Cisco Intrusion Prevention System Appliance and Module Installation Guide for IPS 7.0

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

Text Part Number: OL-18504-01

Cisco Intrusion Prevention System Appliance and Module Installation Guide for IPS 7.0

CONTENTS

Preface

Published: April 22, 2009, OL-18504-01

Revised: October 31, 2012

Contents

This guide describes how to install appliances and modules that support Cisco IPS 7.0. It includes a glossary that contains expanded acronyms and pertinent IPS terms. It is part of the documentation set for Cisco Intrusion Prevention System 7.0. Use this guide in conjunction with the documents listed in Related Documentation, page xvi. This preface contains the following sections:

Audience

This guide is for experienced network security administrators who install and maintain Cisco IPS sensors, including the supported IPS appliances and modules.

Comply with Local and National Electrical Codes

Warning **Installation of the equipment must comply with local and national electrical codes.** Statement 1074

Waarschuwing **Bij installatie van de apparatuur moet worden voldaan aan de lokale en nationale elektriciteitsvoorschriften.**

Varoitus	Laitteisto tulee asentaa paikallisten ja kansallisten sähkömääräysten mukaisesti.
Attention	L'équipement doit être installé conformément aux normes électriques nationales et locales.
Warnung	Die Installation der Geräte muss den Sicherheitsstandards entsprechen.
Avvertenza	L'installazione dell'impianto deve essere conforme ai codici elettrici locali e nazionali.
Advarsel	Installasjon av utstyret må samsvare med lokale og nasjonale elektrisitetsforskrifter.
Aviso	A instalação do equipamento tem de estar em conformidade com os códigos eléctricos locais e nacionais.
¡Advertencia!	La instalación del equipo debe cumplir con las normativas de electricidad locales y nacionales.
Varning!	Installation av utrustningen måste ske i enlighet med gällande elinstallationsföreskrifter.
	A berendezés üzembe helyezését a helyi és a nemzeti elektromossági előírások figyelembevételével kell elvégezni.
Предупреждение	Установка оборудования должна соответствовать местным и национальным электротехническим нормам.
警告	设备安装必须符合本地与本国电气法规。
警告	機器の取り付けは地域および国内の電気工事規定に遵守する必要があります。
주의	현지 및 국가 전기 규정에 따라 장비를 설치해야 합니다.
Aviso	A instalação do equipamento deve estar em conformidade com os códigos elétricos nacionais.
Upozornění	Instalace zařízení musí splňovat příslušné místní a státní elektrotechnické normy.
אזהרה	התקנת הציוד חייבת להיות תואמת את חוקי החשמל המקומיים והארציים.
Ostrzeżenie	Instalacja sprzętu musi być zgodna z lokalnymi i krajowymi normami elektrycznymi.
Upozornenie	Inštalácia zariadenia sa musí vykonať v súlade s miestnymi a národnými predpismi pre inštaláciu elektrických zariadení.

Opozorilo **Priključitev opreme mora potekati v skladu z lokalnimi in državnimi predpisi o električni opremi.**

警告 設備安裝作業必須符合當地或國家電工法。

Organization

This guide includes the following sections:

Section	Title	Description
1	"Introducing the Sensor"	Describes IPS appliances and modules.
2	"Installing the IPS 4240 and the IPS 4255"	Describes how to install the IPS 4240 and the IPS 4255.
3	"Installing the IPS 4260"	Describes how to install the IPS 4260.
4	"Installing the IPS 4270-20"	Describes how to install the IPS 4270-20.
5	"Installing the AIM IPS"	Describes how to install the AIM IPS.
6	"Installing the AIP SSM"	Describes how to install the AIP SSM.
7	"Installing the IDSM2"	Describes how to install the IDSM2.
8	"Installing the NME IPS"	Describes how to install the NME IPS
9	"Logging In to the Sensor"	Describes how to log in to the various sensors.
10	"Initializing the Sensor"	Describes how to use the **setup** command to initialize sensors.
11	"Obtaining Software"	Describes where to go to get the latest IPS software and describes the naming conventions.
12	"Upgrading, Downgrading, and Installing System Images"	Describes how to upgrade sensors and reimage the various sensors.
A	"Troubleshooting"	Contains troubleshooting tips for IPS hardware and software.
	"Glossary"	Contains IPS acronyms and terms.

Conventions

This document uses the following conventions:

Convention	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.

{x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`courier` font	Terminal sessions and information the system displays appear in `courier` font.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means *reader take note*.

Tip Means *the following information will help you solve a problem*.

Caution Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Warning **Means *reader be warned*. In this situation, you might perform an action that could result in bodily injury.**

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*
- *Installling and Removing Interface Cards in Cisco IPS-4260 and IPS 4270-20*

- *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.

CHAPTER 1

Introducing the Sensor

This chapter introduces the sensor and provides information you should know before you install the sensor. In this guide, the term *sensor* refers to all models unless noted otherwise. For a complete list of supported sensors and their model numbers, see Supported Sensors, page 1-17. This chapter contains the following sections:

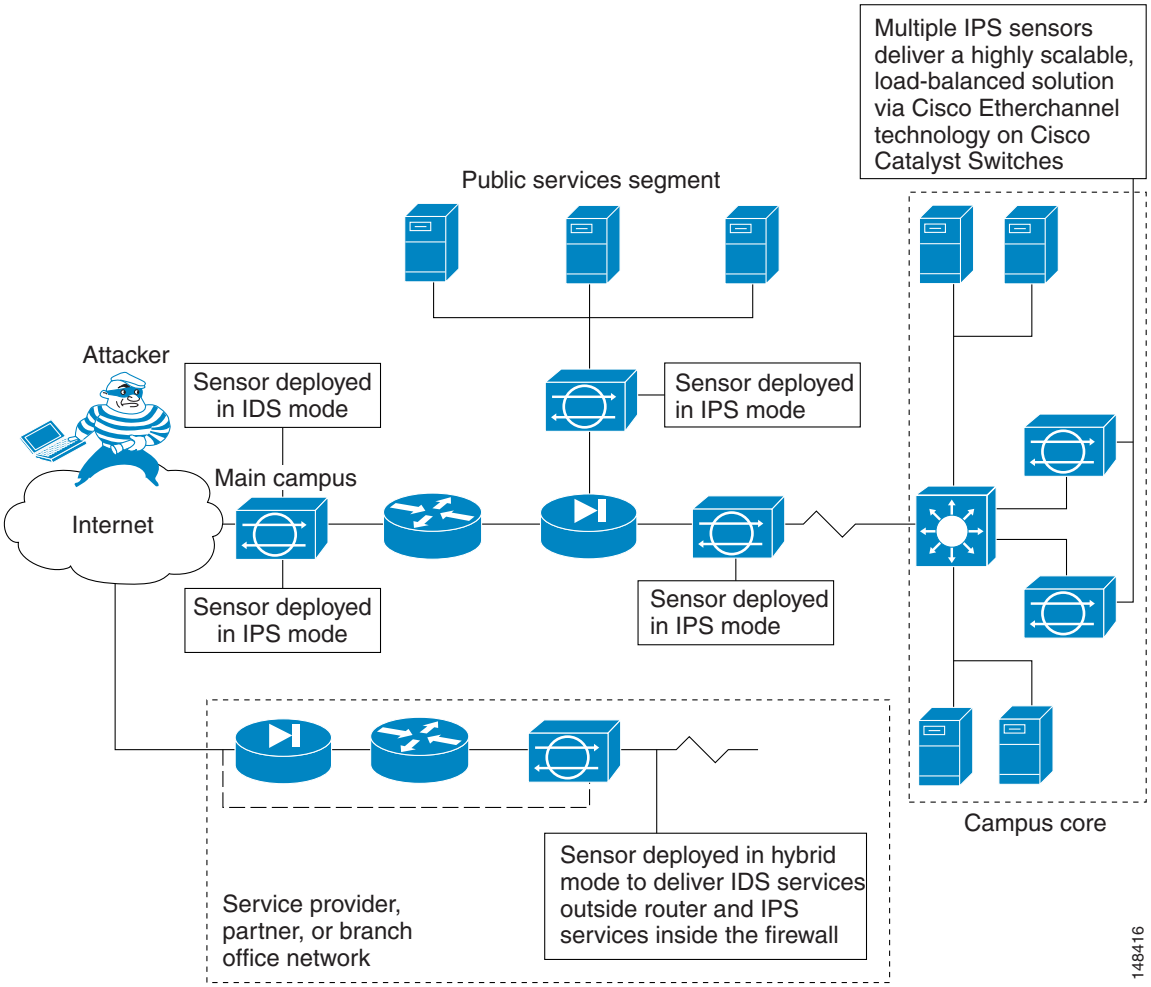
How the Sensor Functions

This section describes how the sensor functions, and contains the following topics:

Capturing Network Traffic

The sensor can operate in either promiscuous or inline mode. Figure 1-1 on page 1-2 shows how you can deploy a combination of sensors operating in both inline (IPS) and promiscuous (IDS) modes to protect your network.

Figure 1-1 Comprehensive Deployment Solutions



The command and control interface is always Ethernet. This interface has an assigned IP address, which allows it to communicate with the manager workstation or network devices (Cisco switches, routers, and firewalls). Because this interface is visible on the network, you should use encryption to maintain data privacy. SSH is used to protect the CLI and TLS/SSL is used to protect the manager workstation. SSH and TLS/SSL are enabled by default on the manager workstations.

When responding to attacks, the sensor can do the following:

- Insert TCP resets via the sensing interface.

Note You should select the TCP reset action only on signatures associated with a TCP-based service. If selected as an action on non-TCP-based services, no action is taken. Additionally, TCP resets are not guaranteed to tear down an offending session because of limitations in the TCP protocol.

- Make ACL changes on switches, routers, and firewalls that the sensor manages.

Note ACLs may block only future traffic, not current traffic.

- Generate IP session logs, session replay, and trigger packets display.

  IP session logs are used to gather information about unauthorized use. IP log files are written when events occur that you have configured the appliance to look for.
- Implement multiple packet drop actions to stop worms and viruses.

Your Network Topology

Before you deploy and configure your sensors, you should understand the following about your network:

- The size and complexity of your network.
- Connections between your network and other networks (and the Internet).
- The amount and type of network traffic on your network.

This knowledge will help you determine how many sensors are required, the hardware configuration for each sensor (for example, the size and type of network interface cards), and how many managers are needed.

Correctly Deploying the Sensor

You should always position the IPS sensor behind a perimeter-filtering device, such as a firewall or adaptive security appliance. The perimeter device filters traffic to match your security policy thus allowing acceptable traffic in to your network. Correct placement significantly reduces the number of alerts, which increases the amount of actionable data you can use to investigate security violations. If you position the IPS sensor on the edge of your network in front of a firewall, your sensor will produce alerts on every single scan and attempted attack even if they have no significance to your network implementation. You will receive hundreds, thousands, or even millions of alerts (in a large enterprise environment) that are not really critical or actionable in your environment. Analyzing this type of data is time consuming and costly.

Tuning the IPS

Tuning the IPS ensures that the alerts you see reflect true actionable information. Without tuning the IPS, it is difficult to do security research or forensics on your network because you will have thousands of benign events, also known as false positives. False positives are a by-product of all IPS devices, but they occur much less frequently in Cisco IPS devices since Cisco IPS devices are stateful, normalized, and use vulnerability signatures for attack evaluation. Cisco IPS devices also provide risk rating, which identifies high risk events, and policy-based management, which lets you deploy rules to enforce IPS signature actions based on risk rating.

Follow these tips when tuning your IPS sensors:

- Place your sensor on your network behind a perimeter-filtering device.

  Proper sensor placement can reduce the number of alerts you need to examine by several thousands a day.
- Deploy the sensor with the default signatures in place.

  The default signature set provides you with a very high security protection posture. The Cisco signature team has spent many hours on testing the defaults to give your sensor the highest protection. If you think that you have lost these defaults, you can restore them.

- Make sure that the event action override is set to drop packets with a risk rating greater than 90.

  This is the default and ensures that high risk alerts are stopped immediately.
- Filter out known false positives caused by specialized software, such as vulnerability scanner and load balancers by one of the following methods:
  - You can configure the sensor to ignore the alerts from the IP addresses of the scanner and load balancer.
  - You can configure the sensor to allow these alerts and then use IME to filter out the false positives.
- Filter the Informational alerts.

  These low priority events notifications could indicate that another device is doing reconnaissance on a device protected by the IPS. Research the source IP addresses from these Informational alerts to determine what the source is.
- Analyze the remaining actionable alerts:
  - Research the alert.
  - Fix the attack source.
  - Fix the destination host.
  - Modify the IPS policy to provide more information.

For More Information

- For a detailed description of risk rating, refer to Calculating the Risk Rating.
- For information on Cisco signatures, for IDM and IME refer to Defining Signatures, and for the CLI refer to Defining Signatures.
- For detailed information on event action overrides, for IDM and IME refer to Configuring Event Action Overrides, and for the CLI, refer to Configuring Event Action Overrides.
- For information on using Cisco IME, refer to *Installing and Using Cisco Intrusion Prevention System Manager Express 7.0*.

Sensor Interfaces

This section describes the sensor interfaces, and contains the following topics:

Understanding Sensor Interfaces

The sensor interfaces are named according to the maximum speed and physical location of the interface. The physical location consists of a port number and a slot number. All interfaces that are built-in on the sensor motherboard are in slot 0, and the PCI expansion slots are numbered beginning with slot 1 for the bottom slot with the slot numbers increasing from bottom to top (except for the IPS 4270-20, where the

ports are numbered from top to bottom). Interfaces with a given slot are numbered beginning with port 0 for the right port with the port numbers increasing from right to left. For example, GigabitEthernet2/1 supports a maximum speed of 1 Gigabit and is the second-from-the-right interface in the second-from-the bottom PCI expansion slot. The IPS 4240, IPS 4255, IPS 4260, and IPS 4270-20 are exceptions to this rule. The command and control interface on these sensors is called Management0/0 rather than GigabitEthernet0/0. The IPS 4270-20 has an additional interface called Management0/1, which is reserved for future use.

There are three interface roles:

- Command and control
- Sensing
- Alternate TCP reset

There are restrictions on which roles you can assign to specific interfaces and some interfaces have multiple roles. You can configure any sensing interface to any other sensing interface as its TCP reset interface. The TCP reset interface can also serve as an IDS (promiscuous) sensing interface at the same time. The following restrictions apply:

- Because the AIM IPS, AIP SSM, and NME IPS only have one sensing interface, you cannot configure a TCP reset interface.
- Because of hardware limitations on the Catalyst switch, both of the IDSM2 sensing interfaces are permanently configured to use System0/1 as the TCP reset interface.
- The TCP reset interface that is assigned to a sensing interface has no effect in inline interface or inline VLAN pair mode, because TCP resets are always sent on the sensing interfaces in those modes.

Note Each physical interface can be divided into VLAN group subinterfaces, each of which consists of a group of VLANs on that interface.

Command and Control Interface

The command and control interface has an IP address and is used for configuring the sensor. It receives security and status events from the sensor and queries the sensor for statistics.

The command and control interface is permanently enabled. It is permanently mapped to a specific physical interface, which depends on the specific model of sensor. You cannot use the command and control interface as either a sensing or alternate TCP reset interface.

Table 1-1 lists the command and control interfaces for each sensor.

Table 1-1 Command and Control Interfaces

Sensor	Command and Control Interface
AIM IPS	Management0/0
AIP SSM-10	GigabitEthernet0/0
AIP SSM-20	GigabitEthernet0/0
AIP SSM-40	GigabitEthernet0/0
IDSM2	GigabitEthernet0/2
IPS 4240	Management0/0

Table 1-1 Command and Control Interfaces (continued)

Sensor	Command and Control Interface
IPS 4255	Management0/0
IPS 4260	Management0/0
IPS 4270-20	Management0/0
NME IPS	Management0/01

Sensing Interfaces

Sensing interfaces are used by the sensor to analyze traffic for security violations. A sensor has one or more sensing interfaces depending on the sensor. Sensing interfaces can operate individually in promiscuous mode or you can pair them to create inline interfaces.

Note On appliances, all sensing interfaces are disabled by default. You must enable them to use them. On modules, the sensing interfaces are permanently enabled.

Some appliances support optional interface cards that add sensing interfaces to the sensor. You must insert or remove these optional cards while the sensor is powered off. The sensor detects the addition or removal of a supported interface card. If you remove an optional interface card, some of the interface configuration is deleted, such as the speed, duplex, description string, enabled/disabled state of the interface, and any inline interface pairings. These settings are restored to their default settings when the card is reinstalled. However, the assignment of promiscuous and inline interfaces to the Analysis Engine is not deleted from the Analysis Engine configuration, but is ignored until those cards are reinserted and you create the inline interface pairs again.

Interface Support

Table 1-2 describes the interface support for appliances and modules running Cisco IPS.

Table 1-2 Interface Support

Base Chassis	Added Interface Cards	Interfaces Supporting Inline VLAN Pairs (Sensing Ports)	Combinations Supporting Inline Interface Pairs	Interfaces Not Supporting Inline (Command and Control Port)
AIM IPS	—	GigabitEthernet0/1 by **ids-service-module** command in the router configuration instead of VLAN pair or inline interface pair	GigabitEthernet0/1 by **ids-service-module** command in the router configuration instead of VLAN pair or inline interface pair	Management0/0
AIP SSM-10	—	GigabitEthernet0/1 by security context instead of VLAN pair or inline interface pair	GigabitEthernet0/1 by security context instead of VLAN pair or inline interface pair	GigabitEthernet0/0

Table 1-2 Interface Support (continued)

Base Chassis	Added Interface Cards	Interfaces Supporting Inline VLAN Pairs (Sensing Ports)	Combinations Supporting Inline Interface Pairs	Interfaces Not Supporting Inline (Command and Control Port)
AIP SSM-20	—	GigabitEthernet0/1 by security context instead of VLAN pair or inline interface pair	GigabitEthernet0/1 by security context instead of VLAN pair or inline interface pair	GigabitEthernet0/0
AIP SSM-40	—	GigabitEthernet0/1 by security context instead of VLAN pair or inline interface pair	GigabitEthernet0/1 by security context instead of VLAN pair or inline interface pair	GigabitEthernet0/0
IDSM2	—	GigabitEthernet0/7 GigabitEthernet0/8	0/7<->0/8	GigabitEthernet0/2
IPS 4240	—	GigabitEthernet0/0 GigabitEthernet0/1 GigabitEthernet0/2 GigabitEthernet0/3	0/0<->0/1 0/0<->0/2 0/0<->0/3 0/1<->0/2 0/1<->0/3 0/2<->0/3	Management0/0
IPS 4255	—	GigabitEthernet0/0 GigabitEthernet0/1 GigabitEthernet0/2 GigabitEthernet0/3	0/0<->0/1 0/0<->0/2 0/0<->0/3 0/1<->0/2 0/1<->0/3 0/2<->0/3	Management0/0
IPS 4260	—	GigabitEthernet0/1	N/A	Management0/0
IPS 4260	4GE-BP Slot 1 Slot 2	GigabitEthernet0/1 GigabitEthernet2/0 GigabitEthernet2/1 GigabitEthernet2/2 GigabitEthernet2/3 GigabitEthernet3/0 GigabitEthernet3/1 GigabitEthernet3/2 GigabitEthernet3/3	 2/0<->2/1[1] 2/2<->2/3 3/0<->3/1 3/2<->3/3	Management0/0
IPS 4260	2SX Slot 1 Slot 2	GigabitEthernet0/1 GigabitEthernet2/0 GigabitEthernet2/1 GigabitEthernet3/0 GigabitEthernet3/1	All sensing ports can be paired together	Management0/0

Table 1-2 Interface Support (continued)

Base Chassis	Added Interface Cards	Interfaces Supporting Inline VLAN Pairs (Sensing Ports)	Combinations Supporting Inline Interface Pairs	Interfaces Not Supporting Inline (Command and Control Port)
IPS 4260	10GE Slot 1	GigabitEthernet0/1 TenGigabitEthernet2/0 TenGigabitEthernet2/1	 2/0<->2/1[2]	Management0/0
IPS 4270-20	—	—	N/A	Management0/0 Management0/1[3]
IPS 4270-20	4GE-BP Slot 1 Slot 2	 GigabitEthernet3/0 GigabitEthernet3/1 GigabitEthernet3/2 GigabitEthernet3/3 GigabitEthernet4/0 GigabitEthernet4/1 GigabitEthernet4/2 GigabitEthernet4/3	 3/0<->3/1[4] 3/2<->3/3 4/0<->4/1 4/2<->4/3	Management0/0 Management0/1[5]
IPS 4270-20	2SX Slot 1 Slot 2	 GigabitEthernet3/0 GigabitEthernet3/1 GigabitEthernet4/0 GigabitEthernet4/1	All sensing ports can be paired together	Management0/0 Management0/1[6]
IPS 4270-20	10GE Slot 1 Slot 2	 TenGigabitEthernet5/0 TenGigabitEthernet5/1 TenGigabitEthernet7/0 TenGigabitEthernet7/1	All sensing ports can be paired together	Management0/0 Management0/1[7]
NME IPS	—	GigabitEthernet0/1 by **ids-service-module** command in the router configuration instead of VLAN pair or inline interface pair	GigabitEthernet0/1 by **ids-service-module** command in the router configuration instead of VLAN pair or inline interface pair	Management0/1

1. To disable hardware bypass, pair the interfaces in any other combination (2/0<->2/2 and 2/1<->2/3, for example).
2. To disable hardware bypass, pair the interfaces in any other combination (2/0<->2/2 and 2/1<->2/3, for example).
3. Reserved for future use.
4. To disable hardware bypass, pair the interfaces in any other combination (2/0<->2/2 and 2/1<->2/3, for example).
5. Reserved for future use.
6. Reserved for future use.
7. Reserved for future use.

Note The IPS 4260 supports a mixture of 4GE-BP, 2SX, and 10GE cards. The IPS 4270-20 also supports a mixture of 4GE-BP, 2SX, and 10GE cards up to a total of either six cards, or sixteen total ports, which ever is reached first, but is limited to only two 10GE card in the mix of cards.

TCP Reset Interfaces

This section explains the TCP reset interfaces and when to use them. It contains the following topics:

- Understanding Alternate TCP Reset Interfaces, page 1-9
- Designating the Alternate TCP Reset Interface, page 1-10

Understanding Alternate TCP Reset Interfaces

Note The alternate TCP reset interface setting is ignored in inline interface or inline VLAN pair mode, because resets are sent inline in these modes.

You can configure sensors to send TCP reset packets to try to reset a network connection between an attacker host and its intended target host. In some installations when the interface is operating in promiscuous mode, the sensor may not be able to send the TCP reset packets over the same sensing interface on which the attack was detected. In such cases, you can associate the sensing interface with an alternate TCP reset interface and any TCP resets that would otherwise be sent on the sensing interface when it is operating in promiscuous mode are instead sent out on the associated alternate TCP reset interface.

If a sensing interface is associated with an alternate TCP reset interface, that association applies when the sensor is configured for promiscuous mode but is ignored when the sensing interface is configured for inline mode.

With the exception of the IDSM2, any sensing interface can serve as the alternate TCP reset interface for another sensing interface. The alternate TCP reset interface on the IDSM2 is fixed because of hardware limitation.

Note There is only one sensing interface on IPS modules (AIM IPS, AIP SSM, and NME IPS).

Table 1-3 lists the alternate TCP reset interfaces.

Table 1-3 Alternate TCP Reset Interfaces

Sensor	Alternate TCP Reset Interface
AIM IPS	None
AIP SSM-10	None
AIP SSM-20	None
AIP SSM-40	None
IDSM2	System0/1[1]
IPS 4240	Any sensing interface
IPS 4255	Any sensing interface

Table 1-3 Alternate TCP Reset Interfaces (continued)

Sensor	Alternate TCP Reset Interface
IPS 4260	Any sensing interface
IPS 4270-20	Any sensing interface
NME IPS	None

1. This is an internal interface on the Catalyst backplane.

Designating the Alternate TCP Reset Interface

You need to designate an alternate TCP reset interface in the following situations:

- When a switch is being monitored with either SPAN or VACL capture and the switch does not accept incoming packets on the SPAN or VACL capture port.
- When a switch is being monitored with either SPAN or VACL capture for multiple VLANs, and the switch does not accept incoming packets with 802.1q headers.

  Note The TCP resets need 802.1q headers to tell which VLAN the resets should be sent on.

- When a network tap is used for monitoring a connection.

  Note Taps do not permit incoming traffic from the sensor.

  You can only assign a sensing interface as an alternate TCP reset interface. You cannot configure the management interface as an alternate TCP reset interface.

Interface Restrictions

The following restrictions apply to configuring interfaces on the sensor:

- Physical Interfaces
  - On modules (AIM IPS, AIP SSM, IDSM2, and NME IPS), all backplane interfaces have fixed speed, duplex, and state settings. These settings are protected in the default configuration on all backplane interfaces.
  - For nonbackplane FastEthernet interfaces the valid speed settings are 10 Mbps, 100 Mbps, and auto. Valid duplex settings are full, half, and auto.
  - For Gigabit copper interfaces (1000-TX on the IPS 4240, IPS 4255, IPS 4260, and IPS 4270-20), valid speed settings are 10 Mbps, 100 Mbps, 1000 Mbps, and auto. Valid duplex settings are full, half, and auto.
  - For Gigabit (copper or fiber) interfaces, if the speed is configured for 1000 Mbps, the only valid duplex setting is auto.
  - The command and control interface cannot also serve as a sensing interface.

- Inline Interface Pairs
  - Inline interface pairs can contain any combination of sensing interfaces regardless of the physical interface type (copper versus fiber), speed, or duplex settings of the interface. However, pairing interfaces of different media type, speeds, and duplex settings may not be fully tested or supported.
  - The command and control interface cannot be a member of an inline interface pair.
  - You cannot pair a physical interface with itself in an inline interface pair.
  - A physical interface can be a member of only one inline interface pair.
  - You can only configure bypass mode and create inline interface pairs on sensor platforms that support inline mode.
  - A physical interface cannot be a member of an inline interface pair unless the subinterface mode of the physical interface is **none**.
- Inline VLAN Pairs
  - You cannot pair a VLAN with itself.
  - You cannot use the default VLAN as one of the paired VLANs in an inline VLAN pair.
  - For a given sensing interface, a VLAN can be a member of only one inline VLAN pair. However, a given VLAN can be a member of an inline VLAN pair on more than one sensing interface.
  - The order in which you specify the VLANs in an inline VLAN pair is not significant.
  - A sensing interface in inline VLAN pair mode can have from 1 to 255 inline VLAN pairs.
- Alternate TCP Reset Interface
  - You can only assign the alternate TCP reset interface to a sensing interface. You cannot configure the command and control interface as an alternate TCP reset interface. The alternate TCP reset interface option is set to **none** as the default and is protected for all interfaces except the sensing interfaces.
  - You can assign the same physical interface as an alternate TCP reset interface for multiple sensing interfaces.
  - A physical interface can serve as both a sensing interface and an alternate TCP reset interface.
  - The command and control interface cannot serve as the alternate TCP reset interface for a sensing interface.
  - A sensing interface cannot serve as its own alternate TCP reset interface.
  - You can only configure interfaces that are capable of TCP resets as alternate TCP reset interfaces.

    Note The exception to this restriction is the IDSM2. The alternate TCP reset interface assignments for both sensing interfaces is System0/1 (protected).

- VLAN Groups
  - You can configure any single interface for promiscuous, inline interface pair, or inline VLAN pair mode, but no combination of these modes is allowed.
  - You cannot add a VLAN to more than one group on each interface.
  - You cannot add a VLAN group to multiple virtual sensors.

- An interface can have no more than 255 user-defined VLAN groups.
- When you pair a physical interface, you cannot subdivide it; you can subdivide the pair.
- You can use a VLAN on multiple interfaces; however, you receive a warning for this configuration.
- You can assign a virtual sensor to any combination of one or more physical interfaces and inline VLAN pairs, subdivided or not.
- You can subdivide both physical and logical interfaces into VLAN groups.
- CLI, IDM, and IME prompt you to remove any dangling references. You can leave the dangling references and continue editing the configuration.
- CLI, IDM, and IME do not allow configuration changes in Analysis Engine that conflict with the interface configuration.
- CLI allows configuration changes in the interface configuration that cause conflicts in the Analysis Engine configuration. IDM and IME do *not* allow changes in the interface configuration that cause conflicts in the Analysis Engine configuration.

Interface Modes

The following section describes the interface modes, and contains the following topics:

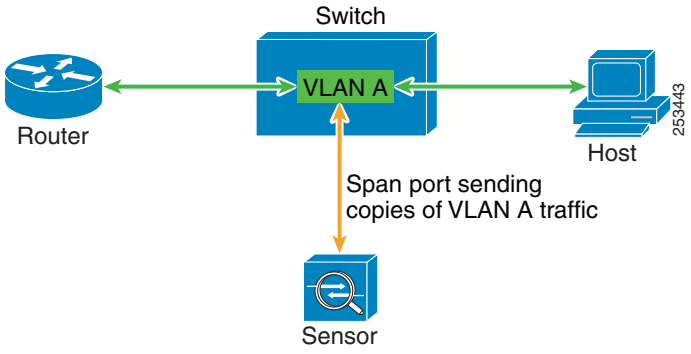
Promiscuous Mode

In promiscuous mode, packets do not flow through the sensor. The sensor analyzes a copy of the monitored traffic rather than the actual forwarded packet. The advantage of operating in promiscuous mode is that the sensor does not affect the packet flow with the forwarded traffic. The disadvantage of operating in promiscuous mode, however, is the sensor cannot stop malicious traffic from reaching its intended target for certain types of attacks, such as atomic attacks (single-packet attacks). The response actions implemented by promiscuous sensor devices are post-event responses and often require assistance from other networking devices, for example, routers and firewalls, to respond to an attack. While such response actions can prevent some classes of attacks, in atomic attacks the single packet has the chance of reaching the target system before the promiscuous-based sensor can apply an ACL modification on a managed device (such as a firewall, switch, or router).

By default, all sensing interfaces are in promiscuous mode. To change an interface from inline interface mode to promiscuous mode, delete any inline interface that contains that interface and delete any inline VLAN pair subinterfaces of that interface from the interface configuration.

Figure 1-2 illustrates promiscuous mode.

Figure 1-2 Promiscuous Mode



For More Information

For a list of restrictions pertaining to IPS sensor interfaces, see Interface Restrictions, page 1-10.

IPv6, Switches, and Lack of VACL Capture

VACLs on Catalyst switches do not have IPv6 support. The most common method for copying traffic to a sensor configured in promiscuous mode is to use VACL capture. If you want to have IPv6 support, you can use SPAN ports.

However, you can only configure up to two monitor sessions on a switch unless you use the following configuration:

- Monitor session
- Multiple trunks to one or more sensors
- Restrict per trunk port which VLANs are allowed to perform monitoring of many VLANs to more than two different sensors or virtual sensors within one IPS

The following configuration uses one SPAN session to send all of the traffic on any of the specified VLANs to all of the specified ports. Each port configuration only allows a particular VLAN or VLANs to pass. Thus you can send data from different VLANs to different sensors or virtual sensors all with one SPAN configuration line:

```
clear trunk 4/1-4 1-4094
set trunk 4/1 on dot1q 930
set trunk 4/2 on dot1q 932
set trunk 4/3 on dot1q 960
set trunk 4/4 on dot1q 962
set span 930, 932, 960, 962 4/1-4 both
```

Note The SPAN/Monitor configuration is valuable when you want to assign different IPS policies per VLAN or when you have more bandwidth to monitor than one interface can handle.

For More Information

- For more information on configuring SPAN/monitor on switches, refer to the following sections in *Catalyst 6500 Series Software Configuration Guide, 8.7*:
  - Configuring SPAN, RSPAN and the Mini Protocol Analyzer
  - Configuring SPAN on the Switch
  - Configuring Ethernet VLAN Trunks
  - Defining the Allowed VLANs on a Trunk
- For more information on promiscuous mode, see Promiscuous Mode, page 1-12.

Inline Interface Pair Mode

Operating in inline interface pair mode puts the IPS directly into the traffic flow and affects packet-forwarding rates making them slower by adding latency. This allows the sensor to stop attacks by dropping malicious traffic before it reaches the intended target, thus providing a protective service. Not only is the inline device processing information on Layers 3 and 4, but it is also analyzing the contents and payload of the packets for more sophisticated embedded attacks (Layers 3 to 7). This deeper analysis lets the system identify and stop and/or block attacks that would normally pass through a traditional firewall device.

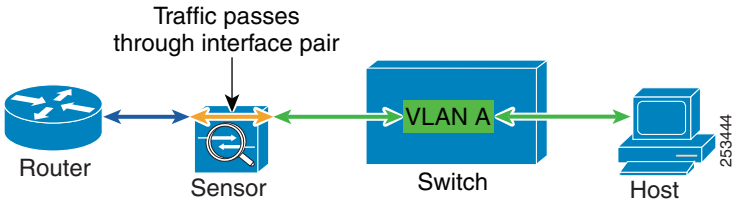
In inline interface pair mode, a packet comes in through the first interface of the pair on the sensor and out the second interface of the pair. The packet is sent to the second interface of the pair unless that packet is being denied or modified by a signature.

Note You can configure the AIM IPS, AIP SSM, and NME IPS to operate inline even though these modules have only one sensing interface.

Note If the paired interfaces are connected to the same switch, you should configure them on the switch as access ports with different access VLANs for the two ports. Otherwise, traffic does not flow through the inline interface.

Figure 1-3 illustrates inline interface pair mode.

Figure 1-3 Inline Interface Pair Mode



For More Information

For a list of restrictions pertaining to IPS sensor interfaces, see Interface Restrictions, page 1-10.

Inline VLAN Pair Mode

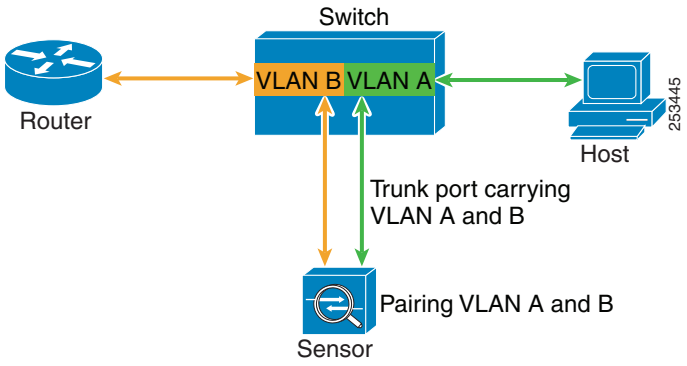
Note Inline VLAN pairs are not supported on the AIM IPS, AIP SSM, and NME IPS.

You can associate VLANs in pairs on a physical interface. This is known as inline VLAN pair mode. Packets received on one of the paired VLANs are analyzed and then forwarded to the other VLAN in the pair.

Inline VLAN pair mode is an active sensing mode where a sensing interface acts as an 802.1q trunk port, and the sensor performs VLAN bridging between pairs of VLANs on the trunk. The sensor inspects the traffic it receives on each VLAN in each pair, and can either forward the packets on the other VLAN in the pair, or drop the packet if an intrusion attempt is detected. You can configure an IPS sensor to simultaneously bridge up to 255 VLAN pairs on each sensing interface. The sensor replaces the VLAN ID field in the 802.1q header of each received packet with the ID of the egress VLAN on which the sensor forwards the packet. The sensor drops all packets received on any VLANs that are not assigned to inline VLAN pairs.

Figure 1-4 illustrates inline VLAN pair mode.

Figure 1-4 Inline VLAN Pair Mode



For More Information

For a list of restrictions pertaining to IPS sensor interfaces, see Interface Restrictions, page 1-10

VLAN Group Mode

Note You cannot divide physical interfaces that are in inline VLAN pairs into VLAN groups.

You can divide each physical interface or inline interface into VLAN group subinterfaces, each of which consists of a group of VLANs on that interface. Analysis Engine supports multiple virtual sensors, each of which can monitor one or more of these interfaces. This lets you apply multiple policies to the same sensor. The advantage is that now you can use a sensor with only a few interfaces as if it had many interfaces.

VLAN group subinterfaces associate a set of VLANs with a physical or inline interface. No VLAN can be a member of more than one VLAN group subinterface. Each VLAN group subinterface is identified by a number between 1 and 255.

Subinterface 0 is a reserved subinterface number used to represent the entire unvirtualized physical or logical interface. You cannot create, delete, or modify subinterface 0 and no statistics are reported for it.

An unassigned VLAN group is maintained that contains all VLANs that are not specifically assigned to another VLAN group. You cannot directly specify the VLANs that are in the unassigned group. When a VLAN is added to or deleted from another VLAN group subinterface, the unassigned group is updated.

Packets in the native VLAN of an 802.1q trunk do not normally have 802.1q encapsulation headers to identify the VLAN number to which the packets belong. A default VLAN variable is associated with each physical interface and you should set this variable to the VLAN number of the native VLAN or to 0. The value 0 indicates that the native VLAN is either unknown or you do not care if it is specified. If the default VLAN setting is 0, the following occurs:

- Any alerts triggered by packets without 802.1q encapsulation have a VLAN value of 0 reported in the alert.
- Non-802.1q encapsulated traffic is associated with the unassigned VLAN group and it is not possible to assign the native VLAN to any other VLAN group.

Note You can configure a port on a switch as either an access port or a trunk port. On an access port, all traffic is in a single VLAN is called the access VLAN. On a trunk port, multiple VLANs can be carried over the port, and each packet has a special header attached called the 802.1q header that contains the VLAN ID. This header is commonly referred as the VLAN tag. However, a trunk port has a special VLAN called the native VLAN. Packets in the native VLAN do not have the 802.1q headers attached. The IDSM2 can read the 802.1q headers for all nonnative traffic to determine the VLAN ID for that packet. However, the IDSM2 does not know which VLAN is configured as the native VLAN for the port in the switch configuration, so it does not know what VLAN the native packets are in. Therefore, you must tell the IDSM2 which VLAN is the native VLAN for that port. Then the IDSM2 treats any untagged packets as if they were tagged with the native VLAN ID.

For More Information

For a list of restrictions pertaining to IPS sensor interfaces, see Interface Restrictions, page 1-10.

Deploying VLAN Groups

Because a VLAN group of an inline pair does not translate the VLAN ID, an inline paired interface must exist between two switches to use VLAN groups on a logical interface. For an appliance, you can connect the two pairs to the same switch, make them access ports, and then set the access VLANs for the two ports differently. In this configuration, the sensor connects between two VLANs, because each of the two ports is in access mode and carries only one VLAN. In this case the two ports must be in different VLANs, and the sensor bridges the two VLANs, monitoring any traffic that flows between the two VLANs. The IDSM2 also operates in this manner, because its two data ports are always connected to the same switch.

You can also connect appliances between two switches. There are two variations. In the first variation, the two ports are configured as access ports, so they carry a single VLAN. In this way, the sensor bridges a single VLAN between the two switches.

In the second variation, the two ports are configured as trunk ports, so they can carry multiple VLANs. In this configuration, the sensor bridges multiple VLANs between the two switches. Because multiple VLANs are carried over the inline interface pair, the VLANs can be divided into groups and each group can be assigned to a virtual sensor. The second variation does not apply to the IDSM2 because it cannot be connected in this way.

For More Information

For the procedures for configuring VLAN groups for the IDSM2, refer to Configuring the IDSM2.

Supported Sensors

Caution Installing the most recent software on unsupported sensors may yield unpredictable results. We do not support software installed on unsupported platforms.

Table 1-4 lists the sensors (IPS appliances and modules) that are supported by Cisco IPS 7.0.

Table 1-4 Supported Sensors

Model Name	Part Number	Optional Interfaces
Appliances		
IPS 4240	IPS 4240-K9 IPS 4240-DC-K9[1]	— —
IPS 4255	IPS 4255-K9	—
IPS 4260	IPS 4260-K9 IPS 4260-4GE-BP-K9 IPS 4260-2SX-K9	IPS-4GE-BP-INT= IPS-2SX-INT= — —
IPS 4270-20	IPS-4270-K9 IPS-4270-4GE-BP-K9 IPS-4270-2SX-K9	IPS-4GE-BP-INT= IPS-2SX-INT= — —
Modules		
AIM IPS	AIM IPS-K9	—
AIP SSM-10	ASA-SSM-AIP-10-K9	—
AIP SSM-20	ASA-SSM-AIP-20-K9	—
AIP SSM-40	ASA-SSM-AIP-40-K9	—
IDSM2	WS-SVC-IDSM2-K9	—
NME IPS	NM-IPS-K9	—

1. The IPS 4240-DC-K9 is a NEBS-compliant product.

The following NRS and IDS appliance models are legacy models and are not supported in this document:

- NRS-2E
- NRS-2E-DM
- NRS-2FE
- NRS-2FE-DM
- NRS-TR

- NRS-TR-DM
- NRS-SFDDI
- NRS-SFDDI-DM
- NRS-DFDDI
- NRS-DFDDI-DM
- IDS-4220-E
- IDS-4220-TR
- IDS-4230-FE
- IDS-4230-SFDDI
- IDS-4230-DFDDI
- IDS-4210
- IDS-4215
- IDS-4235
- IDS-4250
- NM-CIDS

Note The WS-X6381, the IDSM, is a legacy model and is not supported in this document.

For More Information

For instructions on how to obtain the most recent Cisco IPS software, see Obtaining Cisco IPS Software, page 11-1.

IPS Appliances

This section describes the Cisco 4200 series appliance, and contains the following topics:

Introducing the IPS Appliance

The IPS appliance is a high-performance, plug-and-play device. The appliance is a component of the IPS, a network-based, real-time intrusion prevention system. You can use the IPS CLI, IDM, IME, ASDM, or CSM to configure the appliance.

You can configure the appliance to respond to recognized signatures as it captures and analyzes network traffic. These responses include logging the event, forwarding the event to the manager, performing a TCP reset, generating an IP log, capturing the alert trigger packet, and reconfiguring a router. The appliance offer significant protection to your network by helping to detect, classify, and stop threats including worms, spyware and adware, network viruses, and application abuse.

After being installed at key points in the network, the appliance monitors and performs real-time analysis of network traffic by looking for anomalies and misuse based on an extensive, embedded signature library. When the system detects unauthorized activity, appliances can terminate the specific connection, permanently block the attacking host, log the incident, and send an alert to the manager. Other legitimate connections continue to operate independently without interruption.

Appliances are optimized for specific data rates and are packaged in Ethernet, Fast Ethernet, and Gigabit Ethernet configurations. In switched environments, appliances must be connected to the SPAN port or VACL capture port of the switch.

The Cisco IPS 4200 series appliances provide the following:

- Protection of multiple network subnets through the use of up to eight interfaces
- Simultaneous, dual operation in both promiscuous and inline modes
- A wide array of performance options—from 80 Mbps to multiple gigabits
- Embedded web-based management solutions packaged with the sensor

For More Information

- For a list of IPS documents and how to access them, refer to *Documentation Roadmap for Cisco Intrusion Prevention System 7.0*.
- For a list of supported appliances, see Supported Sensors, page 1-17.
- For a description of each IPS appliance, see the following chapters in this document:
  - Chapter 2, “Installing the IPS 4240 and the IPS 4255”
  - Chapter 3, “Installing the IPS 4260”
  - Chapter 4, “Installing the IPS 4270-20”

Appliance Restrictions

The following restrictions apply to using and operating the appliance:

- The appliance is not a general purpose workstation.
- Cisco Systems prohibits using the appliance for anything other than operating Cisco IPS.
- Cisco Systems prohibits modifying or installing any hardware or software in the appliance that is not part of the normal operation of the Cisco IPS.

Connecting an Appliance to a Terminal Server

A terminal server is a router with multiple, low speed, asynchronous ports that are connected to other serial devices. You can use terminal servers to remotely manage network equipment, including appliances.

To set up a Cisco terminal server with RJ-45 or hydra cable assembly connections, follow these steps:

Step 1 Connect to a terminal server using one of the following methods:

- For terminal servers with RJ-45 connections, connect a 180 rollover cable from the console port on the appliance to a port on the terminal server.
- For hydra cable assemblies, connect a straight-through patch cable from the console port on the appliance to a port on the terminal server.

Step 2 Configure the line and port on the terminal server. In enable mode, enter the following configuration, where # is the line number of the port to be configured.

```
config t
line #
login
transport input all
stopbits 1
flowcontrol hardware
speed 9600
exit
exit
wr mem
```

Step 3 Be sure to properly close a terminal session to avoid unauthorized access to the appliance.

If a terminal session is not stopped properly, that is, if it does not receive an exit(0) signal from the application that initiated the session, the terminal session can remain open. When terminal sessions are not stopped properly, authentication is not performed on the next session that is opened on the serial port.

Caution Always exit your session and return to a login prompt before terminating the application used to establish the connection.

Caution If a connection is dropped or terminated by accident, you should reestablish the connection and exit normally to prevent unauthorized access to the appliance.

