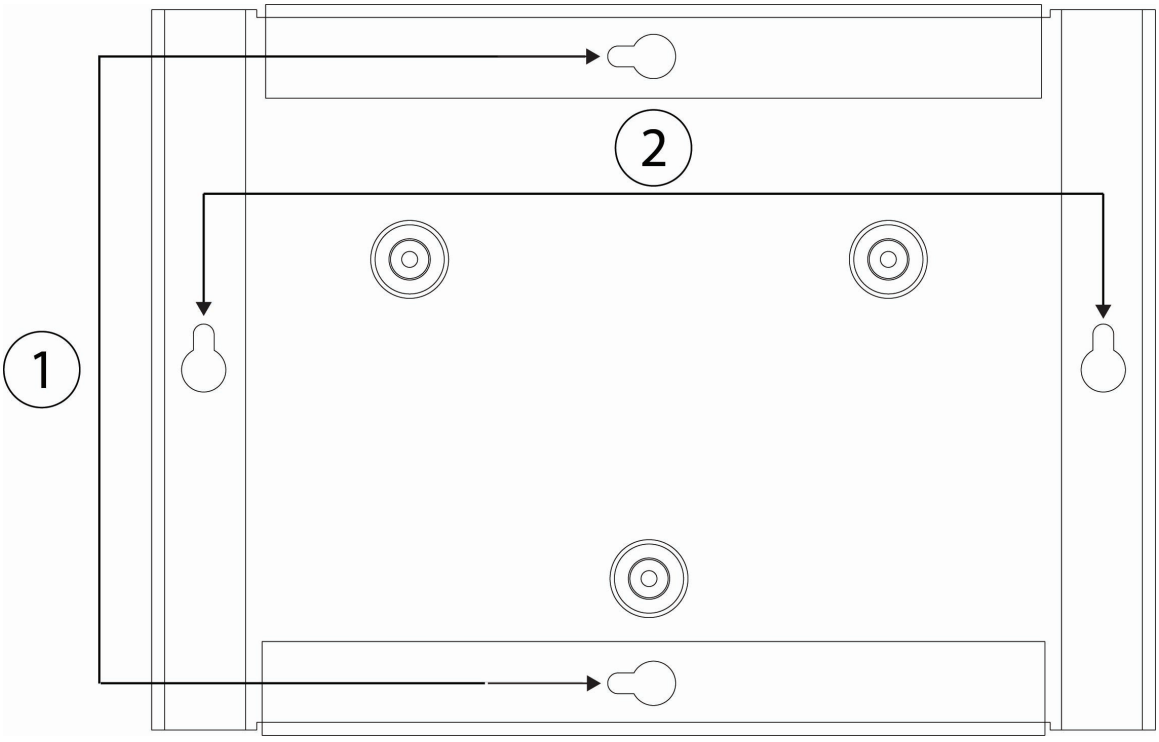
Follow these steps to mount your chassis on a wall.

Procedure

Step 1 Choose an orientation (left-, right-, or rear panel-side up) and a location on the wall for the chassis.

Step 2 Use a pencil, ruler, and level to mark locations for the two mounting screws (#6 x 1¼ inch). You can use the wall-mount bracket itself to mark either the top holes or the side holes.

