



Removing and Installing Interface Cards in Cisco IPS-4260 and IPS 4270-20

This document describes the IPS interface cards and how to install them in IPS-4260 and IPS 4270-20. It contains the following sections:

- [Electrical Safety Guidelines, page 1](#)
- [Working in an ESD Environment, page 2](#)
- [Supported Interface Cards, page 3](#)
- [Hardware and Software Requirements, page 5](#)
- [Hardware Bypass, page 5](#)
- [Installing Interface Cards in IPS-4260, page 7](#)
- [Installing Interface Cards in IPS 4270-20, page 11](#)
- [Related Documentation, page 16](#)
- [Obtaining Documentation and Submitting a Service Request, page 16](#)

Electrical Safety Guidelines



Warning

Before working on a chassis or working near power supplies, unplug the power cord on AC units; disconnect the power at the circuit breaker on DC units.

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 from a circuit; always check the circuit.
- Look carefully for possible hazards in your work area, such as moist floors, ungrounded power extension cables, frayed power cords, and missing safety grounds.



**Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2009 Cisco Systems, Inc. All rights reserved.

- If an electrical accident occurs, proceed as follows:
 - 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 if 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.
- Install the sensor in compliance with local and national electrical codes as listed in *Regulatory Compliance and Safety Information for the Cisco Intrusion Prevention System 4200 Series Appliance Sensor*.
- The sensor models equipped with AC-input power supplies are shipped with a 3-wire electrical cord with a grounding-type plug that fits only a grounding-type power outlet. This is a safety feature that you should not circumvent. Equipment grounding should comply with local and national electrical codes.
- The sensor models equipped with DC-input power supplies must be terminated with the DC input wiring on a DC source capable of supplying at least 15 amps. A 15-amp circuit breaker is required at the 48 VDC facility power source. An easily accessible disconnect device should be incorporated into the facility wiring. Be sure to connect the grounding wire conduit to a solid earth ground. We recommend that you use a Listed closed-loop ring to terminate the ground conductor at the ground stud. The DC return connection to this system is to remain isolated from the system frame and chassis.

Other DC power guidelines are listed in *Regulatory Compliance and Safety Information for the Cisco Intrusion Prevention System 4200 Series Appliance Sensor*.

Working in an ESD Environment

Work on ESD-sensitive parts only at an approved static-safe station on a grounded static dissipative work surface, for example, an ESD workbench or static dissipative mat.

To remove and replace components in a sensor, follow these steps:

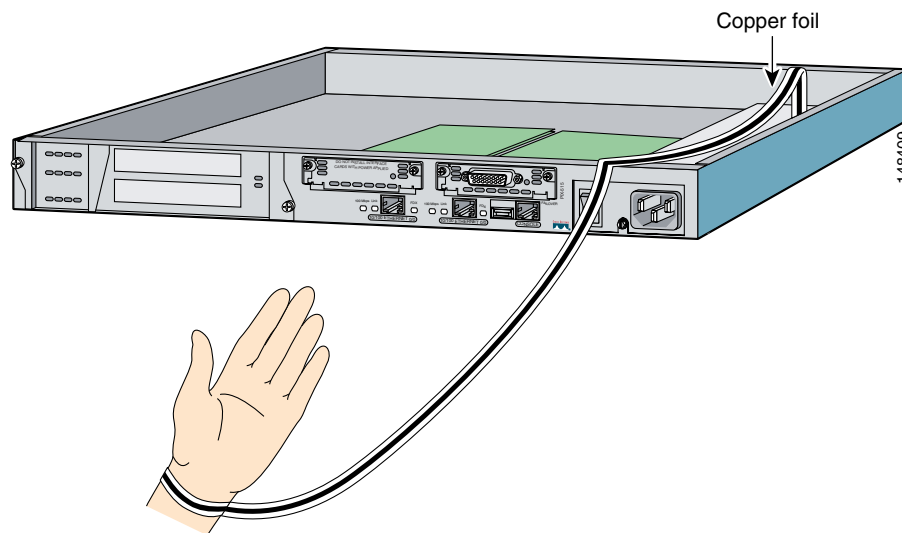
Step 1 Remove all static-generating items from your work area.

Step 2 Use a static dissipative work surface and wrist strap.



Note Disposable wrist straps, typically those included with an upgrade part, are designed for one time use.

- Step 3** Attach the wrist strap to your wrist and to the terminal on the work surface. If you are using a disposable wrist strap, connect the wrist strap directly to an unpainted metal surface of the chassis.



- Step 4** Connect the work surface to the chassis using a grounding cable and alligator clip.



Caution

Always follow ESD-prevention procedures when removing, replacing, or repairing components.



Note

If you are upgrading a component, do not remove the component from the ESD packaging until you are ready to install it.