IPS Modules

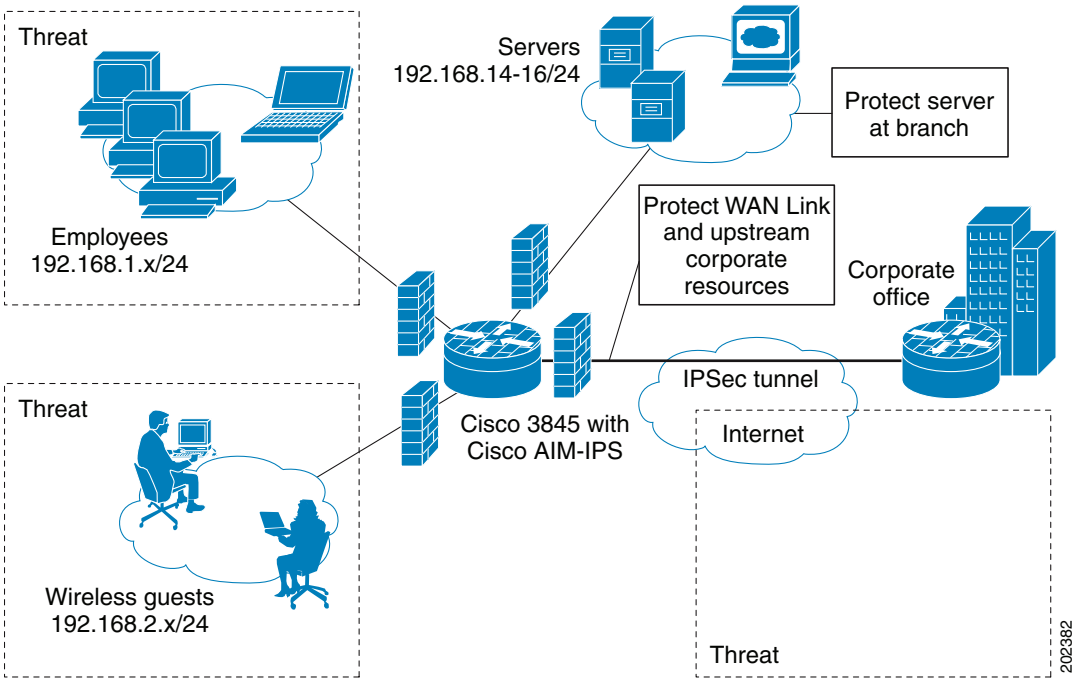
This section describes the IPS modules, and contains the following topics:

Introducing the AIM IPS

Cisco Intrusion Prevention System Advanced Integration Module (AIM IPS) integrates and bring inline Cisco IPS functionality to Cisco access routers. You can install the AIM IPS in Cisco 1841, 2800 series, and 3800 series routers.

Figure 1-5 demonstrates the integration of IPS and the branch office router.

Figure 1-5 AIM IPS and the Branch Router

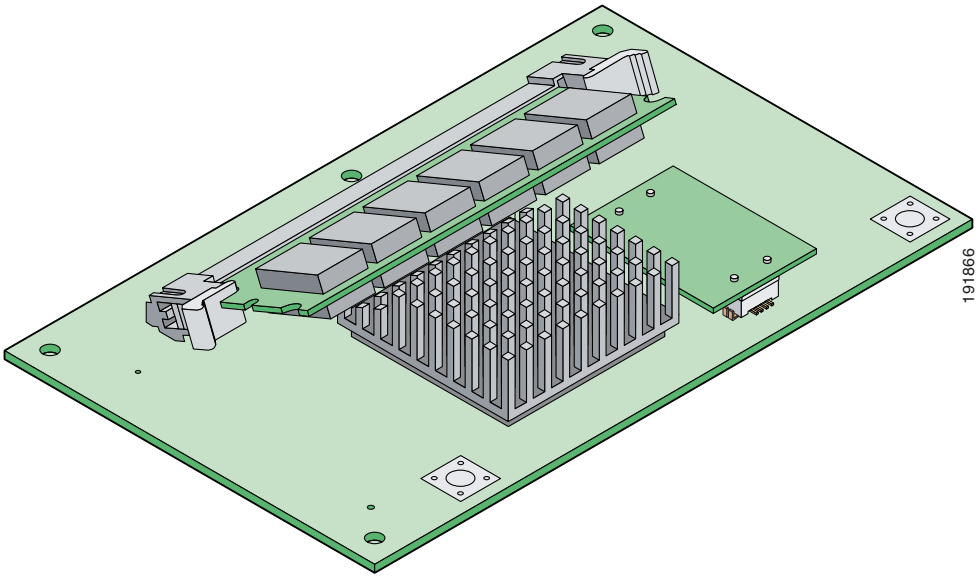


The AIM IPS has its own operating system, Cisco IPS software, startup, and run-time configurations. You launch and configure the AIM IPS through the router by means of a configuration session on the module. After the session, you return to the router CLI and clear the session.

The AIM IPS has a backplane interface, which means that all management traffic passes through the router interface rather than a dedicated port on the module. The AIM IPS does not have an external FastEthernet interface for handling management traffic. Management traffic includes all communications between applications, such as IDM, IME, CSM, and CS-MARS, and the servers on the module for exchange of IPS events, IP logs, configuration, and control messages.

The AIM IPS plugs in to a connector on the motherboard of the router and requires no external interfaces or connections. Figure 1-6 shows the AIM IPS.

Figure 1-6 AIM IPS



For More Information

- For a list of supported router and AIM IPS combinations, see Software and Hardware Requirements, page 5-2.
- For information on installing the AIM IPS, see Installation and Removal Instructions, page 5-5.
- For more information about sessioning to the AIM IPS, see Logging In to the AIM IPS, page 9-4.
- For more information about configuring the AIM IPS, refer to Configuring the AIM IPS.

Introducing the AIP SSM

The Cisco ASA Advanced Inspection and Prevention Security Services Module (AIP SSM) is the IPS plug-in module in the Cisco ASA 5500 series adaptive security appliance. The adaptive security appliance software integrates firewall, VPN, and intrusion detection and prevention capabilities in a single platform.

AIP SSM monitors and performs real-time analysis of network traffic by looking for anomalies and misuse based on an extensive, embedded signature library. When AIP SSM detects unauthorized activity, it can terminate the specific connection, permanently block the attacking host, log the incident, and send an alert to the device manager.

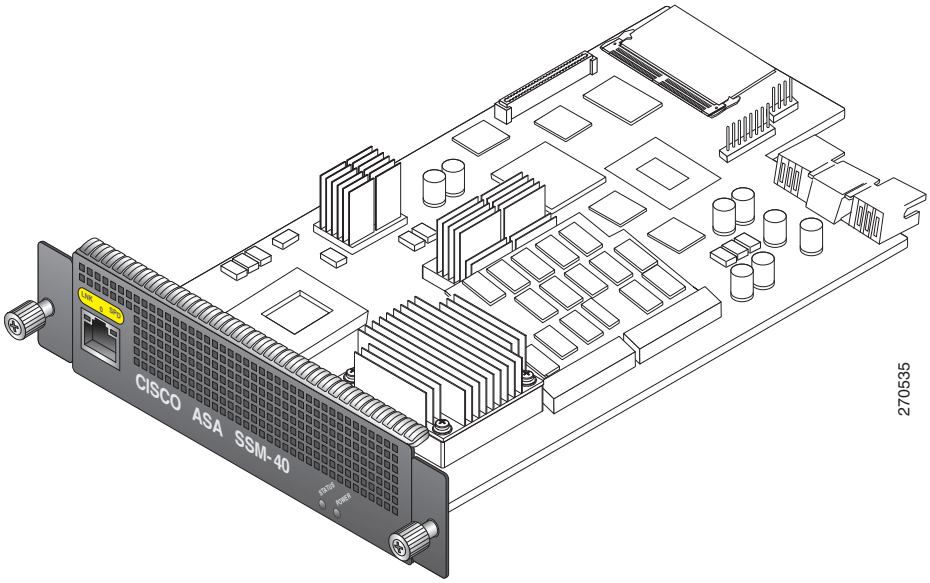
There are three models of AIP SSM:

- ASA-SSM-AIP-10-K9
  - Supports 150 Mbps of IPS throughput when installed in ASA 5510
  - Supports 225 Mbps of IPS throughput when installed in ASA 5520

- ASA-SSM-AIP-20-K9
  - Supports 375 Mbps of IPS throughput when installed in ASA 5520
  - Supports 500 Mbps of IPS throughput when installed in ASA 5540
- ASA-SSM-AIP-40-K9
  - Supports 450 Mbps of IPS throughput on the ASA 5520
  - Supports 650 Mbps IPS throughput on ASA 5540

Figure 1-7 shows the AIP SSM-40.

Figure 1-7 AIP SSM-40

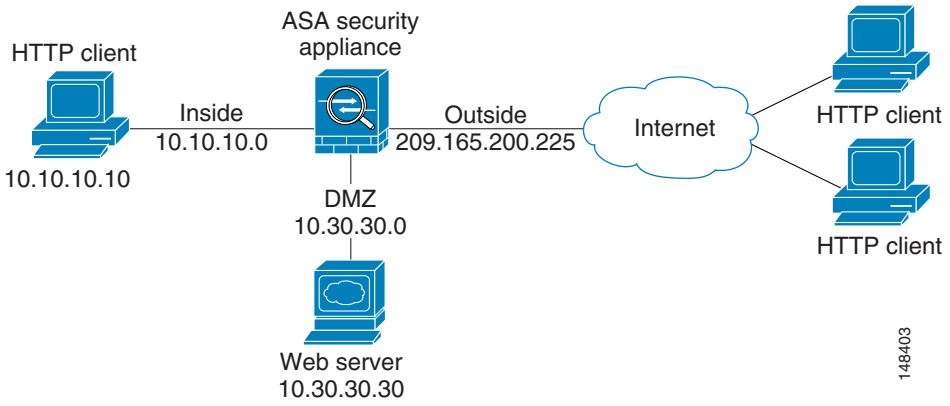


The AIP SSM runs in either inline mode or promiscuous mode. The adaptive security appliance diverts packets to the AIP SSM just before the packet exits the egress interface (or before VPN encryption occurs, if configured) and after other firewall policies are applied. For example, packets that are blocked by an access list are not forwarded to the AIP SSM.

In promiscuous mode, the IPS receives packets over the GigabitEthernet interface, examines them for intrusive behavior, and generates alerts based on a positive result of the examination. In inline mode, there is the additional step of sending all packets, which did not result in an intrusion, back out the GigabitEthernet interface.

Figure 1-8 on page 1-24 shows the adaptive security appliance with the AIP SSM in a typical DMZ configuration. A DMZ is a separate network located in the neutral zone between a private (inside) network and a public (outside) network. The web server is on the DMZ interface, and HTTP clients from both the inside and outside networks can access the web server securely.

Figure 1-8 DMZ Configuration



In Figure 1-8 an HTTP client (10.10.10.10) on the inside network initiates HTTP communications with the DMZ web server (30.30.30.30). HTTP access to the DMZ web server is provided for all clients on the Internet; all other communications are denied. The network is configured to use an IP pool (a range of IP addresses available to the DMZ interface) of addresses between 30.30.30.50 and 30.30.30.60.

For More Information

- For more information on setting up ASA, refer to the Getting Started Guides found at this URL:

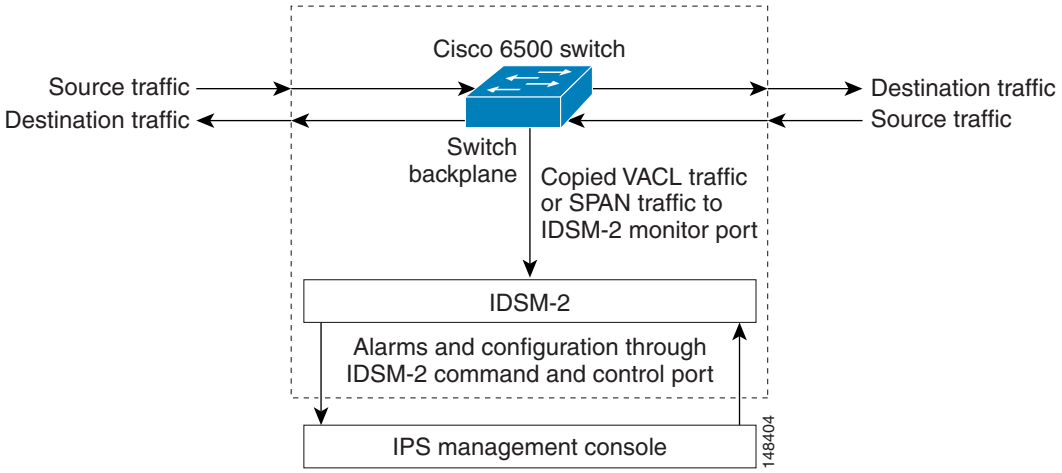
  http://www.cisco.com/en/US/products/ps6120/prod_installation_guides_list.html
- For more information on installing the AIP SSM, see Installing the AIP SSM, page 6-3.
- For more information on configuring the AIP SSM to receive IPS traffic, refer to Configuring the AIP SSM.

Introducing the IDSM2

The Cisco Catalyst 6500 Series Intrusion Detection System Services Module (IDSM2) is a switching module that performs intrusion prevention in the Catalyst 6500 series switch and 7600 series router. You can use the CLI or IDSM to configure the IDSM2. You can configure the IDSM2 for promiscuous or inline mode.

The IDSM2 performs network sensing—real-time monitoring of network packets through packet capture and analysis. The IDSM2 captures network packets and then reassembles and compares the packet data against attack signatures indicating typical intrusion activity. Network traffic is either copied to the IDSM2 based on security VACLs in the switch or is copied to the IDSM2 through the SPAN port feature of the switch. These methods route user-specified traffic to the IDSM2 based on switch ports, VLANs, or traffic type to be inspected (Figure 1-9 on page 1-25).

Figure 1-9 IDSM2 Block Diagram



The IDSM2 searches for patterns of misuse by examining either the data portion and/or the header portion of network packets. Content-based attacks contain potentially malicious data in the packet payload, whereas, context-based attacks contain potentially malicious data in the packet headers.

You can configure the IDSM2 to generate an alert when it detects potential attacks. Additionally, you can configure the IDSM2 to transmit TCP resets on the source VLAN, generate an IP log, and/or initiate blocking countermeasures on a firewall or other managed device. Alerts are generated by the IDSM2 through the Catalyst 6500 series switch backplane to the IPS manager, where they are logged or displayed on a graphical user interface.

For More Information

- For more information on installing the IDSM2, see Installing the IDSM2, page 7-5.
- For more information on configuring the IDSM2 to receive IPS traffic, refer to Configuring the IDSM2.

Introducing the NME IPS

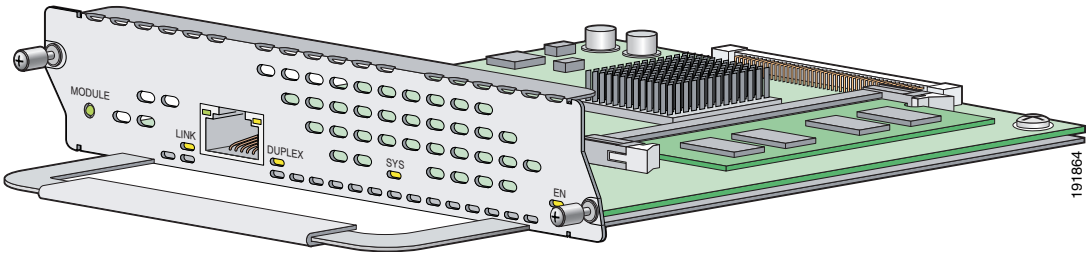
Cisco Intrusion Prevention System Network Module (NME IPS) integrates and brings inline Cisco IPS functionality to Cisco access routers. You can install the NME IPS in any one of the network module slots in the 2800 and 3800 series router.

The NME IPS has its own operating system, Cisco IPS software, startup, and run-time configurations. You launch and configure the modules through the router by means of a configuration session on the modules. After the session, you return to the router CLI and clear the session.

For the NME IPS, all management traffic passes through the external FastEthernet interface on the module. Management traffic includes all communications between applications, such as IDM, IME, CSM, and CS-MARS, and the servers on the module for exchange of IPS events, IP logs, configuration, and control messages.

The NME IPS installs in any slot in the 2800 and 3800 series access routers. Figure 1-10 shows the NME IPS.

Figure 1-10 NME IPS



For More Information

- For a list of supported router and NME IPS combinations, see Software and Hardware Requirements, page 8-2.
- For information on installing the NME IPS, see Installation and Removal Instructions, page 8-5.
- For more information about sessioning to the NME IPS, see Logging In to the NME IPS, page 9-9.
- For more information on configuring the NME IPS, refer to Configuring the NME IPS.

Time Sources and the Sensor

This section explains the importance of having a reliable time source for the sensors and how to correct the time if there is an error. It contains the following topics:

- The Sensor and Time Sources, page 1-26
- Synchronizing IPS Module System Clocks with the Parent Device System Clock, page 1-28
- Verifying the Sensor is Synchronized with the NTP Server, page 1-28
- Correcting the Time on the Sensor, page 1-29

The Sensor and Time Sources

The sensor requires a reliable time source. All events (alerts) must have the correct UTC and local time stamp, otherwise, you cannot correctly analyze the logs after an attack. When you initialize the sensor, you set up the time zones and summertime settings.

Note We recommend that you use an NTP server. You can use authenticated or unauthenticated NTP. For authenticated NTP, you must obtain the NTP server IP address, NTP server key ID, and the key value from the NTP server. You can set up NTP during initialization or you can configure NTP through the CLI, IDM, IME, or ASDM.

Here is a summary of ways to set the time on sensors:

- For appliances
  - Use the **clock set** command to set the time. This is the default.
  - Use NTP—You can configure the appliance to get its time from an NTP time synchronization source.
- For the IDSM2
  - The IDSM2 can automatically synchronize its clock with the switch time. This is the default. The UTC time is synchronized between the switch and the IDSM2. The time zone and summertime settings are not synchronized between the switch and the IDSM2.

    Note Be sure to set the time zone and summertime settings on both the switch and the IDSM2 to ensure that the UTC time settings are correct. The local time of the IDSM2 could be incorrect if the time zone and/or summertime settings do not match between the IDSM2 and the switch.

  - Use NTP—You can configure the IDSM2 to get its time from an NTP time synchronization source.
- For the AIM IPS and the NME IPS
  - The AIM IPS and the NME IPS can automatically synchronize their clock with the clock in the router chassis in which they are installed (parent router). This is the default. The UTC time is synchronized between the parent router and the AIM IPS and the NME IPS. The time zone and summertime settings are not synchronized between the parent router and the AIM IPS and the NME IPS.

    Note Be sure to set the time zone and summertime settings on both the parent router and the AIM IPS and the NME IPS to ensure that the UTC time settings are correct. The local time of the AIM IPS and the NME IPS could be incorrect if the time zone and/or summertime settings do not match between the AIM IPS and the NME IPS and the router.

  - Use NTP—You can configure the AIM IPS and the NME IPS to get their time from an NTP time synchronization source, such as a Cisco router, other than the parent router.
- For the AIP SSM
  - The AIP SSM can automatically synchronize its clock with the clock in the adaptive security appliance in which it is installed. This is the default. The UTC time is synchronized between the adaptive security appliance and the AIP SSM. The time zone and summertime settings are not synchronized between the adaptive security appliance and the AIP SSM.

    Note Be sure to set the time zone and summertime settings on both the adaptive security appliance and the AIP SSM to ensure that the UTC time settings are correct. The local time of the AIP SSM could be incorrect if the time zone and/or summertime settings do not match between the AIP SSM and the adaptive security appliance.

  - Use NTP—You can configure the AIP SSM to get its time from an NTP time synchronization source, such as a Cisco router other than the parent router.

Synchronizing IPS Module System Clocks with the Parent Device System Clock

All IPS modules (AIM IPS, AIP SSM, IDSM2, and NME IPS) synchronize their system clocks to the parent chassis clock (switch, router, or security appliance) each time the module boots up and any time the parent chassis clock is set. The module clock and parent chassis clock tend to drift apart over time. The difference can be as much as several seconds per day. To avoid this problem, make sure that both the module clock and the parent clock are synchronized to an external NTP server. If only the module clock or only the parent chassis clock is synchronized to an NTP server, the time drift occurs.

Verifying the Sensor is Synchronized with the NTP Server

In Cisco IPS, you cannot apply an incorrect NTP configuration, such as an invalid NTP key value or ID, to the sensor. If you try to apply an incorrect configuration, you receive an error message. To verify the NTP configuration, use the **show statistics host** command to gather sensor statistics. The NTP statistics section provides NTP statistics including feedback on sensor synchronization with the NTP server.

To verify the NTP configuration, follow these steps:

Step 1 Log in to the sensor.

Step 2 Generate the host statistics:

```
sensor# show statistics host
     ...
     NTP Statistics
             remote           refid      st t when poll reach   delay   offset  jitter
         11.22.33.44     CHU_AUDIO(1)     8 u   36   64    1    0.536    0.069   0.001
         LOCAL(0)        73.78.73.84      5 l   35   64    1    0.000    0.000   0.001
        ind assID status  conf reach auth condition  last_event cnt
          1 10372  f014   yes   yes   ok     reject   reachable  1
          2 10373  9014   yes   yes  none    reject   reachable  1
        status = Not Synchronized
     ...
```

Step 3 Generate the hosts statistics again after a few minutes:

```
sensor# show statistics host
     ...
     NTP Statistics
             remote           refid      st t when poll reach   delay   offset  jitter
        *11.22.33.44     CHU_AUDIO(1)     8 u   22   64  377    0.518   37.975  33.465
         LOCAL(0)        73.78.73.84      5 l   22   64  377    0.000    0.000   0.001
        ind assID status  conf reach auth condition  last_event cnt
          1 10372  f624   yes   yes   ok   sys.peer   reachable  2
          2 10373  9024   yes   yes  none    reject   reachable  2
        status = Synchronized
```

Step 4 If the status continues to read `Not Synchronized`, check with the NTP server administrator to make sure the NTP server is configured correctly.

Correcting the Time on the Sensor

If you set the time incorrectly, your stored events will have the incorrect time because they are stamped with the time the event was created.

The Event Store time stamp is always based on UTC time. If during the original sensor setup, you set the time incorrectly by specifying 8:00 p.m. rather than 8:00 a.m., when you do correct the error, the corrected time will be set backwards. New events might have times older than old events.

For example, if during the initial setup, you configure the sensor as central time with daylight saving time enabled and the local time is 8:04 p.m., the time is displayed as 20:04:37 CDT and has an offset from UTC of -5 hours (01:04:37 UTC, the next day). A week later at 9:00 a.m., you discover the error: the clock shows 21:00:23 CDT. You then change the time to 9:00 a.m. and now the clock shows 09:01:33 CDT. Because the offset from UTC has not changed, it requires that the UTC time now be 14:01:33 UTC, which creates the time stamp problem.

To ensure the integrity of the time stamp on the event records, you must clear the event archive of the older events by using the **clear events** command.

Note You cannot remove individual events.

For More Information

For the procedure for clearing events, refer to Clearing Events from Event Store.

Installation Preparation

To prepare for installing sensors, follow these steps:

Step 1 Review the safety precautions outlined in *Regulatory Compliance and Safety Information for the Cisco Intrusion Prevention System 4200 Series Appliance Sensor*.

Step 2 To familiarize yourself with the IPS and related documentation and where to find it on Cisco.com, read *Documentation Roadmap for Cisco Intrusion Prevention System 7.0*.

Step 3 Before proceeding with sensor installation, read the appropriate Release Notes.

Step 4 Unpack the sensor.

Step 5 Place the sensor in an ESD-controlled environment.

Step 6 Place the sensor on a stable work surface.

Step 7 In this book, *Installing and Using Cisco Intrusion Prevention System Sensors and Modules 7.0*, see the chapter that pertains to your sensor model.

For More Information

- For ESD guidelines, see Electrical Safety Guidelines, page 1-31.
- For the procedure for working in an ESD environment, see Working in an ESD Environment, page 1-32.

Site and Safety Guidelines

This section describes site guidelines and safety precautions to take when working with electricity, with power supplies, and in an ESD environment. It contains the following topics:

Site Guidelines

Place the appliance on a desktop or mount it in a rack. The location of the appliance and the layout of the equipment rack or wiring room are extremely important for proper system operation. Equipment placed too close together, inadequate ventilation, and inaccessible panels can cause system malfunctions and shutdowns, and can make appliance maintenance difficult.

When planning the site layout and equipment locations, keep in mind the following precautions to help avoid equipment failures and reduce the possibility of environmentally-caused shutdowns. If you are experiencing shutdowns or unusually high errors with your existing equipment, these precautions may help you isolate the cause of failures and prevent future problems.

- 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.
- Always follow the ESD-prevention procedures to avoid damage to equipment. Damage from static discharge can cause immediate or intermittent equipment failure.
- Make sure that the chassis top panel is secure. The chassis is designed to allow cooling air to flow effectively within it. An open chassis allows air leaks, which can interrupt and redirect the flow of cooling air from the internal components.

Rack Configuration Guidelines

Follow these guidelines to plan your equipment rack configuration:

- Enclosed racks must have adequate ventilation. Make sure the rack is not overly congested because each chassis generates heat. An enclosed rack should have louvered sides and a fan to provide cooling air.
- When mounting a chassis in an open rack, make sure the rack frame does not block the intake or exhaust ports. If the chassis is installed on slides, check the position of the chassis when it is seated all the way into the rack.
- In an enclosed rack with a ventilation fan in the top, excessive 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. Make sure 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.

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.
- 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*.

Power Supply Guidelines

Follow these guidelines for power supplies:

- Check the power at the site before installing the chassis to ensure that the power is free of spikes and noise. Install a power conditioner if necessary, to ensure proper voltages and power levels in the source voltage.
- Install proper grounding for the site to avoid damage from lightning and power surges.
- The following applies to a chassis equipped with an AC-input power supply:
  - The chassis does not have a user-selectable operating range. Refer to the label on the chassis for the correct AC-input power requirement.
  - Several types of AC-input power supply cords are available; make sure you have the correct type for your site.
  - Install a UPS for your site.
  - Install proper site-grounding facilities to guard against damage from lightning or power surges.
- The following applies to a chassis equipped with a DC-input power supply:
  - Each DC-input power supply requires dedicated 15-amp service.
  - For DC power cables, we recommend a minimum of 14 AWG wire cable.
  - The DC return connection to this system is to remain isolated from the system frame and chassis.

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.

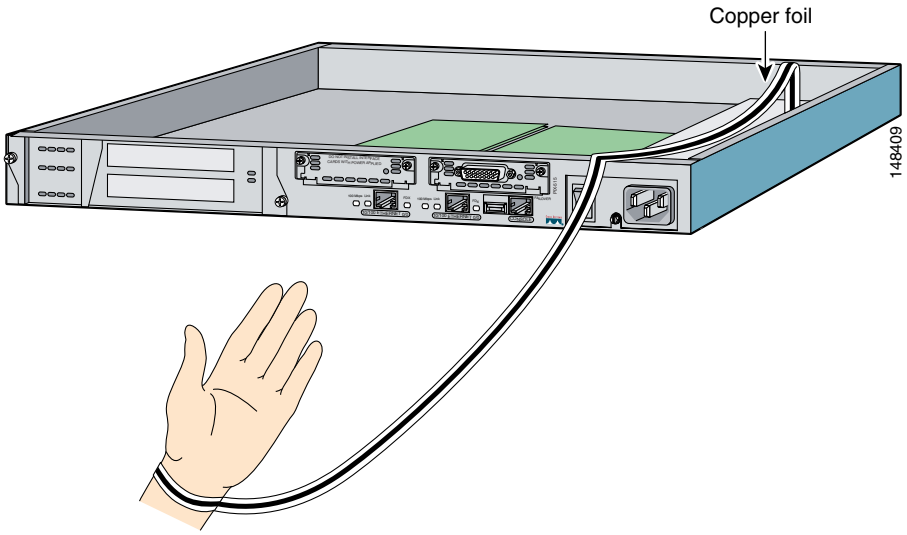
To remove and replace components in a sensor, follow these steps:

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.

Cable Pinouts

This section describes pinout information for 10/100/1000BaseT, console, and RJ 45 to DB 9 ports, and the MGMT 10/100 Ethernet port. It contains the following topics:

10/100BaseT and 10/100/1000BaseT Connectors

Sensors support 10/100/1000BaseT ports. You must use at least a Category 5 cable for 100/1000Base-TX operations. You can use a Category 3 cable for 10Base-TX operations.

Note Some sensors support 10/100BaseT (IDS-4210, IDS-4215, and the optional 4FE card) while others support 10/100/1000BaseT (IDS-4235, IDS-4250-TX, IPS 4240, and IPS 4255). This only applies to the copper appliances. The fiber appliances support 1000Base-SX only.

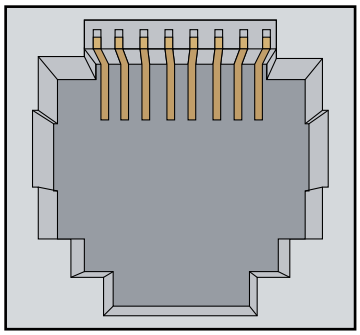
The 10/100/1000BaseT ports use standard RJ-45 connectors and support MDI and MDI-X connectors. Ethernet ports normally use MDI connectors and Ethernet ports on a hub normally use MDI-X connectors.

An Ethernet straight-through cable is used to connect an MDI to an MDI-X port. A cross-over cable is used to connect an MDI to an MDI port, or an MDI-X to an MDI-X port.

Figure 1-11 shows the 10/100BaseT (RJ-45) port pinouts.

Figure 1-11 10/100 Port Pinouts

Pin	Label
1	TD+
2	TD-
3	RD+
4	NC
5	NC
6	RD-
7	NC
8	NC

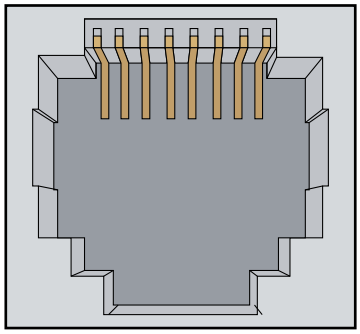


148407

Figure 1-12 shows the 10/100/1000BaseT (RJ-45) port pinouts.

Figure 1-12 10/100/1000 Port Pinouts

Pin	Label
1	TP0+
2	TP0-
3	TP1+
4	TP2+
5	TP2-
6	TP1-
7	TP3+
8	TP3-



148410

Console Port (RJ-45)

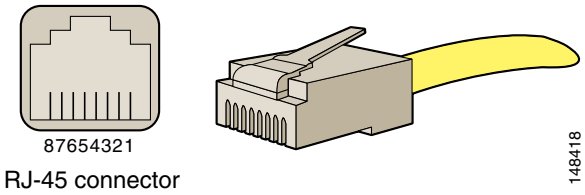
Cisco products use the following types of RJ-45 cables:

- Straight-through
- Cross-over
- Rolled (console)

Note Cisco does not provide these cables; however, they are widely available from other sources.

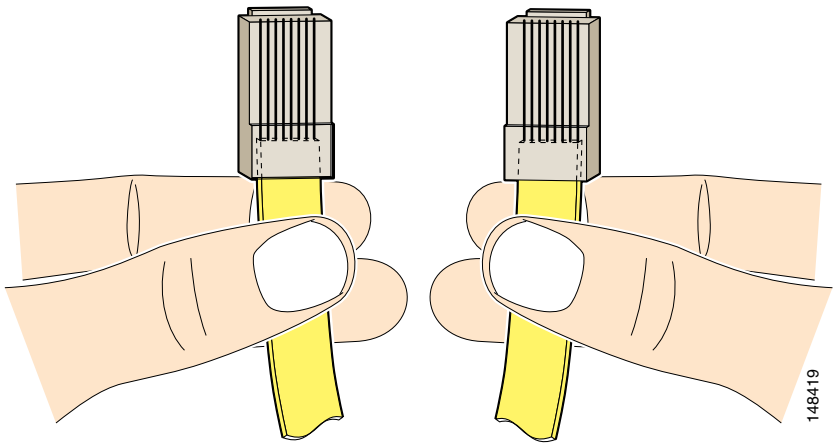
Figure 1-13 shows the RJ 45 cable.

Figure 1-13 RJ-45 Cable



To identify the RJ-45 cable type, hold the two ends of the cable next to each other so that you can see the colored wires inside the ends, as shown in Figure 1-14.

Figure 1-14 RJ-45 Cable Identification



Examine the sequence of colored wires to determine the type of RJ-45 cable, as follows:

- Straight-through—The colored wires are in the same sequence at both ends of the cable.
- Cross-over—The first (far left) colored wire at one end of the cable is the third colored wire at the other end of the cable.
- Rolled—The colored wires are in the opposite sequence at either end of the cable.

RJ-45 to DB-9 or DB-25

Table 1-5 lists the cable pinouts for RJ-45 to DB-9 or DB-25.

Table 1-5 Cable Pinouts for RJ-45 to DB-9 or DB-25

Signal	RJ-45 Pin	DB-9 /DB-25 Pin
RTS	8	8
DTR	7	6
TxD	6	2
GND	5	5
GND	4	5
RxD	3	3
DSR	2	4
CTS	1	7

CHAPTER 2

Installing the IPS 4240 and the IPS 4255

Note All IPS platforms allow ten concurrent CLI sessions.

This chapter describes the IPS 4240 and the IPS 4255 and how to install them. It also describes the accessories and how to install them. This chapter contains the following sections:

Introducing the IPS 4240 and the IPS 4255

The IPS 4240 and the IPS 4255 deliver high port density in a small form factor. They use a compact flash device for storage rather than the hard-disk drives used in other sensor models. The IPS 4240 and the IPS 4255 do not support redundant power supplies.

The IPS 4240 replaces the IDS-4235. There are four 10/100/1000 copper sensing interfaces. The IPS 4240 is available with either AC or DC power. It monitors up to 250 Mbps of aggregate network traffic on multiple sensing interfaces and is inline ready. The 250-Mbps performance for the IPS 4240 is based on the following conditions:

- 2500 new TCP connections per second
- 2500 HTTP transactions per second
- Average packet size of 445 bytes
- Running Cisco IPS 5.1 or later

Note The 250-Mbps performance is traffic combined from all four sensing interfaces.

The IPS 4255 replaces the IDS-4250-TX. There are four 10/100/1000 copper sensing interfaces. It monitors up to 600 Mbps of aggregate network traffic on multiple sensing interfaces and is also inline ready. The 600-Mbps performance for the IPS 4255 is based on the following conditions:

- 6000 new TCP connections per second
- 6000 HTTP transactions per second
- Average packet size of 445 bytes
- Running Cisco IPS 5.1 or later

Note The 600-Mbps performance is traffic combined from all four sensing interfaces.

Front and Back Panel Features

Note Although the illustrations show the IPS 4240, the IPS 4255 has the same front and back panel features and indicators.

This section describes the IPS 4240 and the IPS 4255 front and back panel features and indicators.

Figure 2-1 shows the front view of the IPS 4240 and the IPS 4255.

Figure 2-1 IPS 4240/IPS 4255 Front Panel Features

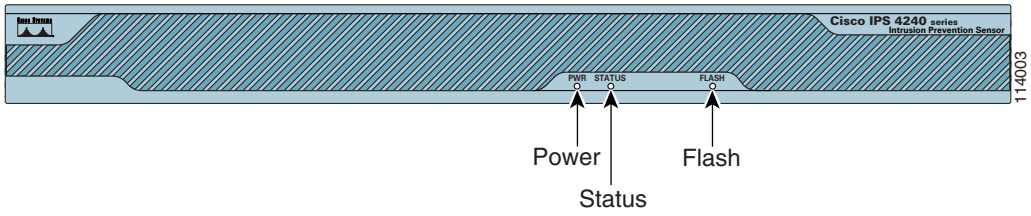


Table 2-1 describes the front panel indicators on the IPS 4240 and the IPS 4255.

Table 2-1 Front Panel Indicators

Indicator	Description
Power	Off indicates no power. Green when the power supply is running.
Status	Blinks green while the power-up diagnostics are running or the system is booting. Solid green when the system has passed power-up diagnostics. Solid amber when the power-up diagnostics have failed.
Flash	Off when the compact flash device is not being accessed. Blinks green when the compact flash device is being accessed.

Figure 2-2 shows the back view of the IPS 4240 and the IPS 4255.

Figure 2-2 IPS 4240 and IPS 4255 Back Panel Features

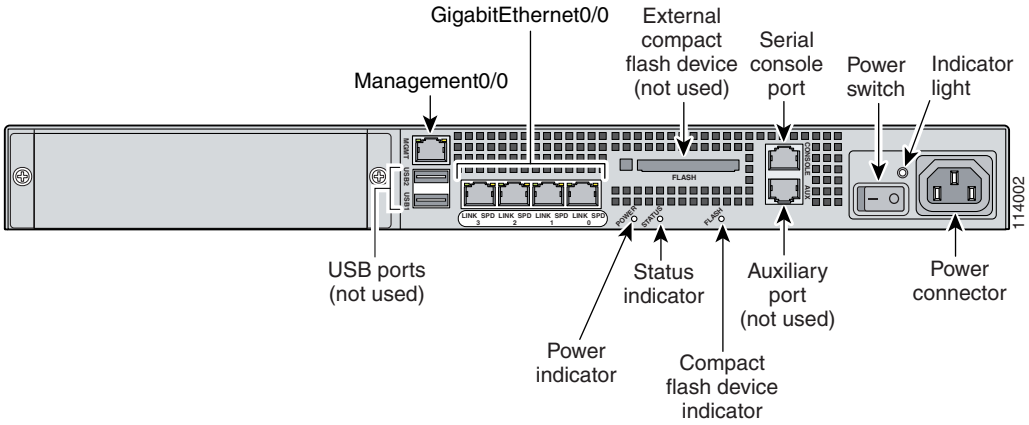


Figure 2-3 shows the four built-in Ethernet ports, which have two indicators per port.

Figure 2-3 Ethernet Port Indicators

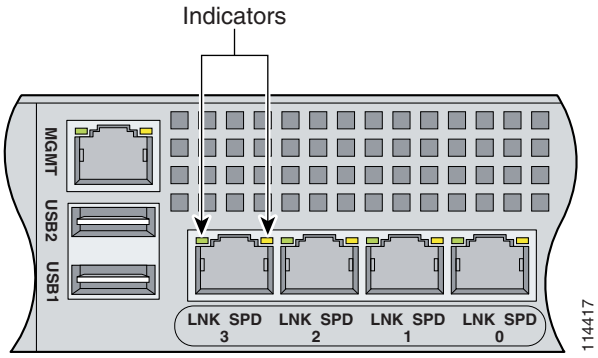


Table 2-2 lists the back panel indicators.

Table 2-2 Back Panel Indicators

Indicator	Color	Description
Left side	Green solid Green blinking	Physical link Network activity
Right side	Not lit Green Amber	10 Mbps 100 Mbps 1000 Mbps

Specifications

Table 2-3 lists the specifications for the IPS 4240 and the IPS 4255.

Table 2-3 IPS 4240 and IPS 4255 Specifications

Dimensions and Weight	
Height	1.75 in. (4.45 cm)
Width	17.5 in. (44.45 cm)
Depth	14.5 in. (36.83 cm)
Weight	20.0 lb (9.07 kg)
Form factor	1 RU, standard 19-inch rack-mountable
Expansion	One chassis expansion slot (not used)
Power	
Autoswitching	100V to 240V AC
Frequency	47 to 63 Hz, single phase
Operating current	3.0 A
Steady state	150 W
Maximum peak	190 W
Maximum heat dissipation	648 BTU/hr, full power usage (65 W)
Environment	
Temperature	Operating +32°F to +104°F (+0°C to +40°C) Nonoperating -13°F to +158°F (-25°C to +70°C)
Relative humidity	Operating 5% to 95% (noncondensing) Nonoperating 5% to 95% (noncondensing)
Altitude	Operating 0 to 9843 ft (3000 m) Nonoperating 0 to 15,000 ft (4750 m)
Shock	Operating 1.14 m/sec (45 in./sec) ½ sine input Nonoperating 30 G
Vibration	0.41 Grms2 (3 to 500 Hz) random input
Acoustic noise	60 dBa (maximum)

Connecting the IPS 4240 to a Cisco 7200 Series Router

When an IPS 4240 is connected directly to a 7200 series router and both the IPS 4240 and the router interfaces are hard-coded to speed 100 with duplex Full, the connection does not work. If you set the IPS 4240 to speed Auto and duplex Auto, it connects to the router but only at speed 100 and duplex Half.

To connect correctly at speed 100 and duplex Full, set the interfaces of both the IPS 4240 and the router to speed Auto and duplex Auto. Also, if either interface is hard-coded, you must make the connection using a crossover cable.

Accessories

The IPS 4240 and the IPS 4255 accessories kit contains the following:

- DB25 connector
- DB9 connector
- Rack mounting kit—screws, washers, and metal bracket
- RJ45 console cable
- Two 6-ft Ethernet cables

Important Safety Instructions

Warning **IMPORTANT SAFETY INSTRUCTIONS**

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

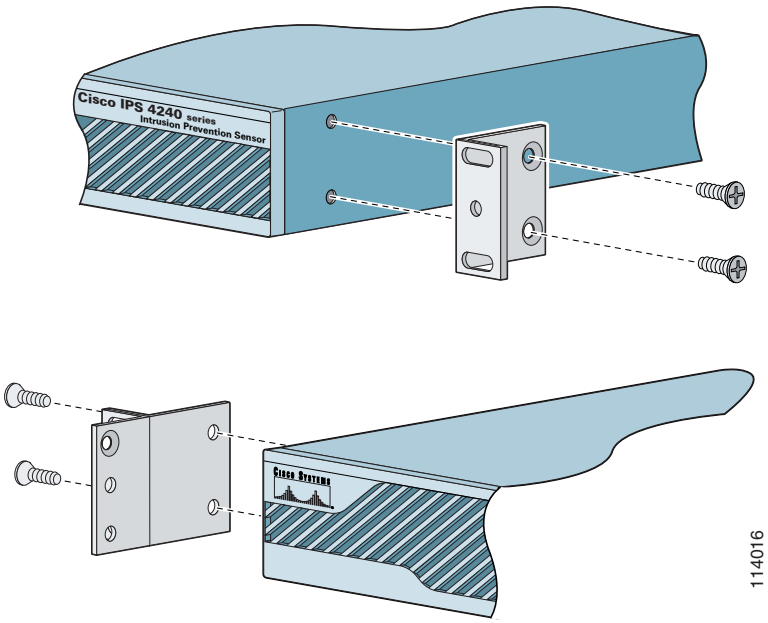
Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment. Statement 1030**

Rack Mounting

To rack mount the IPS 4240 and the IPS 4255, follow these steps:

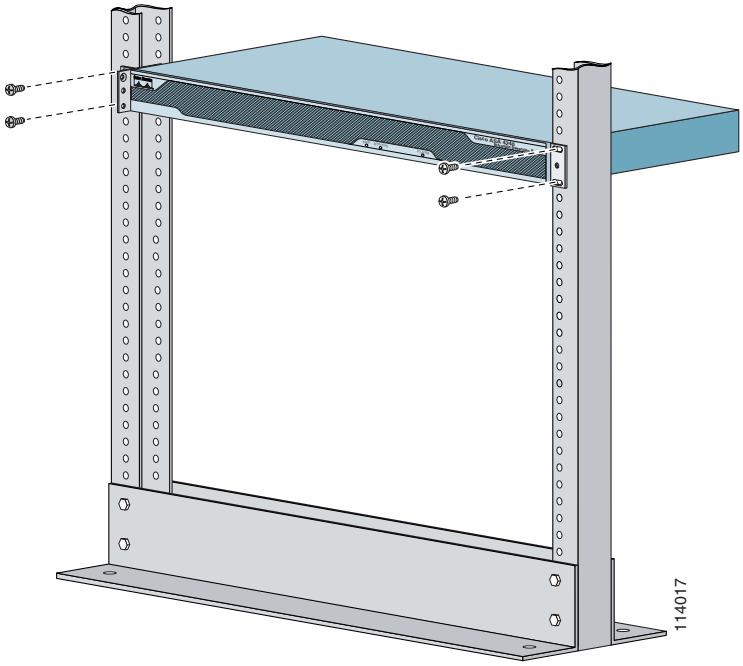
Step 1 Attach the bracket to the appliance using the supplied screws.

You can attach the brackets to the holes near the front of the appliance.



Note The top hole on the left bracket is a banana jack you can use for ESD grounding purposes when you are servicing the system. You can use the two threaded holes to mount a ground lug to ground the chassis.

Step 2 Use the supplied screws to attach the appliance to the equipment rack.



Step 3 To remove the appliance from the rack, remove the screws that attach the appliance to the rack, and then remove the appliance.

Installing the IPS 4240 and the IPS 4255

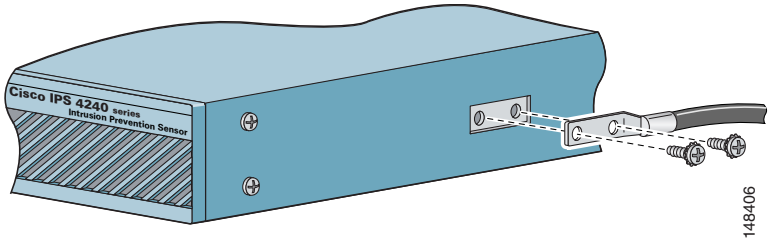
Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment. Statement 1030**

Caution Follow proper safety procedures when performing these steps by reading the safety warnings in *Regulatory Compliance and Safety Information for the Cisco Intrusion Prevention System 4200 Series Appliance Sensor*.

To install the IPS 4240 and the IPS 4255 on the network, follow these steps:

Step 1 Position the appliance on the network.

Step 2 Attach the grounding lug to the side of the appliance.



Note Use 8-32 screws to connect a copper standard barrel grounding lug to the holes. The appliance requires a lug where the distance between the center of each hole is 0.56 inches. The ground lug must be NRTL listed or recognized. In addition, the copper conductor (wires) must be used and the copper conductor must comply with the NEC code for ampacity. A lug is not supplied with the appliance.

Step 3 Place the appliance in a rack, if you are rack mounting it.

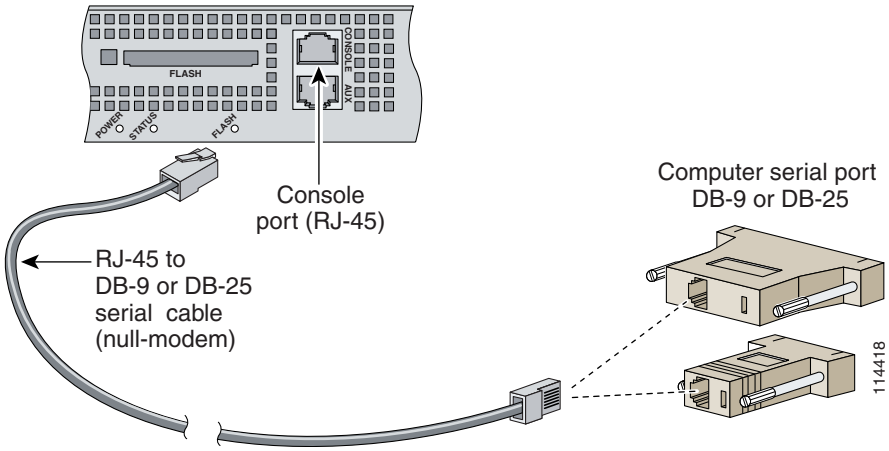
Step 4 Attach the power cord to the appliance and plug it in to a power source (a UPS is recommended).