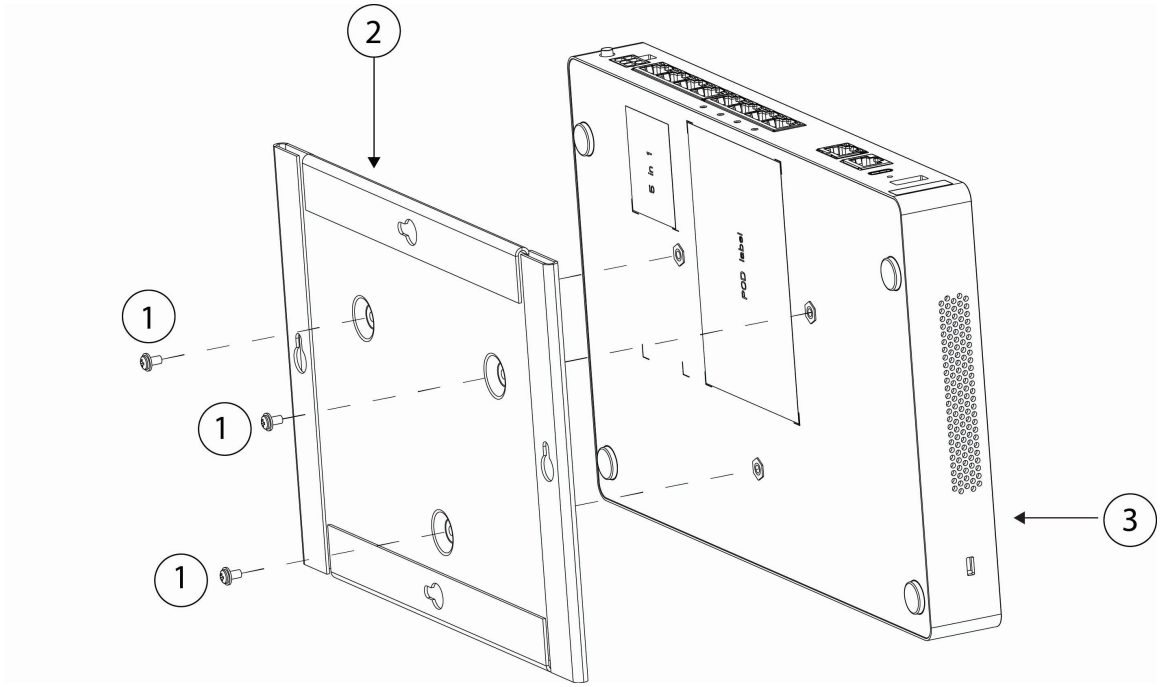
Figure 31: Wall-Mount Bracket



1	Horizontal mounting	**2**	Vertical mounting

Step 3 Attach the wall-mount bracket to the chassis using the three Phillips M3 x 0.5 x 5.2-mm screws.

Figure 32: Attach the Wall-Mount Bracket to the Chassis



1	Three Phillips M3 x 0.5 x 5.2-mm screws	**2**	Wall-mount bracket
3	Bottom of the chassis		—

Step 4 Use the two #6 x 1¼-inch screws to drill into a stud, or use the anchors (#8 wall screw) from the dry-wall kit to hang it into dry wall.

If you are mounting the chassis onto something other than drywall, such as wood or sheet metal, anchors may not be required.

Step 5 Drill a hole into the wall at each mark that you made in Step 2.

These holes should be slightly smaller in diameter than anchors if you are using them. The recommended drill hole size is 3/16 inches.

Step 6 Insert the anchors into the holes if needed, and be sure they are properly seated.

Step 7 Fasten each screw into its anchor until it protrudes about ¼ inch.

Step 8 Pick up the chassis, align the screws in the anchors with the holes in the bottom of the wall-mount bracket, move the chassis toward the wall until the screw heads are in the wall-mount bracket, and then slide it down until it rests on the screws.

Caution
Do not mount the chassis with the rear panel facing downward. This orientation is not supported.

Step 9 To uninstall the chassis from the wall mount, slide the wall-mounted chassis from the wall, and remove the three screws from the bottom of the chassis.

What to do next

Install the cables according to your default software configuration as described in the Cisco Secure Firewall 1210/20 Threat Defense Getting Started Guide.

Rack-Mount the Chassis

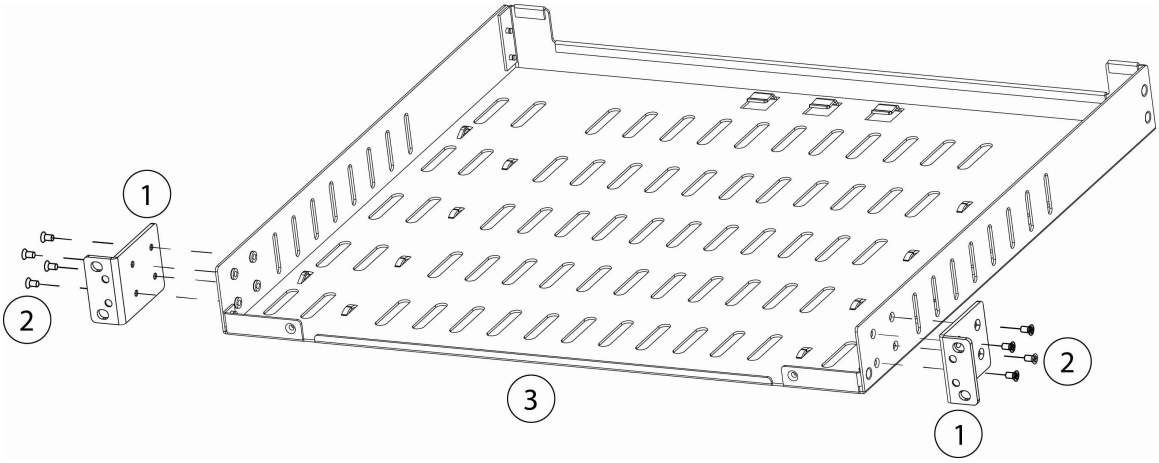
You can mount the chassis into a 1-RU space in a 19-inch EIA rack using the rack-mount shelf. The rack-mount shelf is 1.72 x 18.97 x 16.09 inches (H x W x D) (4.368 x 48.1838 x 40.8686 cm). The rack-mount kit contains the following items:

- Rack shelf
- Sliding rack tray
- Two rack-mount brackets
- Two rack-mount screws that you supply to install the sliding rack tray/shelf into your rack.
- Eight Phillips 6-32 x 25-inch screws; use these screws to secure the brackets to the rack shelf.
- Four Phillips 12-24 x 0.75-inch screws; use these screws to secure the sliding-rack tray to the chassis.

Procedure

Step 1 Install the rack-mount brackets on the rack-shelf tray.

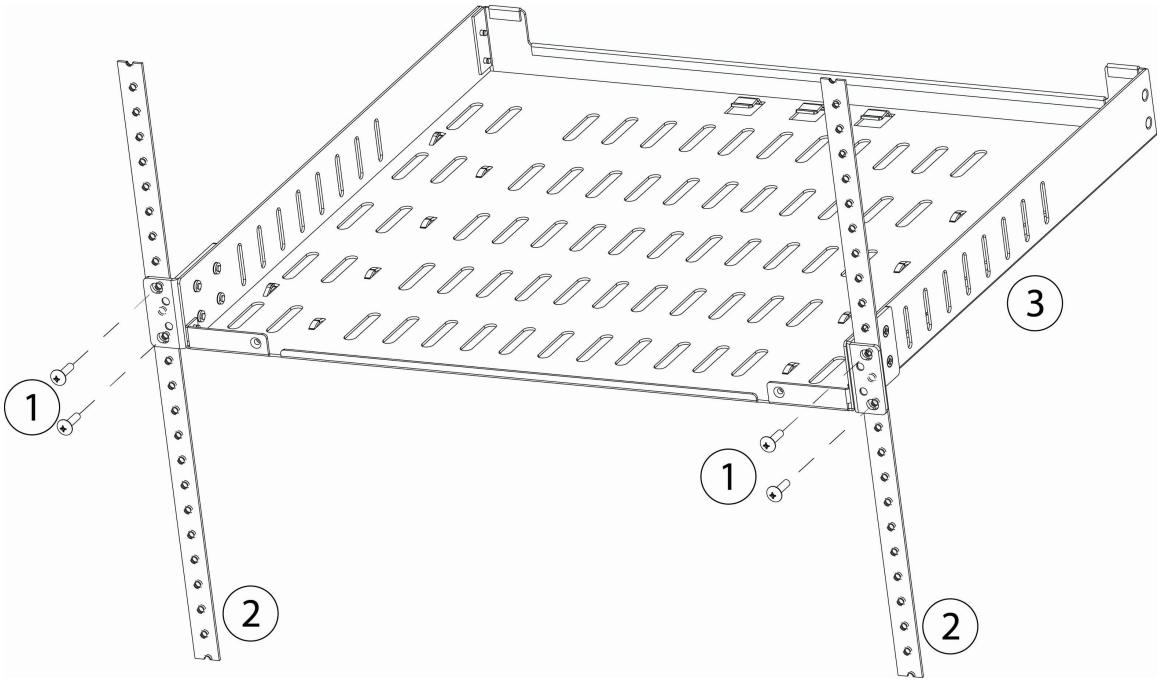
Figure 33: Install the Rack-Mount Brackets onto the Rack Shelf



1	Rack-mount bracket	**2**	Four Phillips 6-32 x 25-inch screws for each rack-mount bracket
3	Rack shelf	**4**	—

Step 2 Install the rack shelf into the rack.