Supported Interface Cards

IPS-4260 and IPS 4270-20 support three interface cards: the 4GE bypass interface card, the 2SX interface card, and the 10GE interface card.

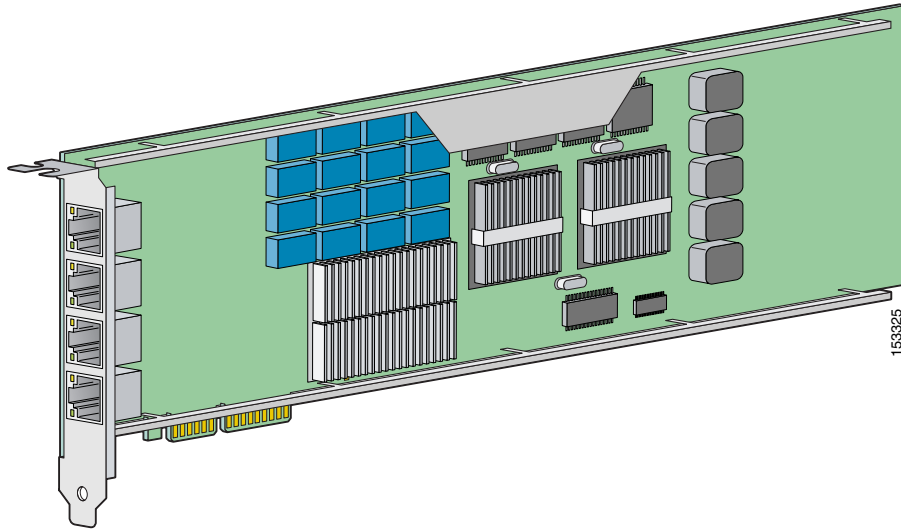
4GE Bypass Interface Card

The 4GE bypass interface card (part numbers IPS-4GE-BP-INT and IPS-4GE-BP-INT=) provides four 10/100/1000BASE-T (4GE) monitoring interfaces. The IPS-4260 supports up to two 4GE bypass interface cards for a total of eight GE bypass interfaces. The IPS 4270-20 supports up to four 4GE bypass interface cards for a total of sixteen GE bypass interfaces.

The 4GE bypass interface card supports hardware bypass.

Figure 1 shows the 4GE bypass interface card.

Figure 1 4GE Bypass Interface Card



2SX Interface Card

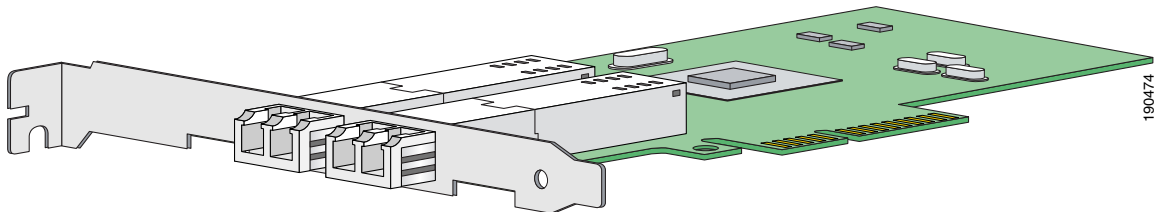
The 2SX interface card (part numbers IPS-2SX-INT and IPS-2SX-INT=) provides two 1000BASE-SX (fiber) monitoring interfaces. The IPS-4260 supports up to two 2SX interface cards for a total of four SX interfaces. The IPS 4270-20 supports up to six 2SX interface cards for a total of twelve SX interfaces.

The 2SX card ports require a multi-mode fiber cable with an LC connector to connect to the SX interface of the sensor.

The 2SX interface card does not support hardware bypass.

Figure 2 shows the 2SX interface card.

Figure 2 2SX Interface Card



10GE Interface Card

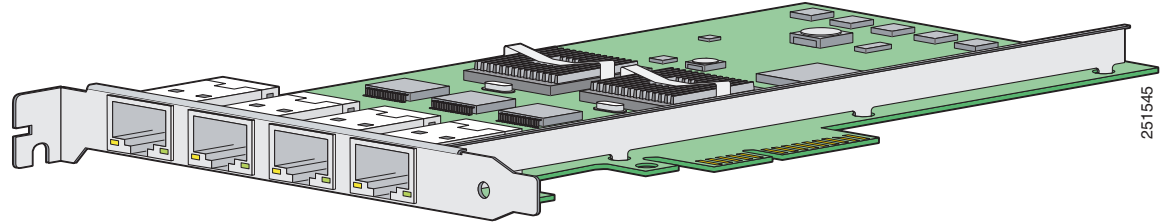
The 10GE interface card (part numbers IPS-2X10GE-SR-INT and IPS-2X10GE-SR-INT=) provides two 10000 Base-SX (fiber) interfaces. The IPS-4260 supports one 10GE interface card for a total of two 10GE fiber interfaces. The IPS 4270-20 supports up to two 10GE interface cards for a total of four 10GE fiber interfaces.