Step 5 Connect the cable as shown in Step 6 so that you have either a DB-9 or DB-25 connector on one end as required by the serial port for your computer, and the other end is the RJ-45 connector.

Note Use the console port to connect to a computer to enter configuration commands. Locate the serial cable from the accessory kit. The serial cable assembly consists of a 180/rollover cable with RJ-45 connectors (DB-9 connector adapter PN 74-0495-01 and DB-25 connector adapter PN 29-0810-01).

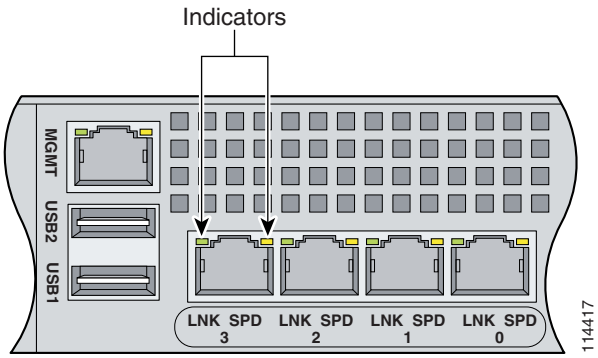
Note You can use a 180/rollover or straight-through patch cable to connect the appliance to a port on a terminal server with RJ-45 or hydra cable assembly connections. Connect the appropriate cable from the console port on the appliance to a port on the terminal server.

Step 6 Connect the RJ-45 connector to the console port and connect the other end to the DB-9 or DB-25 connector on your computer.



Step 7 Attach the network cables to the following interfaces:

- GigabitEthernet0/0, GigabitEthernet0/1, GigabitEthernet0/2, and GigabitEthernet0/3 (from right to left) are sensing ports.
- Management0/0 is the command and control port.



Caution Management and console ports are privileged administrative ports. Connecting them to an untrusted network can create security concerns.

Step 8 Power on the appliance.

Step 9 Initialize the appliance.

Step 10 Upgrade the appliance with the most recent Cisco IPS software. You are now ready to configure intrusion prevention on the appliance.

For More Information

- DC power guidelines are listed in *Regulatory Compliance and Safety Information for the Cisco Intrusion Detection and Prevention System 4200 Series Appliance Sensor*.
- For more information on working with electrical power and in an ESD environment, see Site and Safety Guidelines, page 1-30.
- For the procedure for placing IPS 4250-DC in a rack, see Rack Mounting, page 2-6.
- For the instructions for setting up a terminal server, see Connecting an Appliance to a Terminal Server, page 1-19.
- For the procedure for using the **setup** command to initialize IPS 4250-DC, see Basic Sensor Setup, page 10-4.
- For the procedure for updating IPS-4250-DC with the most recent cisco IPS software, see Obtaining Cisco IPS Software, page 11-1.
- If you have the IPS 4240-DC model, see Installing the IPS 4240-DC, page 2-10.
- For the procedure for using HTTPS to log in to IDM, refer to Logging In to IDM.
- For the procedures for configuring intrusion prevention on your sensor, refer to the following documents:
  - *Installing and Using Cisco Intrusion Prevention System Device Manager 7.0*
  - *Installing and Using Cisco Intrusion Prevention System Manager Express 7.0*
  - *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 7.0*

Installing the IPS 4240-DC

The the IPS 4240-DC-K9 (NEBS-compliant) model equipped with DC-input power supply 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.

Warning **Before performing any of the following procedures, ensure that power is removed from the DC circuit. To ensure that all power is OFF, locate the circuit breaker on the panel board that services the DC circuit, switch the circuit breaker to the OFF position, and tape the switch handle of the circuit breaker in the OFF position.**

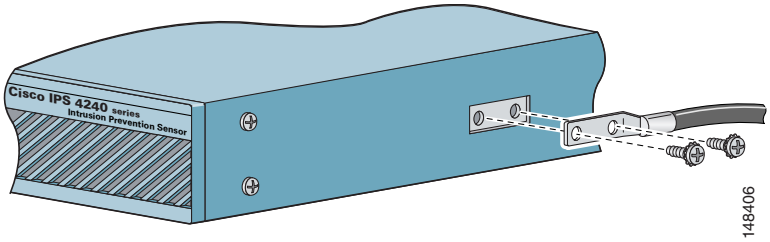
Note The DC return connection should remain isolated from the system frame and chassis (DC-I). This equipment is suitable for connection to intra-building wiring only.

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment. Statement 1030**

To install the IPS 4240-DC, follow these steps:

Step 1 Position the IPS 4240-DC on the network.

Step 2 Attach the grounding lug to the side of the appliance.



Note Use 8-32 screws to connect a copper standard barrel grounding lug to the holes. The appliance requires a lug where the distance between the center of each hole is 0.56 inches. The ground lug must be NRTL listed or recognized. In addition, the copper conductor (wires) must be used and the copper conductor must comply with the NEC code for ampacity. A lug is not supplied with the appliance.

Step 3 Place the appliance in a rack, if you are rack mounting it.

Step 4 Terminate 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.

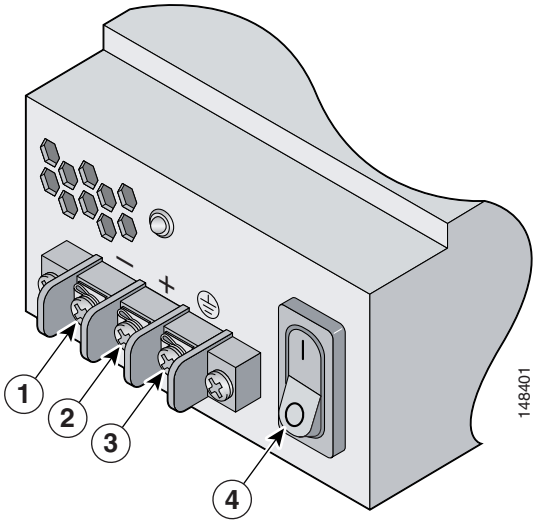
Step 5 Locate the DC-input terminal box.

Step 6 Power off the IPS 4240-DC.

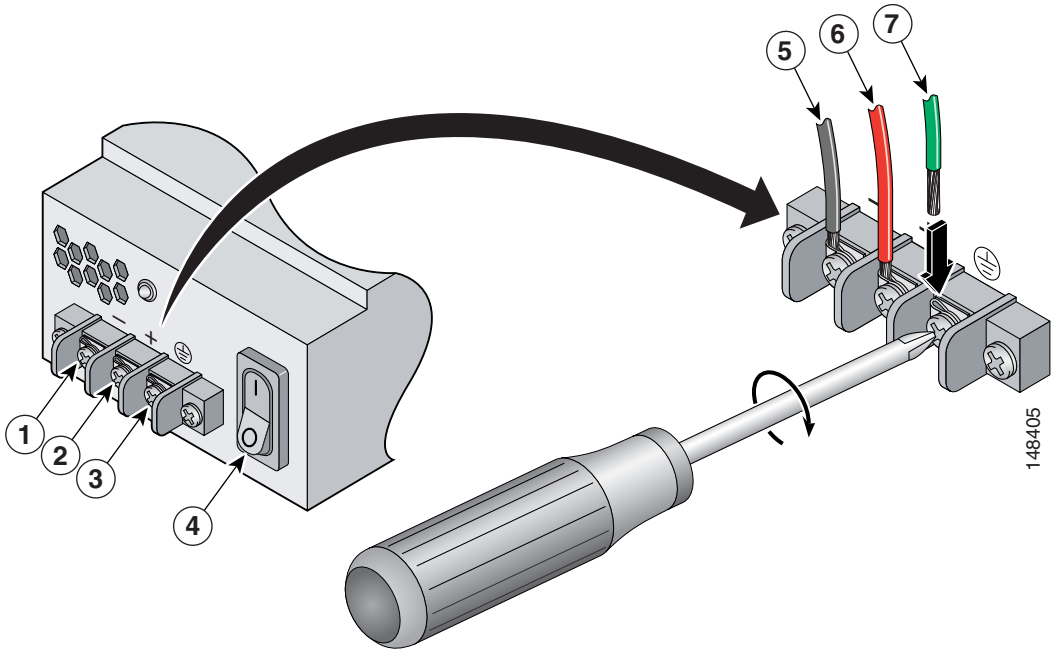
Make sure that power is removed from the DC circuit. To make sure all power is OFF, locate the circuit breaker on the panel board that services the DC circuit, switch the circuit breaker to the OFF position, and tape the switch handle of the circuit breaker in the OFF position.

Step 7 Remove the DC power supply plastic shield.

Step 8 Strip the ends of the wires for insertion into the power connect lugs on the IPS 4240-DC.



Step 9 Insert the ground wire into the connector for the earth ground and tighten the screw on the connector. Using the same method as for the ground wire, connect the negative wire and then the positive wire.



1	Negative	**5**	Negative
2	Positive	**6**	Positive
3	Ground	**7**	Ground
4	On/Off Switch		

Note The DC return connection to this system is to remain isolated from the system frame and chassis.

Step 10 After wiring the DC power supply, remove the tape from the circuit breaker switch handle and reinstate power by moving the handle of the circuit breaker to the ON position.

Step 11 Replace the DC power supply plastic shield.

Step 12 Power on the IPS 4240-DC from the switch at the back of the chassis.

Note If you need to power cycle the IPS 4240-DC, wait at least 5 seconds between powering it off and powering it back on.

Step 13 Initialize the IPS 4240-DC.

Step 14 Upgrade the IPS 4240-DC with the most recent Cisco IPS software.

You are now ready to configure intrusion prevention on the appliance.

For More Information

- DC power guidelines are listed in *Regulatory Compliance and Safety Information for the Cisco Intrusion Prevention System 4200 Series Appliance Sensor*.
- For more information on working with electrical power and in an ESD environment, see Site and Safety Guidelines, page 1-30.
- For the procedure for placing IPS 4250-DC in a rack, see Rack Mounting, page 2-6.
- For the procedure for using the **setup** command to initialize IPS 4250-DC, see Basic Sensor Setup, page 10-4.
- For the procedure for updating IPS 4250-DC with the most recent cisco IPS software, see Obtaining Cisco IPS Software, page 11-1.
- For the procedure for using HTTPS to log in to IDM, refer to Logging In to IDM.
- For the procedures for configuring intrusion prevention on your sensor, refer to the following guides:
  - *Installing and Using Cisco Intrusion Prevention System Device Manager 7.0*
  - *Installing and Using Cisco Intrusion Prevention System Manager Express 7.0*
  - *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 7.0*

CHAPTER 3

Installing the IPS 4260

Note All IPS platforms allow ten concurrent CLI sessions.

This chapter describes the IPS 4260 and how to install it. It also describes the accessories and how to install them. This chapter contains the following sections:

Introducing the IPS 4260

Caution The BIOS on the IPS 4260 is specific to the IPS 4260 and must only be upgraded under instructions from Cisco with BIOS files obtained from the Cisco website. Installing a non-Cisco or third-party BIOS on the IPS 4260 voids the warranty.

The IPS 4260 delivers 1 Gigabit of intrusion prevention performance. You can use the IPS 4260 to protect both Gigabit subnets and aggregated traffic traversing switches from multiple subnets. The IPS 4260 is a purpose-built device that has support for both copper and fiber NIC environments thus providing flexibility of deployment in any environment. It replaces IDS-4250-XL.

The IPS 4260 has two built-in Gigabit Ethernet network ports and six expansion slots. The network port numbers increase from right to left and the expansion slot numbers increase from bottom to top and from right to left as shown in Figure 3-5 on page 3-7. Slots 2 and 3 are PCI-Express connectors and the other expansion slots are PCI-X slots. Slots 1 through 3 are full-height slots and slots 4 though 6 are half-height slots. The built-in management port is called Management0/0 and the built-in sensing interface is Gigabit-Ethernet0/1.

Note Only expansion slots 2 and 3 are supported at this time.

For improved reliability, the IPS 4260 uses a flash device for storage rather than a hard-disk drive. The IPS 4260 supports two optional network interface cards, the 2SX Fiber card, and the 4GE bypass interface card that contains the hardware-bypass feature. Initially the IPS 4260 supports only the built-in interfaces and these two interface cards.

The IPS 4260 monitors greater than 1 Gbps of aggregate network traffic on multiple sensing interfaces and is also inline ready. It supports both copper and fiber interfaces. The 1-Gbps performance is traffic combined from all sensing interfaces. The 1-Gbps performance for the IPS 4260 is based on the following conditions:

- 10,000 new TCP connections per second
- 100,000 HTTP transactions per second
- Average packet size of 450 bytes
- System running IPS 6.0 software

The IPS 4260 ships with one power supply, but it supports redundant power supplies. The IPS 4260 operates in load-sharing mode when the optional redundant power supply is installed.

Note On IPS sensors with multiple processors (for example, the IPS 4260 and IPS 4270-20), packets may be captured out of order in the IP logs and by the **packet** command. Because the packets are not processed using a single processor, the packets can become out of sync when received from multiple processors.

For More Information

- For more information on how to obtain instructions and BIOS files from the Cisco website, see Obtaining Cisco IPS Software, page 11-1.
- For more information on sensor interfaces, see Sensor Interfaces, page 1-4.
- For more information on the 4GE bypass interface card, see Hardware Bypass, page 3-4.
- For more information on installing and removing the power supply, see Installing and Removing the Power Supply, page 3-22.

Supported Interface Cards

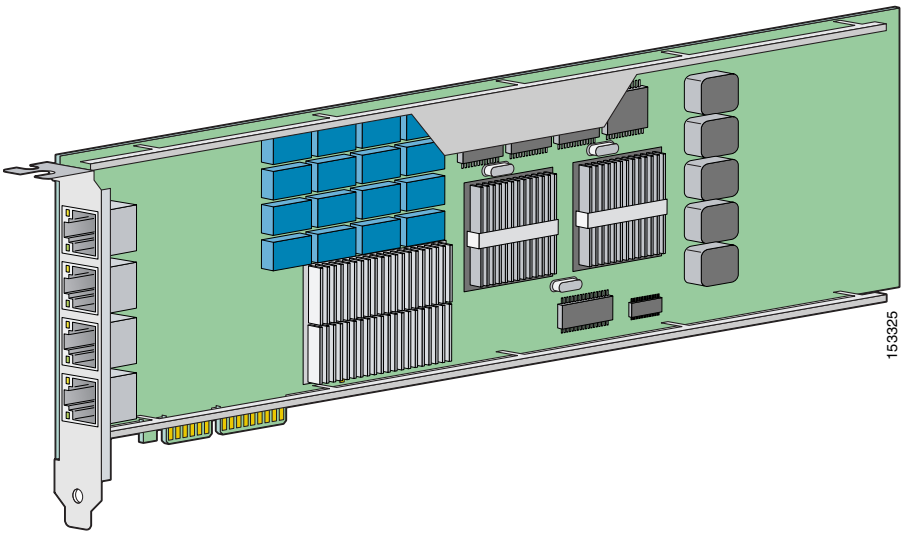
The IPS 4260 supports three interface cards: the 4GE bypass interface card, the 2SX interface card, and the 10GE interface card.

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 interfaces cards for a total of eight GE bypass interfaces. The 4GE bypass interface card supports hardware bypass.

Figure 3-1 shows the 4GE bypass interface card.

Figure 3-1 4GE Bypass Interface Card

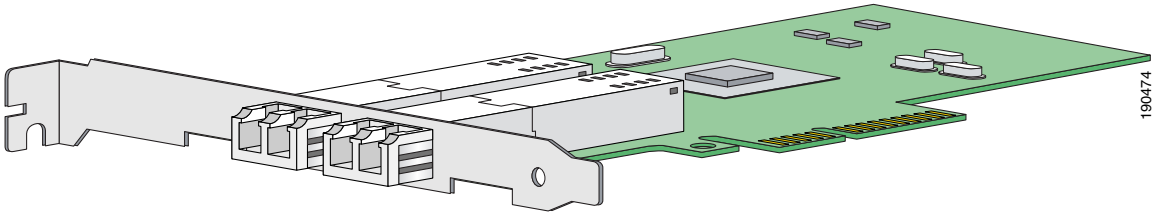


2SX Interface Card

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 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 3-2 shows the 2SX interface card.

Figure 3-2 2SX Interface Card

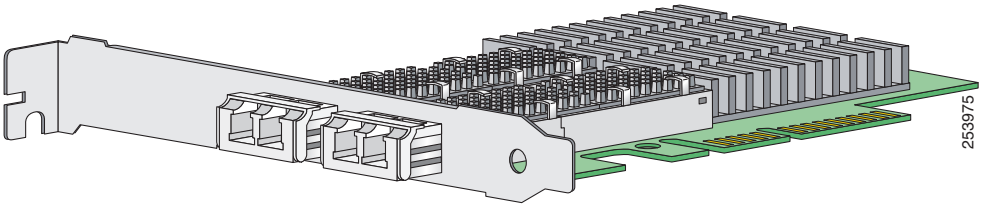


10GE Interface Card

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 card ports require a multi-mode fiber cable with an LC connector to connect to the SX interface of the IPS 4260. The 10GE interface card does not support hardware bypass.

Figure 3-3 shows the 10GE interface card.

Figure 3-3 10GE Interface Card



GigabitEthernet*slot_number*/*port_number* is the expansion card interface naming convention for the IPS 4260. The slot number is shown to the right of the slot in the chassis and the port number is numbered from right to left starting with 0.

Hardware Bypass

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

- 4GE Bypass Interface Card, page 3-4
- Hardware Bypass Configuration Restrictions, page 3-5
- Hardware Bypass and Link Changes and Drops, page 3-6

4GE Bypass Interface Card

The IPS 4260 supports 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.

For More Information

For the procedure for installing and removing the 4GE bypass interface card, see Installing and Removing Interface Cards, page 3-20.

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 the IPS 4260.
- 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 the IPS 4260.

  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.

Hardware Bypass and Link Changes and Drops

Properly configuring and deploying hardware bypass protects against complete link failure if the IPS appliance experiences a power loss, critical hardware failure, or is rebooted; however, a link status change still occurs when hardware bypass engages (and again when it disengages).

During engagement, the interface card disconnects both physical connections from itself and bridges them together. The interfaces of the connected devices can then negotiate the link and traffic forwarding can resume. Once the appliance is back online, hardware bypass disengages and the interface card interrupts the bypass and reconnects the links back to itself. The interface card then negotiates both links and traffic resumes.

There is no built-in way to completely avoid link status changes and drops. However, you can greatly reduce the interruption time (in some cases to sub-second times) by doing the following:

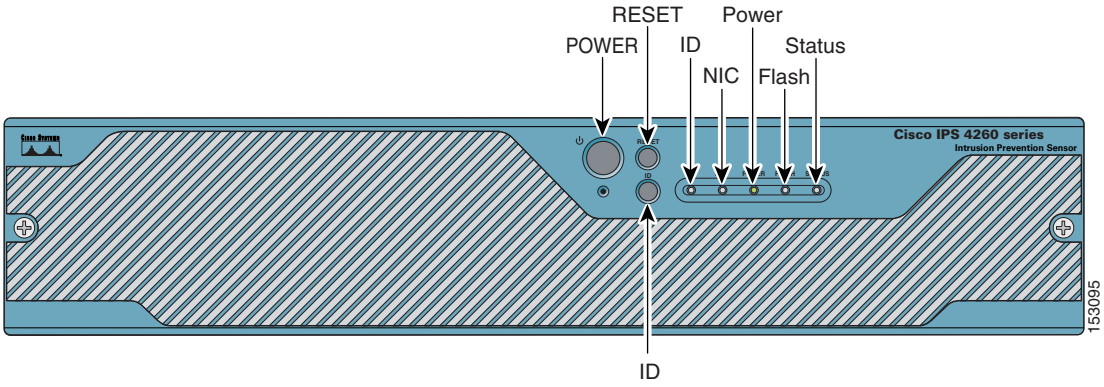
- Make sure you use CAT 5e/6-certified cabling for all connections.
- Make sure the interfaces of the connected devices are configured to match the interfaces of the appliance for speed/duplex negotiation (auto/auto).
- Enable portfast on connected switchports to reduce spanning-tree forwarding delays.

Front and Back Panel Features

This section describes the IPS 4260 front and back panel features and indicators.

Figure 3-4 shows the front view of the IPS 4260.

Figure 3-4 IPS 4260Front Panel Features



There are three switches on the front panel of the IPS 4260:

- Power—Toggles the system power.
- Reset—Resets the system.
- ID—Toggles the system ID indicator.

Table 3-1 describes the front panel indicators on the IPS 4260.

Table 3-1 Front Panel Indicators

Indicator	Description
ID (blue)	Continuously lit when activated by the front panel ID switch.
NIC (green)	Indicates activity on either the GigabitEthernetO/1 or MGMT interfaces.
Power (green)	When continuously lit, indicates DC power. The indicator is off when power is turned off or the power source is disrupted.
Flash (green/amber)	Off when the compact flash device is not being accessed. Blinks green when the compact flash device is being accessed. Solid amber when a device has failed.
Status (green/amber)	Blinks green while the power-up diagnostics are running or the system is booting. Solid green when the system has passed power-up diagnostics. Solid amber when the power-up diagnostics have failed.

Figure 3-5 shows the back view of the IPS 4260.

Figure 3-5 IPS 4260 Back Panel Features

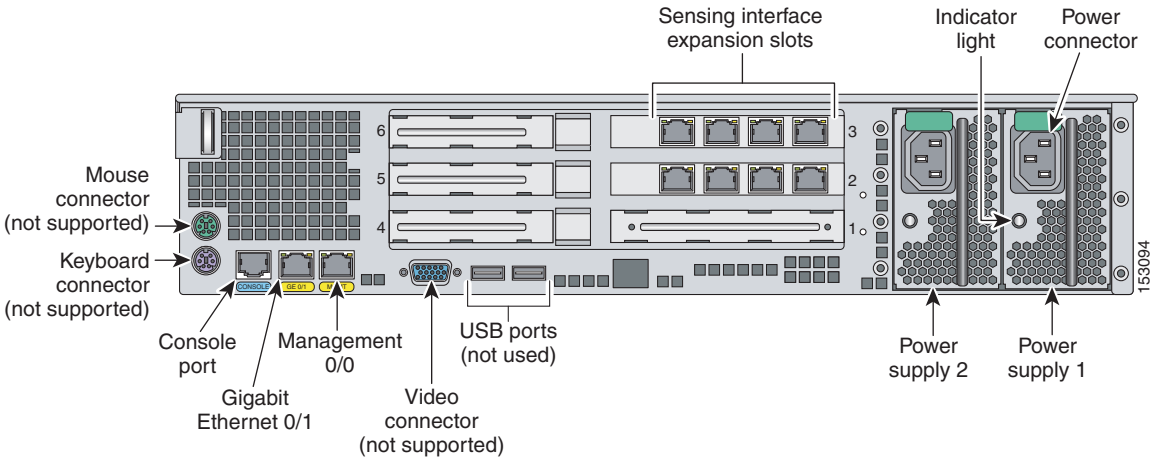


Figure 3-6 shows the two built-in Ethernet ports, which have two indicators per port.

Figure 3-6 Ethernet Port Indicators

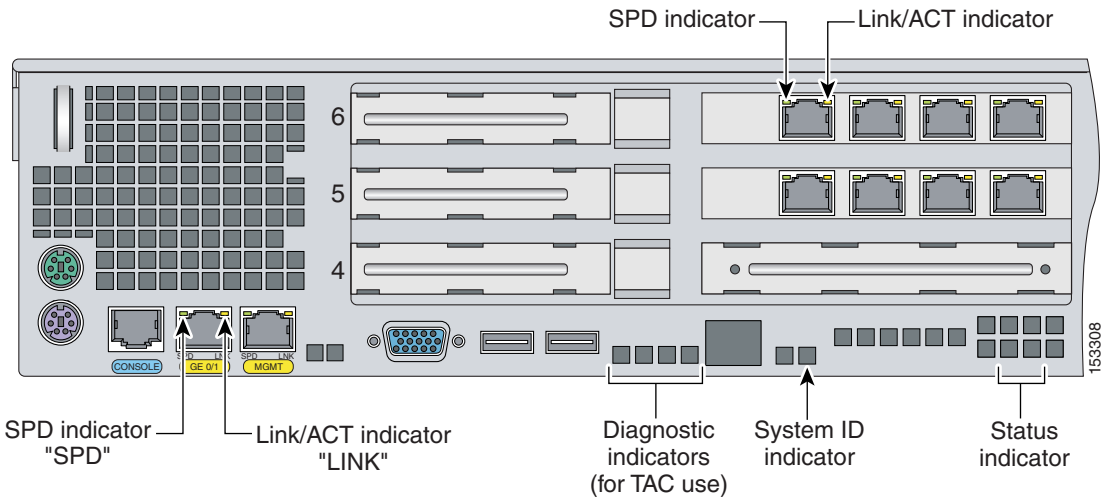


Table 3-2 lists the back panel indicators.

Table 3-2 Back Panel Indicators

Indicator	Color	Description
Left side	Green solid Green blinking	Physical link Network activity
Right side	Not lit Green Amber	10 Mbps 100 Mbps 1000 Mbps

Table 3-3 lists the power supply indicator.

Table 3-3 Power Supply Indicators

Color	Description
Off	No AC power to all power supplies.
Green solid	Output on and ok.
Green blinking	AC present, only 5Vsb on (power supply off).
Amber	No AC power to this power supply (for 1+1 configuration) or power supply critical event causing a shutdown: failure, fuse blown (1+1 only), OCP 12 V, OVP 12 V, or fan failed.
Amber blinking	Power supply warning events where the power supply continues to operate: high temperature, high power/high current, or slow fan.

Specifications

Table 3-4 lists the specifications for the IPS 4260.

Table 3-4 IPS 4260 Specifications

Dimensions and Weight	
Height	3.45 in. (87.6 cm)
Width	17.14 in. (435.3 cm)
Depth	20 in. (508 cm)
Weight	20.0 lb (9.07 kg)
Form factor	2 RU, standard 19-inch rack-mountable
Power	
Autoswitching	100V to 240V AC
Frequency	47 to 63 Hz, single phase
Operating current	8.9 A
Steady state	588 W max continuous
Maximum peak	657 W
Maximum heat dissipation	648 BTU/hr
Environment	
Temperature	Operating +32°F to +104°F (+0°C to +40°C) Nonoperating -104°F to +158°F (-40°C to +70°C)
Relative humidity	Operating 10% to 85% (noncondensing) Nonoperating 5% to 95% (noncondensing)
Altitude	Operating 0 to 9843 ft (3000 m) Nonoperating 0 to 15,000 ft (4750 m)
Shock	Operating Half-sine 2 G, 11 ms pulse, 100 pulses Nonoperating 25 G, 170 inches/sec delta V
Vibration	2.2 Grms, 10 minutes per axis on all three axes

Accessories

The IPS 4260 accessories kit contains the following:

- DB25 connector
- DB9 connector
- Rack mounting kit—screws, washers, and metal bracket
- RJ45 console cable
- Two 6-ft Ethernet cables

Important Safety Instructions

Warning **IMPORTANT SAFETY INSTRUCTIONS**

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment. Statement 1030**

Rack Mounting

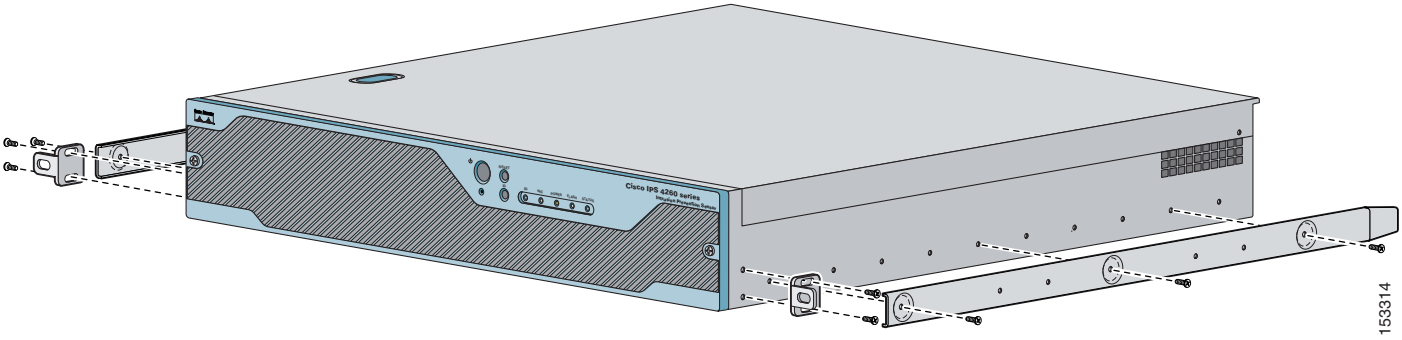
You can rack mount the IPS 4260 in a 2- or 4-post rack. This section describes how to rack mount the IPS 4260 and contains the following topics:

- Installing the IPS 4260 in a 4-Post Rack, page 3-10
- Installing the IPS 4260 in a 2-Post Rack, page 3-13

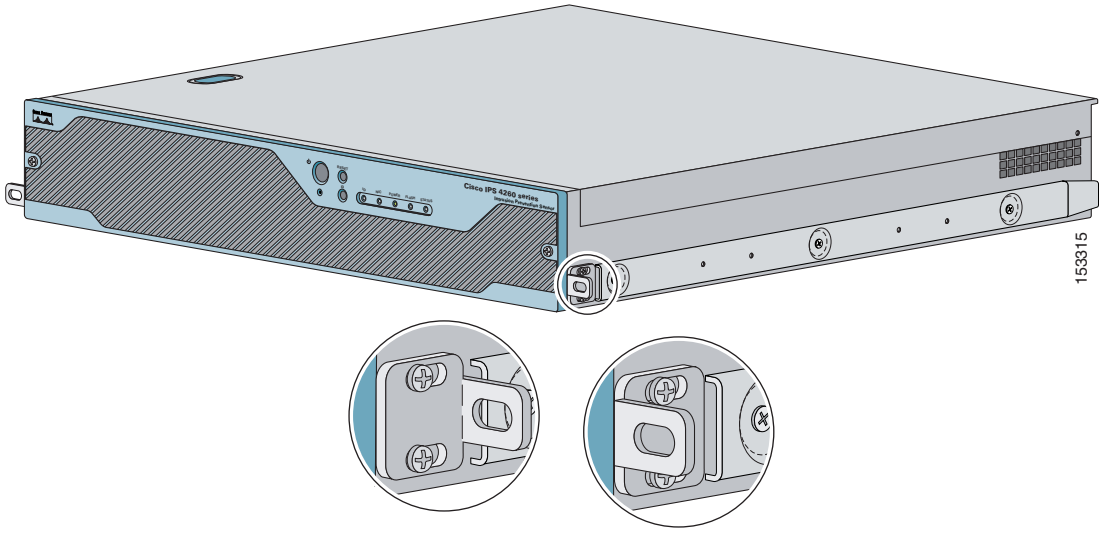
Installing the IPS 4260 in a 4-Post Rack

To rack mount the IPS 4260 in a 4-post rack, follow these steps:

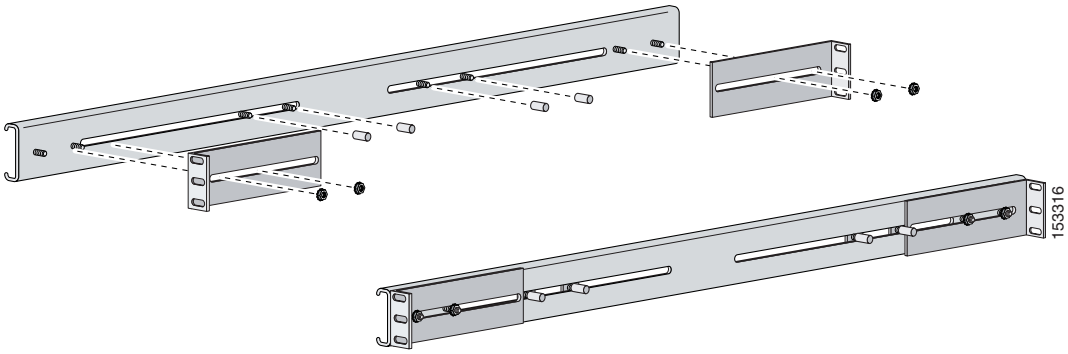
Step 1 Attach each inner rail to each side of the chassis with three 8-32x1/4” SEMS screws.



Step 2 Attach the front-tab mounting bracket to the chassis with two 8-32x1/4' SEMS screws. You can flip the bracket to push the system forward in the rack.

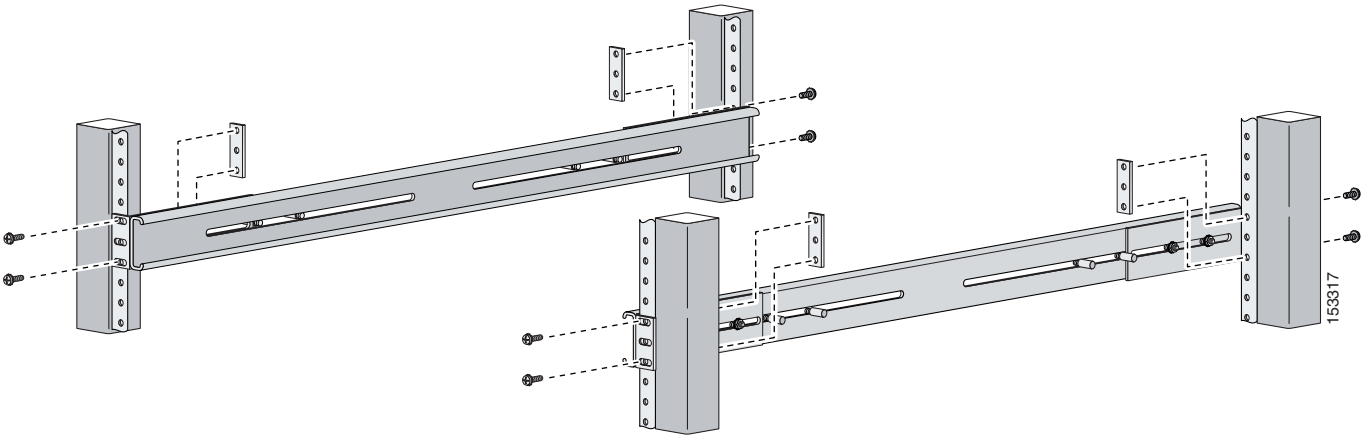


Step 3 Using the four inner studs, install the mounting brackets to the outer rail with four 8-32 KEPS nuts. Insert four thread covers over the four outer studs on each side.

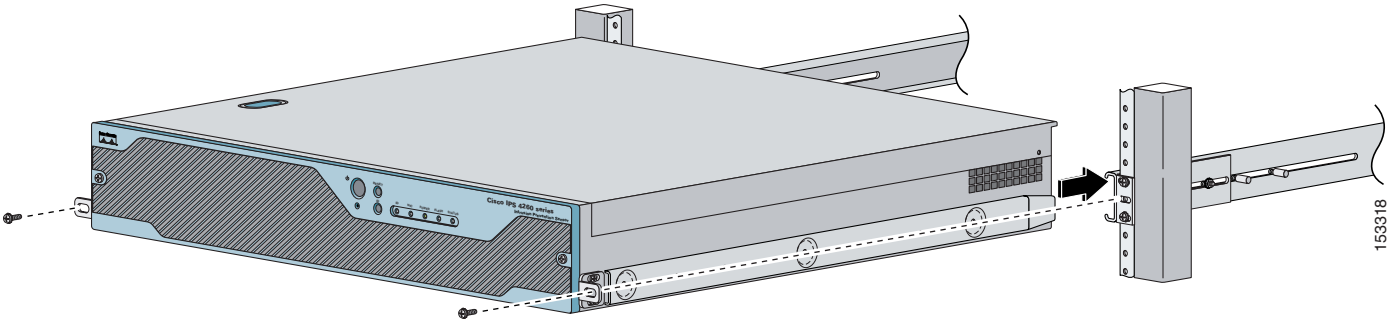


Step 4 Install the two outer rail subassemblies in the rack using eight 10-32x1/2” SEMS screws. You can use four bar nuts if necessary.

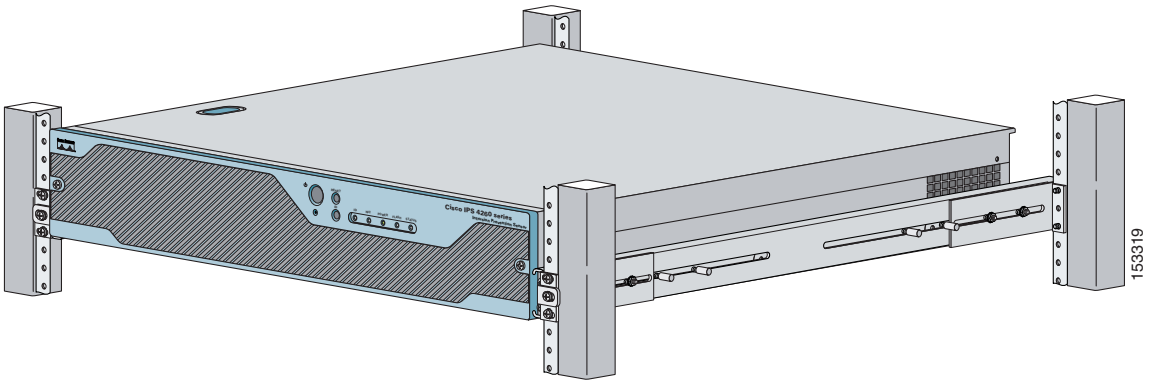
Note Adjust the mounting brackets based on rack depth.



Step 5 Slide the IPS 4260 into the rack making sure the inner rail is aligned with the outer rail.



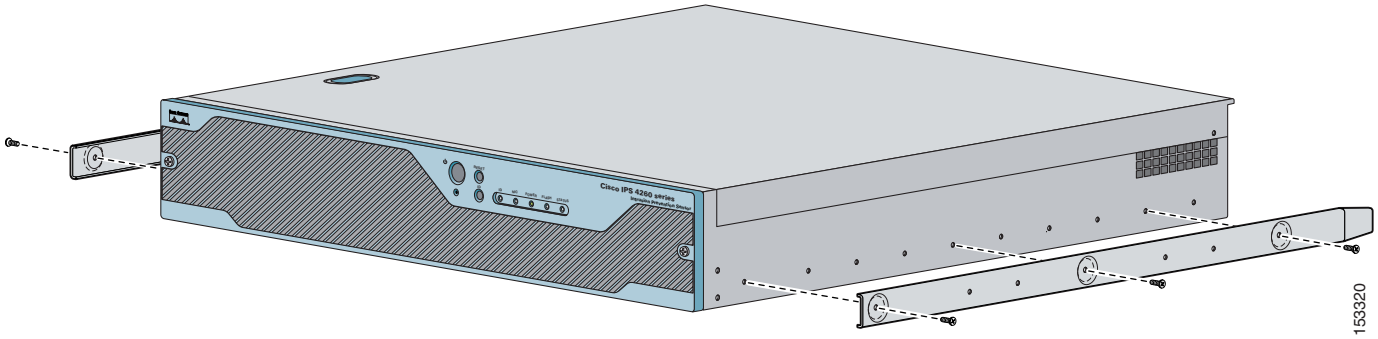
Step 6 Install two 10-32x1/2” SEMS screws to hold the front-tab mounting bracket to the rail.



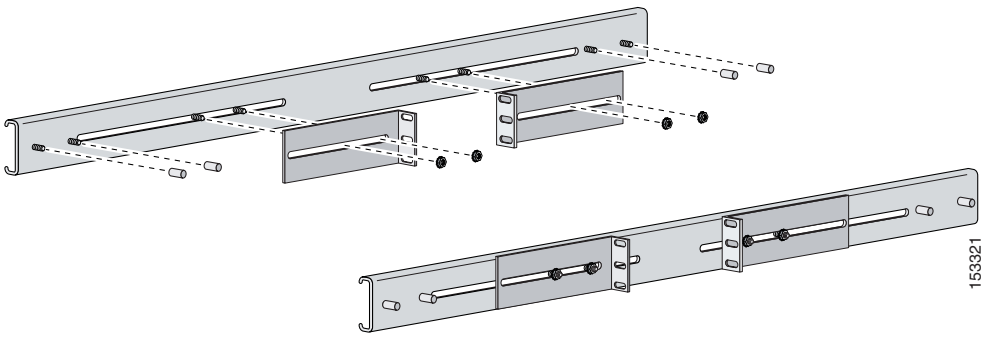
Installing the IPS 4260 in a 2-Post Rack

To rack mount the IPS 4260 in a 2-post rack, follow these steps:

Step 1 Attach the inner rail to each side of the chassis with three 8-32x1/4” SEMS screws.

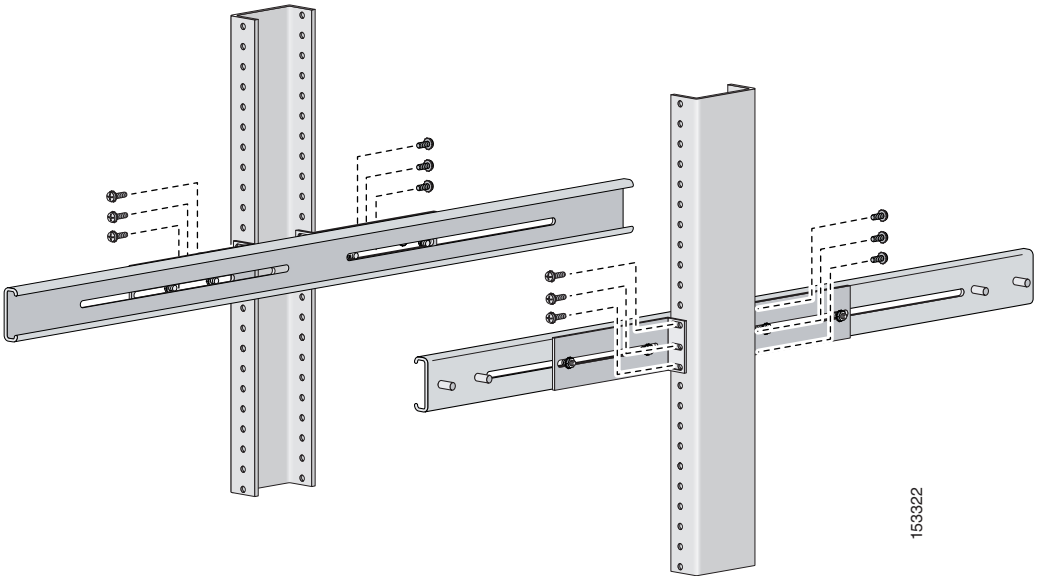


Step 2 Using the four inner studs, install the mounting brackets to the outer rail with four 8-32 KEPS nuts. Insert four thread covers over the four outer studs on each side.

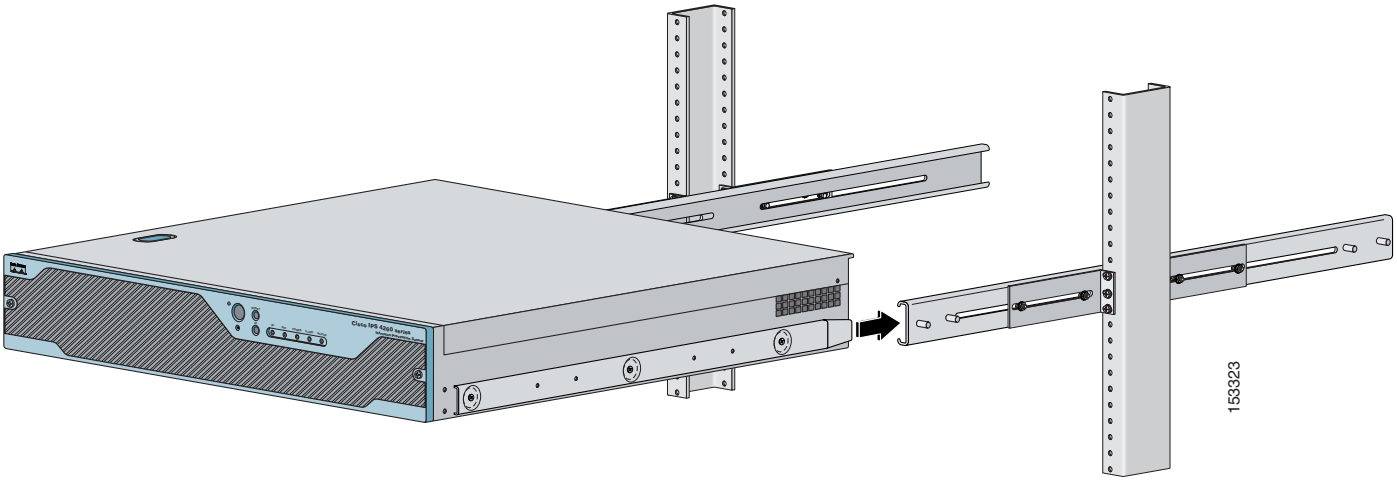


Step 3 Install the two outer rail subassemblies in the rack using twelve 10-32x1/2” SEMS screws or whatever rack hardware is necessary.

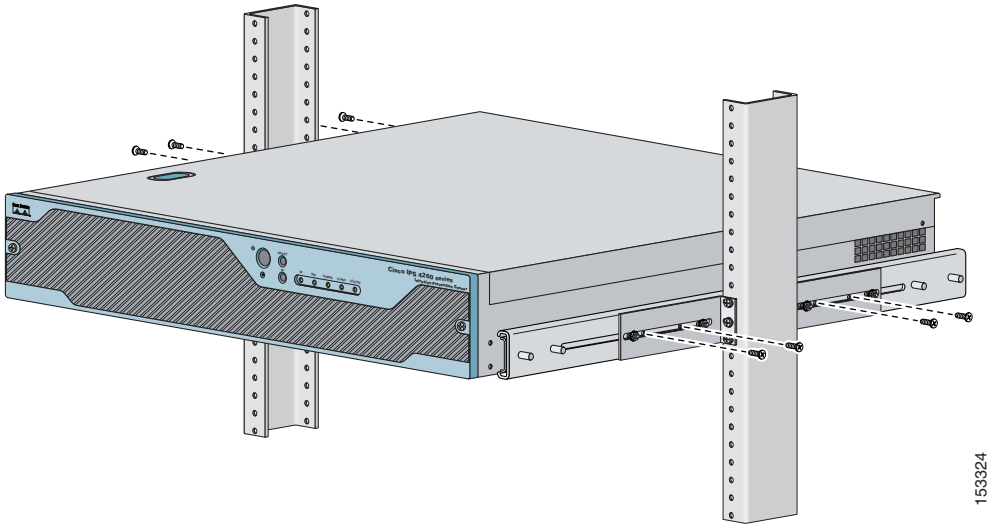
Note Adjust the mounting brackets based on the rack-channel depth.