Figure 34: Install the Rack Shelf into the Rack

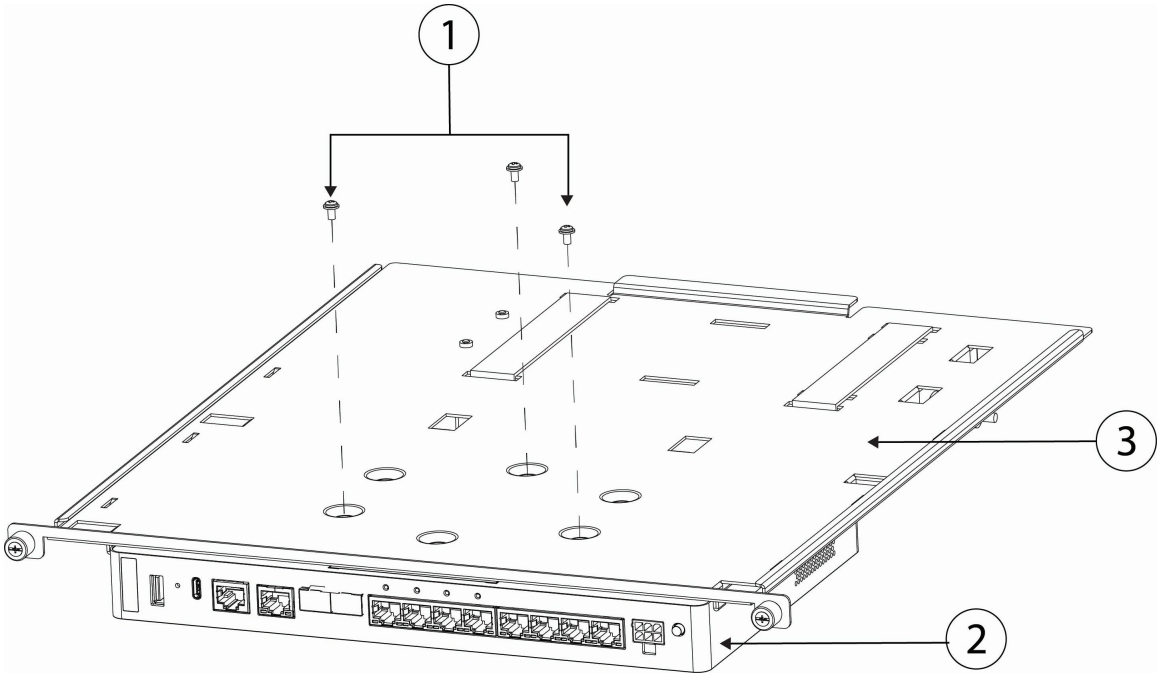


1	Rack screws (you supply the screws that fit your rack)	**2**	Rack
3	Rack shelf	**4**	—

Step 3 Place the chassis with the top facing down on a large, stable work area.

Step 4 Invert the sliding rack tray and position it on the chassis. You can mount the chassis with the front or rear panel facing front.

Figure 35: Install the Sliding Rack Tray on the Chassis



1	Three Phillips M3 x 0.5 x 5.2-mm screws	**2**	Chassis with rear panel facing (I/O side) **Note** You can also install the chassis with the front panel facing
3	Sliding rack tray		—