The card ports require a multi-mode fiber cable with an LC connector to connect to the SX interface of IPS-4260 and IPS 4270-20.

The 10GE interface card does not support hardware bypass.

Figure 3 shows the 10GE interface card.

Figure 3 10GE Interface Card



Hardware and Software Requirements

The IPS interface cards have the following hardware and software requirements:

- Hardware requirements
 - IPS-4260
 - IPS 4270-20
- Software requirements
 - 4GE bypass interface card—IPS 5.1(1) or later
 - 2SX interface card—IPS 5.1(1) or later
 - 10GE interface card—IPS 6.1(2) and IPS 6.2(1) or later

Hardware Bypass

This section describes the 4GE bypass interface card and its configuration restrictions. It contains the following topics:

- [4GE Bypass Interface Card, page 5](#)
- [Hardware Bypass Configuration Restrictions, page 6](#)

4GE Bypass Interface Card

IPS-4260 and IPS 4270-20 support the 4-port GigabitEthernet card (part number IPS-4GE-BP-INT=) with hardware bypass. This 4GE bypass interface card supports hardware bypass only between ports 0 and 1 and between ports 2 and 3.



Note

To disable hardware bypass, pair the interfaces in any other combination, for example 2/0<->2/2 and 2/1<->2/3.

Hardware bypass complements the existing software bypass feature in Cisco IPS. The following conditions apply to hardware bypass and software bypass:

- When bypass is set to OFF, software bypass is not active.

For each inline interface for which hardware bypass is available, the component interfaces are set to disable the fail-open capability. If SensorApp fails, the sensor is powered off, reset, or if the NIC interface drivers fail or are unloaded, the paired interfaces enter the fail-closed state (no traffic flows through inline interface or inline VLAN subinterfaces).

- When bypass is set to ON, software bypass is active.

Software bypass forwards packets between the paired physical interfaces in each inline interface and between the paired VLANs in each inline VLAN subinterface. For each inline interface on which hardware bypass is available, the component interfaces are set to standby mode. If the sensor is powered off, reset, or if the NIC interfaces fail or are unloaded, those paired interfaces enter fail-open state in hardware (traffic flows unimpeded through inline interface). Any other inline interfaces enter fail-closed state.

- When bypass is set to AUTO (traffic flows without inspection), software bypass is activated if SensorApp fails.

For each inline interface on which hardware bypass is available, the component interfaces are set to standby mode. If the sensor is powered off, reset, or if the NIC interfaces fail or are unloaded, those paired interfaces enter fail-open state in hardware. Any other inline interfaces enter the fail-closed state.


Note

To test fail-over, set the bypass mode to ON or AUTO, create one or more inline interfaces and power down the sensor and verify that traffic still flows through the inline path.

Hardware Bypass Configuration Restrictions

To use the hardware bypass feature on the 4GE bypass interface card, you must pair interfaces to support the hardware design of the card. If you create an inline interface that pairs a hardware-bypass-capable interface with an interface that violates one or more of the hardware-bypass configuration restrictions, hardware bypass is deactivated on the inline interface and you receive a warning message similar to the following:

```
Hardware bypass functionality is not available on Inline-interface pair0.
Physical-interface GigabitEthernet2/0 is capable of performing hardware bypass only when
paired with GigabitEthernet2/1, and both interfaces are enabled and configured with the
same speed and duplex settings.
```

The following configuration restrictions apply to hardware bypass:

- The 4-port bypass card is only supported on IPS-4260 and IPS 4270-20.
- Fail-open hardware bypass only works on inline interfaces (interface pairs), not on inline VLAN pairs.
- Fail-open hardware bypass is available on an inline interface if all of the following conditions are met:
 - Both of the physical interfaces support hardware bypass.
 - Both of the physical interfaces are on the same interface card.
 - The two physical interfaces are associated in hardware as a bypass pair.

- The speed and duplex settings are identical on the physical interfaces.
- Both of the interfaces are administratively enabled.
- Autonegotiation must be set on MDI/X switch ports connected to IPS-4260 and IPS 4270-20.

You must configure both the sensor ports and the switch ports for autonegotiation for hardware bypass to work. The switch ports must support MDI/X, which automatically reverses the transmit and receive lines if necessary to correct any cabling problems. The sensor is only guaranteed to operate correctly with the switch if both of them are configured for identical speed and duplex, which means that the sensor must be set for autonegotiation too.