Step 4 Slide the IPS 4260 into the rack making sure the inner rail is aligned with the outer rail.



Step 5 Install four 8-32x7/16” SEMS screws through the clearance slots in the side of each outer rail assembly into the inner rail.



Installing the IPS 4260

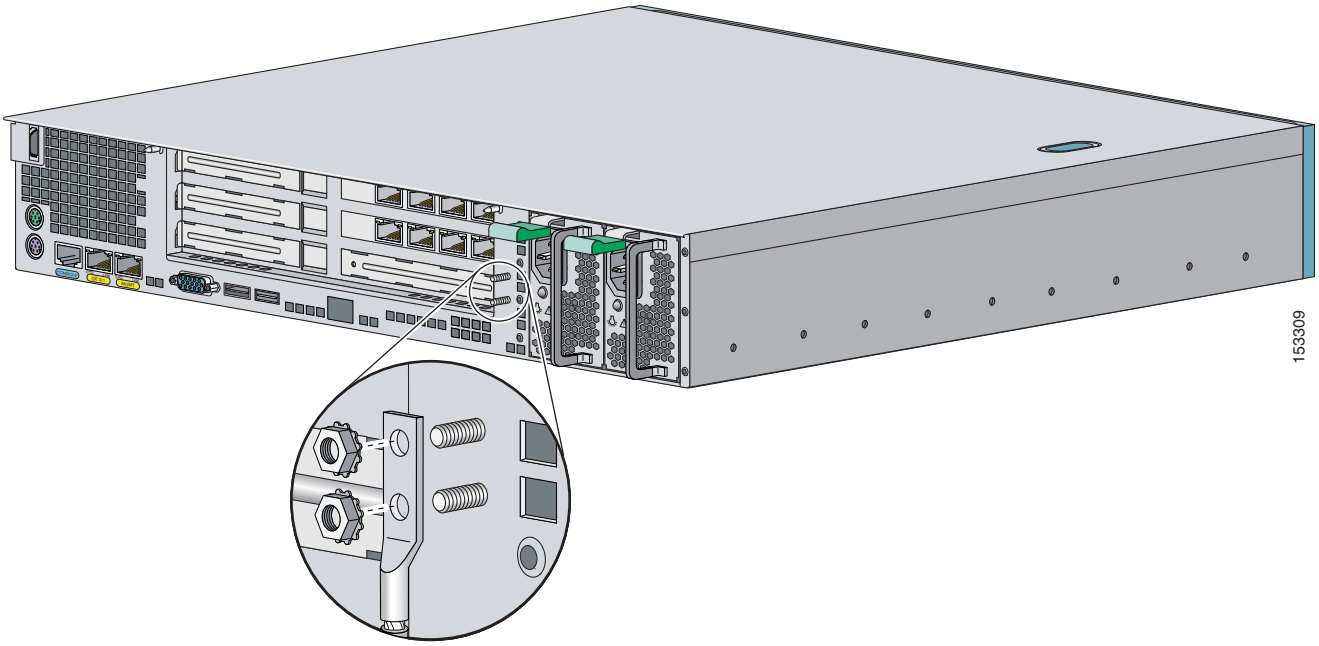
Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment. Statement 1030**

Caution Follow proper safety procedures when performing these steps by reading the safety warnings in *Regulatory Compliance and Safety Information for the Cisco Intrusion Prevention System 4200 Series Appliance Sensor*.

To install the IPS 4260 on the network, follow these steps:

Step 1 Position the IPS 4260 on the network.

Step 2 Attach the grounding lugs to the back of the IPS 4260.



Note Use 8-32 locknuts to connect a copper standard barrel grounding lug to the holes. The appliance requires a lug where the distance between the center of each hole is 0.56 inches. The ground lug must be NRTL listed or recognized. In addition, the copper conductor (wires) must be used and the copper conductor must comply with the NEC code for ampacity. A lug is not supplied with the appliance.

Step 3 Place the IPS 4260 in a rack, if you are rack mounting it.

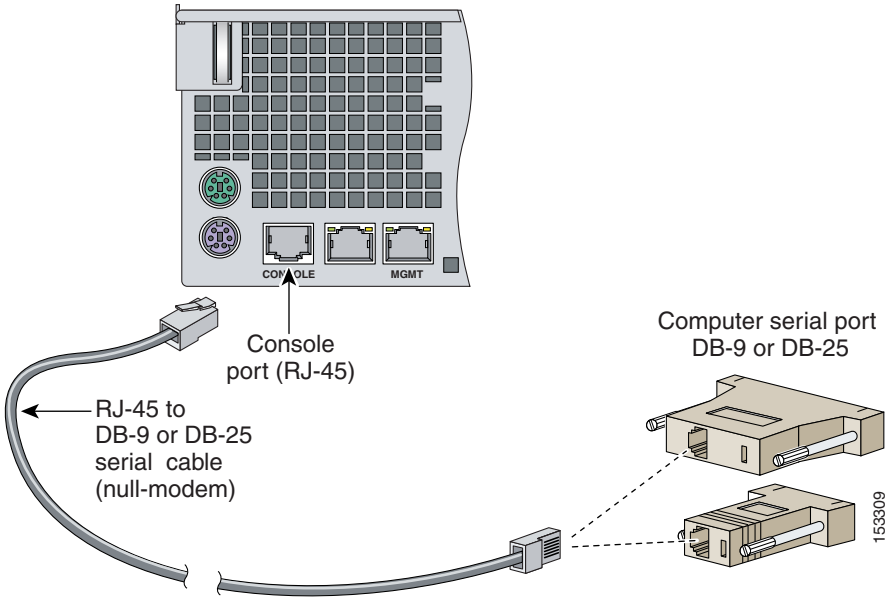
Step 4 Attach the power cord to the IPS 4260 and plug it in to a power source (a UPS is recommended).

Step 5 Connect the cable as shown in Step 6 so that you have either a DB-9 or DB-25 connector on one end as required by the serial port for your computer, and the other end is the RJ-45 connector.

Note Use the console port to connect to a computer to enter configuration commands. Locate the serial cable from the accessory kit. The serial cable assembly consists of a 180/rollover cable with RJ-45 connectors (DB-9 connector adapter PN 74-0495-01 and DB-25 connector adapter PN 29-0810-01).

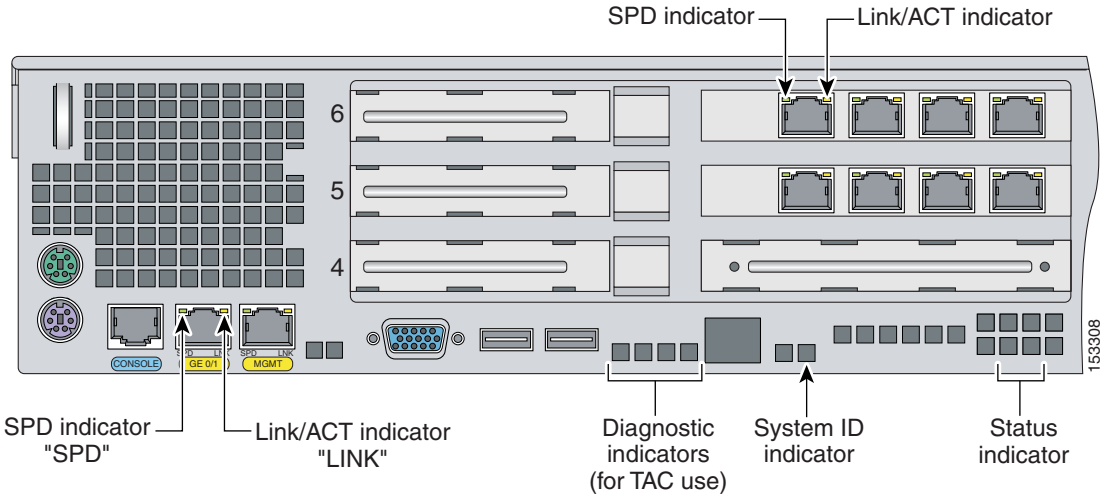
Note You can use a 180/rollover or straight-through patch cable to connect the appliance to a port on a terminal server with RJ-45 or hydra cable assembly connections. Connect the appropriate cable from the console port on the appliance to a port on the terminal server.

Step 6 Connect the RJ-45 connector to the console port and connect the other end to the DB-9 or DB-25 connector on your computer.



Step 7 Attach the network cables to the following interfaces:

- GigabitEthernet0/1 (GE 0/1) is the sensing port.
- Management0/0 (MGMT) is the command and control port.
- GigabitEthernet*slot_number/port_number* through GigabitEthernet*slot_number/port_number* are the additional expansion port slots.



Caution Management and console ports are privileged administrative ports. Connecting them to an untrusted network can create security concerns.

Step 8 Power on the IPS 4260.

Step 9 Initialize the IPS 4260.

Step 10 Upgrade the IPS 4260 with the most recent Cisco IPS software. You are now ready to configure intrusion prevention on the IPS 4260.

For More Information

- For more information on working with electrical power and in an ESD environment, see Site and Safety Guidelines, page 1-30.
- For the procedure for installing the IPS 4260 in a rack, see Rack Mounting, page 3-10.
- For the instructions for setting up a terminal server, see Connecting an Appliance to a Terminal Server, page 1-19.
- For the procedure for using the **setup** command to initialize the IPS 4260, see Initializing the Sensor, page 10-1.
- For the procedure for obtaining and installing the most recent IPS software, see Obtaining Cisco IPS Software, page 11-1.
- For the procedure for using HTTPS to log in to IDM, refer to Logging In to IDM.
- For the procedures for configuring intrusion prevention, refer to the following documents:
  - *Installing and Using Cisco Intrusion Prevention System Device Manager 7.0*
  - *Installing and Using Cisco Intrusion Prevention System Manager Express 7.0*
  - *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 7.0*

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 the 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 the 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 the IPS 4260 using IDM or IME.

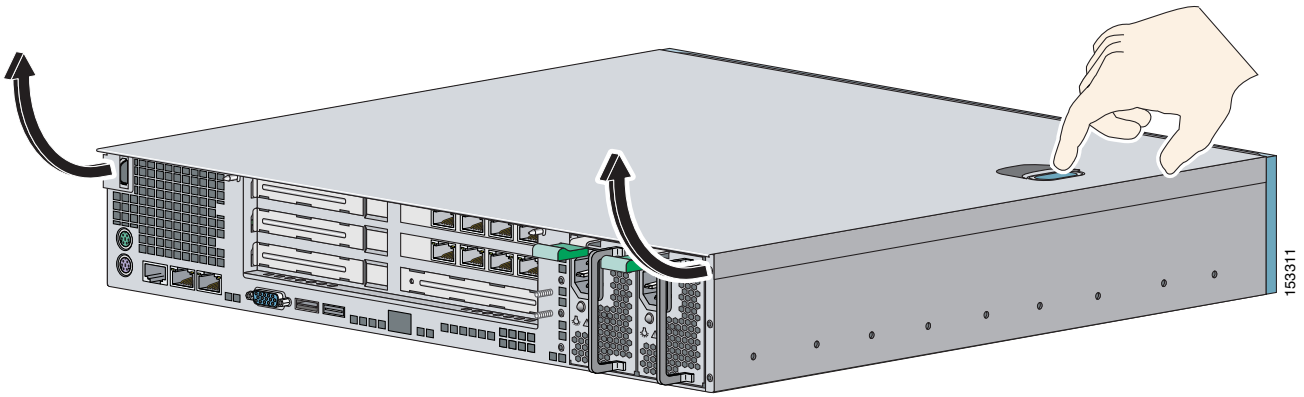
Step 3 Power off the IPS 4260.

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

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

Step 6 Make sure the 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 the 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 the IPS 4260.

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

Step 11 Power on the IPS 4260.

For More Information

- For the IDM procedure for resetting the IPS 4260, refer to Rebooting the Sensor; for the IME procedure for resetting the IPS 4260, refer to Rebooting the Sensor.
- For the procedure for removing the IPS 4260 from a rack, see Rack Mounting, page 3-10.
- For more information on ESD-controlled environments, see Working in an ESD Environment, page 1-32.
- If you are reinstalling the IPS 4260 in a rack, see Rack Mounting, page 3-10.

Installing and Removing Interface Cards

The 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. The IPS 4260 supports up to two network interface cards.

Note The 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 interface cards, follow these steps:

Step 1 Log in to the CLI.

Step 2 Prepare the 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 the IPS 4260 using IDM or IME.

Step 3 Power off the IPS 4260.

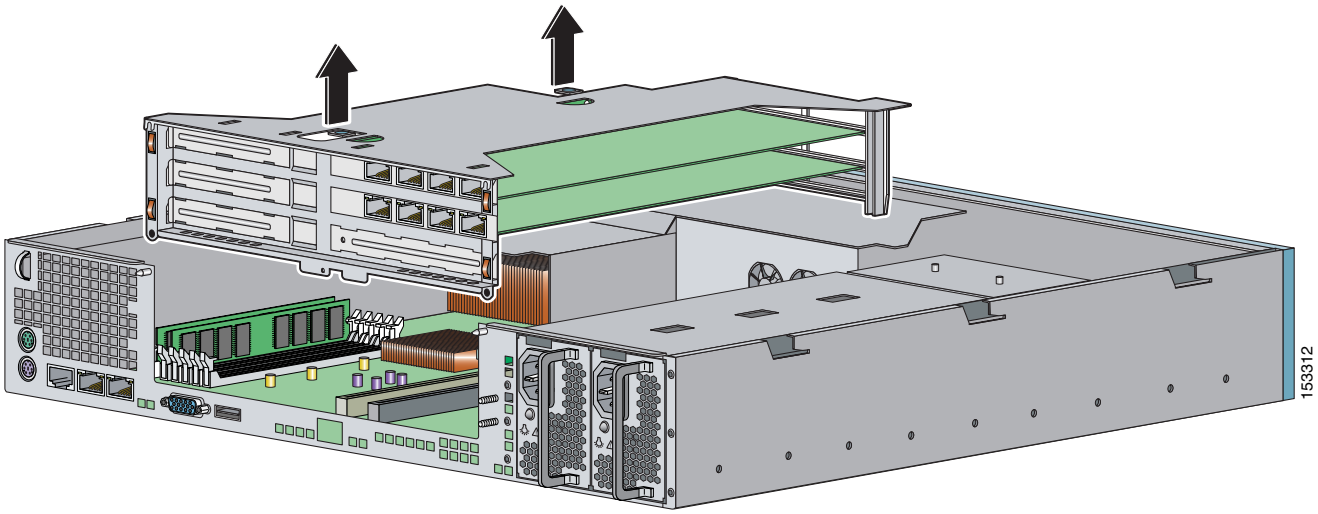
Step 4 Remove the power cable and other cables from the IPS 4260.

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

Step 6 Make sure the 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.

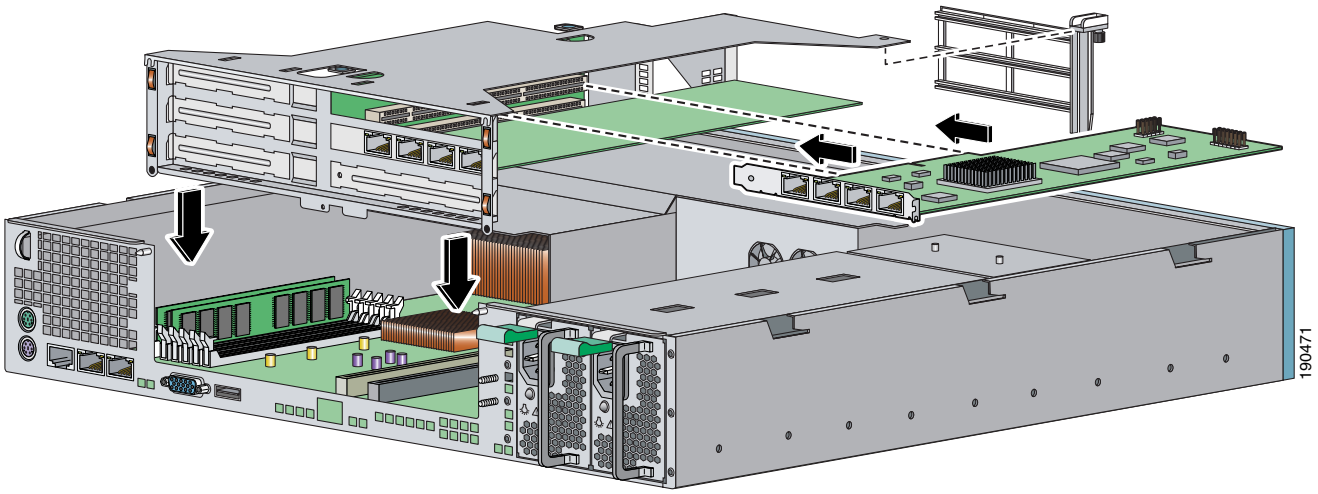


Step 9 With a screw driver, remove the screw from the desired slot cover.

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 interface 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.

For More Information

- For the procedure for attaching power cords and cables to the IPS 4260, see Installing the IPS 4260, page 3-15.
- For an illustration of the expansion card slots, see Figure 3-6 on page 3-8.
- For an illustration of the supported interface cards, see Supported Interface Cards, page 3-3.
- For the IDM procedure for resetting the IPS 4260, refer to Rebooting the Sensor; for the IME procedure for resetting the IPS 4260, refer to Rebooting the Sensor.
- For the procedure for removing the IPS 4260 from a rack, see Rack Mounting, page 3-10.
- For more information on ESD-controlled environments, see Working in an ESD Environment, page 1-32.
- For the procedure for removing the chassis cover, see Removing and Replacing the Chassis Cover, page 3-18.

Installing and Removing the Power Supply

The IPS 4260 ships with one power supply, but you can order it with two power supplies so that you have a redundant power supply.

To install and remove power supplies, follow these steps:

Step 1 Log in to the CLI.

Step 2 Prepare the IPS 4260 to be powered off:

```
sensor# reset powerdown
```

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

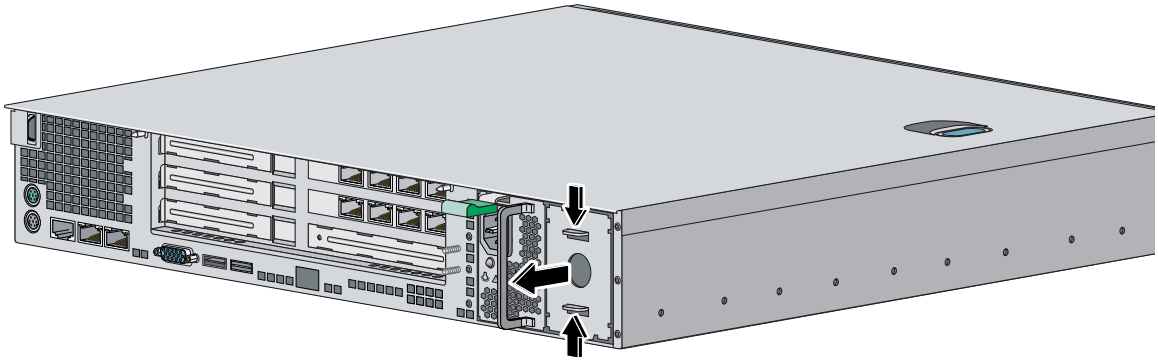
Note You can also power down the IPS 4260 using IDM or IME.

Step 3 Power off the IPS 4260.

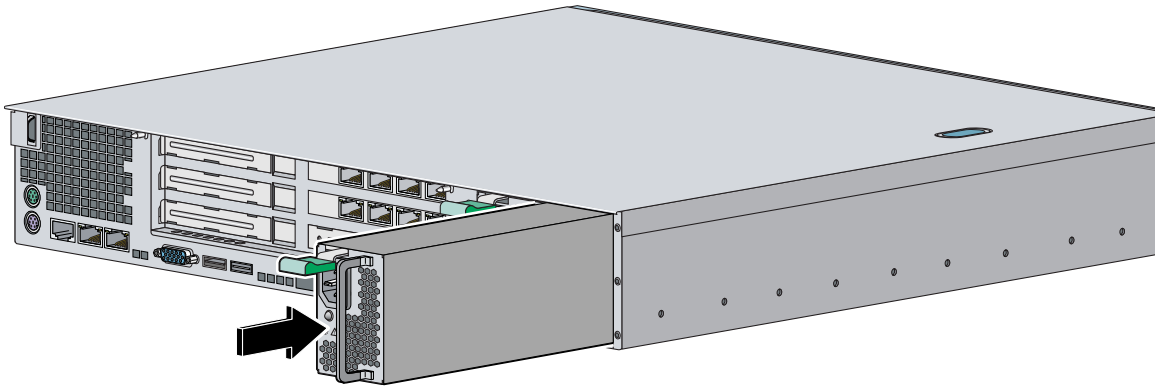
Step 4 Remove the power cable and other cables from the IPS 4260.

Note Power supplies are hot-swappable. You can replace a power supply while the IPS 4260 is running, if you are replacing a redundant power supply.

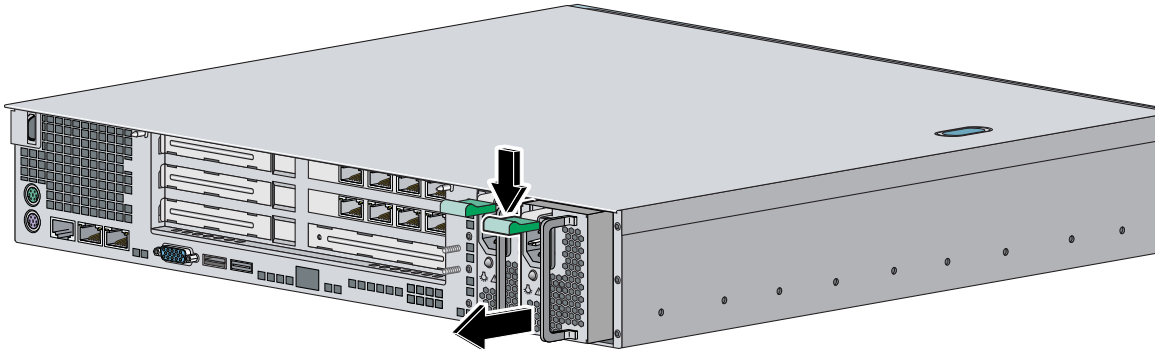
Step 5 Squeeze the tabs to remove the filler plate.



Step 6 Install the power supply.



Step 7 To remove the power supply, push down the green tab and pull out the power supply.



Step 8 After installing or removing the power supply, replace the power cord and other cables.

Step 9 Power on the IPS 4260.

For More Information

For the IDM procedure for resetting the IPS 4260, refer to Rebooting the Sensor; for the IME procedure for resetting the IPS 4260, refer to Rebooting the Sensor.

CHAPTER 4

Installing the IPS 4270-20

Note All IPS platforms allow ten concurrent CLI sessions.

This chapter describes the IPS 4270-20 and how to install it. It also describes the accessories and how to install them. This chapter contains the following sections:

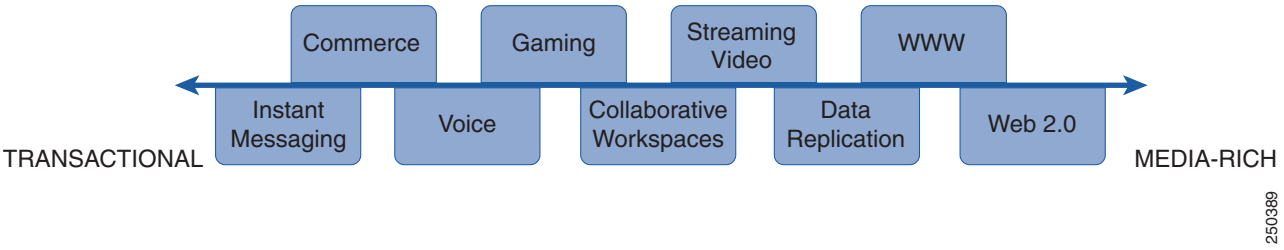
Introducing the IPS 4270-20

Caution The BIOS on the IPS 4270-20 is specific to the IPS 4270-20 and must only be upgraded under instructions from Cisco with BIOS files obtained from the Cisco website. Installing a non-Cisco or third-party BIOS on the IPS 4270-20 voids the warranty.

The IPS 4270-20 delivers up to 4 Gbps of performance in media-rich environments and 2 Gbps in transactional environments enabling you to protect fully saturated Gigabit networks and aggregate network traffic on multiple sensing interfaces. The IPS 4270-20 is also inline ready and has support for both copper and fiber NICs thus providing flexibility of deployment in any environment.

Media-rich environments are characterized by content, such as that seen on popular websites with video and file transfer. Transactional environments are characterized by connections, such as E-commerce, instant messaging, and voice. Figure 4-1 demonstrates the spectrum of media-rich and transactional environments.

Figure 4-1 Media-rich and Transactional Environments



The IPS 4270-20 has two built-in GigabitEthernet network ports and nine expansion slots. The network port numbers are numbered from top to bottom beginning with 0 and the expansion slot numbers increase from right to left. The two built-in GigabitEthernet ports are used for management and are called Management0/0 and Management0/1. Management0/1 is reserved for future use. Slots 1 and 2 are reserved for future use. You can populate slots 3 through 8 with supported network interface cards. Slot 9 is populated by a RAID controller card and is not available for use by network interface cards. The sensing interfaces are called GigabitEthernet.

Because of the multiple interfaces on the IPS 4270-20, it can cover multiple subnets, each of which have bandwidth requirements in the multi-T3 range or Gigabit range, and the multiple interfaces can be connected directly to the additional monitoring interfaces without needing to SPAN the traffic through a switch.

For improved reliability, the IPS 4270-20 uses a compact flash device for storage rather than a hard-disk drive. The IPS 4270-20 supports two optional network interface cards, the 2SX interface card with fiber-optic ports, and the 4GE bypass interface card with copper ports that contains the hardware-bypass feature. Initially the IPS 4270-20 supports only the built-in interfaces and these two interface cards.

The IPS 4270-20 supports a maximum of 16 sensing ports. Any additional configured ports will not be monitored and will not appear in the IPS configuration or statistics and no inline traffic will be forwarded on or between these ports. You receive the following error if you exceed the number of supported ports:

```
The number of installed network interfaces exceeds the limit of 16. The excess interfaces
are ignored.
```

Note If you add a new interface card that exceeds the limit, one or more of the previous sensing interfaces may become disabled.

The IPS 4270-20 ships with two power supplies, thus supporting a redundant power supply configuration. The IPS 4270-20 operates in load-sharing mode when the redundant power supply is installed.

Note On IPS sensors with multiple processors (for example, the IPS 4260 and IPS 4270-20), packets may be captured out of order in the IP logs and by the **packet** command. Because the packets are not processed using a single processor, the packets can become out of sync when received from multiple processors.

For More Information

- For more information on how to obtain instructions and BIOS files from the Cisco website, see Obtaining Cisco IPS Software, page 11-1.
- For more information on sensor interfaces, see Sensor Interfaces, page 1-4.
- For more information on the supported interface cards, see Supported Interface Cards, page 4-3.
- For more information on the 4GE bypass interface card, see Hardware Bypass, page 4-5.
- For more information about the power supplies, see Installing and Removing the Power Supply, page 4-44.

Supported Interface Cards

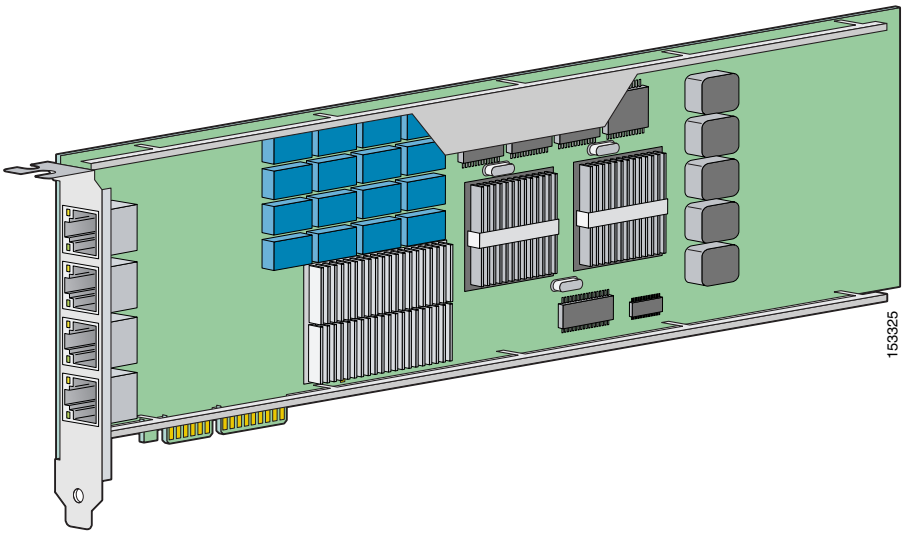
The IPS 4270-20 supports three interface cards: the 4GE bypass interface card, the 2SX interface card, and the 10GE interface card.

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 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 4-2 shows the 4GE bypass interface card.

Figure 4-2 4GE Bypass Interface Card

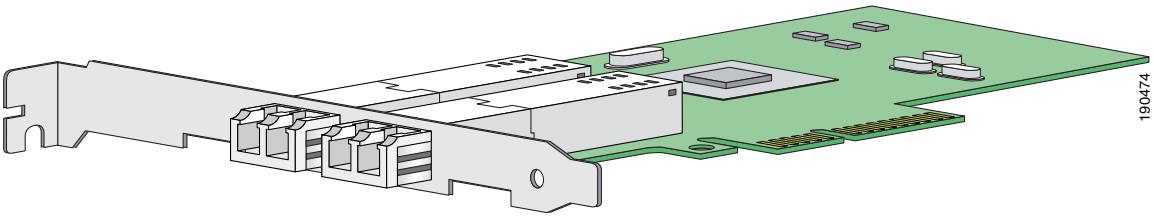


2SX Interface Card

The 2SX interface card (part numbers IPS-2SX-INT and IPS-2SX-INT=) provides two 1000BASE-SX (fiber) monitoring interfaces. The IPS 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 4-3 shows the 2SX interface card.

Figure 4-3 2SX Interface Card

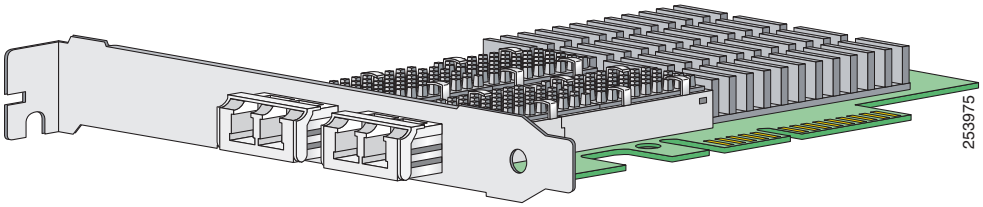


10GE Interface Card

The 10GE interface card (part numbers IPS-2X10GE-SR-INT and IPS-2X10GE-SR-INT=) provides two 10000 Base-SX (fiber) interfaces. The IPS 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 the IPS 4270-20. The 10GE interface card does not support hardware bypass.

Figure 4-4 shows the 10GE interface card.

Figure 4-4 10GE Interface Card



GigabitEthernet*slot_number*/*port_number* is the expansion card interface naming convention for the IPS 4270-20. The slot number is shown above the slot in the chassis and the port number is numbered from top to bottom starting with 0.

Hardware Bypass

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

- 4GE Bypass Interface Card, page 4-5
- Hardware Bypass Configuration Restrictions, page 4-6
- Hardware Bypass and Link Changes and Drops, page 4-7

4GE Bypass Interface Card

The IPS 4270-20 supports 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.

For More Information

For the procedure for installing and removing the 4GE bypass interface card, see Installing and Removing Interface Cards, page 4-41.

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 the 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 the 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.

Hardware Bypass and Link Changes and Drops

Properly configuring and deploying hardware bypass protects against complete link failure if the IPS appliance experiences a power loss, critical hardware failure, or is rebooted; however, a link status change still occurs when hardware bypass engages (and again when it disengages).

During engagement, the interface card disconnects both physical connections from itself and bridges them together. The interfaces of the connected devices can then negotiate the link and traffic forwarding can resume. Once the appliance is back online, hardware bypass disengages and the interface card interrupts the bypass and reconnects the links back to itself. The interface card then negotiates both links and traffic resumes.

There is no built-in way to completely avoid link status changes and drops. However, you can greatly reduce the interruption time (in some cases to sub-second times) by doing the following:

- Make sure you use CAT 5e/6-certified cabling for all connections.
- Make sure the interfaces of the connected devices are configured to match the interfaces of the appliance for speed/duplex negotiation (auto/auto).
- Enable portfast on connected switchports to reduce spanning-tree forwarding delays.

Front and Back Panel Features

This section describes the IPS 4270-20 front and back panel features and indicators. Figure 4-5 shows the front view of the IPS 4270-20.

Figure 4-5 IPS 4270-20 Front View

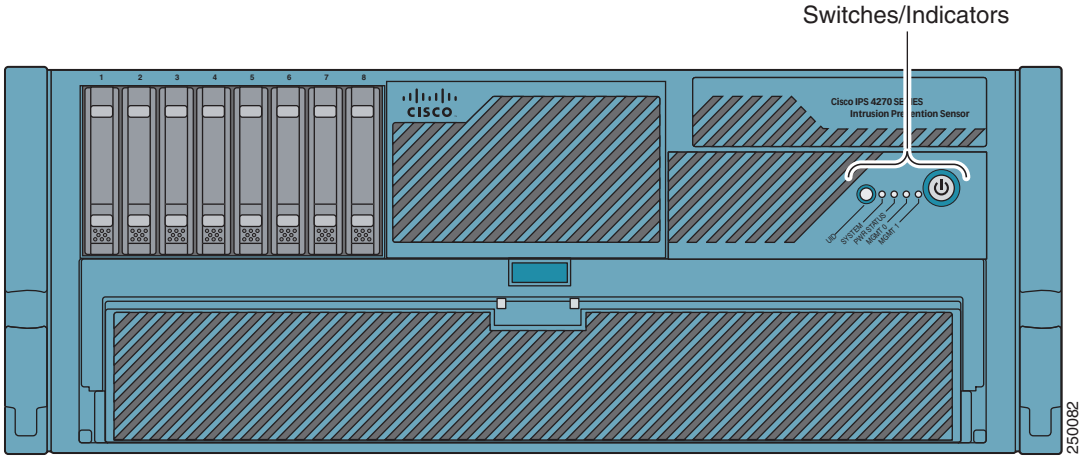


Figure 4-6 shows the front panel switches and indicators.

Figure 4-6 IPS 4270-20 Front Panel Switches and Indicators

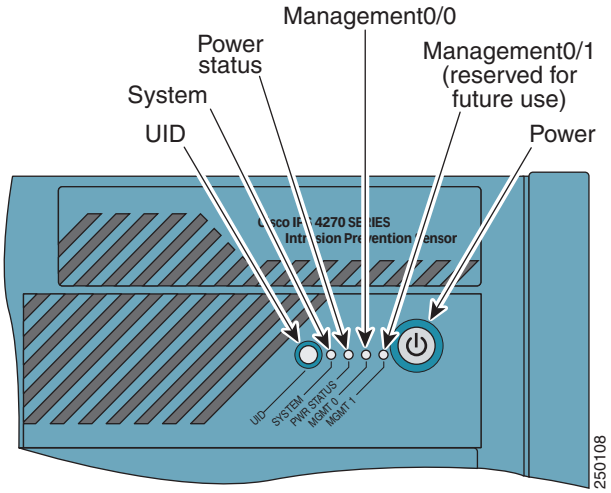


Table 4-1 describes the front panel switches and indicators on the IPS 4270-20.

Table 4-1 Front Panel Switches and Indicators

Indicator	Description
UID switch and indicator	Toggles the system ID indicator, which assists with chassis location in a rack: • Blue—Activated • Off—Deactivated **Note** The ID switch is activated by a switch on the front of the chassis.
Internal system health indicator	Indicates internal system health: • Green—System on • Flashing amber—System health degraded • Flashing red—System health critical • Off—System off
Power status indicator	Indicates the power supply status: • Green—Power supply on • Flashing amber—Power supply health degraded • Flashing red—Power supply health critical • Off—Power supply off
MGMT0/0 indicator	Indicates the status of the management port: • Green—Linked to network • Flashing green—Linked with activity on the network • Off—No network connection

Table 4-1 Front Panel Switches and Indicators (continued)

Indicator	Description
MGMT0/1 indicator	Reserved for future use
Power switch and indicator	Turns power on and off: • Amber—System has AC power and is in standby mode • Green—System has AC power and is turned on • Off—System has no AC power

Figure 4-7 shows the back view of the IPS 4270-20.

Figure 4-7 IPS 4270-20 Back Panel Features

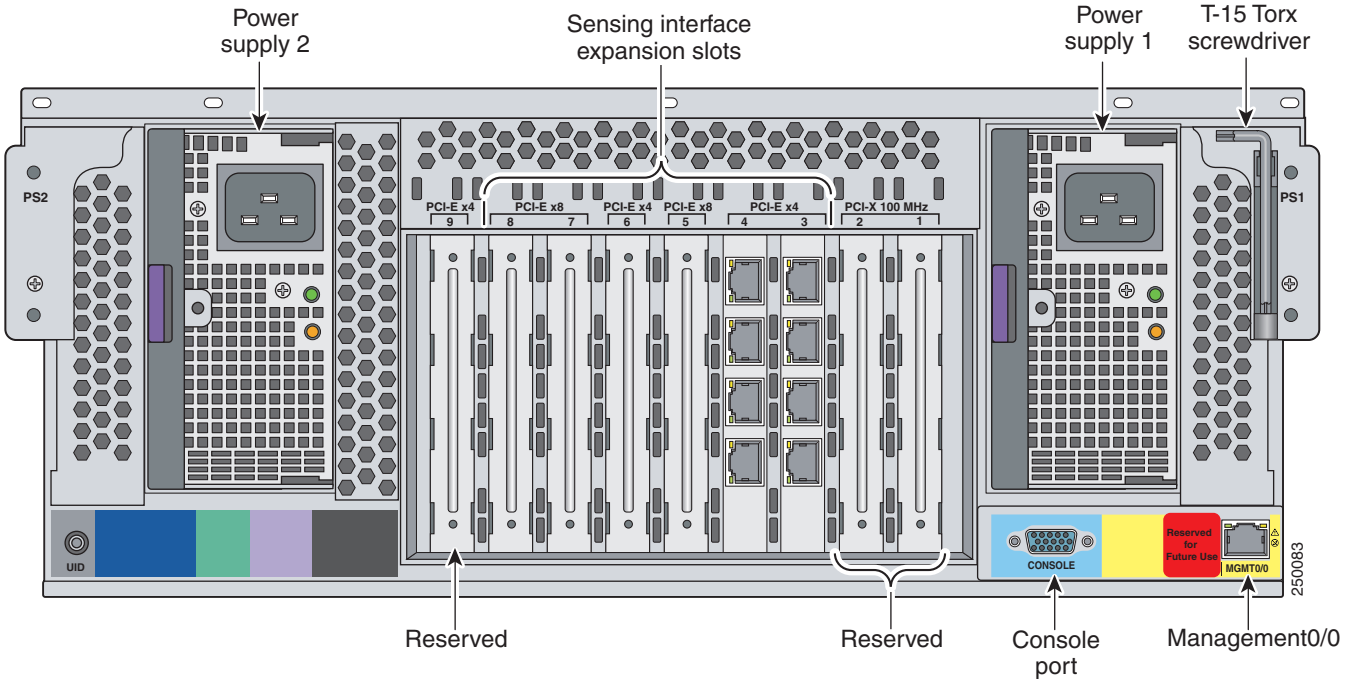


Figure 4-8 shows the built-in Ethernet port, which has two indicators per port, and the power supply indicators.

Figure 4-8 Ethernet Port Indicators

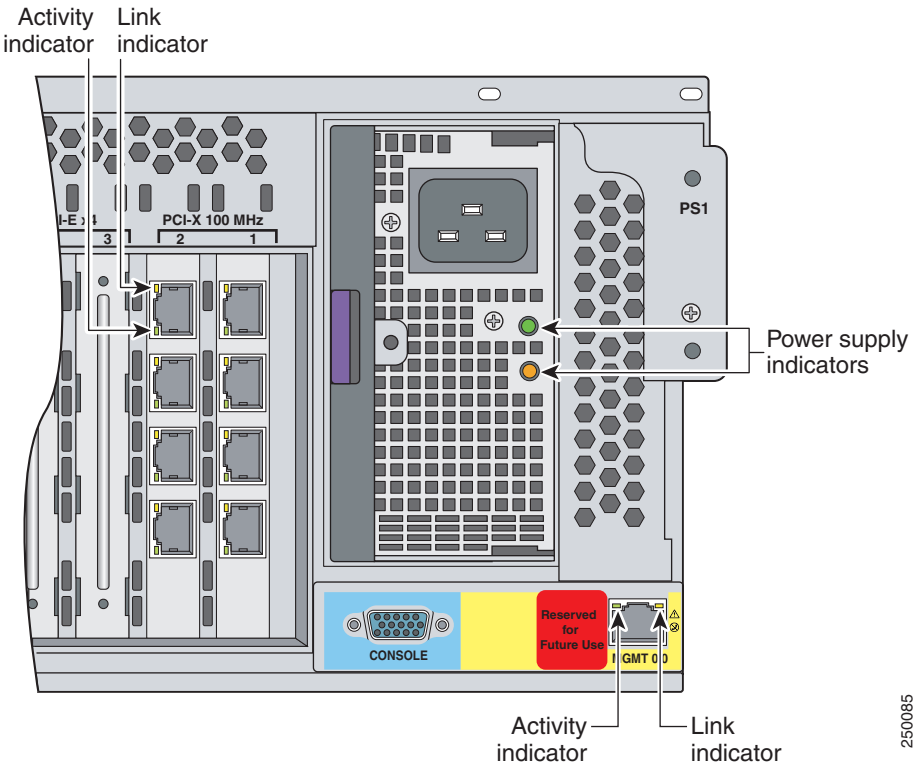


Table 4-2 describes the Ethernet port indicators.

Table 4-2 Ethernet Port Indicators

Indicator	Indicator (Green)	Description
Activity	On or flashing Off	Network activity No network activity
Link	On Off	Linked to network Not linked to network

Table 4-3 describes the power supply indicators.

Table 4-3 Power Supply Indicators

Fail Indicator 1 Amber	Power Indicator 2 Green	Description
Off	Off	No AC power to any power supply
Flashing	Off	Power supply failure (over current)
On	Off	No AC power to this power supply
Off	Flashing	• AC power present • Standby mode
Off	On	Normal

Diagnostic Panel

The front panel health indicators only indicate the current hardware status. The Diagnostic Panel indicators identify components experiencing an error, event, or failure. All indicators are off unless one of the component fails.

Note When you remove the chassis cover to view the Diagnostic Panel, leave the IPS 4270-20 powered on. Powering off the IPS 4270-20 clears the Diagnostic Panel indicators.

Figure 4-9 shows the Diagnostic Panel.