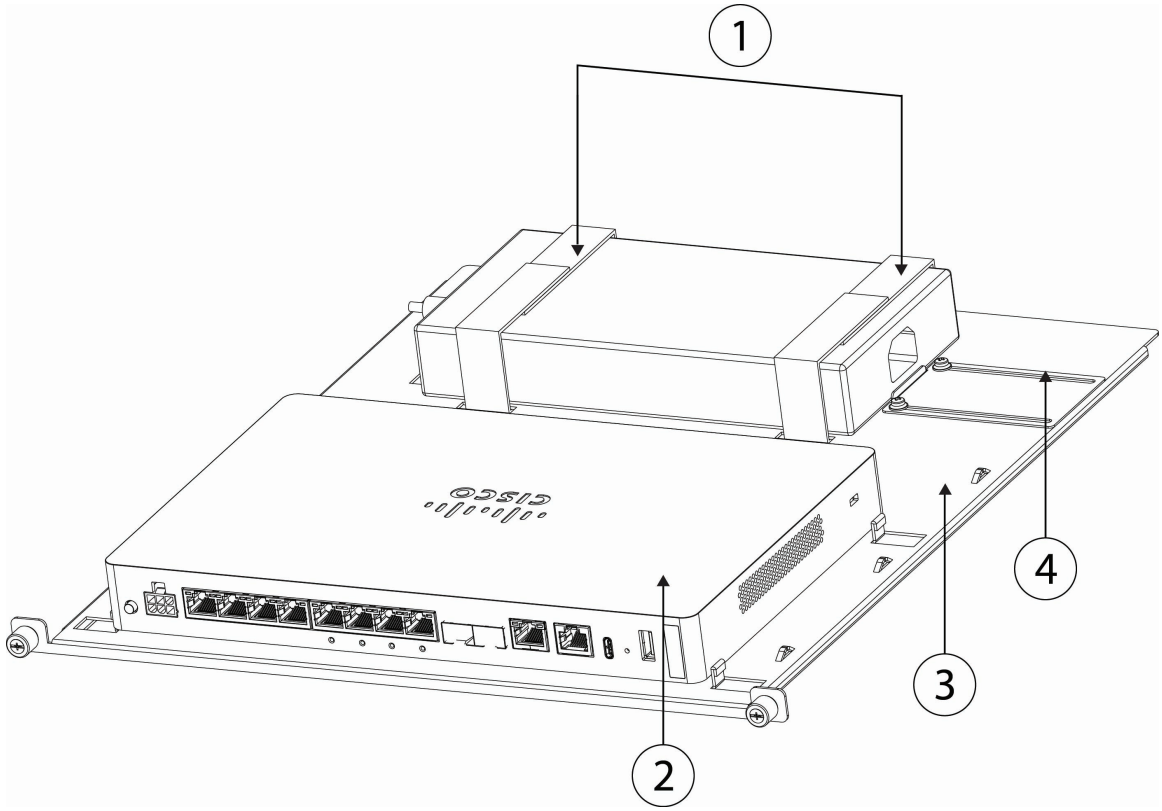
Step 5 Adjust the position of the chassis and the sliding rack tray until the three mounting holes in the dimples in the bottom of the sliding rack tray are aligned with the mounting holes in the bottom of the chassis.

Step 6 Tighten the three Phillips M3 x 0.5 x 5.2-mm screws to lock the chassis into place on the sliding rack tray (see the figure above).

Step 7 Carefully turn the sliding rack tray right-side up.

Step 8 Install the power supply in the sliding rack tray behind the chassis and tighten the Velcro straps to fit.

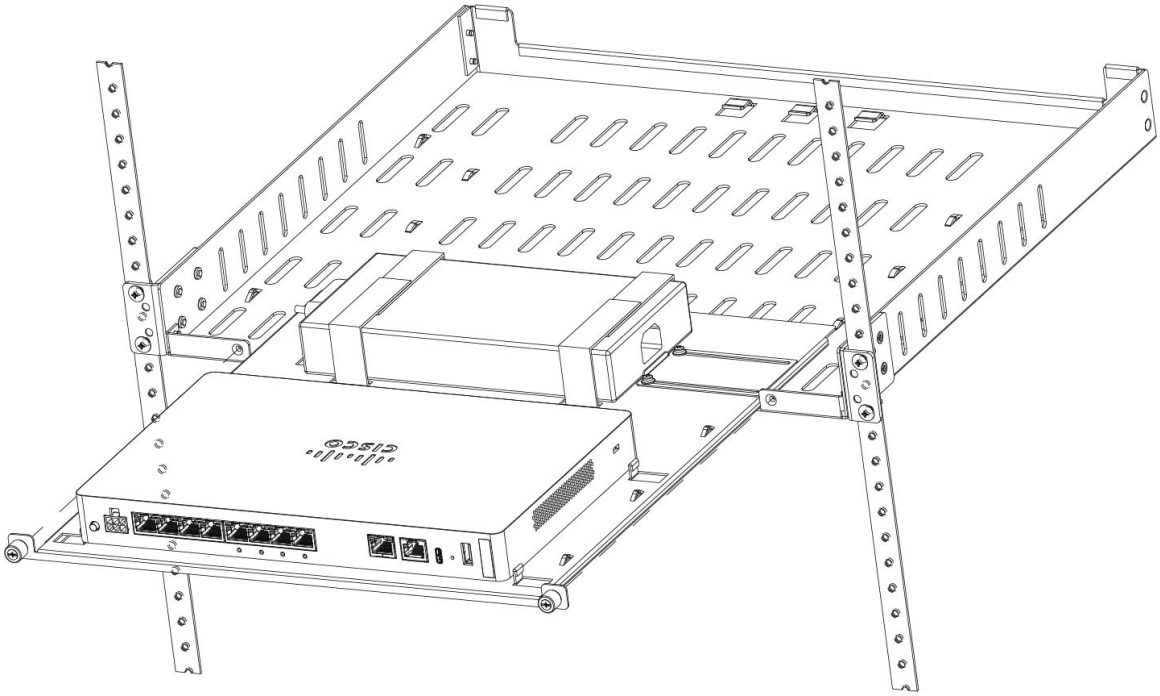
Figure 36: Install the Power Supply in the Sliding Rack Tray and Tighten the Velcro Straps