Installing Interface Cards in IPS-4260

This section describes how to install interface cards in IPS-4260, and contains the following topics:

- [Removing and Replacing the Chassis Cover, page 11](#)
- [Installing and Removing Interface Cards, page 13](#)

Removing and Replacing the Chassis Cover



Warning

This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than 120 VAC, 20 A U.S. (240 VAC, 16-20 A International). Statement 1005



Warning

This equipment must be grounded. 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. Statement 1024



Warning

Blank faceplates and cover panels serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; 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. Statement 1029



Warning

This unit might have more than one power supply connection. All connections must be removed to de-energize the unit. Statement 1028



Caution

Follow proper safety procedures when removing and replacing the chassis cover by reading the safety warnings in *Regulatory Compliance and Safety Information for the Cisco Intrusion Prevention System 4200 Series Appliance Sensor*.

**Note**

Removing the appliance chassis cover does not affect your Cisco warranty. Upgrading IPS-4260 does not require any special tools and does not create any radio frequency leaks.

To remove and replace the chassis cover, follow these steps:

Step 1 Log in to the CLI.

Step 2 Prepare IPS-4260 to be powered off:

```
sensor# reset powerdown
```

Wait for the power down message before continuing with Step 3.

**Note**

You can also power down IPS-4260 using IDM or IME.

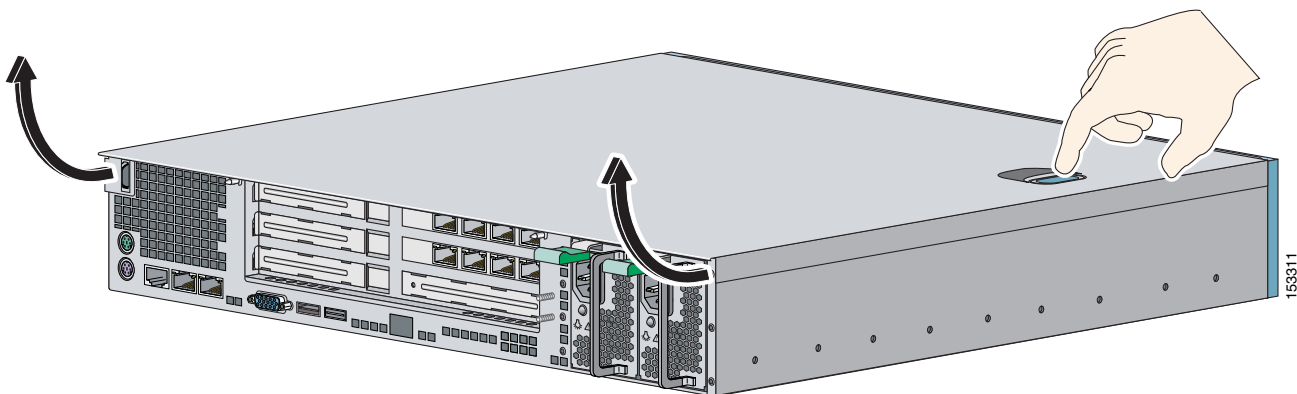
Step 3 Power off IPS-4260.

Step 4 Remove the power cord and other cables from IPS-4260.

Step 5 If rack-mounted, remove IPS-4260 from the rack.

Step 6 Make sure IPS-4260 is in an ESD-controlled environment.

Step 7 Press the blue button on the top of the chassis cover and slide the chassis cover back.

**Caution**

Do not operate IPS-4260 without the chassis cover installed. The chassis cover protects the internal components, prevents electrical shorts, and provides proper air flow for cooling the electronic components.

Step 8 To replace the chassis cover, position it at the back of the chassis and slide it on until it snaps into place.

Step 9 Reattach the power cord and other cables to IPS-4260.

Step 10 Reinstall IPS-4260 on a rack, desktop, or table.

Step 11 Power on IPS-4260.

For More Information

For the procedure for removing IPS-4260 from a rack, refer to “Installing IPS-4260,” in *Installing Cisco Intrusion Prevention System Appliances and Modules*.

Installing and Removing Interface Cards

IPS-4260 has 6 expansion card slots, three full-height and three half-height slots. You can install the optional network interface cards in the two top full-height slots, slots 2 and 3. IPS-4260 supports up to two network interface cards.

**Note**

IPS 4260 supports only one 10GE fiber interface card, which you can install in either of the supported slots (slots 2 and 3).

**Note**

We recommend that you install the 4GE bypass interface card in slot 2 if you are installing only one 4GE bypass card. This improves accessibility to the RJ45 cable connectors.

To install and remove PCI cards, follow these steps:

Step 1 Log in to the CLI.

Step 2 Prepare IPS-4260 to be powered off:

```
sensor# reset powerdown
```

Wait for the power down message before continuing with Step 3.

**Note**

You can also power down IPS-4260 using IDM or IME.

Step 3 Power off IPS-4260.