Figure 4-9 Diagnostic Panel

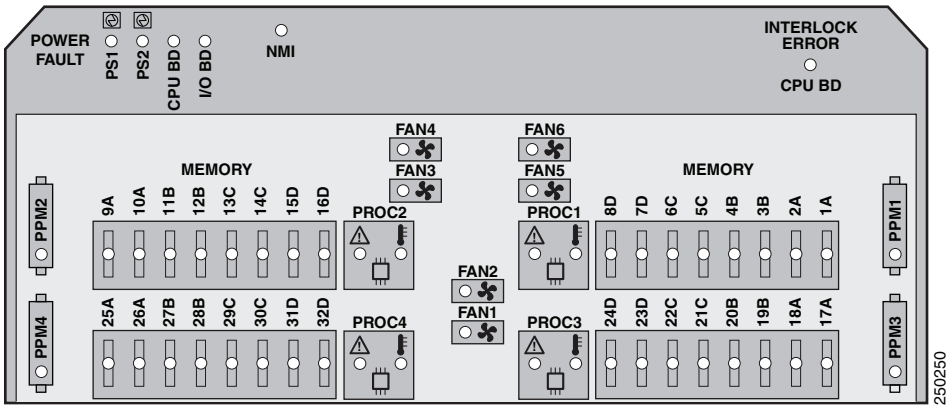


Table 4-4 lists the indicators that display health status for each component:

Table 4-4 Diagnostic Panel Indicators

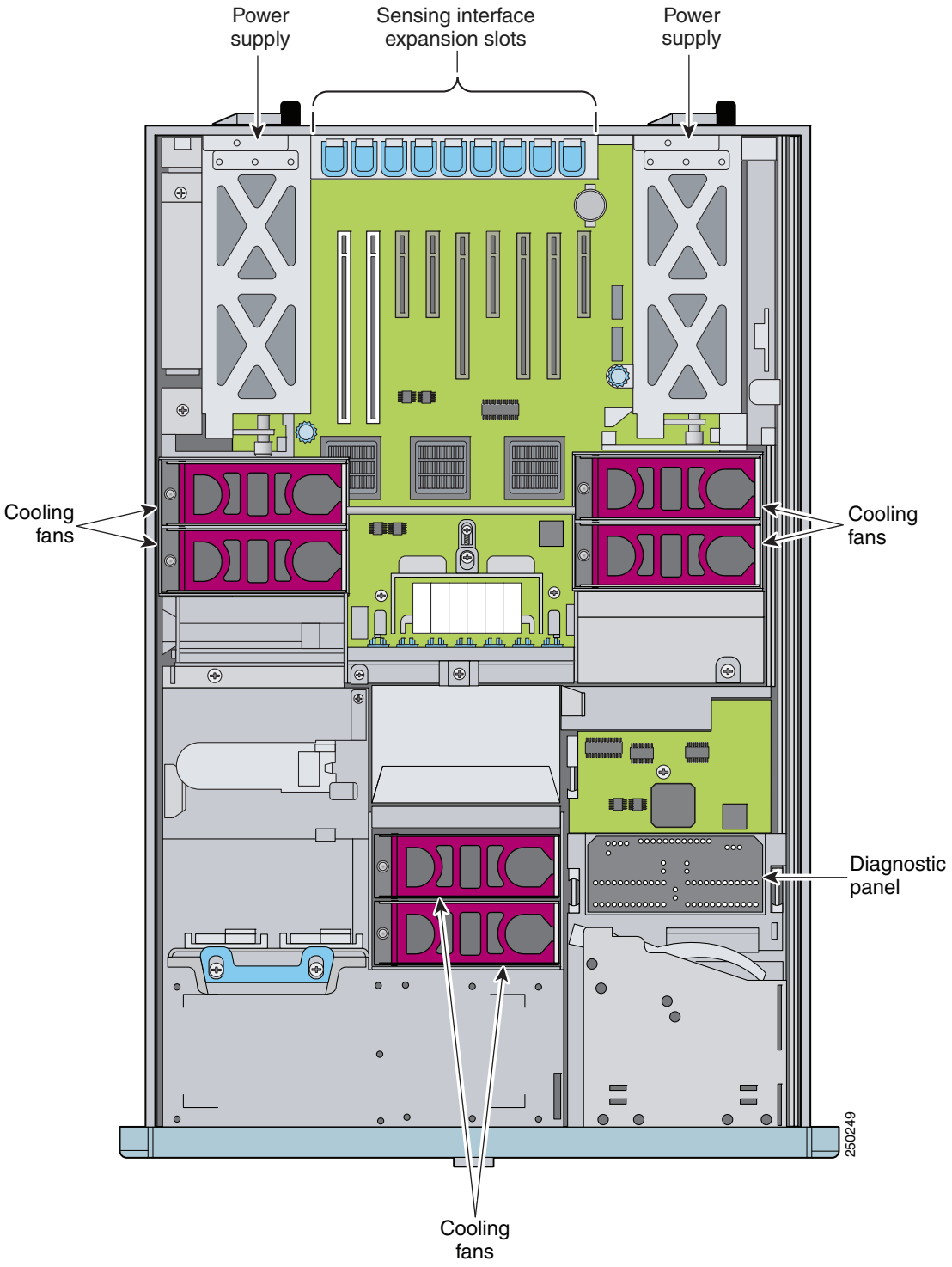
Indicator	Component
PS1	Power supply (primary)
PS2	Power supply (optional)
CPU BD (power fault)	Processor memory module board
I/O BD	System board
NMI	System NMI switch
Slot X	Expansion slot
CPU BD (interlock error)	System board
PPM X	Processor power module
1A-32D	DIMM Slot
PROC X	Processor
FAN X	Fan

For More Information

- For the location of the Diagnostic Panel in the IPS 4270-20 chassis, see Figure 4-10 on page 4-13.
- For information on how to access the Diagnostic Panel, see Accessing the Diagnostic Panel, page 4-41.

Internal Components

Figure 4-10 IPS 4270-20 Internal Components



Specifications

Table 4-5 lists the specifications for the IPS 4270-20.

Table 4-5 IPS 4270-20 Specifications

Dimensions and Weight	
Height	6.94 in. (17.6 cm)
Width	19.0 in. (46.3 cm)
Depth	26.5 in. (67.3 cm)
Weight	80 lb (36.3 kg)
Form factor	4 RU, standard 19-inch rack-mountable
Power	
Rated input voltage	100 to 127 VAC 200 to 240 VAC
Rated input frequency	50 to 60 Hz
Rated input power	1161W @ 100 VAC 1598W @ 200 VAC
Rated input current	12A (100 VAC) 8A (200 VAC)
Maximum heat dissipation	3960 BTU/hr (100 VAC) 5450 BTU/hr (200 VAC)
Power supply output	910 W (low line) 1300 W (high line)
Environment	
Temperature	Operating 50 to 95°F (10 to 35°C)[1] Nonoperating -40°F to 158°F (-40°C to 70°C)
Maximum wet bulb temperature	82.4°F (28°C)
Relative humidity (noncondensing)	Operating 10% to 90% Nonoperating 5% to 95%
Altitude	Operating 0 to 10,000 ft (3050 m) Nonoperating 0 to 30,000 ft (9144 m)
Shock	Operating Half-sine 2 G, 11 ms pulse, 100 pulses Nonoperating 25 G, 170 inches/sec delta V
Vibration	2.2 Grms, 10 minutes per axis on all three axes

1. At sea level with an altitude derating of 1.8°F per every 1000 ft (1.0°C per every 3.0m) above sea level to a maximum of 10,000 ft (3050 m). no direct sustained sunlight.

Accessories

The IPS 4270-20 accessories kit contains the following:

- DB-9 connector
- DB-9/RJ-45 console cable
- Two Ethernet RJ-45 cables
- *Regulatory Compliance and Safety Information for the Cisco Intrusion Detection and Prevention System 4200 Series Appliance Sensor*
- *Documentation Roadmap for Cisco Intrusion Prevention System*

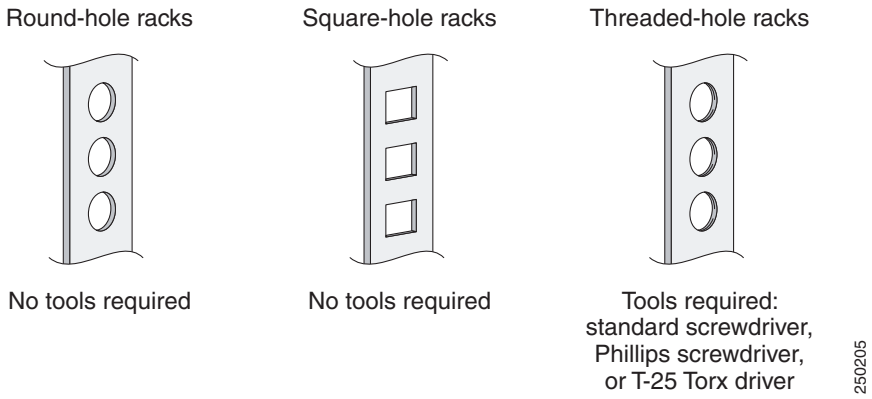
Installing the Rail System Kit

You can install the IPS 4270-20 in a 4-post rack. This section describes how to install the IPS 4270-20 in a rack, and contains the following sections:

Understanding the Rail System Kit

This rail system supports a variety of products that can be installed in round-, square, or threaded-hole racks. The following illustration shows the three rack hole-types. Use Figure 4-11 to identify your rack type and then follow the installation steps accordingly.

Figure 4-11 Round-, Square-, and Threaded-Hole Racks



No tools are required for the round- and square-hole racks. You may need screws that fit the threaded-hole rack and a driver for those screws.You need a standard screwdriver to remove the round- and square-hole studs from the slide assemblies when you install the security appliance in a threaded-whole rack.

This rail system supports a minimum rack depth of 24 in. (60.96 cm) and a maximum rack depth of 36.5 in. (92.71 cm).

Rail System Kit Contents

The rail system kit contains the following items:

- Two slide assemblies
- Two chassis rails
- Four Velcro straps
- Six zip ties
- One cable management arm
- A package of miscellaneous parts (screws, and so forth)
- One cable management arm stop bracket

Space and Airflow Requirements

To allow for servicing and adequate airflow, follow these space and airflow requirements when choosing where to place a rack:

- Leave a minimum clearance of 25 in. (63.5 cm) in front of the rack.
- Leave a minimum clearance of 30 in. (76.2 cm) behind the rack.
- Leave a minimum clearance of 48 in. (121.9 cm) from the back of the rack to the back of another rack or row of racks.

The IPS 4270-20 draws in cool air through the front and expels warm air through the back. The front and back rack doors must be adequately ventilated to allow ambient room air to enter the chassis and the back must be adequately ventilated to allow warm air to escape from the chassis.

Installing the IPS 4270-20 in the Rack

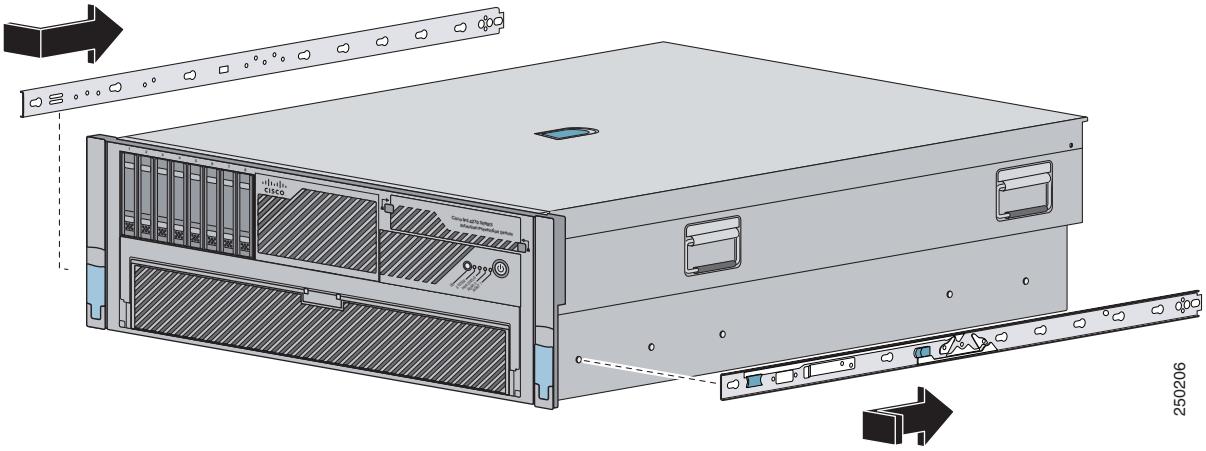
Warning **To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:**

- **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.** Statement 1006

Warning **This procedure requires two or more people to position the IPS 4270-20 on the slide assemblies before pushing it in to the rack.**

To install the IPS 4270-20 in the rack, follow these steps:

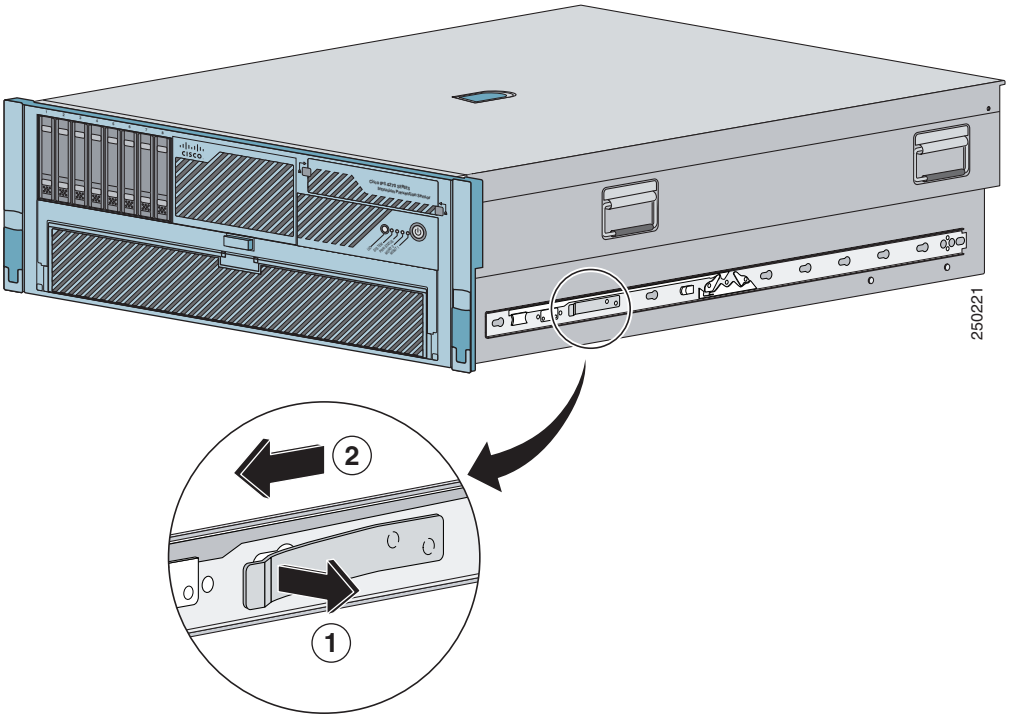
Step 1 Attach the chassis side rail to the IPS 4270-20 by aligning the chassis rail to the stud on the IPS 4270-20, pressing the chassis side rail in to the stud, and then sliding the chassis side rail backwards until you hear the latch catch.



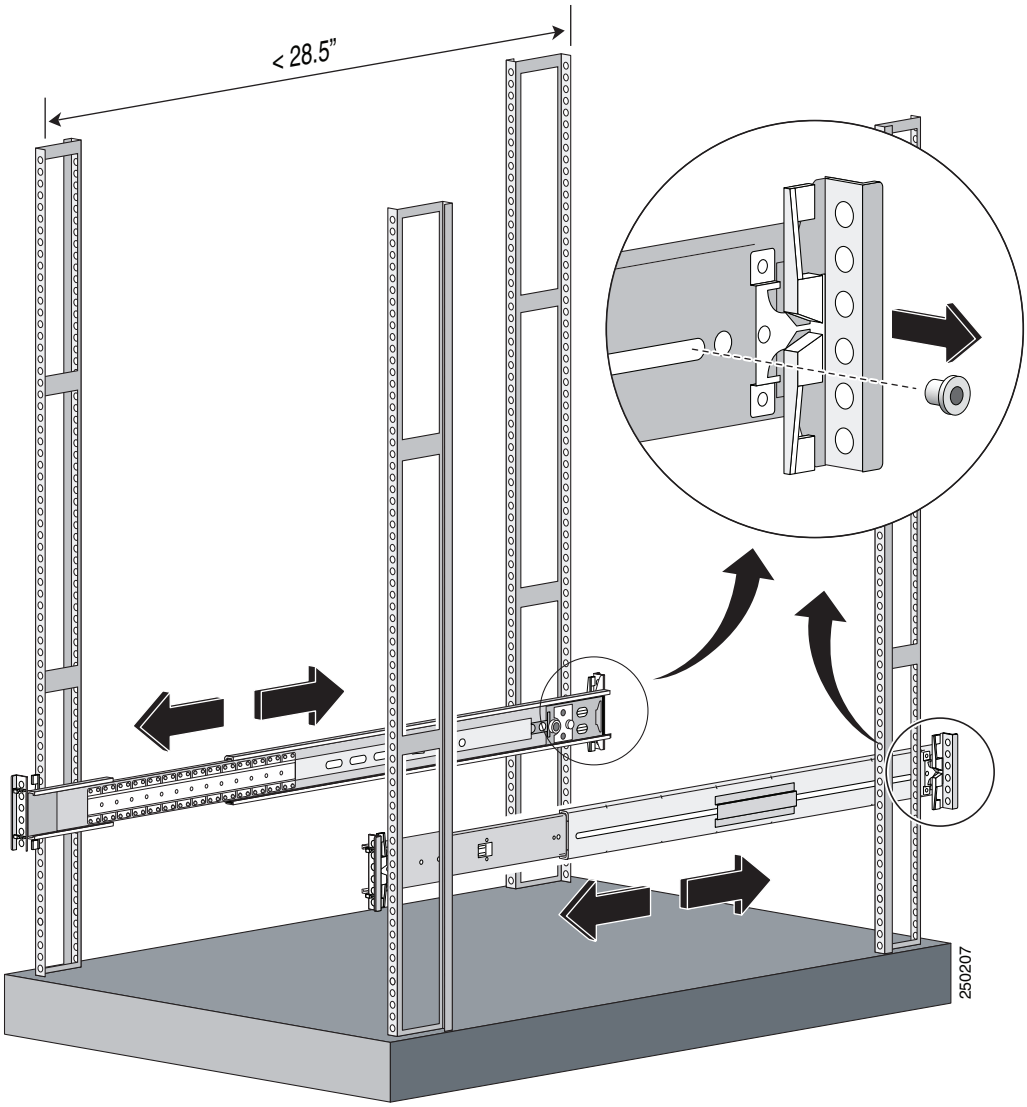
Note The tapered end of the chassis side rail should be at the back of the IPS 4270-20. The chassis side rail is held in place by the inner latch.

Step 2 Repeat Step 1 for each chassis side rail.

Step 3 To remove the chassis side rail, lift the latch, and slide the rail forward.



Step 4 If you are installing the IPS 4270-20 in a shallow rack, one that is less than 28.5 in. (72.39 cm), remove the screw from the inside of the slide assembly before continuing with Step 5.

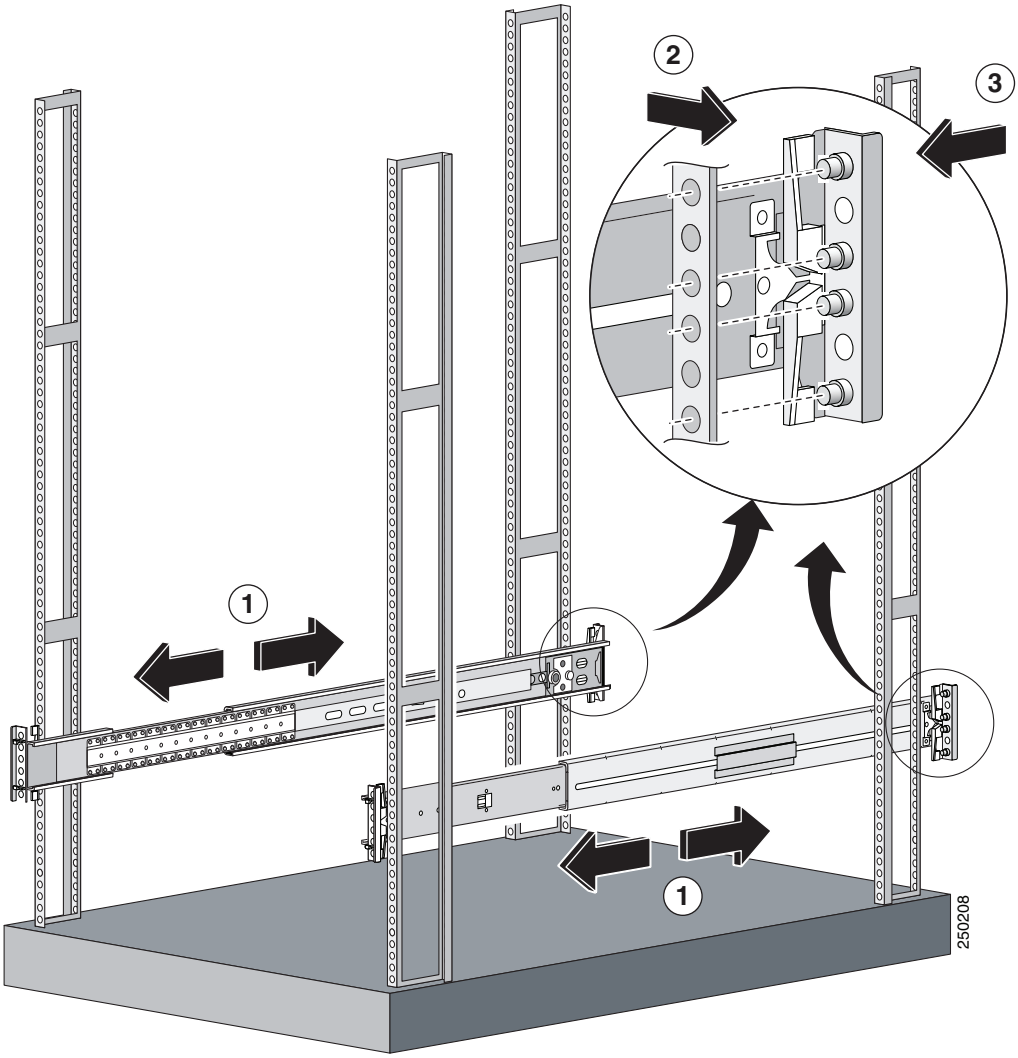


Step 5 Attach the slide assemblies to the rack.

For round- and square-hole racks:

a. Line up the studs on the slide assembly with the holes on the inside of the rack and snap in to place.

b. Adjust the slide assembly lengthwise to fit the rack. The spring latch locks the slide assembly into position.



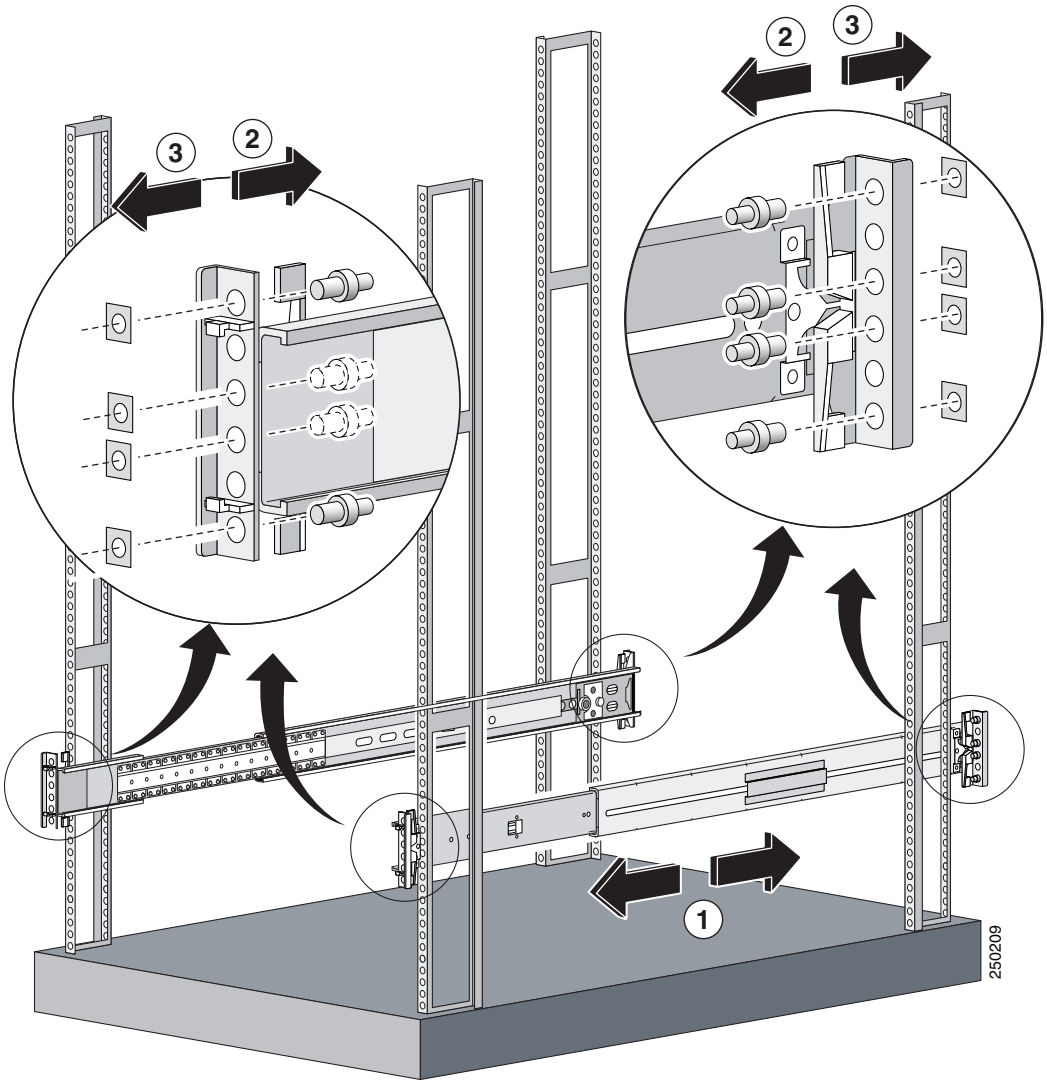
c. Repeat for each slide assembly. Make sure the slide assemblies line up with each other in the rack.

d. Lift the spring latch to release the slide assembly if you need to reposition it.

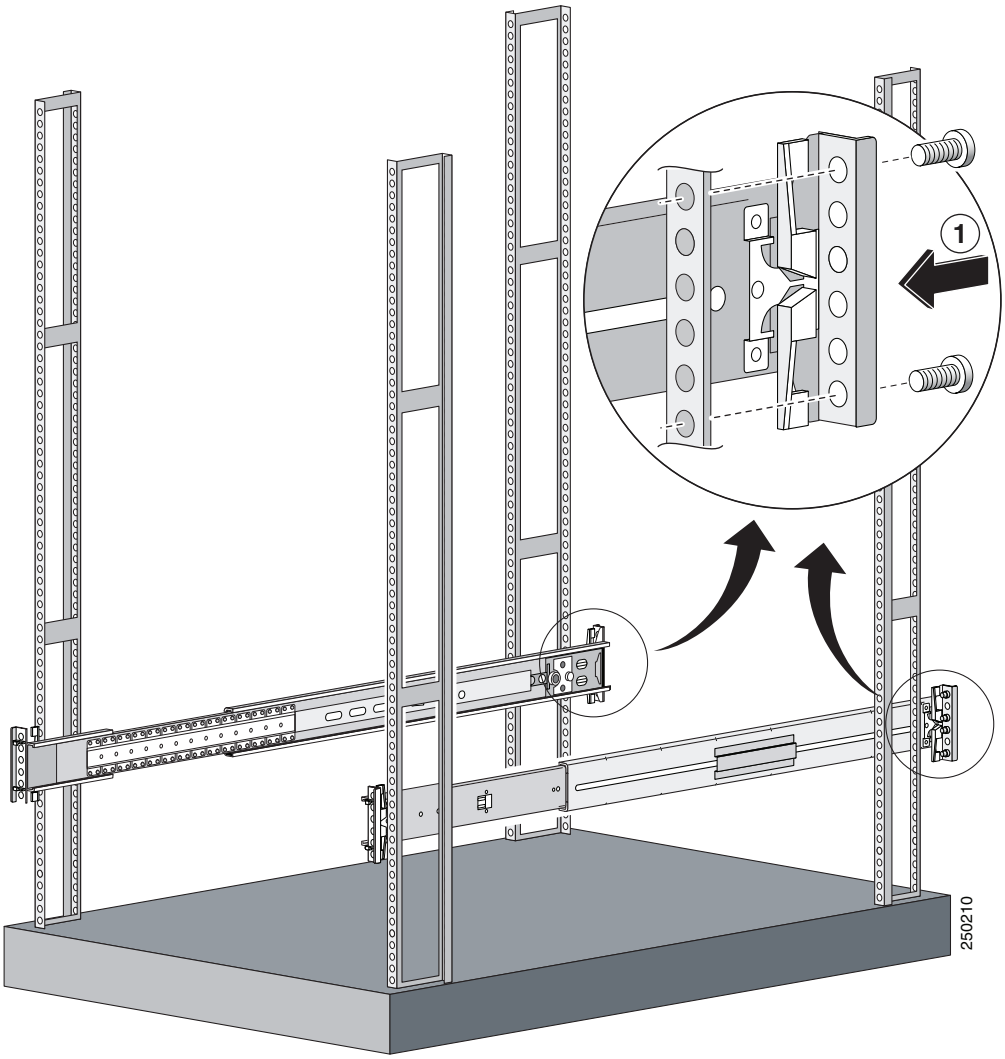
For threaded-hole racks:

a. Remove the eight round- or square-hole studs on each slide assembly using a standard screwdriver.

Note You may need a pair of pliers to hold the retaining nut.

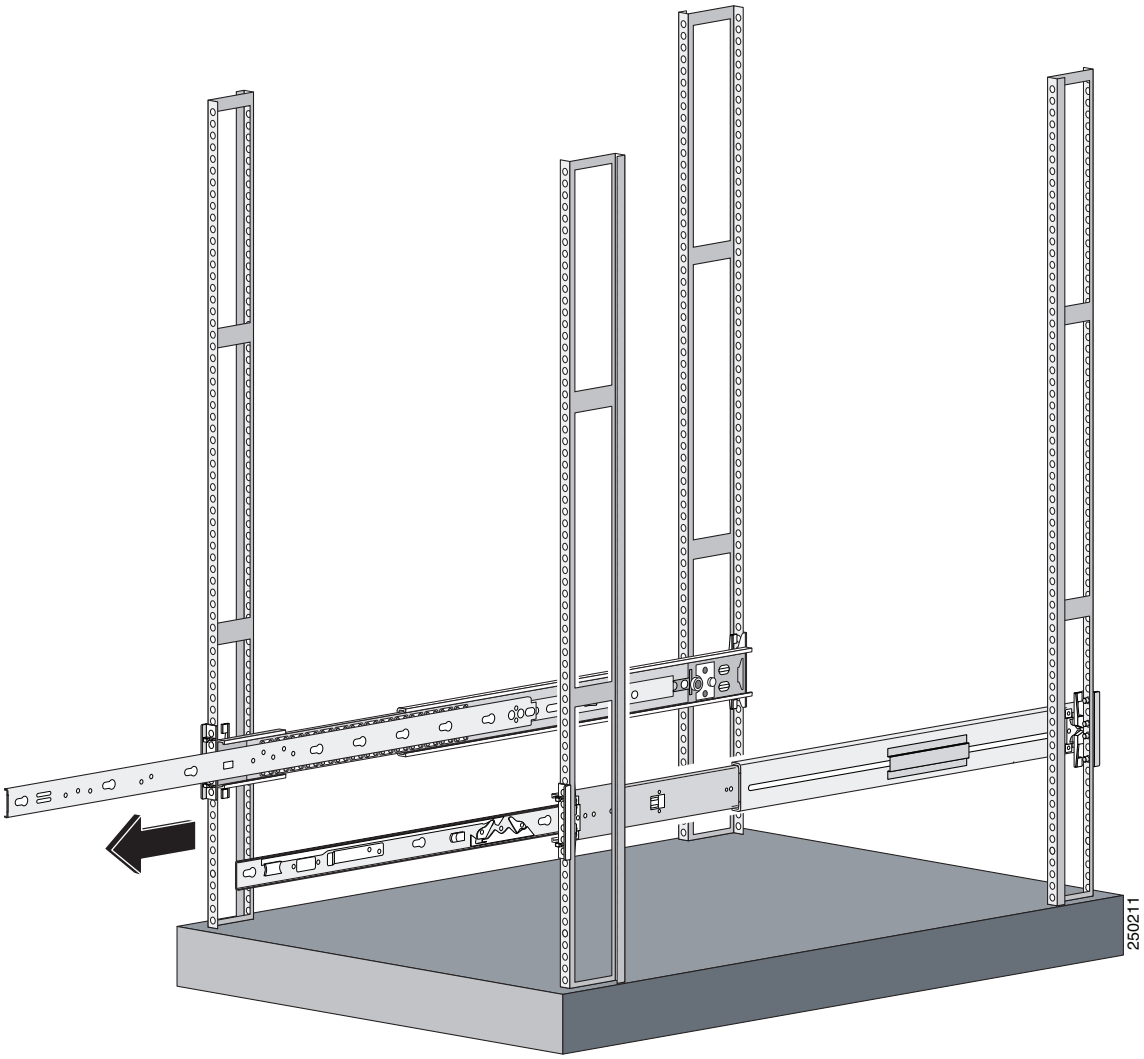


b. Line up the bracket on the slide assembly with the rack holes, install two screws (top and bottom) on each end of the slide assembly.

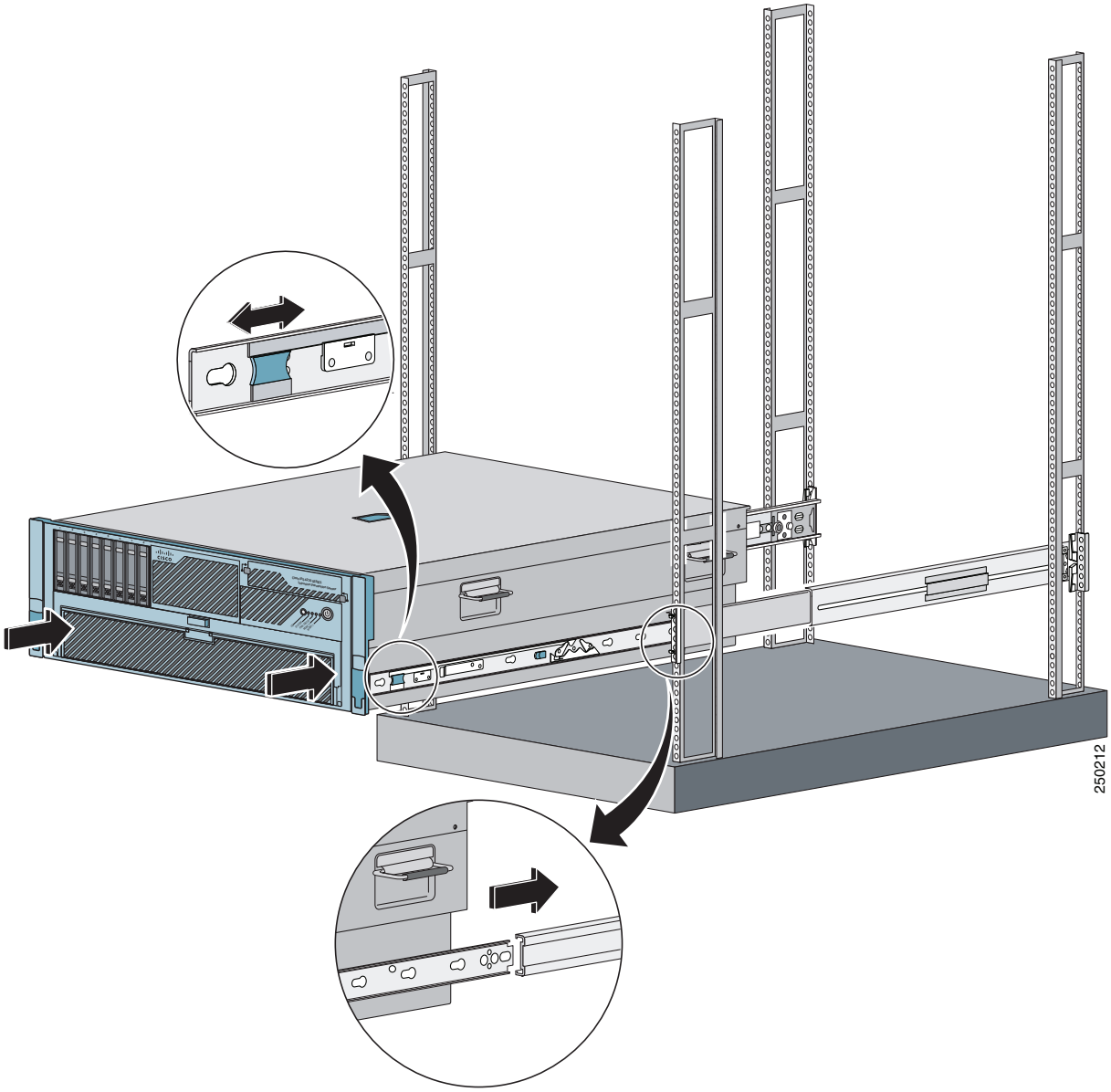


c. Repeat for each slide assembly.

Step 6 Extend the slide assemblies out of the rack.



Step 7 Align the chassis side rails on the IPS 4270-20 with the slide assembly on both sides of the rack, release the blue slide tab (by either pulling the tab forward or pushing the tab back), and carefully push the IPS 4270-20 in to place.

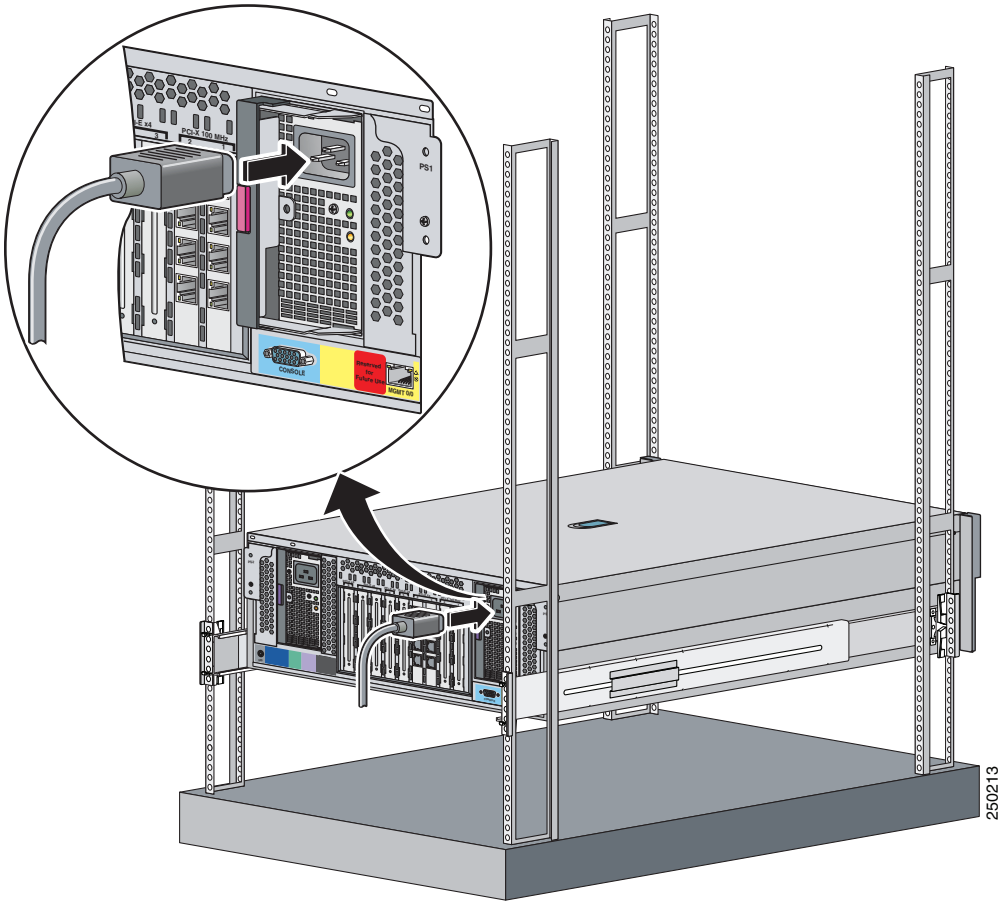


Caution Keep the IPS 4270-20 parallel to the floor as you slide it into the rails. Tilting the IPS 4270-20 up or down can damage the slide rails.

Step 8 If you are using the cable management arm, install it before you connect and route any cables.

Note You may also need longer cables when the arm is installed (an extra length of around 3 feet is required).

Step 9 Install the electrical cables at the back of the IPS 4270-20.



For More Information

- For the procedure for installing the cable management arm, see Installing the Cable Management Arm, page 4-28.
- For information on installing connections to the IPS 4270-20, see Installing the IPS 4270-20, page 4-35.

Extending the IPS 4270-20 from the Rack

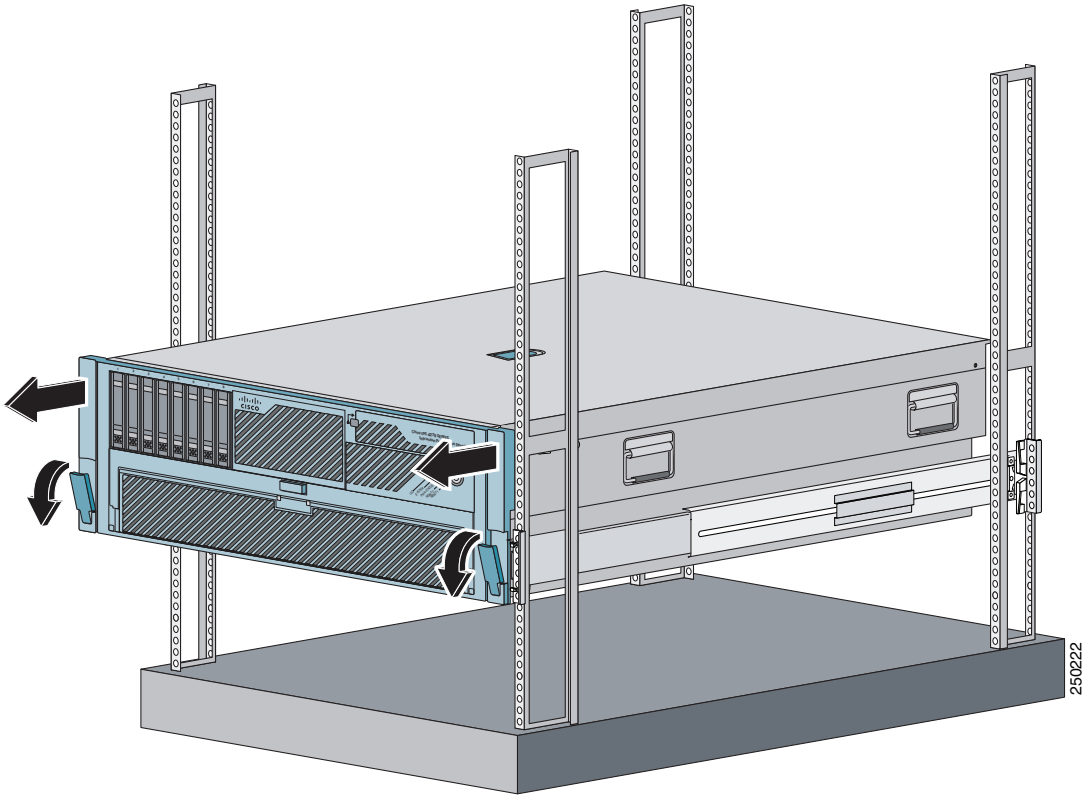
You can extend the IPS 4270-20 from the rack for service or removal.

Caution You can only extend the IPS 4270-20 from the rack if the cable management arm is correctly installed with the cables routed through it or if all cables are disconnected from the back of the chassis. Otherwise, you risk damage to the cables and a possible shock hazard if the power cables get caught between the chassis and the rack.

To extend the IPS 4270-20 from the rack, follow these steps:

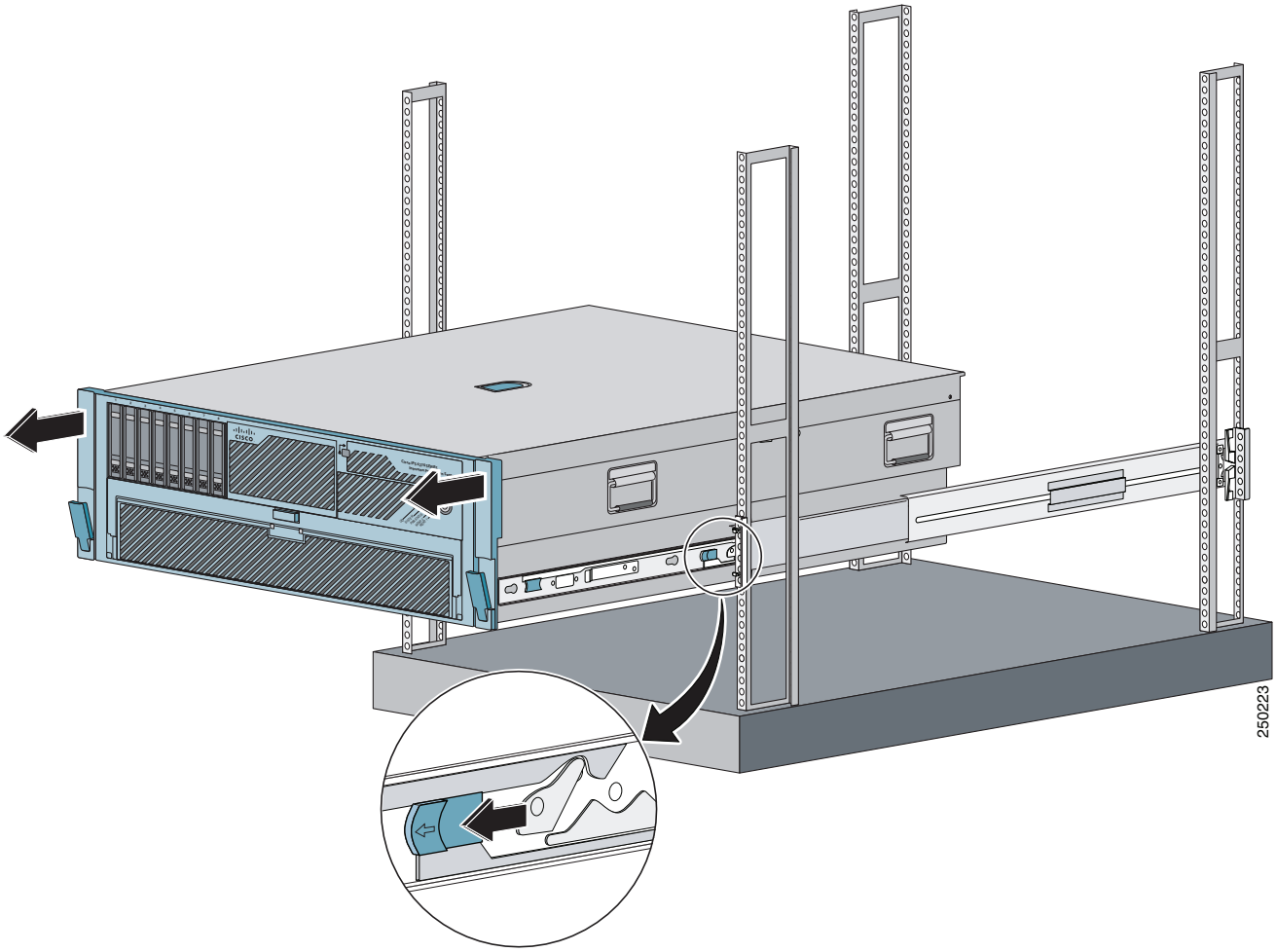
Step 1 Pull the quick-release levers on each side of the front bezel of the IPS 4270-20 to release it from the rack and extend it on the rack rails until the rail-release latches engage.