1	Power supply with Velcro straps	**2**	Chassis
3	Sliding rack tray	**4**	Slider to fix different size power supplies

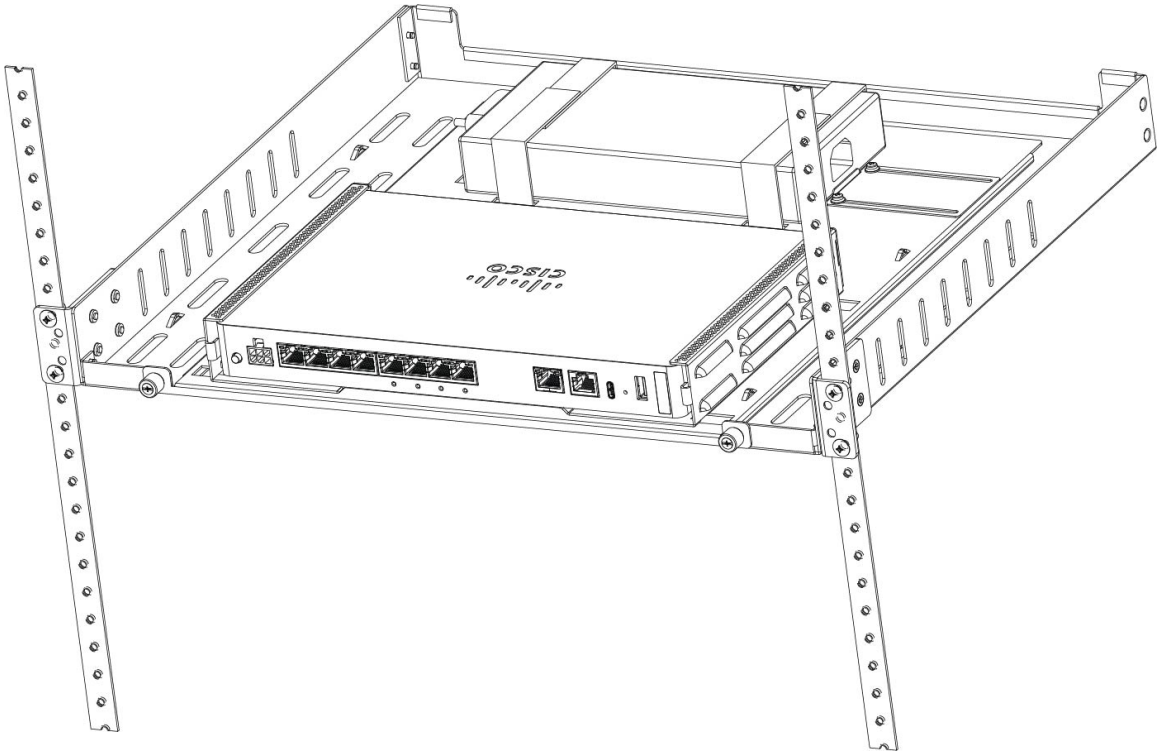
Step 9 Slide the sliding rack tray into the rack shelf.

Figure 37: Slide the Sliding Rack Tray Into the Rack Shelf



Step 10 The chassis is now installed in the sliding rack tray, which is installed in the rack shelf.

Figure 38: Sliding Rack Tray Installed in Rack Shelf



What to do next

Install the cables according to your default software configuration as described in the Cisco Secure Firewall 1210/20 Threat Defense Getting Started Guide.