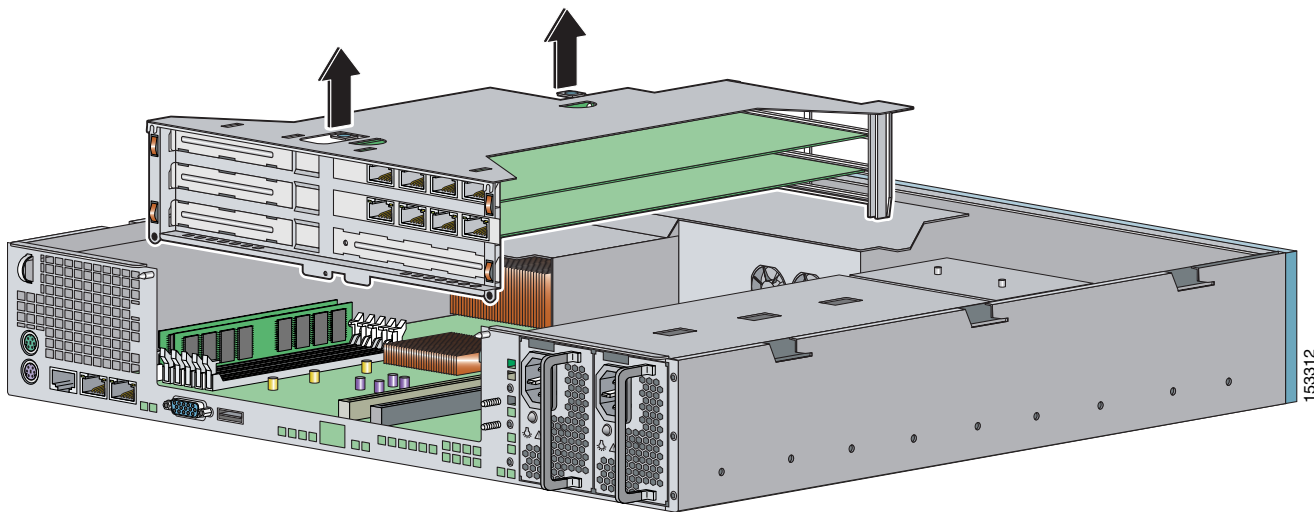
Step 4 Remove the power cable and other cables from IPS-4260.

Step 5 If rack-mounted, remove IPS-4260 from the rack.

Step 6 Make sure IPS-4260 is in an ESD-controlled environment.

Step 7 Remove the chassis cover.

- Step 8** Remove the card carrier by pulling up on the two blue release tabs. Use equal pressure and lift the card carrier out of the chassis.

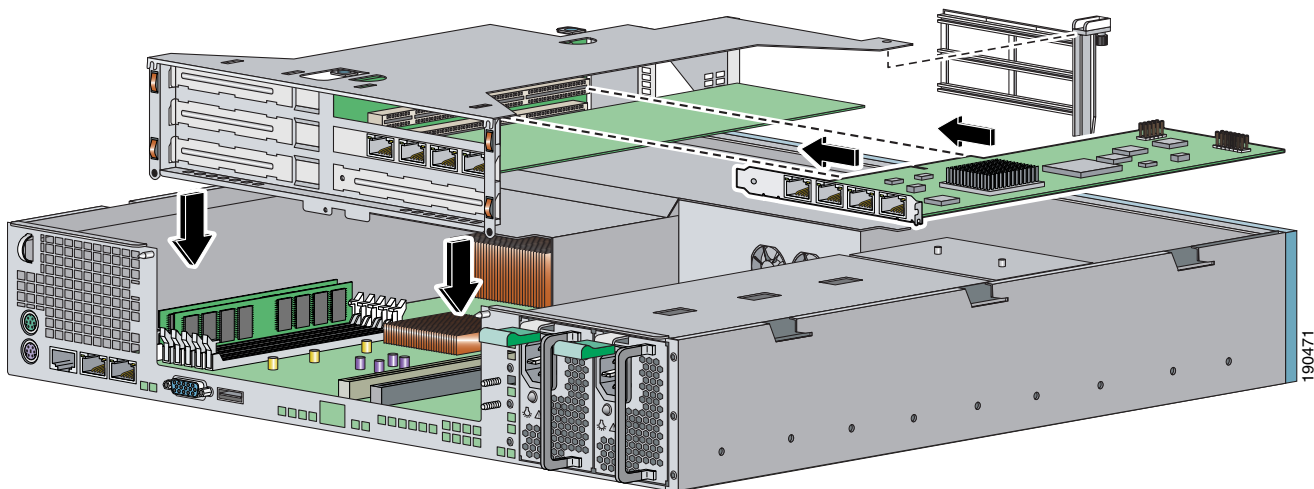


- Step 9** With a screw driver, remove the screw from the desired slot cover.

- Step 10** Remove the slot cover by pressing on it from inside the chassis.

If the card is full length, use a screw driver to remove the blue thumb screw from the card support at the back of the card carrier.