Note The release latches lock in to place when the rails are fully extended.



Step 2 After performing the installation or maintenance procedure, slide the IPS 4270-20 in to the rack by pressing the rail-release latches.

Step 3 To completely remove the IPS 4270-20 from the rack, disconnect the cables from the back of the IPS 4270-20, push the release tab in the middle of the slide assembly forward, and pull the IPS 4270-20 from the rack.

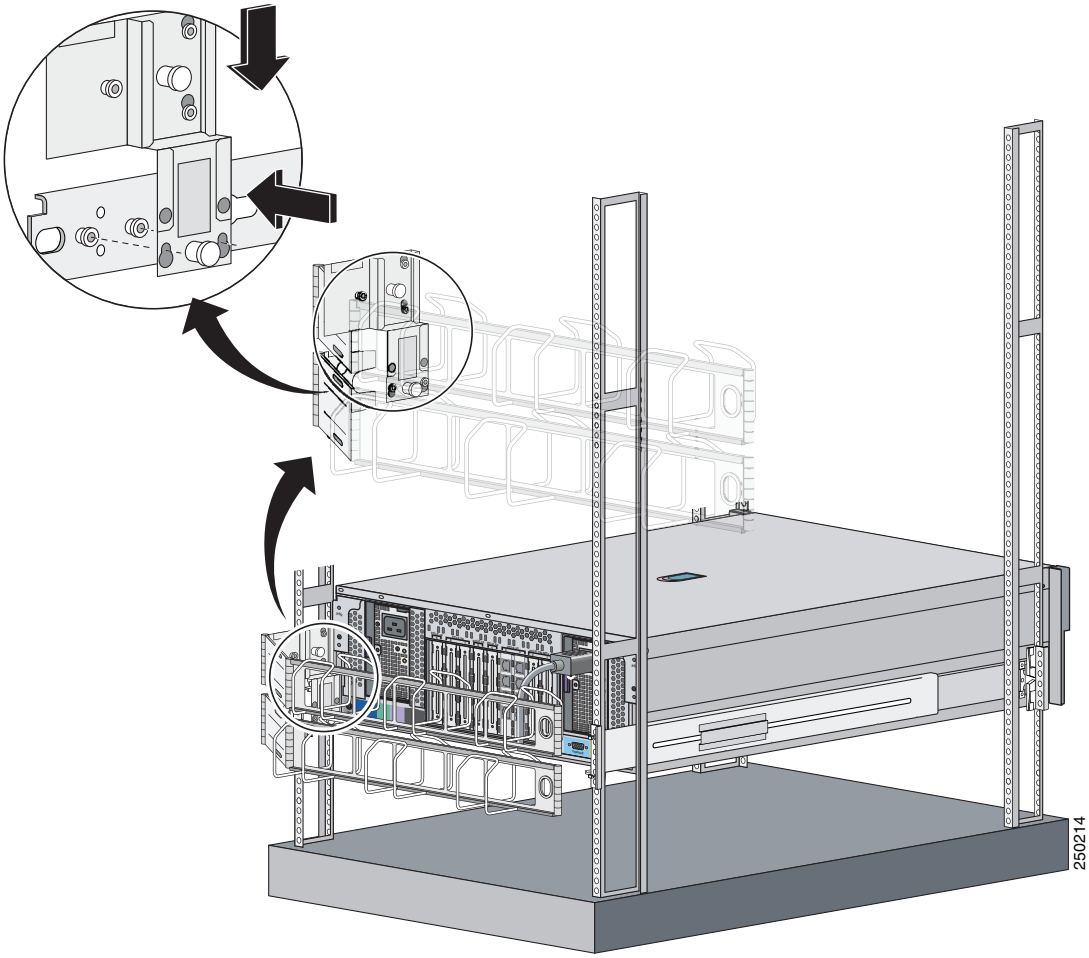


Installing the Cable Management Arm

Note To hinge the cable management arm on the back right-hand side of the rack, see Converting the Cable Management Arm, page 4-31.

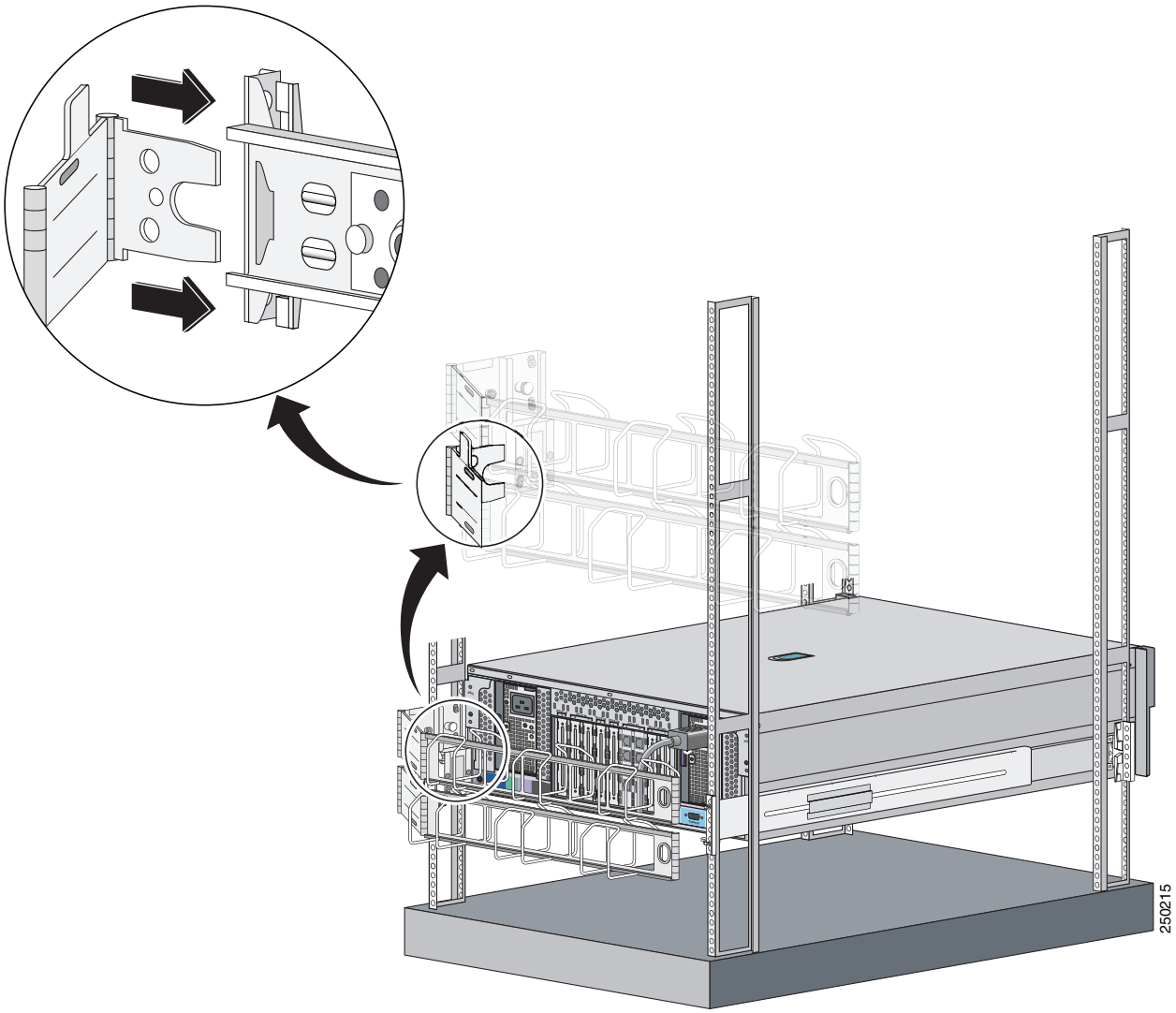
To install the cable management arm, follow these steps:

Step 1 Align the slide bracket on the cable management arm with the stud on the back of the IPS 4270-20 and align the two studs at the back of the chassis side rail, then slide down and lock in to place.



Step 2 Attach the cable trough to the back of the rack by pushing the lower metal tab on the cable management arm in to the slide assembly, then lifting the spring pin to lock it in to place.

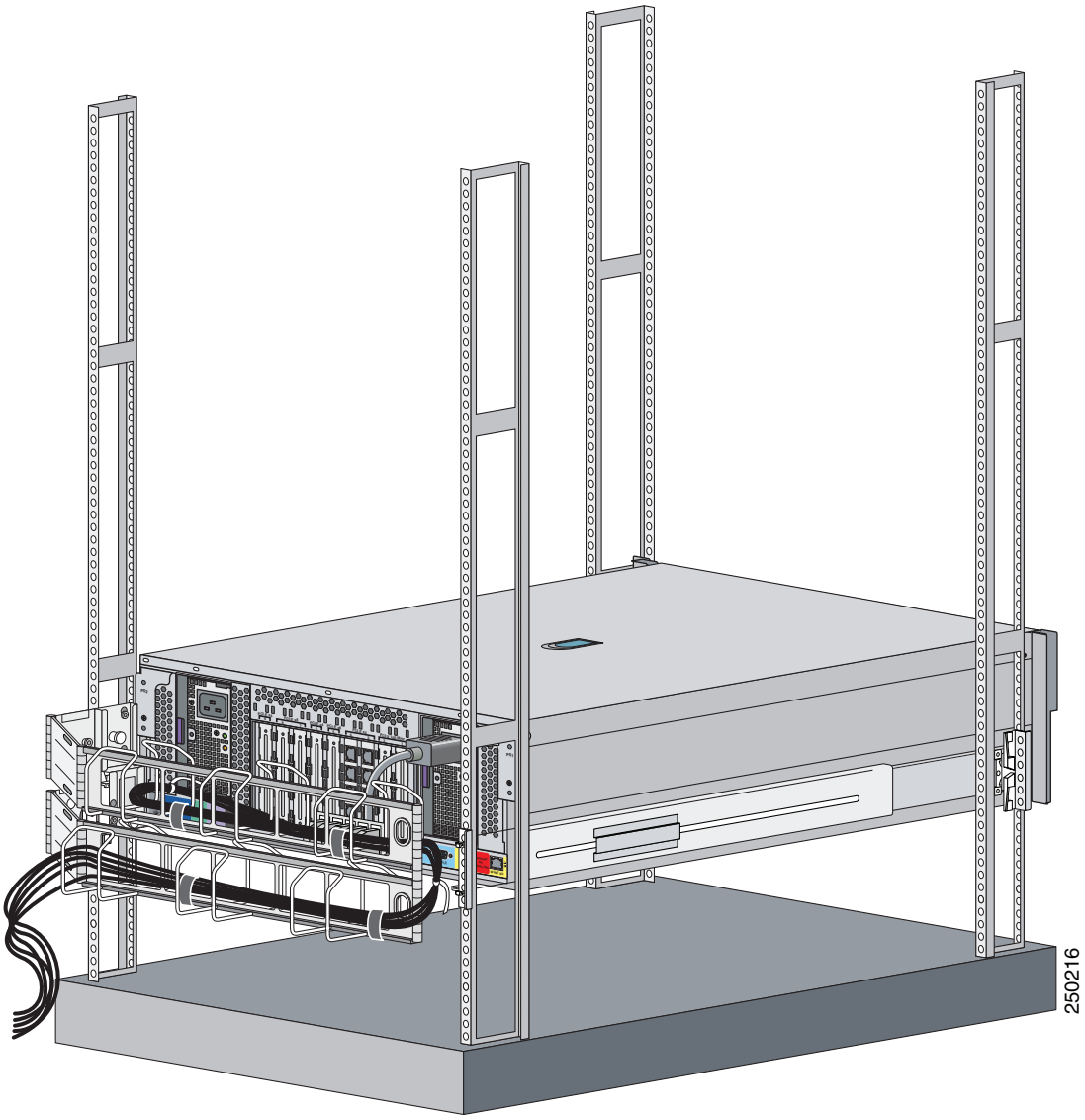
Caution Make sure the metal tab is on the outside of the upper part of the cable management arm.



Note When properly installed, the cable management arm is attached to the IPS 4270-20 and the rack rail.

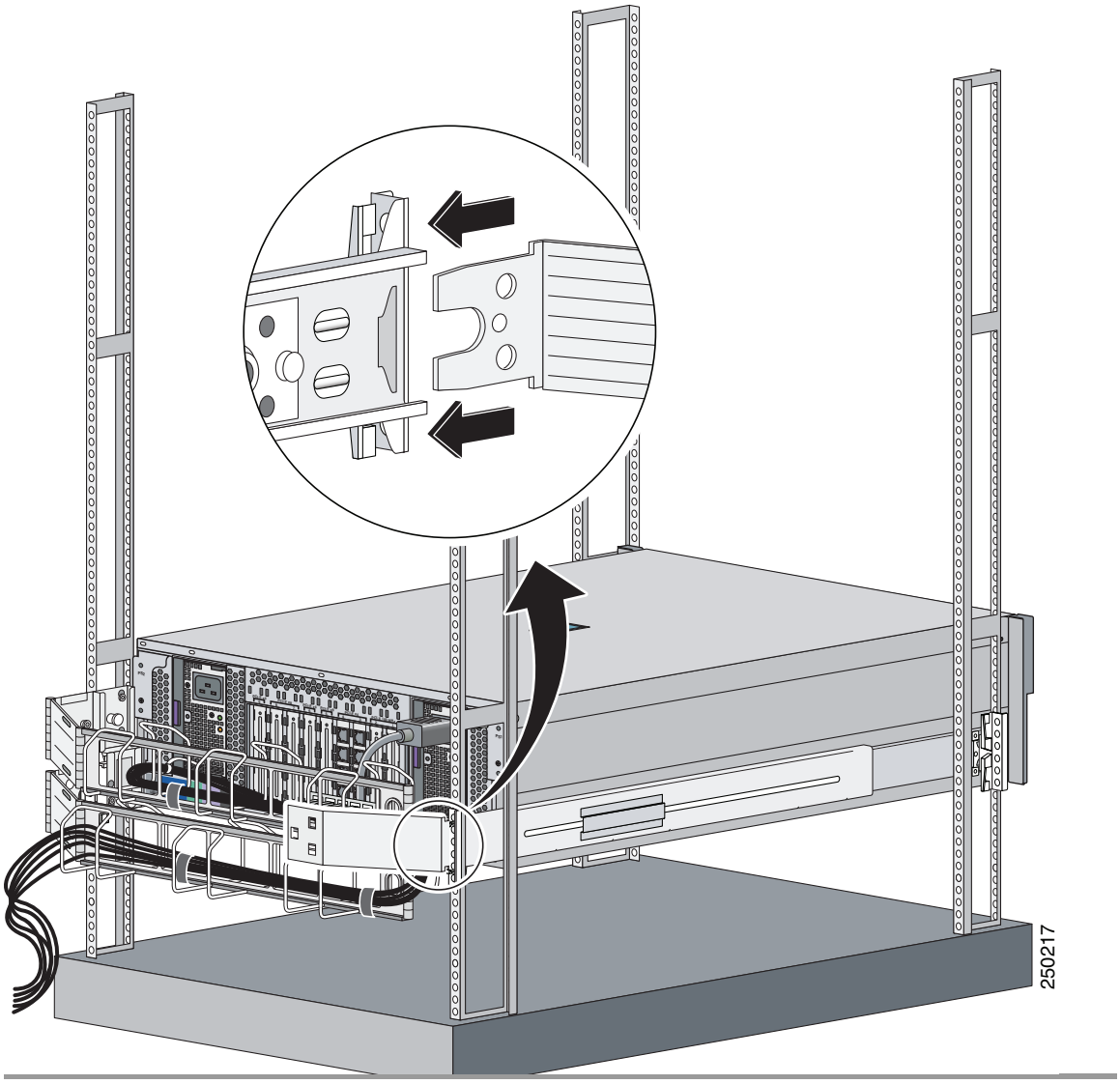
Step 3 Route the cables through the cable trough and secure the cables with the Velcro straps and black tie wraps.

Note After you route the cables through the cable management arm, make sure the cables are not pulled tight when the IPS 4270-20 is fully extended.



Caution Do not use the straps and zip ties to tie the two parts of the cable management arm together.

Step 4 Attach the cable management arm stop bracket to the ride side of the back of the rack by inserting the stop bracket into the cable management arm bracket.



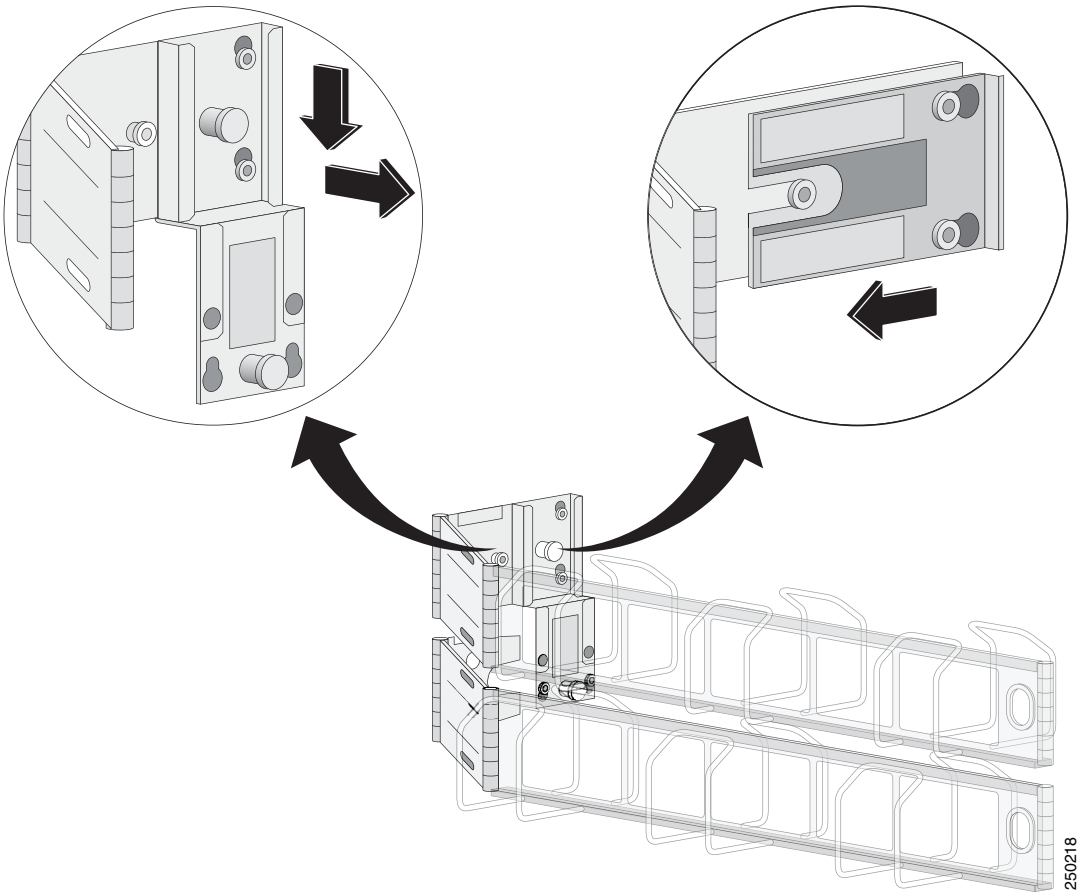
Converting the Cable Management Arm

Note The cable management arm is designed for ambidextrous use. You can convert the cable management arm from a left-hand swing to a right-hand swing.

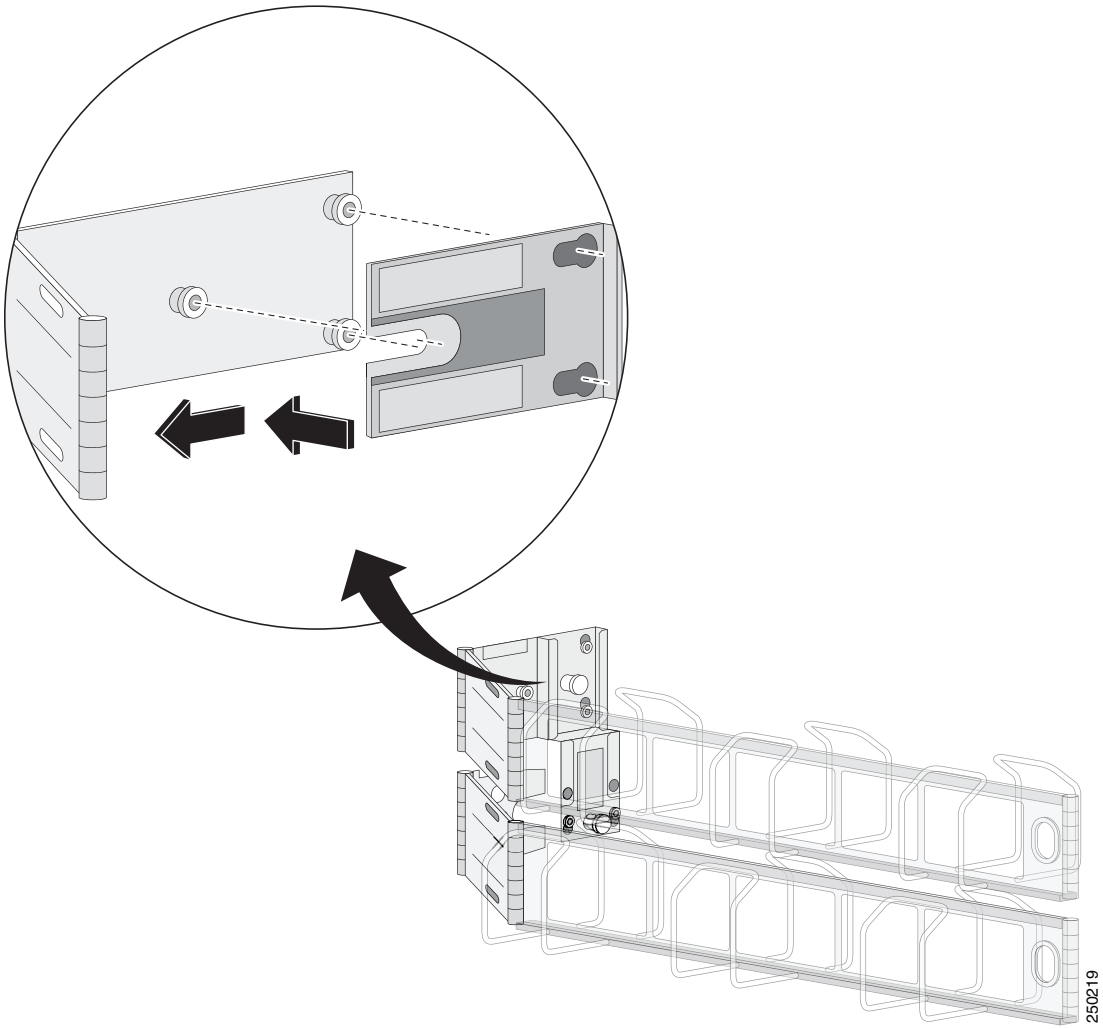
Note Make sure to orient the management arm with the cable trough facing upward.

To convert the cable management arm swing, follow these steps:

Step 1 Pull up the spring pin and slide the bracket off the cable management arm.

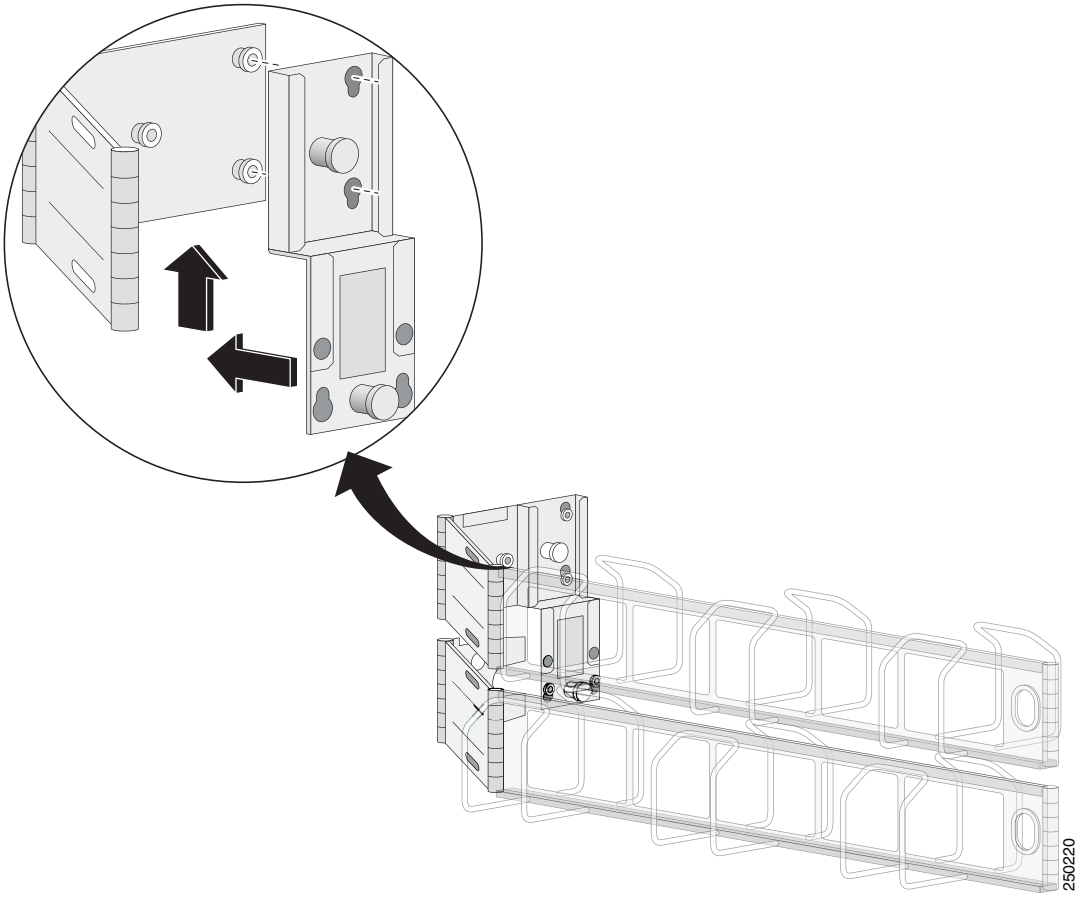


Step 2 Remove the bottom sliding bracket and flip it over to the top of the bracket aligning the studs.



Step 3 On the other side of the sliding bracket, align the spring pin with the studs and key holes, and slide until the pin snaps in to place.

Note The sliding bracket only fits one way because the hole for the spring pin is offset.



Installing the IPS 4270-20

Caution Follow proper safety procedures when performing these steps by reading the safety warnings in *Regulatory Compliance and Safety Information for the Cisco Intrusion Prevention System 4200 Series Appliance Sensor*.

Warning **IMPORTANT SAFETY INSTRUCTIONS**

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment. Statement 1030**

To install the IPS 4270-20 on the network, follow these steps:

Step 1 Position the IPS 4270-20 on the network.

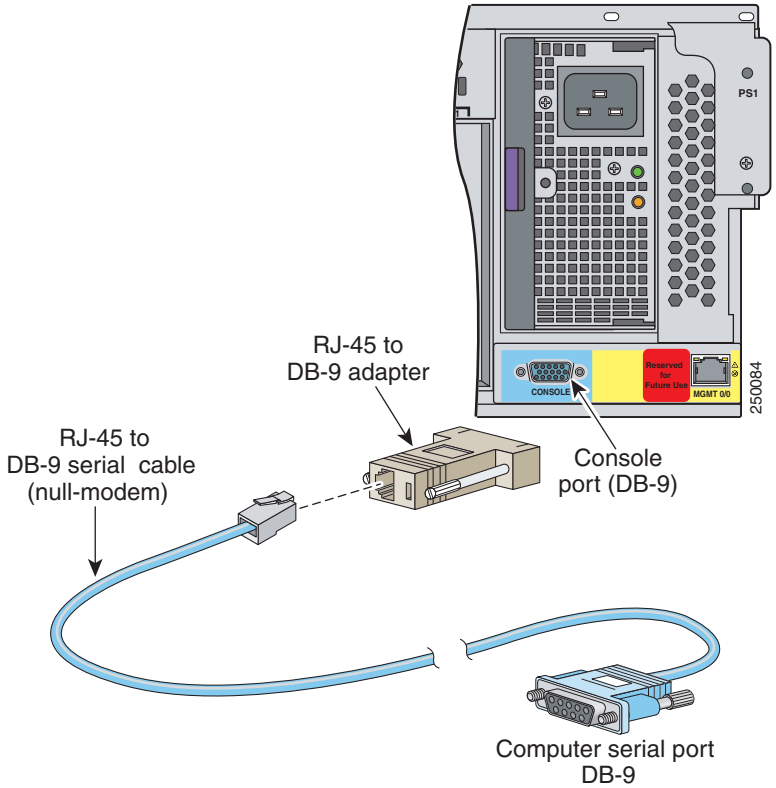
Step 2 Install the IPS 4270-20 in a rack, if you are rack mounting it.

Step 3 Connect the cable as shown in Step 4 so that you have either a DB-9 connector on one end as required by the serial port for your computer, and the other end is the RJ-45 connector.

Note Use the console port to connect to a computer to enter configuration commands. Locate the serial cable from the accessory kit. The serial cable assembly consists of a 180/rollover cable with RJ-45 connectors (DB-9 connector adapter PN 74-0495-01).

Note You can use a 180/rollover or straight-through patch cable to connect the appliance to a port on a terminal server with RJ-45 or hydra cable assembly connections. Connect the appropriate cable from the console port on the appliance to a port on the terminal server.

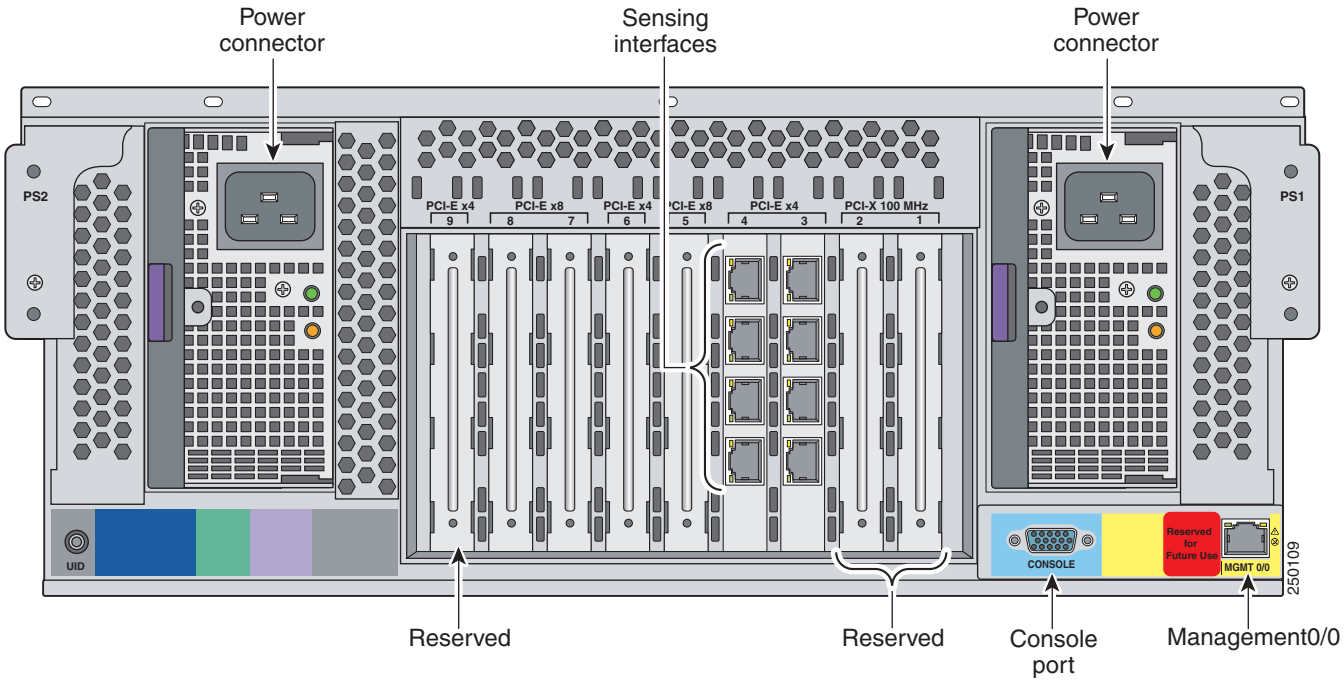
Step 4 Connect the RJ-45 to DB-9 adapter connector to the console port and connect the other end to the DB-9 connector on your computer.



Step 5 Attach the network cables to the following interfaces:

- Management0/0 (MGMT0/0) is the command and control port.
- GigabitEthernet*slot_number*/*port_number* through GigabitEthernet*slot_number*/*port_number* are the expansion ports.

Caution Management and console ports are privileged administrative ports. Connecting them to an untrusted network can create security concerns.



Step 6 Attach the power cables (there are two power supplies) to the IPS 4270-20 and plug them in to a power source (a UPS is recommended).

Step 7 Power on the IPS 4270-20.

Step 8 Initialize the IPS 4270-20.

Step 9 Upgrade the IPS 4270-20 with the most recent Cisco IPS software. You are now ready to configure intrusion prevention on the IPS 4270-20.

For More Information

- For more information on working with electrical power and in an ESD environment, see Site and Safety Guidelines, page 1-30.
- For more information on the best place to position your sensor on the network, see Your Network Topology, page 1-3.
- For the procedure for installing the IPS 4270-20 in a rack, see Installing the IPS 4270-20 in the Rack, page 4-17.
- For the instructions for setting up a terminal server, see Connecting an Appliance to a Terminal Server, page 1-19.
- For the procedure for using the **setup** command to initialize the IPS 4270-20, see Initializing the Sensor, page 10-1.
- For the procedure for obtaining the most recent Cisco IPS software, see Obtaining Cisco IPS Software, page 11-1.

- For the procedure for using HTTPS to log in to IDM, refer to Logging In to IDM.
- For the procedures for configuring intrusion prevention on your sensor, refer to the following guides:
  - *Installing and Using Cisco Intrusion Prevention System Device Manager 7.0*
  - *Installing and Using Cisco Intrusion Prevention System Manager Express 7.0*
  - *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 7.0*

Removing and Replacing the Chassis Cover

Caution Follow proper safety procedures when performing these steps by reading the safety warnings in *Regulatory Compliance and Safety Information for the Cisco Intrusion Prevention System 4200 Series Appliance Sensor*.

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 the IPS 4270-20 does not require any special tools and does not create any radio frequency leaks.

Caution Do not operate the 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 the 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 the IPS 4270-20 using IDM or IME.

Step 3 Power off the IPS 4270-20.

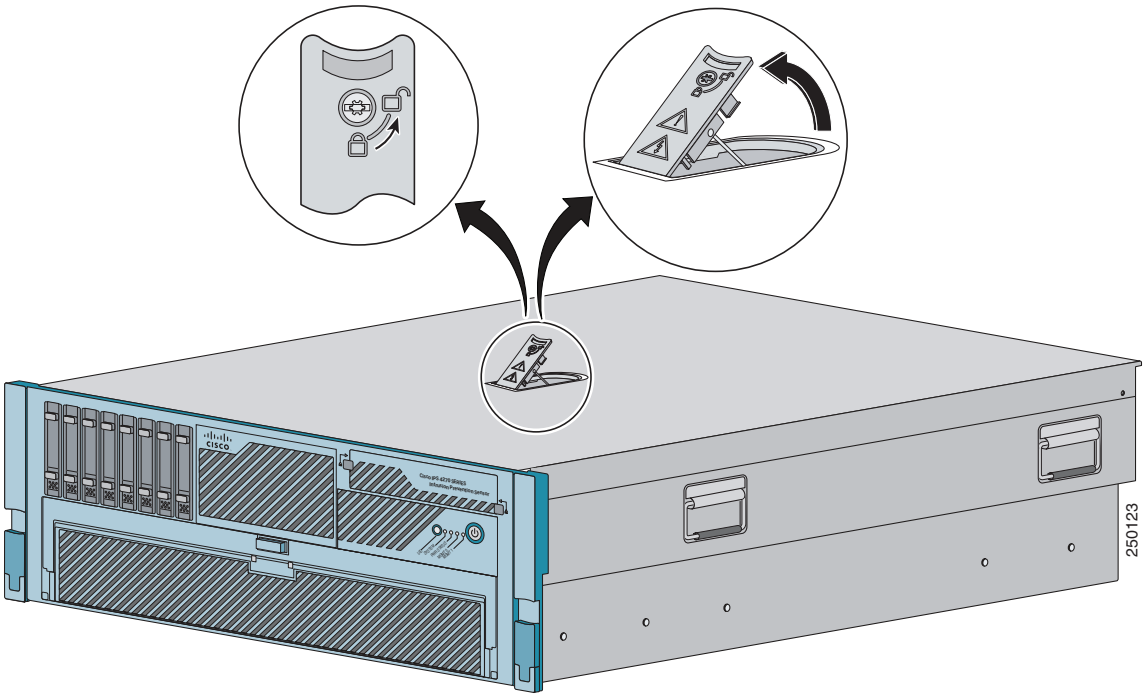
Step 4 Remove both power cables from the IPS 4270-20.

Step 5 Extend the IPS 4270-20 out of the rack if it is rack-mounted.

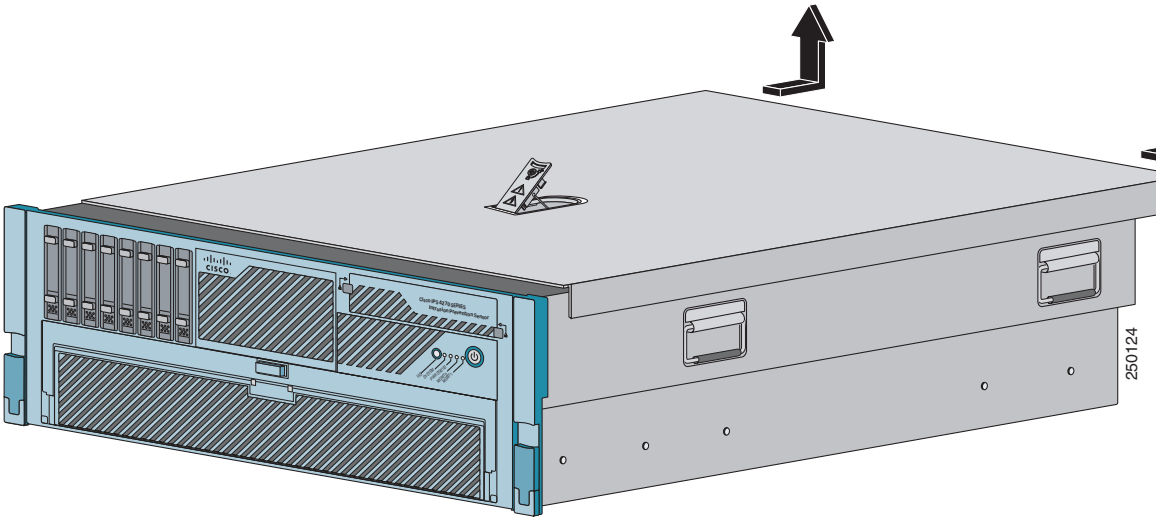
Step 6 Make sure the IPS 4270-20 is in an ESD-controlled environment.

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 the 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 the IPS 4270-20.

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

Step 12 Reinstall the 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 the IPS 4270-20.

For More Information

- For the procedure extending the IPS 4270-20 from the rack, see Extending the IPS 4270-20 from the Rack, page 4-25.
- For more information on working in an ESD-controlled environment, see Working in an ESD Environment, page 1-32.
- For the IDM procedure for powering down the IPS 4270-20, refer to Rebooting the Sensor; for the IME procedure for powering down the IPS 4270-20, refer to Rebooting the Sensor.
- For an illustration of the screwdriver and where it is located, see Figure 4-7 on page 4-9.
- For the procedure for installing the power cables on the IPS 4270-20, see Installing the IPS 4270-20, page 4-35.
- If you are reinstalling the IPS 4270-20 in a rack, see Installing the Rail System Kit, page 4-15.

Accessing the Diagnostic Panel

Note When you remove the chassis cover to view the Diagnostic Panel, leave the IPS 4270-20 powered on. Powering off the IPS 4270-20 clears the Diagnostic Panel indicators.

To access the Diagnostic Panel, follow these steps:

Step 1 Extend the IPS 4270-20 from the rack.

Step 2 Remove the chassis cover.

Step 3 Locate the Diagnostic Panel.

Follow the instructions in this chapter to remove and install failed components. For aid in troubleshooting, use the internal health indicators information when contacting TAC.

For More Information

- For the procedure for extending the IPS 4270-20 from the rack, see Extending the IPS 4270-20 from the Rack, page 4-25.
- For the procedure for removing the chassis cover, see Removing and Replacing the Chassis Cover, page 4-38.
- For the location of the Diagnostic Panel, see Figure 4-10 on page 4-13.
- For information on what internal health information each indicator displays on the Diagnostic Panel, see Diagnostic Panel, page 4-11.

Installing and Removing Interface Cards

Caution Follow proper safety procedures when performing these steps by reading the safety warnings in *Regulatory Compliance and Safety Information for the Cisco Intrusion Prevention System 4200 Series Appliance Sensor*.

The 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 The 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 the IPS 4270-20 or the expansion cards, power down the 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 the IPS 4270-20 unless all expansion slots have a cover or a card installed.

To install and remove interface cards, follow these steps:

Step 1 Log in to the CLI.

Step 2 Prepare the 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 the IPS 4270-20 using IDM or IME.

Step 3 Power off the IPS 4270-20.

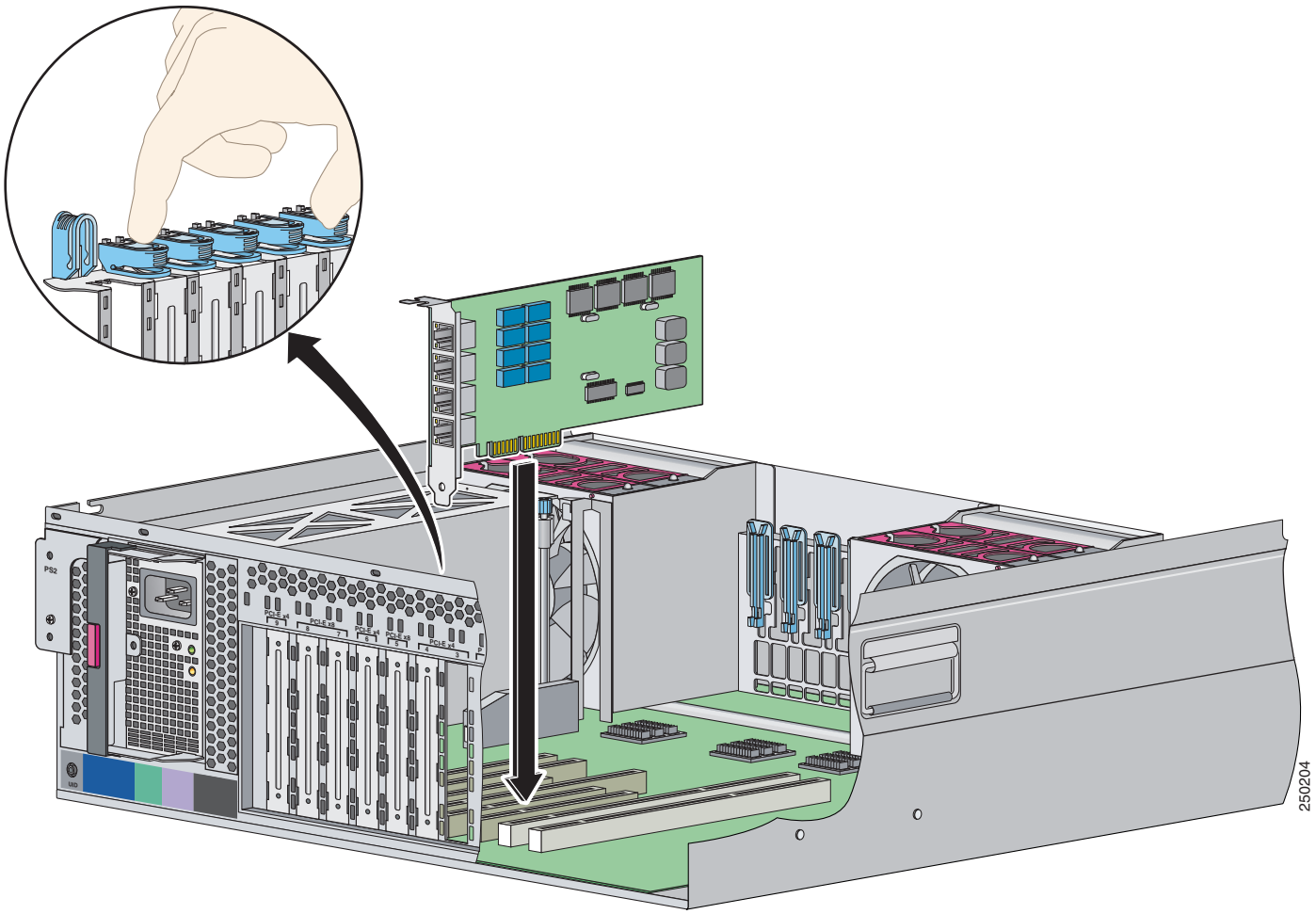
Step 4 Remove the power cables from the IPS 4270-20.

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

Step 6 Make sure the 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 mother board 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 the IPS 4270-20.

Step 13 Power on the IPS 4270-20.

For More Information

- For an illustration of the expansion card slots, see Figure 4-7 on page 4-9.
- For an illustration of the supported interface cards, see Supported Interface Cards, page 4-3.
- For the IDM procedure for powering down the IPS 4270-20, refer to Rebooting the Sensor; for the IME procedure for powering down the IPS 4270-20, refer to Rebooting the Sensor.
- For the procedure for extending the IPS 4270-20 from the rack, see Extending the IPS 4270-20 from the Rack, page 4-25.
- For more information on working in an ESD-controlled environment, see Working in an ESD Environment, page 1-32.
- For the procedure for removing the chassis cover, see Removing and Replacing the Chassis Cover, page 4-38.

Installing and Removing the Power Supply

Caution Follow proper safety procedures when performing these steps by reading the safety warnings in *Regulatory Compliance and Safety Information for the Cisco Intrusion Prevention System 4200 Series Appliance Sensor*.

The IPS 4270-20 ships with two hot-pluggable power supplies, thus providing a redundant power supply configuration. You can install or replace either power supply without powering down the IPS 4270-20, as long as one power supply is active and functioning correctly.

Caution If only one power supply is installed, do not remove the power supply unless the IPS 4270-20 has been powered down. Removing the only operational power supply causes an immediate power loss.

To install and remove power supplies, follow these steps:

Step 1 Log in to the CLI.

Note Power supplies are hot-pluggable. You can replace a power supply while the IPS 4270-20 is running, if you are replacing a redundant power supply.

Step 2 Prepare the IPS 4270-20 to be powered off (if you only have one active, functioning power supply):

```
sensor# reset powerdown
```

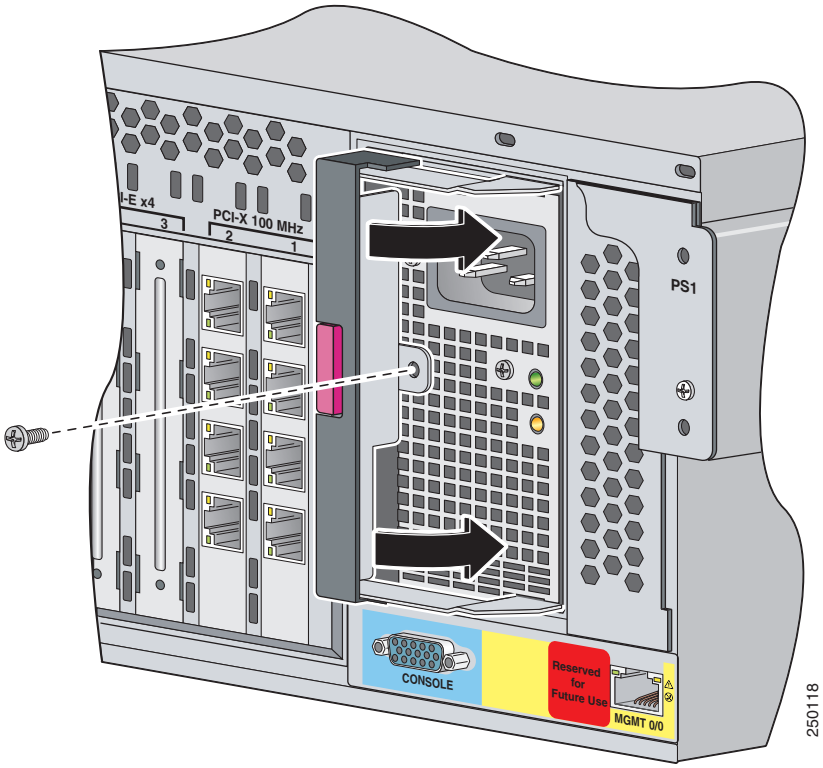
Wait for the power down message before continuing with Step 3.

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

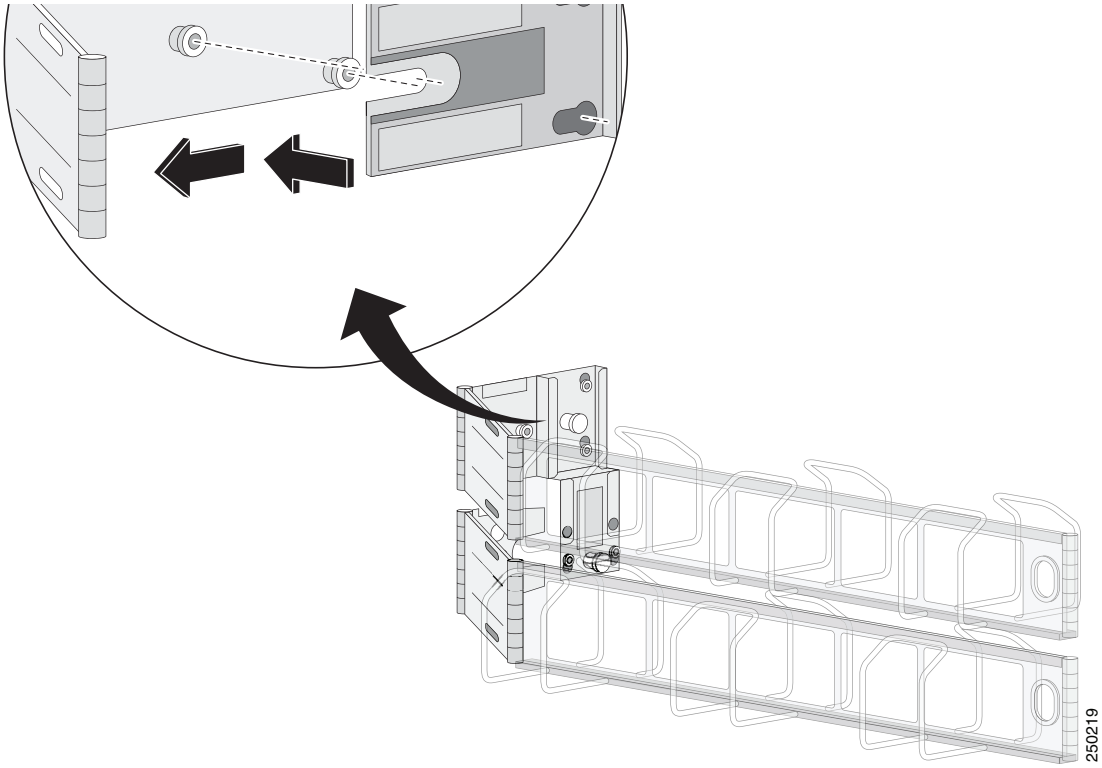
Step 3 Power off the IPS 4270-20 (if you only have one active, functioning power supply).

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

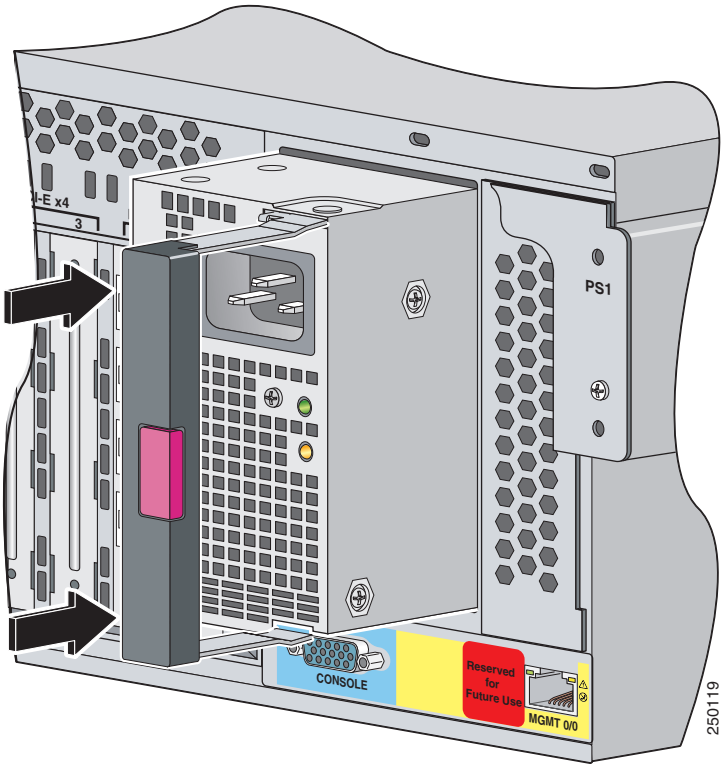
Step 5 Use the T-15 Torx screwdriver that shipped with the IPS 4270-20 to remove the shipping screw. The T-15 Torx screwdriver is located to the right of power supply.



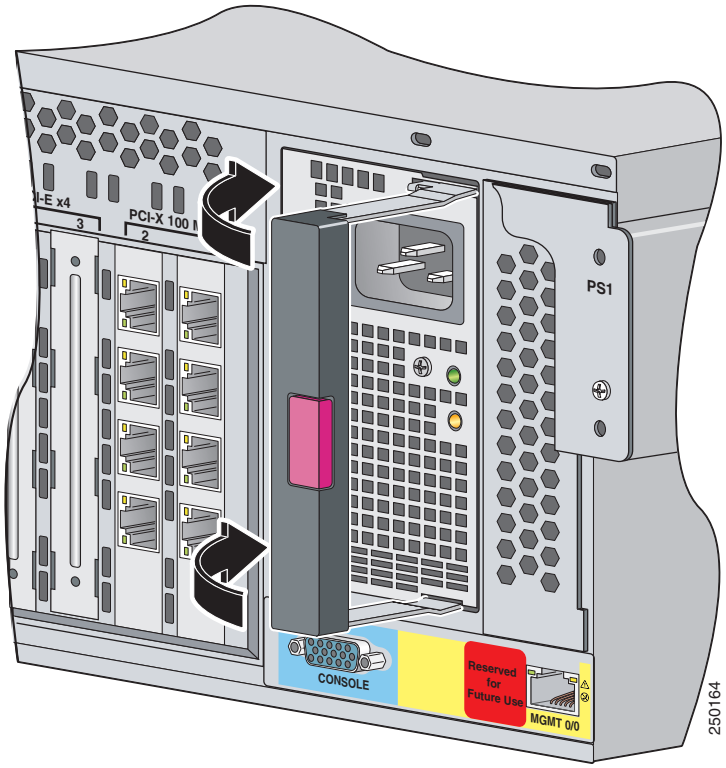
Step 6 Remove the power supply by pulling it away from the chassis.



Step 7 Install the power supply. Make sure the handle is open and slide the power supply into the bay.



Step 8 Lock the power supply handle.



Step 9 Reconnect the power cables. Be sure that the power supply indicator is green and the front panel health indicator is green.

Note Make sure the two power supplies are powered by separate AC power sources so that the IPS 4270-20 is always available.

Step 10 Power on the IPS 4270-20.

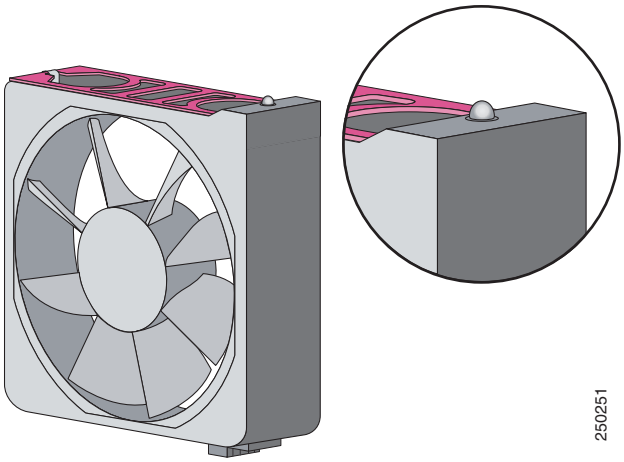
For More Information

- For the IDM procedure for powering down the IPS 4270-20, refer to Rebooting the Sensor; for the IME procedure for powering down the IPS 4270-20, refer to Rebooting the Sensor.
- For an illustration of the screwdriver and where it is located, see Figure 4-7 on page 4-9.

Installing and Removing Fans

There are six fans in the IPS 4270-20. The IPS 4270-20 supports redundant hot-pluggable fans in a 5 + 1 configuration to provide proper airflow. Figure 4-12 shows the fan, its connector, and its indicator.

Figure 4-12 Fan, Connector, and Indicator



The fan indicators provide the following information:

- Green—Operating normally
- Amber—Failed
- Off— No power

To install and remove fans in the IPS 4270-20, follow these steps:

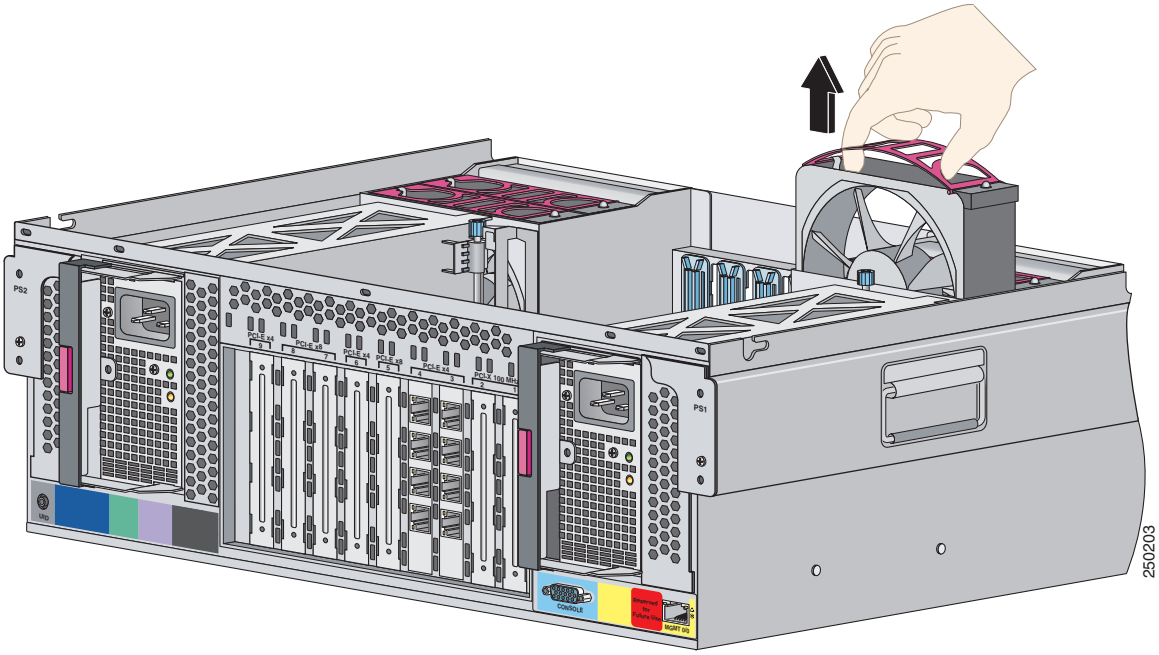
Step 1 Extend the server from the rack.

Step 2 Remove the chassis cover.

Step 3 Identify the failed fan by locating an amber indicator on top of the failed fan or a lighted FAN X indicator on the Diagnostic Panel.

Step 4 Remove the failed fan by grasping the red plastic handle and pulling up.

Note Remove and replace one fan at a time. If the IPS 4270-20 detects two failed fans, it shuts down to avoid thermal damage.



Step 5 Install a new fan by positioning the fan over the slot so that the connector below the fan indicator lines up with the connection on the motherboard. Push down until the fan clicks in to place.

Step 6 Make sure the indicator on each fan is green.

Note If the front panel internal system health indicator is not green after you install a fan, reseat the fan.

Step 7 Replace the chassis cover.

Step 8 Slide the IPS 4270-20 back in to the rack by pressing the rail-release handles.

Step 9 Power on the IPS 4270-20.

For More Information

- For the fan locations, see Figure 4-10 on page 4-13.
- For the procedure for extending the IPS 4270-20 from the rack, see Extending the IPS 4270-20 from the Rack, page 4-25.
- For more information about the Diagnostic Panel, see Diagnostic Panel, page 4-11.
- For the procedure for removing the chassis cover, see Removing and Replacing the Chassis Cover, page 4-38.

Troubleshooting Loose Connections

Perform the following actions to troubleshoot loose connections on a sensor:

- Make sure all power cords are securely connected.
- Make sure all cables are properly aligned and securely connected for all external and internal components.
- Remove and check all data and power cables for damage. Make sure no cables have bent pins or damaged connectors.
- Make sure each device is properly seated.
- If a device has latches, make sure they are completely closed and locked.
- Check any interlock or interconnect indicators that indicate a component is not connected properly.
- If problems continue, remove and reinstall each device, checking the connectors and sockets for bent pins or other damage.

CHAPTER 5

Installing the AIM IPS

Note All IPS platforms allow ten concurrent CLI sessions.

This chapter describes how to install the AIM IPS. It contains the following sections:

Specifications

Table 5-1 lists the specifications for the AIM IPS.

Table 5-1 AIM IPS Specifications

Specification	Description
Dimensions (H x W x D)	0.85 x 3.25 x 5.25 in. (2.16 x 8.26 x 13.34 cm)
Weight	4 oz (113.41 cg) (maximum)
Operating temperature	+32° to +104°F (+0° to +40°C)
Nonoperating temperature	–40° to +185°F (–40° to +85°C)
Humidity	5% to 95% noncondensing
Operating altitude	0 to 10,000 ft (0 to 3,000 m)
Memory	1 GB
eUSB	512 MB

Before Installing the AIM IPS

Follow these recommendations before installing the AIM IPS:

- Upgrade or downgrade software when you can take all applications that run on the router out of service or offline.
- Make sure that you have the correct router and software for the module.
- For safety and regulatory information, read *Cisco Network Modules and Interface Cards Regulatory Compliance and Safety Information*.
- Make a note of the location of the module in the router (*slot_number/port_number*). The slot value is 0, and the port number field specifies the physical slot number for the AIM IPS (0/IDS-Sensor *port*).

Note After you install the module, you can get this information by using the **show running-config** command. You need the module slot number to configure the interfaces on the module.

For More Information

- For the supported routers and software, see Software and Hardware Requirements, page 5-2.
- For more information, refer to Setting Up Interfaces on the AIM IPS and the Router.

Software and Hardware Requirements

The router and the AIM IPS have the following software and hardware requirements:

- The router must be running Cisco IOS release 12.4(15)XY or 12.4(20)T or later.

  Note Use the **show version** command in the router CLI to determine which Cisco IOS release your router is running.

- The module must be running IPS 6.0(3) or later.

  Note Use the **service-module IDS-Sensor** *slot/port* **status** command in the IOS CLI to determine which IPS release your sensor is running. Or use the **show version** command in the module CLI.

- Supported routers:
  - Cisco 1841 and 2801
  - Cisco 2800 series (2811, 2821, and 2851)
  - Cisco 3800 series (3825 and 3845)

  Note The Cisco routers support up to one AIM IPS per platform.

- Supported Cisco IOS Feature Sets:
  - Cisco IOS Advanced Security
  - Cisco IOS Advanced IP Services
  - Cisco IOS Advanced Enterprise Services

Interoperability With Other IPS Modules

Caution You cannot upgrade an NM CIDS to an NME IPS.

The Cisco access routers only support one IDS/IPS module per router. If you have more than one IDS/IPS module installed, the most capable card is enabled. The most capable hierarchy is:

1. NME IPS
2. AIM IPS
3. NM CIDS

This means, for example, that if all modules are installed, the NME IPS disables all other modules. The AIM IPS disables all NM CIDS. If there are multiple modules with the same level of capability, the first one discovered is enabled and all others are disabled.

You cannot bring up, enable, or configure a disabled module. To bring up a less capable module, you must remove the more capable module from the router and reboot. Disabled modules are reported in the **show diag** command output. The state of the module is reported as present but disabled.

If the most capable module slot and port do not match the **interface ids slot/port** configuration command, the most capable module is disabled with the following warning:

```
The module in slot x will be disabled and configuration ignored.
```

The correct slot/port number are displayed so that you can change the configuration.

For More Information

For more information on NM CIDS, refer to Introducing NM CIDS and Installing NM CIDS.

Restrictions

The following restrictions apply to the AIM IPS:

- Do not deploy IOS IPS and the AIM IPS at the same time.
- When the AIM IPS is used with an IOS firewall, make sure SYN flood prevention is done by the IOS firewall.

  The AIM IPS and the IOS firewall complement each other's abilities to create security zones in the network and inspect traffic in those zones. Because the AIM IPS and the IOS firewall operate independently, sometimes they are unaware of the other's activities. In this situation, the IOS firewall is the best defense against a SYN flood attack.

- The Cisco access routers only support one IDS/IPS per router.
- When you reload the router, the AIM IPS also reloads. To ensure that there is no loss of data on the AIM IPS, make sure you shut down the module using the **shutdown** command before you use the **reload** command to reboot the router.

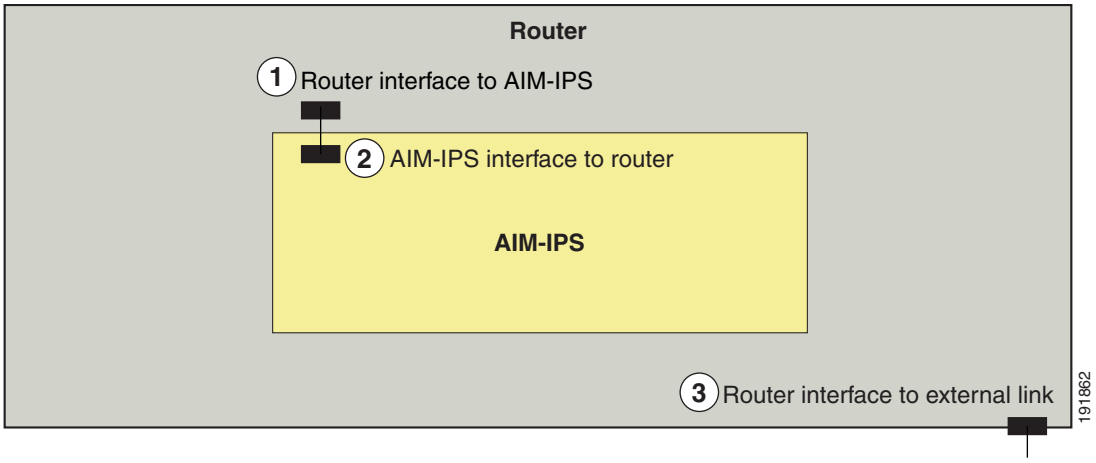
For More Information

For more information on which modules work with each other, see Interoperability With Other IPS Modules, page 5-3.

Hardware Interfaces

Figure 5-1 shows the router and the AIM IPS interfaces used for internal communication. You can configure the router interfaces through the Cisco IOS CLI and the AIM IPS interfaces through the IPS CLI, IDM, IME, or CSM.

Figure 5-1 AIM IPS and Router Interfaces



1	Router interface to the AIM IPS (IDS-Sensor 0/1) Uses the Cisco OS CLI to configure the IP address of the router interface that connects to the AIM IPS. This router IP address is used as the default router IP address when you configure Cisco IPS on the AIM IPS.
2	The AIM IPS interface to router (GigabitEthernet0/1) Configure the command and control interface using the IPS CLI, IDM, IME, or CSM.
3	Router interface to external link.

Note You need two IP addresses to configure the AIM IPS. The AIM IPS has a command and control IP address that you configure through the Cisco IPS CLI. You also assign an IP address to the router for its internal interface (IDS-Sensor 0/x) to the AIM IPS. This IP address belongs to the router itself and is used for routing traffic to the command and control interface of the AIM IPS. It is used as the default router IP address when you set up the AIM IPS command and control interface.

For More Information

- For more information on the IPS CLI, refer to *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 7.0*.
- For more information on IDM, refer to *Installing and Using Cisco Intrusion Prevention System Device Manager 7.0*.
- For more information on IME, refer to *Installing and Using Cisco Intrusion Prevention System Manager Express 7.0*.

Installation and Removal Instructions

For instructions on how to install and remove the AIM IPS, refer to the following documents:

- *Cisco 1800 Series Hardware Installation Guide (Modular)*

  For instructions, refer to "Installing and Upgrading Internal Modules in Cisco 1800 Series Routers (Modular)."
- *Cisco 2800 Series Hardware Installation*

  For instructions, refer to "*Installing and Upgrading Internal Modules in Cisco 2800 Series Routers*."
- *Cisco 3800 Series Hardware Installation*

  For instructions, refer to "*Installing and Upgrading Internal Components in Cisco 3800 Series Routers*."

Perform the following tasks after installing the AIM IPS:

1. Verify that the AIM IPS is installed properly.
2. After you install the AIM IPS, you must initialize it.
3. After you initialize the AIM IPS, you should make sure you have the latest IPS software.
4. Configure the AIM IPS to receive IPS Traffic.

For More Information

- For the procedure for verifying that the AIM IPS is installed properly, see Verifying Installation, page 5-6.
- For the procedure for using the **setup** command to initialize the AIM IPS, see Initializing the Sensor, page 10-1.
- For more information about obtaining the most recent Cisco IPS software, see Obtaining Cisco IPS Software, page 11-1.
- For the procedure to configure the AIM IPS to receive IPS traffic, refer to Setting Up Interfaces on the AIM IPS and the Router.
- For the procedure for using HTTPS to log in to IDM, refer to Logging In to IDM.
- For the procedures for configuring intrusion prevention on your sensor, refer to the following guides:
  - *Installing and Using Cisco Intrusion Prevention System Device Manager 7.0*
  - *Installing and Using Cisco Intrusion Prevention System Manager Express 7.0*
  - *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 7.0*

Verifying Installation

Use the **show inventory** command in privileged EXEC mode to verify the installation of the AIM IPS.

Note You can also use this command to find the serial number of your AIM IPS for use in troubleshooting with TAC. The serial number appears in the PID line, for example, SN: FOC11372M9X.

To verify the installation of the AIM IPS, follow these steps:

Step 1 Log in to the router.

Step 2 Enter privileged EXEC mode on the router.

```
router> enable
```

Step 3 Verify that the AIM IPS is part of the router inventory.

```
router# show inventory
NAME: "3825 chassis", DESCR: "3825 chassis"
PID: CISCO3825 , VID: V01 , SN: FTX1009C3KT

NAME: "Cisco Intrusion Prevention System AIM in AIM slot: 1", DESCR: "Cisco Intrusion
Prevention"
PID: AIM IPS-K9 , VID: V01 , SN: FOC11372M9X

router#
```

CHAPTER 6

Installing the AIP SSM

Note All IPS platforms allow ten concurrent CLI sessions.

This chapter describes how to install the AIP SSM. It contains the following sections:

Specifications

Table 6-1 lists the specifications for the AIP SSM:

Table 6-1 AIP SSM Specifications

Specification	Description
Dimensions (H x W x D)	1.70 x 6.80 x 11.00 inches
Weight	Minimum: 2.50 lb Maximum: 3.00 lb[1]
Operating temperature	+32° to +104°F (+0° to +40°C)
Nonoperating temperature	–40° to +167°F (–40° to +75°C)
Humidity	10% to 90%, noncondensing

1. 2.70 lb for 45 c heatsink, approximately 3.00 lb for the 55c maximum

Memory Specifications

Table 6-2 lists the memory specifications for the AIP SSM.

Table 6-2 AIP SSM Memory Specifications

Model	CPU	DRAM
ASA-SSM-AIP-10-K9	2.0 GHz Celeron	1.0 GB
ASA-SSM-AIP-20-K9	2.4 GHz Pentium 4	2.0 GB

Hardware and Software Requirements

The AIP SSM has the following hardware and software requirements:

- Cisco ASA 5500 series adaptive security appliance
  - ASA 5510 (ASA-SSM-AIP-10-K9)
  - ASA 5520 (ASA-SSM-AIP-10-K9 and ASA-SSM-AIP-20-K9)
  - ASA 5540 (ASA-SSM-AIP-20-K9)
- Cisco Adaptive Security Appliance Software 7.0 or later
- Cisco Intrusion Prevention System Software 5.0(2) or later
- DES or 3DES-enabled

Indicators

Figure 6-1 shows the AIP SSM indicators.

Figure 6-1 AIP SSM Indicators

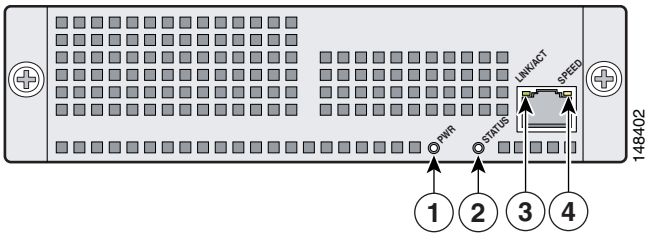


Table 6-3 describes the AIP SSM indicators.

Table 6-3 AIP SSM Indicators

	LED	Color	State	Description
1	PWR	Green	On	The system has power.
2	STATUS	Green	Flashing	The system is booting.
			Solid	The system has passed power-up diagnostics.

Table 6-3 AIP SSM Indicators

	LED	Color	State	Description
3	LINK/ACT	Green	Solid	There is Ethernet link.
			Flashing	There is Ethernet activity.
4	SPEED	Green	100 MB	There is network activity.
		Amber	1000 MB (GigabitEthernet)	There is network activity.

Installation and Removal Instructions

This section describes how to install and remove the AIP SSM, and contains the following topics:

- Installing the AIP SSM, page 6-3
- Verifying the Status of the AIP SSM, page 6-4
- Removing the AIP SSM, page 6-5

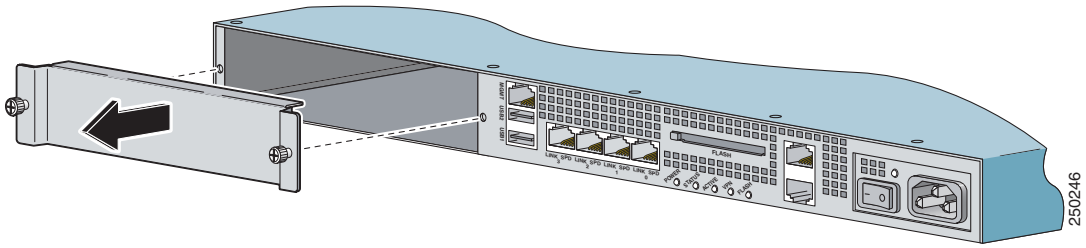
Installing the AIP SSM

To install the AIP SSM for the first time, follow these steps:

Step 1 Power off the adaptive security appliance.

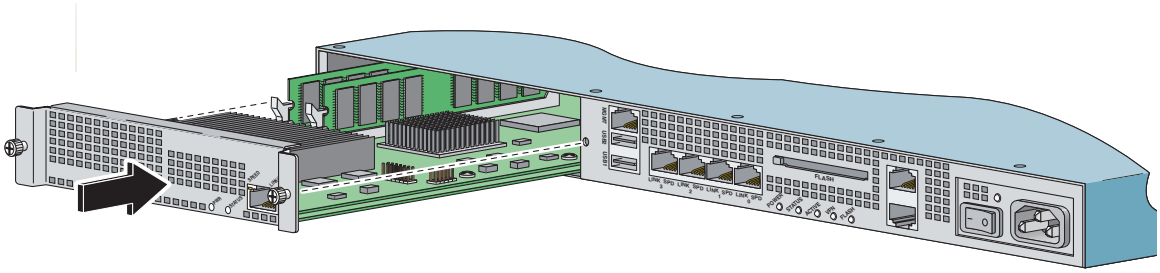
Step 2 Locate the grounding strap from the accessory kit and fasten it to your wrist so that it contacts your bare skin. Attach the other end to the chassis.

Step 3 Remove the two screws at the left back end of the chassis, and remove the slot cover.



Note Store the slot cover in a safe place for future use. You must install slot covers on all empty slots. This prevents EMI, which can disrupt other equipment.

Step 4 Insert the AIP SSM through the slot opening.



Step 5 Attach the screws to secure the AIP SSM to the chassis.

Step 6 Power on the adaptive security appliance by pushing the power switch at the back of the chassis.

Step 7 Check the indicators. If the AIP SSM is properly installed, the POWER indicator is solid green and the STATUS indicator is flashing green. You can also verify that the AIP SSM is online using the **show module 1** command.

Step 8 Initialize the AIP SSM.

Step 9 Install the most recent Cisco IPS software.

Step 10 Configure the AIP SSM to receive IPS traffic.

For More Information

- For more information about ESD, see Working in an ESD Environment, page 1-32.
- For the procedure for verifying that the AIP SSM is properly installed, see Verifying the Status of the AIP SSM, page 6-4.
- For the procedure for using the **setup** command to initialize the AIP SSM, see Initializing the Sensor, page 10-1.
- For the procedure for obtaining the latest Cisco IPS software, see Obtaining Cisco IPS Software, page 11-1.
- For the procedure for configuring the AIP SSM to receive IPS traffic, refer to Configuring the AIP SSM.
- For the procedure for using HTTPS to log in to IDM, refer to Logging In to IDM.

Verifying the Status of the AIP SSM

You can use the **show module 1** command to verify that the AIP SSM is up and running.

The following values are valid for the Status field:

- `Initializing`—The AIP SSM is being detected and the control communication is being initialized by the system.
- `Up`—The AIP SSM has completed initialization by the system.
- `Unresponsive`—The system encountered an error communicating with the AIP SSM.
- `Reloading`—The AIP SSM is reloading.
- `Shutting Down`—The AIP SSM is shutting down.

- `Down`—The AIP SSM is shut down.
- `Recover`—The AIP SSM is attempting to download a recovery image.

To verify the status of the AIP SSM, follow these steps:

Step 1 Log in to the adaptive security appliance.

Step 2 Verify the status of the AIP SSM:

```
asa# show module 1
Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  1 ASA 5500 Series Security Services Module-20  ASA-SSM-20         P2B000005D0

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  1 000b.fcf8.0144 to 000b.fcf8.0144  0.2          1.0(9)0      5.0(0.27)S129.0

Mod Status
--- ------------------
  1 Up
asa#
```

If the status reads `Up`, the AIP SSM has been properly installed.

Removing the AIP SSM

To remove the AIP SSM from the adaptive security appliance, follow these steps:

Step 1 Shut down the AIP SSM:

```
asa# hw-module module 1 shutdown
Shutdown module in slot 1? [confirm]
```

Step 2 Press **Enter** to confirm.

Step 3 Verify that the AIP SSM is shut down by checking the indicators.

Step 4 Power off the adaptive security appliance.

Step 5 Locate the grounding strap from the accessory kit and fasten it to your wrist so that it contacts your bare skin. Attach the other end to the chassis.

Step 6 Remove the two screws at the left back end of the chassis.

Step 7 Remove the AIP SSM and set it aside.

Note If you are not replacing the AIP SSM immediately, install the blank slot cover. Slot covers must cover all empty slots. This prevents EMI from disrupting other equipment.

Step 8 If you need to replace the existing the AIP SSM, insert the new AIP SSM through the slot opening.

Note Do not replace the AIP SSM with a different model. The the adaptive security appliance will not recognize it.

Step 9 Attach the screws to secure the AIP SSM to the chassis.

Step 10 Power on the adaptive security appliance.

Step 11 Reset the AIP SSM:

```
hostname# hw-module module 1 reset
Reset module in slot 1? [confirm]
```

Step 12 Press **Enter** to confirm.

Step 13 Check the indicators to see if the AIP SSM is properly installed. If the AIP SSM is properly installed, the POWER indicator is solid green and the STATUS indicator is flashing green. Or you can verify installation using the **show module 1**command.

For More Information

- For more information on ESD, see Working in an ESD Environment, page 1-32.
- For the procedure for verifying whether the AIP SSM is properly installed, see Verifying the Status of the AIP SSM, page 6-4.

CHAPTER 7

Installing the IDSM2

Note All IPS platforms allow ten concurrent CLI sessions.

This chapter lists the software and hardware requirements of the IDSM2, and describes how to remove and install it. It contains the following sections:

Specifications

Table 7-1 lists the specifications for the IDSM2.

Table 7-1 IDSM2 Specifications

Specification	Description
Dimensions (H x W x D)	1.18 x 15.51 x 16.34 in. (30 x 394 x 415 mm)
Weight	Minimum: 3 lb (1.36 kg) Maximum: 5 lb (2.27 kg)
Operating temperature	+32° to +104°F (+0° to +40°C)
Nonoperating temperature	–40° to +167°F (–40° to +75°C)
Humidity	10% to 90%, noncondensing

Software and Hardware Requirements

The following are the IDSM2 software and hardware requirements:

- Catalyst software release 7.5(1) or later with Supervisor Engine 1A with MSFC2
- Catalyst software release 7.5(1) or later with Supervisor Engine 2 with MSFC2 or PFC2
- Cisco IOS software release 12.2(14)SY with Supervisor Engine 2 with MSFC2
- Cisco IOS software release 12.1(19)E or later with Supervisor Engine 2 with MSFC2
- Cisco IOS software release 12.1(19)E1 or later with Supervisor Engine 1A with MSFC2
- Cisco IOS software release 12.2(14)SX1 with Supervisor Engine 720
- Cisco IDS software release 4.0 or later
- Any Catalyst 6500 series switch chassis or 7600 router

Minimum Supported the IDSM2 Configurations

Note The following matrix is not intended to recommend any particular version, but rather lists the earliest supported versions.

Table 7-2 lists the minimum supported configurations for the IDSM2.

Table 7-2 Minimum Catalyst 6500 Software Version for IDSM2 Feature Support

Catalyst/IDSM2 Feature	Catalyst Software				Cisco IOS Software			
	Sup1	Sup2	Sup32	Sup720	Sup1	Sup2	Sup32	Sup720
SPAN	7.5(1)	7.5(1)	8.4(1)	8.1(1)	12.1(19)E1	12.1(19)E1 12.2(18)SXF1	12.2(18)SXF1	12.2(14)SX1
VACL capture[1]	7.5(1)	7.5(1)	8.4(1)	8.1(1)	12.1(19)E1	12.1(19)E1 12.2(18)SXF1	12.2(18)SXF1	12.2(14)SX1
ECLB with VACL capture[2]	8.5(1)	8.5(1)	8.5(1)	8.5(1)	N/A	12.2(18)SXF4	12.2(18)SXF1	12.2(18)SXE1
Inline interface pairs	8.4(1)	8.4(1)	8.4(1)	8.4(1)	N/A	12.2(18)SXF4	12.2(18)SXF4	12.2(18)SXE1
ECLB with inline interface pairs	8.5(1)	8.5(1)	8.5(1)	8.5(1)	N/A	12.2(18)SXF4	12.2(18)SXF4	12.2(18)SXF4
Inline VLAN pairs	8.4(1)	8.4(1)	8.4(1)	8.4(1)	N/A	12.2(18)SXF4	12.2(18)SXF4	12.2(18)SXF4
ECLB with inline VLAN pairs	8.5(1)	8.5(1)	8.5(1)	8.5(1)	N/A	12.2(18)SXF4	12.2(18)SXF4	12.2(18)SXF4

1. Requires PFC2/3 or MSFC2/3.
2. Requires PFC2/3 or MSFC2/3.

Using the TCP Reset Interface

The IDSM2 has a TCP reset interface—port 1. The IDSM2 has a specific TCP reset interface because it cannot send TCP resets on its sensing ports.

If you have reset problems with the IDSM2, and the switch is running Catalyst software, try the following:

- If the sensing ports are access ports (a single VLAN), you need to configure the reset port to be in the same VLAN.
- If the sensing ports are dot1q trunk ports (multi-VLAN), the sensing ports and reset port all must have the same native VLAN, and the reset port must trunk all the VLANs being trunked by both the sensing ports.

Note In Cisco IOS when the IDSM2 is in promiscuous mode, the IDSM2 ports are always dot1q trunk ports (even when monitoring only 1 VLAN), and the TCP reset port is automatically set to a trunk port and is not configurable.

Front Panel Features

The IDSM2 has a status indicator and a Shutdown button. Figure 7-1 shows the front panel features.

Figure 7-1 IDSM2 Front Panel

Table 7-3 describes the IDSM2 states as indicated by the status indicator.

Table 7-3 Status Indicator

Color	Description
Green	All diagnostics tests pass—The IDSM2 is operational.
Red	A diagnostics test other than an individual port test failed.
Amber	The IDSM2 is running through its boot and self-test diagnostics sequence, or the IDSM2 is disabled, or the IDSM2 is in the shutdown state.
Off	The IDSM2 power is off.

To prevent corruption of the IDSM2, you must use the **shutdown** command to shut it down properly. For instructions on properly shutting down the IDSM2, see Step 1 of Removing the IDSM2, page 7-10. If the IDSM2 does not respond, firmly press the Shutdown button on the faceplate and wait for the Status indicator to turn amber. The shutdown procedure may take several minutes.

Caution Do not remove the IDSM2 from the switch until the module shuts down completely. Removing the module without going through a shutdown procedure can corrupt the application partition on the module and result in data loss.

Installation and Removal Instructions

All Catalyst 6500 series switches support hot swapping, which lets you install, remove, replace, and rearrange modules without turning off the system power to the switch. When the system detects that a module has been installed or removed, it runs diagnostic and discovery routines, acknowledges the presence or absence of the module, and resumes system operation with no operator intervention.

Caution You must first shut down the IDSM2 before removing it from a Catalyst 6500 series switch. For the procedure for removing an IDSM2 from a Catalyst 6500 series switch, see Removing the IDSM2, page 7-10.

This section contains the following topics:

Required Tools

Note You must have at least one supervisor engine running in the Catalyst 6500 series switch with the IDSM2.

You need the following tools to install the IDSM2 in the Catalyst 6500 series switches:

- Flat-blade screwdriver
- Wrist strap or other grounding device
- Antistatic mat or antistatic foam

  Whenever you handle the IDSM2, always use a wrist strap or other grounding device to prevent serious damage from ESD.

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment. Statement 1030**

For More Information

- For more information about supervisor engines, refer to the *Catalyst 6500 Series Switch Installation Guide*.
- For more information on handling ESD, see Working in an ESD Environment, page 1-32.

Slot Assignments

Note The Catalyst 6509-NEB switch has vertical slots numbered 1 to 9 from right to left. Install the IDSM2 with the component side facing to the right.

The Catalyst 6006 and 6506 switch chassis each have six slots. The Catalyst 6009 and 6509 switch chassis each have nine slots. The Catalyst 6513 switch chassis has 13 slots. You can install the IDSM2 in the following ways:

- You can install the IDSM2 in any slot that is not used by the supervisor engine.
- You can install up to eight IDSM2s in a single chassis.

Caution Install module filler plates (blank module carriers) in the empty slots to maintain consistent airflow through the switch chassis.

Note The IDSM2 works with any supervisor engine using SPAN, but the copy capture feature with security VACLs requires that the supervisor engine has the PFC or the MSFC option.

Installing the IDSM2

To install the IDSM2 in the Catalyst 6500 series switch, follow these steps:

Step 1 Make sure that you take necessary ESD precautions.

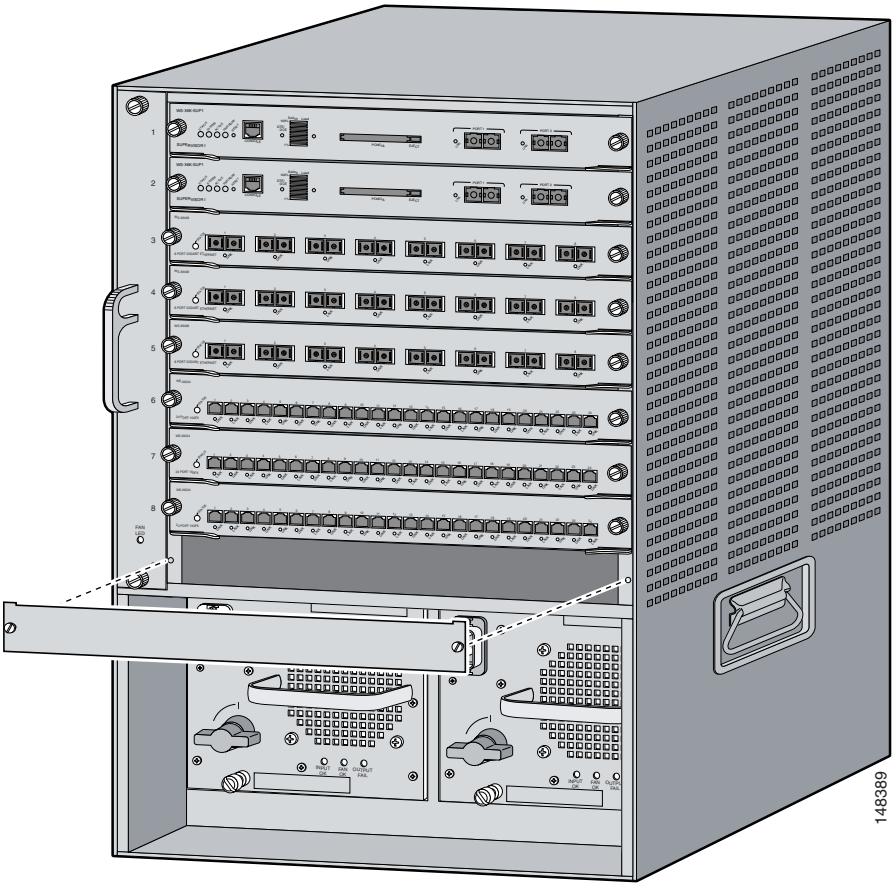
Warning **During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not touch the backplane with your hand or any metal tool, or you could shock yourself.**

Step 2 Choose a slot for the IDSM2.

Note You can install the IDSM2 in any slot that is not reserved for a supervisor engine or other module. Refer to your switch documentation for information about which slots are reserved for the supervisor engine or other modules.

Step 3 Remove the installation screws (use a screwdriver, if necessary) that secure the filler plate to the desired slot.

Step 4 Remove the filler plate by prying it out carefully.