- Step 11** Carefully align the PCI card with the PCI-Express connector and alignment grooves for the appropriate slot. Apply firm even pressure until the card is fully seated in the connector.



- Step 12** Reinstall the slot cover screw to hold the card to the carrier. If necessary, reinstall the card support at the back of the card carrier.

- Step 13** Replace the card carrier in the chassis.

- Step 14** Replace the chassis cover.

Installing Interface Cards in IPS 4270-20

This section describes how to install interface cards in IPS 4270-20, and contains the following topics:

- [Removing and Replacing the Chassis Cover, page 7](#)
- [Installing and Removing Interface Cards, page 9](#)

Removing and Replacing the Chassis Cover



Warning

This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than 120 VAC, 20 A U.S. (240 VAC, 16-20 A International). Statement 1005



Warning

This equipment must be grounded. 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. Statement 1024



Warning

Blank faceplates and cover panels serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; 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. Statement 1029



Warning

This unit might have more than one power supply connection. All connections must be removed to de-energize the unit. Statement 1028



Note

Removing the appliance chassis cover does not affect your Cisco warranty. Upgrading IPS 4270-20 does not require any special tools and does not create any radio frequency leaks.



Caution

Do not operate IPS 4270-20 for long periods with the chassis cover open or removed. Operating it in this manner results in improper airflow and improper cooling that can lead to thermal damage.

To remove and replace the chassis cover, follow these steps:

Step 1 Log in to the CLI.

Step 2 Prepare IPS 4270-20 to be powered off:

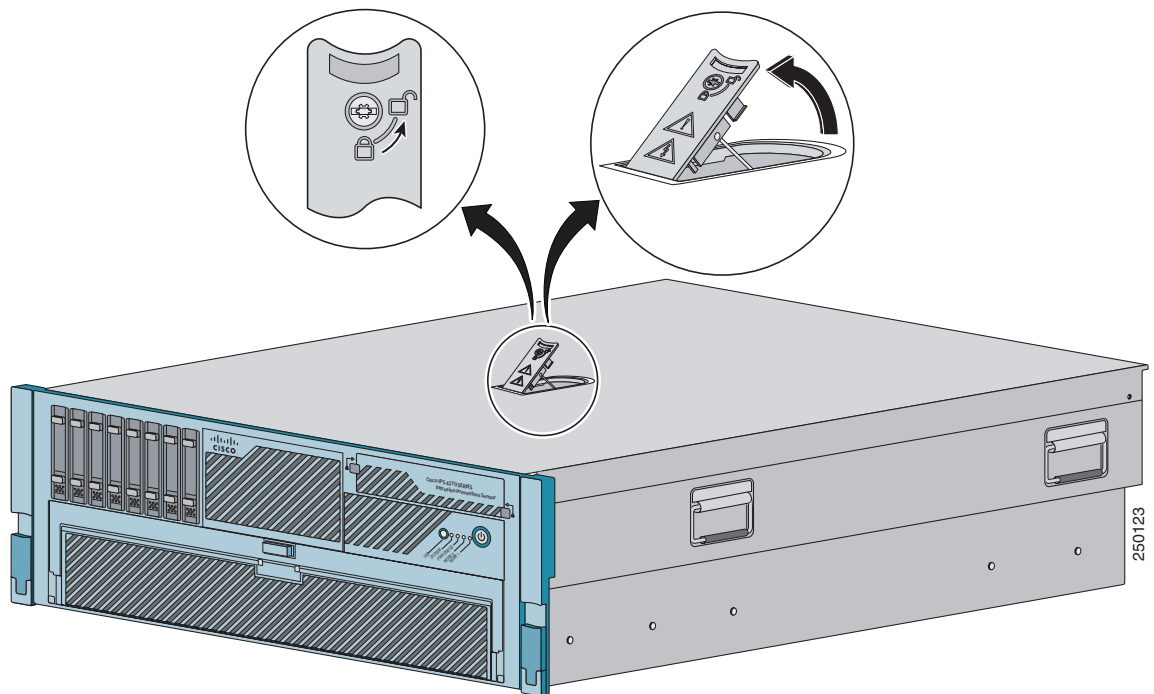
```
sensor# reset powerdown
```

Wait for the power down message before continuing with Step 3.

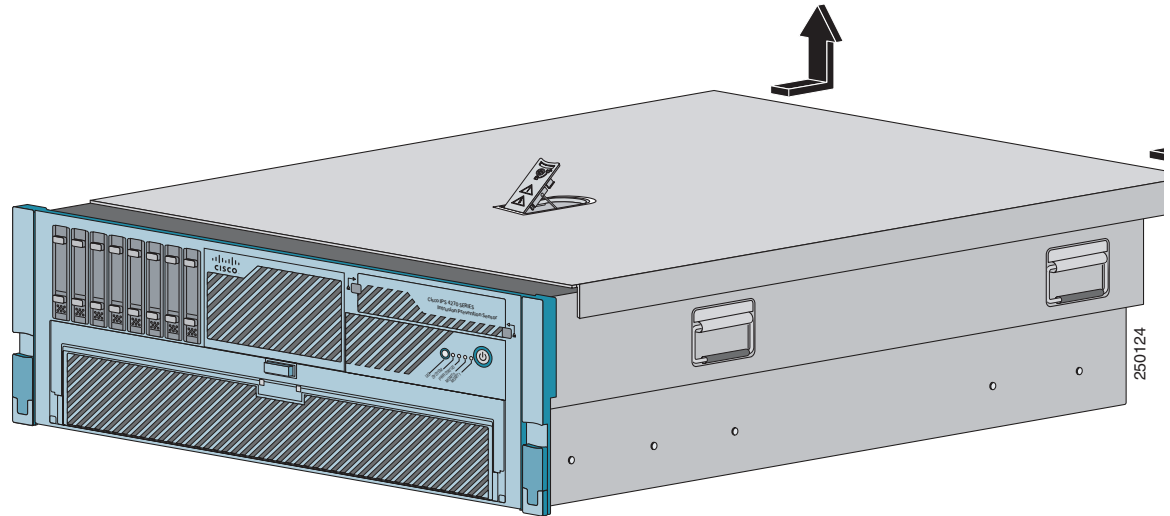


Note You can also power down IPS 4270-20 using IDM or IME.

- Step 3** Power off IPS 4270-20.
- Step 4** Remove both power cables from IPS 4270-20.
- Step 5** Extend IPS 4270-20 out of the rack if it is rack-mounted.
- Step 6** Make sure IPS 4270-20 is in an ESD-controlled environment.
- Step 7** If the locking latch is locked, use the T-15 Torx screwdriver located on the back of the chassis to unlock it. Turn the locking screw a quarter of a turn counterclockwise to unlock it.
- Step 8** Lift up the cover latch on the top of the chassis.



Step 9 Slide the chassis cover back and up to remove it.



Caution

Do not operate IPS 4270-20 without the chassis cover installed. The chassis cover protects the internal components, prevents electrical shorts, and provides proper air flow for cooling the electronic components.

Step 10 To replace the chassis cover, position it on top of the chassis and slide it on. Push down on the cover latch to lock into place.



Note Make sure the chassis cover is securely locked in to place before powering up IPS 4270-20.

Step 11 Reattach the power cables to IPS 4270-20.

Step 12 Reinstall IPS 4270-20 in a rack, on a desktop, or on a table, or extend it back in to the rack.

Step 13 Power on IPS 4270-20.

For More Information

For the procedure for removing IPS 4270-20 from a rack, refer to “Installing IPS 4270-20,” in *Installing Cisco Intrusion Prevention System Appliances and Modules*.

Installing and Removing Interface Cards

IPS 4270-20 has nine expansion card slots. Slots 1 and 2 are PCI-X slots and are reserved for future use. Slots 3 through 9 are PCI-Express slots. All slots are full-height slots. Slot 9 is populated by a RAID controller card and is not available for use by network interface cards.



Note

IPS 4270-20 supports two 10GE fiber interface cards, which you can install in any of the supported six slots (slots 3 to 8).

**Caution**

To prevent damage to IPS 4270-20 or the expansion cards, power down IPS 4270-20 and remove all AC power cables before removing or installing expansion cards.

**Caution**

To prevent improper cooling and thermal damage, do not operate IPS 4270-20 unless all expansion slots have a cover or a card installed.

To install and remove PCI cards, follow these steps:

Step 1 Log in to the CLI.

Step 2 Prepare IPS 4270-20 to be powered off:

```
sensor# reset powerdown
```

Wait for the power down message before continuing with Step 3.



Note You can also power down IPS 4270-20 using IDM or IME.

Step 3 Power off IPS 4270-20.

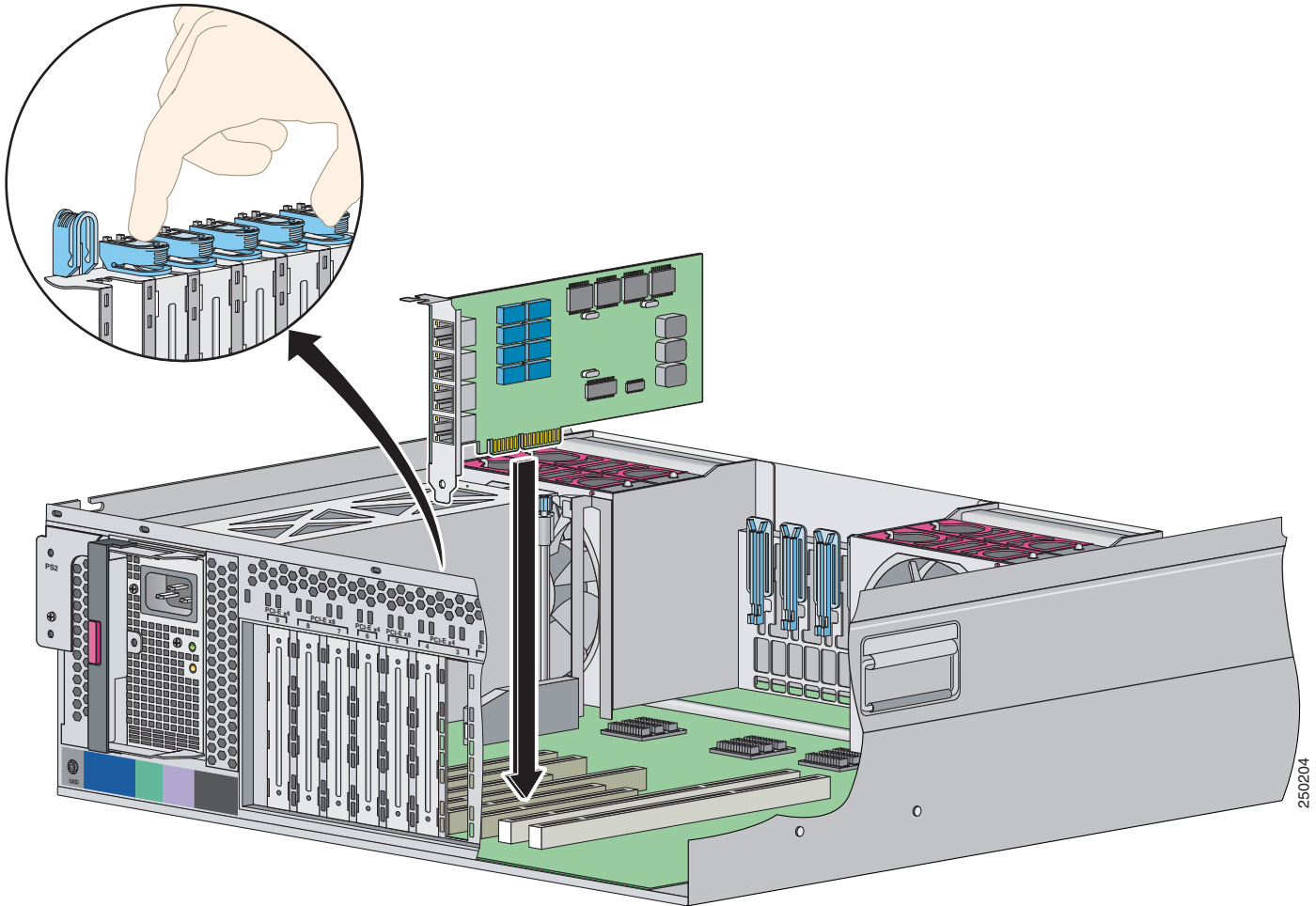
Step 4 Remove the power cables from IPS 4270-20.

Step 5 If rack-mounted, extend IPS 4270-20 from the rack.

Step 6 Make sure IPS 4270-20 is in an ESD-controlled environment.

Step 7 Remove the chassis cover.

Step 8 To unlock the expansion card slot, push down on the center part of the blue tab and open the latch.



Step 9 To uninstall a card, lift the card out of the socket. To install a card, position the card so that its connector lines up over the socket on the motherboard and push the card down in to the socket. Press down on the outer edge of the blue tab to lock the card in to place.



Note To remove full-length expansion cards, unlock the retaining clip. To install full-length expansion cards, lock the retaining clip.

Step 10 Replace the chassis cover.

Step 11 Slide the server back in to the rack by pressing the server rail-release handles.

Step 12 Reconnect the power cables to IPS 4270-20.

Step 13 Power on IPS 4270-20.

Related Documentation

For more information on Cisco IPS, refer to the following documentation found at this URL:

http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/tsd_products_support_series_home.html

- *Documentation Roadmap for Cisco Intrusion Prevention System*
- *Release Notes for Cisco Intrusion Prevention System*
- *Installing and Using Cisco Intrusion Prevention System Device Manager*
- *Installing and Using Cisco Intrusion Prevention System Manager Express*
- *Cisco Intrusion Prevention System Command Reference*
- *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface*
- *Installing Cisco Intrusion Prevention System Appliances and Modules*
- *Regulatory Compliance and Safety Information for the Cisco Intrusion Prevention System 4200 Series Appliance Sensor*

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0903R)

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

© 2009 Cisco Systems, Inc. All rights reserved.

♻️ Printed in the USA on recycled paper containing 10% postconsumer waste.