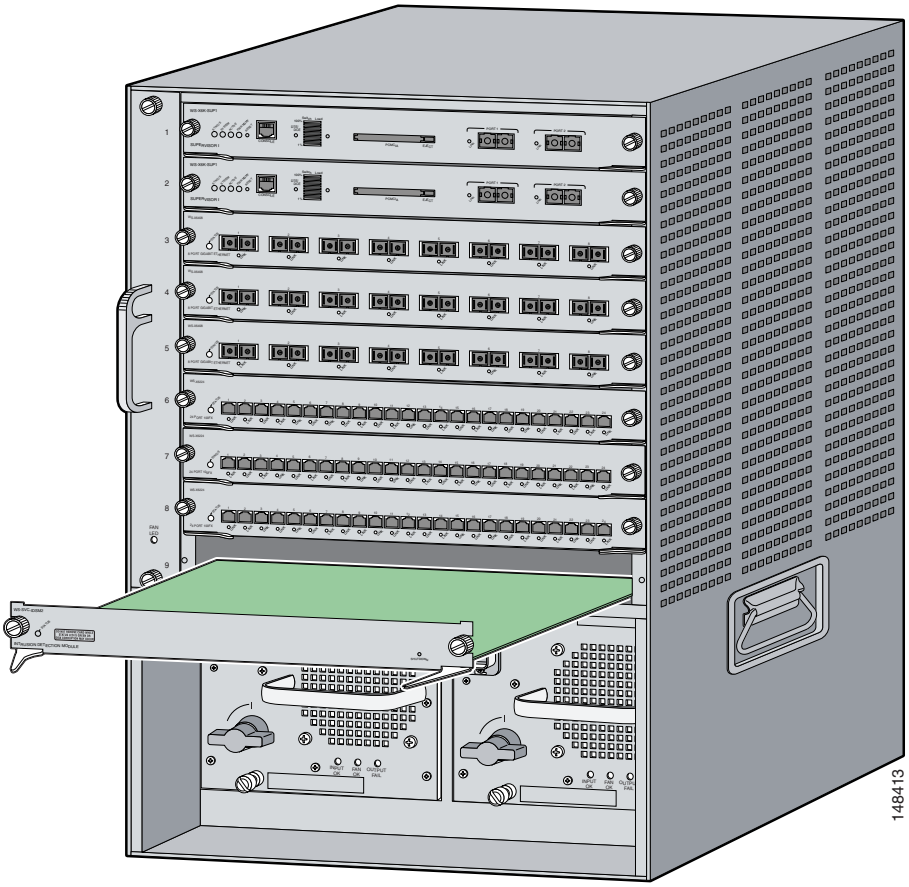


Warning **Blank faceplates and cover panels serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place. Statement 1029**

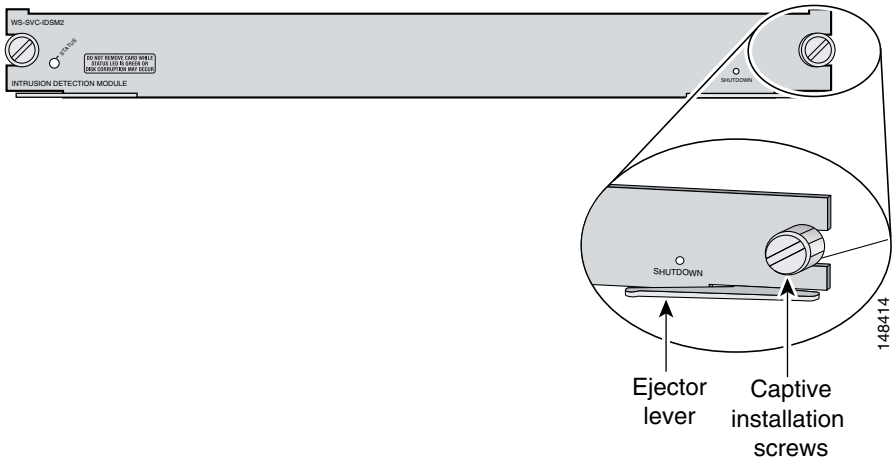
Step 5 Hold the the IDSM2 with one hand, and place your other hand under the IDSM2 carrier to support it.

Caution Do not touch the printed circuit boards or connector pins on the IDSM2.

Step 6 Place the IDSM2 in the slot by aligning the notch on the sides of the IDSM2 carrier with the groove in the slot.



Step 7 Keeping the IDSM2 at a 90-degree orientation to the backplane, carefully push it into the slot until the notches on both ejector levers engage the chassis sides.



Step 8 Using the thumb and forefinger of each hand, simultaneously pivot in both ejector levers to fully seat the IDSM2 in the backplane connector.

Caution Always use the ejector levers when installing or removing the IDSM2. A module that is partially seated in the backplane causes the system to halt and subsequently crash.

Caution If you perform a hot swap, the console displays the message `Module x has been inserted`. This message does not appear, however, if you are connected to the Catalyst 6500 series switch through a Telnet session.

Step 9 Use a screwdriver to tighten the installation screws on the left and right ends of the IDSM2.

Step 10 Verify that you have correctly installed the IDSM2 and can bring it online.

Step 11 Initialize the IDSM2.

Step 12 Configure the switch for command and control access to the IDSM2.

Step 13 Upgrade the IDSM2 to the most recent Cisco IDS software.

Step 14 Set up the IDSM2 to capture IPS traffic. You are now ready to configure the IDSM2 for intrusion prevention.

For More Information

- For more information on ESD-controlled environments, see Working in an ESD Environment, page 1-32.
- For the procedure for verifying the IDSM2 installation, see Verifying Installation, page 7-9.
- For the procedure for using the **setup** command to initialize the IDSM2, see Initializing the Sensor, page 10-1.
- For the procedure for configuring the switch for command and control access to the IDSM2, refer to Configuring the Catalyst 6500 Series Switch for Command and Control Access to the IDSM2.
- For the procedure for obtaining and installing the most recent IPS software, see Obtaining Cisco IPS Software, page 11-1.
- For the procedure for configuring the IDSM2 to capture IPS traffic, refer to Configuring the IDSM2.
- For the procedure for using HTTPS to log in to IDM, refer to Logging In to IDM.
- For the procedures for configuring intrusion prevention on your sensor, refer to the following guides:
  - *Installing and Using Cisco Intrusion Prevention System Device Manager 7.0*
  - *Installing and Using Cisco Intrusion Prevention System Manager Express 7.0*
  - *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 7.0*

Verifying Installation

Note It is normal for the status to read `other` when the IDSM2 is first installed. After the IDSM2 completes the diagnostics routines and comes online, the status reads `ok`. Allow up to 5 minutes for the IDSM2 to come online.

Use the **show module** command to verify that the switch acknowledges the IDSM2 and has brought it online. To verify the installation, follow these steps:

Step 1 Log in to the console.

Step 2 Verify that the IDSM2 is online:

- Catalyst Software

```
console> (enable) show module
Mod Slot Ports Module-Type                Model               Sub Status
--- ---- ----- ------------------------- ------------------- --- --------
1   1    2     1000BaseX Supervisor      WS-X6K-SUP1A-2GE    yes ok
15  1    1     Multilayer Switch Feature WS-F6K-MSFC         no  ok
2   2    48    10/100BaseTX Ethernet     WS-X6248-RJ-45      no  ok
3   3    48    10/100/1000BaseT Ethernet WS-X6548-GE-TX      no  ok
4   4    16    1000BaseX Ethernet        WS-X6516A-GBIC      no  ok
6   6    8     Intrusion Detection Mod   WS-SVC-IDSM2        yes ok

Mod Module-Name          Serial-Num
--- -------------------- -----------
1                        SAD041308AN
15                       SAD04120BRB
2                        SAD03475400
3                        SAD073906RC
4                        SAL0751QYN0
6                        SAD062004LV

Mod MAC-Address(es)                        Hw     Fw          Sw
--- -------------------------------------- ------ ---------- -----------------
1   00-d0-c0-cc-0e-d2 to 00-d0-c0-cc-0e-d3 3.1    5.3.1      8.4(1)
    00-d0-c0-cc-0e-d0 to 00-d0-c0-cc-0e-d1
    00-30-71-34-10-00 to 00-30-71-34-13-ff
15  00-30-7b-91-77-b0 to 00-30-7b-91-77-ef 1.4    12.1(23)E2 12.1(23)E2
2   00-30-96-2b-c7-2c to 00-30-96-2b-c7-5b 1.1    4.2(0.24)V 8.4(1)
3   00-0d-29-f6-01-98 to 00-0d-29-f6-01-c7 5.0    7.2(1)     8.4(1)
4   00-0e-83-af-15-48 to 00-0e-83-af-15-57 1.0    7.2(1)     8.4(1)
6   00-e0-b0-ff-3b-80 to 00-e0-b0-ff-3b-87 0.102  7.2(0.67)  5.0(0.30)

Mod Sub-Type                Sub-Model           Sub-Serial  Sub-Hw Sub-Sw
--- ----------------------- ------------------- ----------- ------ ------
1   L3 Switching Engine     WS-F6K-PFC          SAD041303G6 1.1
6   IDS 2 accelerator board WS-SVC-IDSUPG       .           2.0
console> (enable)
```

- Cisco IOS Software

```
router# show module
Mod Ports Card Type                                Model              Serial No.
--- ----- ------------------------------------- ------------------ -----------
  1   48  48 port 10/100 mb RJ-45 ethernet       WS-X6248-RJ-45     SAD0401012S
  2   48  48 port 10/100 mb RJ45                 WS-X6348-RJ-45     SAL04483QBL
  3   48  SFM-capable 48 port 10/100/1000mb RJ45 WS-X6548-GE-TX     SAD073906GH
  6   16  SFM-capable 16 port 1000mb GBIC        WS-X6516A-GBIC     SAL0740MMYJ
```

```
  7    2  Supervisor Engine 720 (Active)         WS-SUP720-3BXL     SAD08320L2T
  9    1  1 port 10-Gigabit Ethernet Module      WS-X6502-10GE      SAD071903BT
 10    3  Anomaly Detector Module                WS-SVC-ADM-1-K9    SAD084104JR
 11    8  Intrusion Detection System             WS-SVC-IDSM2       SAD05380608
 13    8  Intrusion Detection System             WS-SVC-IDSM2      SAD072405D8

Mod MAC addresses                       Hw    Fw           Sw           Status
--- ---------------------------------- ------ ------------ ------------ -------
  1  00d0.d328.e2ac to 00d0.d328.e2db   1.1   4.2(0.24)VAI 8.5(0.46)ROC Ok
  2  0003.6c14.e1d0 to 0003.6c14.e1ff   1.4   5.4(2)       8.5(0.46)ROC Ok
  3  000d.29f6.7a80 to 000d.29f6.7aaf   5.0   7.2(1)       8.5(0.46)ROC Ok
  6  000d.ed23.1658 to 000d.ed23.1667   1.0   7.2(1)       8.5(0.46)ROC Ok
  7  0011.21a1.1398 to 0011.21a1.139b   4.0   8.1(3)       12.2(PIKESPE Ok
  9  000d.29c1.41bc to 000d.29c1.41bc   1.3   Unknown      Unknown      PwrDown
 10  000b.fcf8.2ca8 to 000b.fcf8.2caf   0.101 7.2(1)       4.0(0.25)    Ok
 11  00e0.b0ff.3340 to 00e0.b0ff.3347   0.102 7.2(0.67)    5.0(1)       Ok
 13  0003.feab.c850 to 0003.feab.c857   4.0   7.2(1)       5.0(1)       Ok

Mod Sub-Module                  Model               Serial        Hw     Status
--- --------------------------- ------------------ ------------ ------- -------
  7 Policy Feature Card 3       WS-F6K-PFC3BXL     SAD083305A1   1.3    Ok
  7 MSFC3 Daughterboard         WS-SUP720          SAD083206JX   2.1    Ok
 11 IDS 2 accelerator board     WS-SVC-IDSUPG      .             2.0    Ok
 13 IDS 2 accelerator board     WS-SVC-IDSUPG      0347331976    2.0    Ok

Mod Online Diag Status
--- ------------------
  1 Pass
  2 Pass
  3 Pass
  6 Pass
  7 Pass
  9 Unknown
 10 Not Applicable
 11 Pass
 13 Pass
router#
```

Removing the IDSM2

This procedure describes how to remove the IDSM2 from the Catalyst 6500 series switch.

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment. Statement 1030**

Caution Before removing the IDSM2, be sure to perform the shutdown procedure. If the IDSM2 is not shut down correctly, you could corrupt the software.

Warning **During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not touch the backplane with your hand or any metal tool, or you could shock yourself.**

To remove the IDSM2, follow these steps:

Step 1 Shut down the IDSM2 by one of these methods:

- Log in to the IDSM2 CLI and enter **reset powerdown**.

  Note The **reset powerdown** command performs a shut down but does not remove power from the IDSM2. To remove power from the IDSM2, use the **set module power down** *module_number* command.

- Log in to the switch CLI and enter one of the following commands:
  - For Catalyst software

    set module shutdown *module_number*

  - For Cisco IOS software

    hw-module module *module_number* **shutdown**

- Shut down the IDSM2 through IDM.
- Press the Shutdown button.

Note Shutdown may take several minutes.

Caution If the IDSM2 is removed from the switch chassis without first being shut down, or the chassis loses power, you may need to reset the IDSM2 more than once. If the module fails to respond after three reset attempts, boot the maintenance partition, and perform the instructions for restoring the application partition.

Step 2 Verify that the IDSM2 shuts down. Do not remove the IDSM2 until the status indicator is amber or off.

Step 3 Use a screwdriver to loosen the installation screws at the left and right sides of the IDSM2.

Step 4 Grasp the left and right ejector levers and simultaneously pull the left lever to the left and the right lever to the right to release the IDSM2 from the backplane connector.

Step 5 As you pull the IDSM2 out of the slot, place one hand under the carrier to support it.

Caution Do not touch the printed circuit boards or connector pins.

Step 6 Carefully pull the IDSM2 straight out of the slot, keeping your other hand under the carrier to guide it.

Note Keep the IDSM2 at a 90-degree orientation to the backplane (horizontal to the floor).

Step 7 Place the IDSM2 on an antistatic mat or antistatic foam.

Step 8 If the slot is to remain empty, install a filler plate (part number 800-00292-01) to keep dust out of the chassis and to maintain proper airflow through the module compartment.

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**

For More Information

- For more information on ESD-controlled environments, see Working in an ESD Environment, page 1-32.
- For the procedure for resetting the IDSM2, see Resetting the IDSM2, page 7-13.
- For the procedure for restoring the application partition, see Installing the IDSM2 System Image, page 12-27.
- For the procedure for powering the IDSM2 up and down, see Powering the IDSM2 Up and Down, page 7-15.

Enabling Full Memory Tests

When the IDSM2 initially boots, by default it runs a partial memory test. You can enable a full memory test in Catalyst software and Cisco IOS software. This section describes how to enable memory tests, and contains the following topics:

Catalyst Software

Use the **set boot device** *boot_sequence module_number* **mem-test-full** command to enable a full memory test. The full memory test takes about 12 minutes. To enable a full memory test, follow these steps:

Step 1 Log in to the console.

Step 2 Enter privileged mode.

```
console> enable
```

Step 3 Enable the full memory test.

```
console> (enable) set boot dev cf:1 3 mem-test-full
Device BOOT variable = cf:1
Memory-test set to FULL
Warning: Device list is not verified but still set in the boot string.
console> (enable) set boot dev hdd:1 3 mem-test-full
Device BOOT variable = hdd:1
Memory-test set to FULL
Warning: Device list is not verified but still set in the boot string.
console> (enable)
```

The **set boot device** command can either contain **cf:1** or **hdd:1**.

Step 4 Reset the IDSM2. The full memory test runs.

Note A full memory test takes more time to complete than a partial memory test.

Cisco IOS Software

Use the **hw-module module** *module_number* **reset mem-test-full** command to enable a full memory test. The full memory test takes about 12 minutes. To enable a full memory test, follow these steps:

Step 1 Log in to the console.

Step 2 Enable the full memory test.

```
router# hw-module module 9 reset mem-test-full
    Device BOOT variable for reset = <empty>
    Warning: Device list is not verified.

    Proceed with reload of module?[confirm]
    % reset issued for module 9
router#
```

Step 3 Reset the IDSM2. The full memory test runs.

Note A full memory test takes more time to complete than a partial memory test.

Resetting the IDSM2

If for some reason you cannot communicate with the IDSM2 through SSH, Telnet, or the switch **session** command, you must reset the IDSM2 from the switch console. The reset process requires several minutes. This section describes how to reset the IDSM2, and contains the following topics:

- Catalyst Software, page 7-13
- Cisco IOS Software, page 7-14

Catalyst Software

To reset the IDSM2 from the CLI, follow these steps:

Step 1 Log in to the console.

Step 2 Enter privileged mode.

```
console> enable
```

Step 3 Reset the IDSM2 to the application partition or the maintenance partition.

```
console> (enable) reset module_number [hdd:1 | cf:1]
```

Note If you do not specify either the application partition (hdd:1 the default) or the maintenance partition (cf:1), the IDSM2 uses the boot device variable.

Example

```
console> (enable) reset 3
2003 Feb 01 00:18:23 %SYS-5-MOD_RESET: Module 3 reset from console//
Resetting module 3... This may take several minutes.
2003 Feb 01 00:20:03 %SYS-5-MOD_OK: Module 3 is online.
console> (enable)
```

Caution If the IDSM2 is removed from the switch chassis without first being shut down, or the chassis loses power, you may need to reset the IDSM2 more than once. If the IDSM2 fails to respond after three reset attempts, boot the maintenance partition, and perform the instructions for restoring the application partition.

Cisco IOS Software

Use the **hw-module module** *slot_number* **reset** [**hdd:1 | cf:1**] command in EXEC mode to reset the IDSM2. The reset process takes several minutes. The IDSM2 boots into the boot partition you specify. If you do not specify the boot string, the default boot string is used.

To reset the IDSM2 from the CLI, follow these steps:

Step 1 Log in to the console.

Step 2 Reset the IDSM2.

```
router# hw-module module module-number reset [hdd:1 | cf:1]
```

Note If you do not specify either the application partition (**hdd:1** the default) or the maintenance partition (**cf:1**), the IDSM2 uses the boot device variable.

Example

```
router# hw-module module 8 reset
Device BOOT variable for reset =
Warning: Device list is not verified.
Proceed with reload of module? [confirm]
% reset issued for module 8
router#
```

Powering the IDSM2 Up and Down

You can remove and restore power to the IDSM2 through the switch CLI. This section describes how to power the IDSM2 up and down through the switch CLI, and contains the following sections:

- Catalyst Software, page 7-15
- Cisco IOS Software, page 7-16

Catalyst Software

Once you power off the IDSM2, you must power it up through the switch CLI.

Note The IDSM2 CLI **reset powerdown** command performs a shut down, but does not remove power from the IDSM2.

To power the IDSM2 up and down from the switch CLI, follow these steps:

Step 1 Log in to the console.

Step 2 Enter privileged mode.

```
console> enable
```

Step 3 Power up the IDSM2.

```
console> (enable) set module power up module_number
```

Step 4 Power down the IDSM2.

```
console> (enable) set module power down module_number
```

Cisco IOS Software

Once you power off the IDSM2, you must power it up through the switch CLI.

Note The IDSM2 CLI **reset powerdown** command performs a shut down, but does not remove power from the IDSM2.

To power the IDSM2 up and down from the switch CLI, follow these steps:

Step 1 Log in to the console.

Step 2 Enter configure terminal mode.

```
router# configure terminal
```

Step 3 Power up the IDSM2.

```
router(config)# power enable module module_number
```

Step 4 Power down the IDSM2.

```
router(config)# no power enable module module_number
```

CHAPTER 8

Installing the NME IPS

Note All IPS platforms allow ten concurrent CLI sessions.

This chapter describes how to install the NME IPS. It contains the following sections:

Specifications

Table 8-1 lists the specifications for the NME IPS.

Table 8-1 NME IPS Specifications

Specification	Description
Dimensions (H x W x D)	1.55 x 7.10 x 7.2 in. (3.9 x 18.0 x 19.3 cm)
Weight	1 lb (0.45 kg) (maximum)
Operating temperature	+32° to +104°F (+0° to +40°C)
Nonoperating temperature	–40° to +185°F (–40° to +85°C)
Humidity	5% to 95% noncondensing
Operating altitude	0 to 10,000 ft (0 to 3,000 m)
Memory	2 GB
eUSB	512 MB

Before Installing the NME IPS

Follow these recommendations before installing the NME IPS:

- Upgrade or downgrade software when you can take all applications that run on the router out of service or offline.
- Make sure that you have the correct router and software for the module.
- For safety and regulatory information, read *Cisco Network Modules and Interface Cards Regulatory Compliance and Safety Information*.
- Make a note of the location of the module in the router (*slot_number/port_number*). The port value is 0, and the slot number field specifies the physical slot number for the NME IPS (*slot_number*/IDS-Sensor 0).

Note After you install the module, you can get this information by using the **show running-config** command. You need the module slot number to configure the interfaces on the module.

For More Information

- For the supported routers and software, see Software and Hardware Requirements, page 8-2.
- For more information, refer to Setting Up Interfaces on the NME IPS and the Router.

Software and Hardware Requirements

The router and the NME IPS have the following software and hardware requirements:

- The router must be running Cisco IOS release 12.4(20)YA or 12.4(22)T or later.

  Note Use the **show version** command in the router CLI to determine which Cisco IOS release your router is running.

- The module must be running IPS 6.1(1) or later.

  Note Use the **service-module IDS-Sensor** *slot/port* **status** command in the IOS CLI to determine which IPS release your sensor is running. Or use the **show version** command in the module CLI.

- Supported routers:
  - Cisco 2800 series (2811, 2821, and 2851)
  - Cisco 3800 series (3825 and 3845)

  Note The Cisco routers support up to one NME IPS per platform.

- Supported Cisco IOS Feature Sets:
  - Cisco IOS Advanced Security
  - Cisco IOS Advanced IP Services
  - Cisco IOS Advanced Enterprise Services

Interoperability With Other IPS Modules

Caution You cannot upgrade an NM CIDS to an NME IPS.

The Cisco access routers only support one IDS/IPS module per router. If you have more than one IDS/IPS module installed, the most capable card is enabled. The most capable hierarchy is:

1. NME IPS
2. AIM IPS
3. NM CIDS

This means, for example, that if all modules are installed, the NME IPS disables all other modules. The AIM IPS disables all NM CIDS. If there are multiple modules with the same level of capability, the first one discovered is enabled and all others are disabled.

You cannot bring up, enable, or configure a disabled module. To bring up a less capable module, you must remove the more capable module from the router and reboot. Disabled modules are reported in the **show diag** command output. The state of the module is reported as present but disabled.

If the most capable module slot and port do not match the **interface ids slot/port** configuration command, the most capable module is disabled with the following warning:

```
The module in slot x will be disabled and configuration ignored.
```

The correct slot/port number are displayed so that you can change the configuration.

For More Information

For more information on NM CIDS, refer to Introducing NM CIDS and Installing NM CIDS.

Restrictions

The following restrictions apply to the NME IPS:

- Do not deploy IOS IPS and the NME IPS at the same time.
- When the NME IPS is used with an IOS firewall, make sure SYN flood prevention is done by the IOS firewall.

  The NME IPS and the IOS firewall complement each other's abilities to create security zones in the network and inspect traffic in those zones. Because the NME IPS and the IOS firewall operate independently, sometimes they are unaware of the other's activities. In this situation, the IOS firewall is the best defense against a SYN flood attack.

- The Cisco access routers only support one IDS/IPS per router.
- When you reload the router, the NME IPS also reloads. To ensure that there is no loss of data on the NME IPS, make sure you shut down the module using the **shutdown** command before you use the **reload** command to reboot the router.

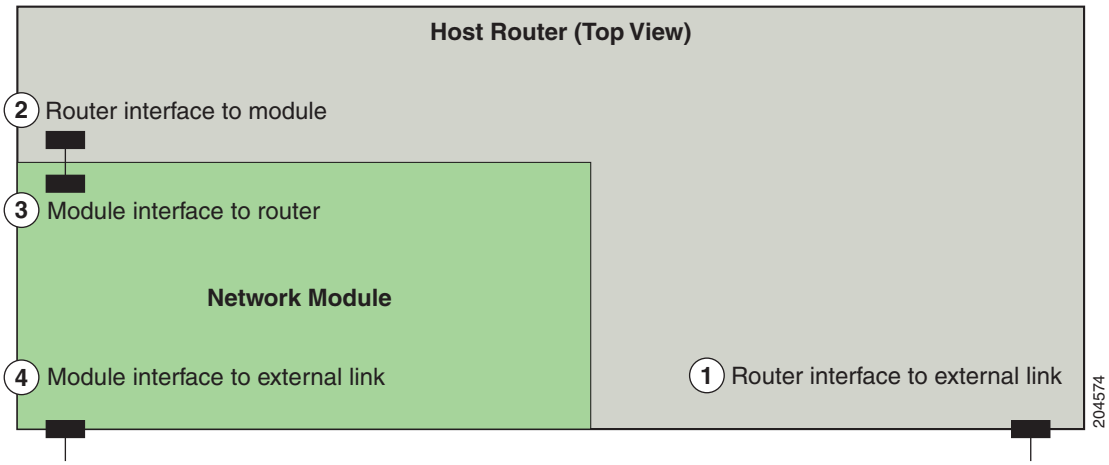
For More Information

- For more information on how the NME IPS functions with other IPS modules, see Interoperability With Other IPS Modules, page 8-3.
- For more information about shutting down the NME IPS, refer to Rebooting, Resetting, and Shutting Down the NME IPS.

Hardware Interfaces

Figure 8-1 shows the router and the NME IPS interfaces used for internal and external communication. You can configure the router interfaces through the Cisco IOS CLI and the NME IPS interfaces through the IPS CLI, IDM, IME, or CSM.

Figure 8-1 NME IPS and Router Interfaces



1	Router interface to external link Configure the standard router settings using the Cisco IOS CLI.
2	Router interface to the NME IPS (ids-sensor x/0) Configure the IP address and default gateway router of the NME IPS using the Cisco IOS CLI.
3	The NME IPS interface to router (GigabitEthernet0/1) Configure the interface as inline or promiscuous using the Cisco IOS CLI.
4	The NME IPS interface to external link (Management0/1) Configure the command and control interface using the IPS CLI, IDM, IME, or CSM.

For More Information

- For more information on the IPS CLI, refer to *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 7.0*.
- For more information on IDM, refer to *Installing and Using Cisco Intrusion Prevention System Device Manager 7.0*.
- For IME, refer to *Installing and Using Cisco Intrusion Prevention System Manager Express 7.0*.

Installation and Removal Instructions

For instructions on how to install and remove the NME IPS, refer to *Installing Cisco Network Modules in Cisco Access Routers.*

To comply with the Telcordia GR-1089 NEBS standard for electromagnetic compatibility and safety, connect the NME IPS only to intrabuilding or nonexposed wiring or cabling. The intrabuilding cable must be shielded and the shield must be grounded at both ends.

For More Information

- For the procedure for verifying that the NME IPS is installed properly, see Verifying Installation, page 8-6.
- For the procedure for using the **setup** command to initialize the NME IPS, see Initializing the Sensor, page 10-1.
- For more information about obtaining the most recent Cisco IPS software, see Obtaining Cisco IPS Software, page 11-1.
- For the procedure to configure the NME IPS to receive IPS traffic, refer to Setting Up Interfaces on the NME IPS and the Router.
- For the procedure for using HTTPS to log in to IDM, refer to Logging In to IDM.
- For the procedures for configuring intrusion prevention on your sensor, refer to the following guides:
  - *Installing and Using Cisco Intrusion Prevention System Device Manager 7.0*
  - *Installing and Using Cisco Intrusion Prevention System Manager Express 7.0*
  - *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 7.0*

Verifying Installation

Use the **show inventory** command in privileged EXEC mode to verify the installation of the NME IPS.

Note You can also use this command to find the serial number of your NME IPS for use in troubleshooting with TAC. The serial number appears in the PID line, for example, SN: FHH1117001R.

To verify the installation of the NME IPS, follow these steps:

Step 1 Log in to the router.

Step 2 Enter privileged EXEC mode on the router.

```
router> enable
```

Step 3 Verify that the NME IPS is part of the router inventory.

```
router# show inventory
NAME: "3845 chassis", DESCR: "3845 chassis"
PID: CISCO3845         , VID: V01 , SN: FTX1002C255

NAME: "c3845 Motherboard with Gigabit Ethernet on Slot 0", DESCR: "c3845 Motherb
oard with Gigabit Ethernet"
PID: CISCO3845-MB      , VID: V03 , SN: FOC09514J4Y

NAME: "4 Port FE Switch on Slot 0 SubSlot 0", DESCR: "4 Port FE Switch"
PID: HWIC-4ESW         , VID: V01 , SN: FOC1102394U

NAME: "High Speed WAN Interface Card - 1 Port Gigabit Ethernet on Slot 0 SubSlot
 3", DESCR: "High Speed WAN Interface Card - 1 Port Gigabit Ethernet"
PID: HWIC-1GE-SFP      , VID: V01 , SN: FOC10164DAR

NAME: "1000BASE-T SFP", DESCR: "1000BASE-T SFP"
PID: SP7041            , VID: C  , SN: 00000MTC101608RB

NAME: "Cisco Intrusion Prevention System NM on Slot 2", DESCR: "Cisco Intrusion
Prevention System NM"
PID: NME IPS-K9        , VID: V01, SN: FHH1117001R


router#
```

CHAPTER 9

Logging In to the Sensor

Note All IPS platforms allow ten concurrent CLI sessions.

This chapter explains how to log in to the sensor. It contains the following sections:

Supported User Roles

You can log in with the following user privileges:

- Administrator
- Operator
- Viewer
- Service

  The service role does not have direct access to the CLI. Service account users are logged directly into a bash shell. Use this account for support and troubleshooting purposes only. Unauthorized modifications are not supported and will require the sensor to be reimaged to guarantee proper operation. You can create only one user with the service role.

  When you log in to the service account, you receive the following warning:

```
******************************** WARNING ****************************************
UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED.
This account is intended to be used for support and troubleshooting purposes only.
Unauthorized modifications are not supported and will require this device to be
re-imaged to guarantee proper operation.
*********************************************************************************
```

Note The service role is a special role that allows you to bypass the CLI if needed. Only a user with administrator privileges can edit the service account.

Note For IPS 5.0 and later, you can no longer remove the **cisco** account. You can disable it using the **no password cisco** command, but you cannot remove it. To use the **no password cisco** command, there must be another administrator account on the sensor. Removing the **cisco** account through the service account is not supported. If you remove the **cisco** account through the service account, the sensor most likely will not boot up, so to recover the sensor you must reinstall the sensor system image.

For More Information

For the procedure for creating the service account, refer to Creating the Service Account, page A-5.

Logging In to the Appliance

Note You must initialize the appliance (run the **setup** command) from the console. After networking is configured, SSH and Telnet are available.

You can log in to the appliance from a console port. To log in to the appliance, follow these steps:

Step 1 Connect a console port to the sensor to log in to the appliance.

Step 2 Enter your username and password at the login prompt.

Note The default username and password are both **cisco**. You are prompted to change them the first time you log in to the appliance.You must first enter the UNIX password, which is **cisco**. Then you must enter the new password twice.

```
login: cisco
Password:
***NOTICE***
This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco cryptographic
products does not imply third-party authority to import, export, distribute or use
encryption. Importers, exporters, distributors and users are responsible for compliance
with U.S. and local country laws. By using this product you agree to comply with
applicable laws and regulations. If you are unable to comply with U.S. and local laws,
return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to export@cisco.com.
```

```
***LICENSE NOTICE***
There is no license key installed on the system.
Please go to http://www.cisco.com/go/license to obtain a new license or install a license.
IPS 4240#
```

For More Information

- For the procedure for connecting an appliance to a terminal server, see Connecting an Appliance to a Terminal Server, page 9-3.
- For the procedure for using the **setup** command to initialize the appliance, see Chapter 10, "Initializing the Sensor."

Connecting an Appliance to a Terminal Server

A terminal server is a router with multiple, low speed, asynchronous ports that are connected to other serial devices. You can use terminal servers to remotely manage network equipment, including appliances.

To set up a Cisco terminal server with RJ-45 or hydra cable assembly connections, follow these steps:

Step 1 Connect to a terminal server using one of the following methods:

- For terminal servers with RJ-45 connections, connect a 180 rollover cable from the console port on the appliance to a port on the terminal server.
- For hydra cable assemblies, connect a straight-through patch cable from the console port on the appliance to a port on the terminal server.

Step 2 Configure the line and port on the terminal server. In enable mode, enter the following configuration, where # is the line number of the port to be configured.

```
config t
line #
login
transport input all
stopbits 1
flowcontrol hardware
speed 9600
exit
exit
wr mem
```

Step 3 Be sure to properly close a terminal session to avoid unauthorized access to the appliance.

If a terminal session is not stopped properly, that is, if it does not receive an exit(0) signal from the application that initiated the session, the terminal session can remain open. When terminal sessions are not stopped properly, authentication is not performed on the next session that is opened on the serial port.

Caution Always exit your session and return to a login prompt before terminating the application used to establish the connection.

Caution If a connection is dropped or terminated by accident, you should reestablish the connection and exit normally to prevent unauthorized access to the appliance.

Logging In to the AIM IPS

This section describes how to use the **session** command to log in to the AIM IPS, and contains the following topics:

- The AIM IPS and the session Command, page 9-4
- Sessioning In to the AIM IPS, page 9-5

The AIM IPS and the session Command

Because the AIM IPS does not have an external console port, console access to the AIM IPS is enabled when you issue the **service-module ids-sensor** *slot*/*port* **session** command on the router, or when you initiate a Telnet connection into the router with the slot number corresponding to the AIM IPS port number. The lack of an external console port means that the initial bootup configuration is possible only through the router.

When you issue the **service-module ids-sensor** *slot*/*port* **session** command, you create a console session with the AIM IPS, in which you can issue any IPS configuration commands. After completing work in the session and exiting the IPS CLI, you are returned to the Cisco IOS CLI.

The **session** command starts a reverse Telnet connection using the IP address of the IDS-Sensor interface. The IDS-Sensor interface is an interface between the AIM IPS and the router. You must assign an IP address to the IDS-Sensor interface before invoking the **session** command. Assigning a routable IP address can make the IDS-Sensor interface itself vulnerable to attacks, because the AIM IPS is visible on the network through that routable IP address, meaning you can communicate with the AIM IPS outside the router. To counter this vulnerability, assign an unnumbered IP address to the IDS-Sensor interface. Then the AIM IPS IP address is only used locally between the router and the AIM IPS, and is isolated for the purposes of sessioning in to the AIM IPS.

Note Before you install your application software or reimage the module, opening a session brings up the bootloader. After you install the software, opening a session brings up the application.

Caution If you session to the module and perform large console transfers, character traffic may be lost unless the host console interface speed is set to 115200/bps or higher. Use the **show running config** command to check that the speed is set to 115200/bps.

For More Information

For the procedure for configuring an unnumbered IP address interface for the AIM IPS, refer to Using an Unnumbered IP Address Interface.

Sessioning In to the AIM IPS

Note You must initialize the AIM IPS (run the **setup** command) from the router. After networking is configured, SSH and Telnet are available.

Use the **service-module ids-sensor** *slot/port* **session** command to establish a session from the AIM IPS to the module. Press **Ctrl-Shift-6**, then **x**, to return a session prompt to a router prompt, that is, to go from the AIM IPS prompt back to the router prompt. Press **Enter** on a blank line to go back to the session prompt, which is also the router prompt. You should only suspend a session to the router if you will be returning to the session after executing router commands. If you do not plan on returning to the AIM IPS session, you should close the session rather than suspend it.

When you close a session, you are logged completely out of the AIM IPS CLI and a new session connection requires a username and password to log in. A suspended session leaves you logged in to the CLI. When you connect with the **session** command, you can go back to the same CLI without having to provide your username and password.

Note Telnet clients vary. In some cases, you may have to press **Ctrl-6 + x**. The control character is specified as ^^, Ctrl-^, or ASCII value 30 (hex 1E).

Caution If you use the **disconnect** command to leave the session, the session remains running. The open session can be exploited by someone wanting to take advantage of a connection that is still in place.

To open and close sessions to the AIM IPS, follow these steps:

Step 1 Log in to the router.

Step 2 Check the status of the AIM IPS to make sure it is running.

```
router# service-module ids-sensor 0/1 status
Service Module is Cisco IDS-Sensor0/1
Service Module supports session via TTY line 322
Service Module is in Steady state
Getting status from the Service Module, please wait..
Cisco Systems Intrusion Prevention System Network Module
  Software version:  6.2(1)E3
  Model:             AIM IPS
  Memory:            443508 KB
  Mgmt IP addr:      10.89.148.196
  Mgmt web ports:    443
  Mgmt TLS enabled:  true


router#
```

Step 3 Open a session from the router to the AIM IPS.

```
router# service-module ids-sensor 0/1 session
Trying 10.89.148.196, 2322 ... Open
```

Step 4 Exit, or suspend and close the module session.

- `sensor# exit`

Note If you are in submodes of the IPS CLI, you must exit all submodes. Enter **exit** until the sensor login prompt appears.

Caution Failing to close a session properly makes it possible for others to exploit a connection that is still in place. Remember to enter **exit** at the `router#` prompt to close the Cisco IOS session completely.

- To suspend and close the session to the AIM IPS, press **Ctrl-Shift** and press **6**. Release all keys, and then press **x**.

  Note When you are finished with a session, you need to return to the router to establish the association between a session (the IPS application) and the router interfaces you want to monitor.

Step 5 Disconnect from the router.

```
router# disconnect
```

Step 6 Press **Enter** to confirm the disconnection.

```
router# Closing connection to 10.89.148.196 [confirm] <Enter>
```

For More Information

For the procedure for using the **setup** command to initialize the AIM IPS, see Advanced Setup for the AIM IPS, page 10-13.

Logging In to AIP SSM

Note You must initialize the AIP SSM (run the **setup** command) from the adaptive security appliance. After networking is configured, SSH and Telnet are available.

You log in to the AIP SSM from the adaptive security appliance. To session in to the module from the adaptive security appliance, follow these steps:

Step 1 Log in to the adaptive security appliance.

Note If the adaptive security appliance is operating in multi-mode, use the **change system** command to get to the system level prompt before continuing.

Step 2 Session to the module.

```
asa# session 1
Opening command session with slot 1.
Connected to slot 1. Escape character sequence is 'CTRL-^X'.
```

You have 60 seconds to log in before the session times out.

Step 3 Enter your username and password at the login prompt.

Note The default username and password are both **cisco**. You are prompted to change them the first time you log in to the module. You must first enter the UNIX password, which is **cisco**. Then you must enter the new password twice.

```
login: cisco
Password:
***NOTICE***
This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco cryptographic
products does not imply third-party authority to import, export, distribute or use
encryption. Importers, exporters, distributors and users are responsible for compliance
with U.S. and local country laws. By using this product you agree to comply with
applicable laws and regulations. If you are unable to comply with U.S. and local laws,
return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to export@cisco.com.

***LICENSE NOTICE***
There is no license key installed on the system.
Please go to http://www.cisco.com/go/license to obtain a new license or install a license.
AIP SSM#
```

Step 4 To escape from a session and return to the adaptive security appliance prompt, do one of the following:

- Enter **exit**.
- Press **CTRL-Shift-6-x** (represented as **CTRL^X**).

For More Information

- For the procedure for using the **setup** command to initialize the AIP SSM, see Advanced Setup for the AIP SSM, page 10-16.

Logging In to the IDSM2

Note You must initialize the IDSM2 (run the **setup** command) from the switch. After networking is configured, SSH and Telnet are available.

You log in to the IDSM2 from the switch. To session in to the IDSM2, follow these steps:

Step 1 Session to the IDSM2 from the switch:

- For Catalyst software

  console> (enable) **session** *slot_number*

- For Cisco IOS software

  router# **session** *slot_number* **processor 1**

Step 2 Enter your username and password at the login prompt.

Note The default username and password are both **cisco**. You are prompted to change them the first time you log in to the IDSM2.You must first enter the UNIX password, which is **cisco**. Then you must enter the new password twice.

```
login: cisco
Password:
***NOTICE***
This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco cryptographic
products does not imply third-party authority to import, export, distribute or use
encryption. Importers, exporters, distributors and users are responsible for compliance
with U.S. and local country laws. By using this product you agree to comply with
applicable laws and regulations. If you are unable to comply with U.S. and local laws,
return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to export@cisco.com.

***LICENSE NOTICE***
There is no license key installed on the system.
Please go to http://www.cisco.com/go/license to obtain a new license or install a license.
IDSM2#
```

For More Information

For the procedure for using the **setup** command to initialize the IDSM2, see Advanced Setup for the IDSM2, page 10-20.

Logging In to the NME IPS

This section describes how to use the **session** command to log in to the NME IPS, and contains the following topics:

The NME IPS and the session Command

Because the NME IPS does not have an external console port, console access to the NME IPS is enabled when you issue the **service-module ids-sensor** *slot/port* **session** command on the router, or when you initiate a Telnet connection into the router with the slot number corresponding to the NME IPS port number. The lack of an external console port means that the initial bootup configuration is possible only through the router.

When you issue the **service-module ids-sensor** *slot/port* **session** command, you create a console session with the NME IPS, in which you can issue any IPS configuration commands. After completing work in the session and exiting the IPS CLI, you are returned to the Cisco IOS CLI.

The **session** command starts a reverse Telnet connection using the IP address of the IDS-Sensor interface. The IDS-Sensor interface is an interface between the NME IPS and the router. You must assign an IP address to the IDS-Sensor interface before invoking the **session** command. Assigning a routable IP address can make the IDS-Sensor interface itself vulnerable to attacks, because the NME IPS is visible on the network through that routable IP address, meaning you can communicate with the NME IPS outside the router. To counter this vulnerability, assign an unnumbered IP address to the IDS-Sensor interface. Then the NME IPS IP address is only used locally between the router and the NME IPS, and is isolated for the purposes of sessioning in to the NME IPS.

Note Before you install your application software or reimage the module, opening a session brings up the bootloader. After you install the software, opening a session brings up the application.

Caution If you session to the module and perform large console transfers, character traffic may be lost unless the host console interface speed is set to 115200/bps or higher. Use the **show running config** command to check that the speed is set to 115200/bps.

For More Information

For the procedure for configuring monitoring interfaces for the NME IPS, refer to Configuring Monitoring on the Router Interface.

Sessioning In to the NME IPS

Note You must initialize the NME IPS (run the **setup** command) from the router. After networking is configured, SSH and Telnet are available.

Use the **service-module ids-sensor** *slot/port* **session** command to establish a session from the NME IPS to the module. Press **Ctrl-Shift-6**, then **x**, to return a session prompt to a router prompt, that is, to go from the NME IPS prompt back to the router prompt. Press **Enter** on a blank line to go back to the session prompt, which is also the router prompt. You should only suspend a session to the router if you will be returning to the session after executing router commands. If you do not plan on returning to the NME IPS session, you should close the session rather than suspend it.

When you close a session, you are logged completely out of the NME IPS CLI and a new session connection requires a username and password to log in. A suspended session leaves you logged in to the CLI. When you connect with the **session** command, you can go back to the same CLI without having to provide your username and password.

Note Telnet clients vary. In some cases, you may have to press **Ctrl-6 + x**. The control character is specified as ^^, Ctrl-^, or ASCII value 30 (hex 1E).

Caution If you use the **disconnect** command to leave the session, the session remains running. The open session can be exploited by someone wanting to take advantage of a connection that is still in place.

To open and close sessions to the NME IPS, follow these steps:

Step 1 Log in to the router.

Step 2 Check the status of the NME IPS to make sure it is running.

```
router# service-module ids-sensor 1/0 status
Service Module is Cisco IDS-Sensor1/0
Service Module supports session via TTY line 130
Service Module is in Steady state
Service Module heartbeat-reset is disabled
Getting status from the Service Module, please wait..

Cisco Systems Intrusion Prevention System Network Module
  Software version:  6.2(1)E3
  Model:             NME IPS
  Memory:            443508 KB
  Mgmt IP addr:      10.89.148.195
  Mgmt web ports:    443
  Mgmt TLS enabled:  true


router#
```

Step 3 Open a session from the router to the NME IPS.

```
router# service-module ids-sensor 1/0 session
Trying 10.89.148.195, 2322 ... Open
```

Step 4 Exit, or suspend and close the module session.

- `sensor# exit`

Note If you are in submodes of the IPS CLI, you must exit all submodes. Enter **exit** until the sensor login prompt appears.

Caution Failing to close a session properly makes it possible for others to exploit a connection that is still in place. Remember to enter **exit** at the `router#` prompt to close the Cisco IOS session completely.

- To suspend and close the session to the NME IPS, press **Ctrl-Shift** and press **6**. Release all keys, and then press **x**.

  Note When you are finished with a session, you need to return to the router to establish the association between a session (the IPS application) and the router interfaces you want to monitor.

Step 5 Disconnect from the router.

```
router# disconnect
```

Step 6 Press **Enter** to confirm the disconnection.

```
router# Closing connection to 10.89.148.196 [confirm] <Enter>
```

For More Information

For the procedure for using the **setup** command to initialize the NME IPS, see Advanced Setup for the NME IPS, page 10-25.

Logging In to the Sensor

Note After you have initialized the sensor using the **setup** command and enabled Telnet, you can use SSH or Telnet to log in to the sensor.

To log in to the sensor, follow these steps:

Step 1 To log in to the sensor over the network using SSH or Telnet.

```
ssh sensor_ip_address
telnet sensor_ip_address
```

Step 2 Enter your username and password at the login prompt.

```
login: ******
Password: ******
***NOTICE***
```

```
This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco cryptographic
products does not imply third-party authority to import, export, distribute or use
encryption. Importers, exporters, distributors and users are responsible for compliance
with U.S. and local country laws. By using this product you agree to comply with
applicable law s and regulations. If you are unable to comply with U.S. and local laws,
return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to export@cisco.com.

***LICENSE NOTICE***
There is no license key installed on the system.
Please go to http://www.cisco.com/go/license to obtain a new license or install a license.
sensor#
```

CHAPTER 10

Initializing the Sensor

This chapter describes how to use the **setup** command to initialize the sensor, and contains the following sections:

Understanding Initialization

Note You must be administrator to use the **setup** command.

After you install the sensor on your network, you must use the **setup** command to initialize it so that you can communicate with it over the network. With the **setup** command, you configure basic sensor settings, including the hostname, IP interfaces, access control lists, Global Correlation servers, and time settings. You can continue using advanced setup in the CLI to enable Telnet, configure the Web server, and assign and enable virtual sensors and interfaces, or you can use the Startup Wizard in IDM or IME.

Simplified Setup Mode

The sensor automatically calls the **setup** command when you connect to the sensor using a console cable and the sensor basic network settings have not yet been configured. The sensor does not call automatic setup under the following conditions:

- When initialization has already been successfully completed.
- If you have recovered or downgraded the sensor.
- If you have set the host configuration to default after successfully configuring the sensor using automatic setup.

When you enter the **setup** command, an interactive dialog called the System Configuration Dialog appears on the system console screen. The System Configuration Dialog guides you through the configuration process. The values shown in brackets next to each prompt are the default values last set.

System Configuration Dialog

When you enter the **setup** command, an interactive dialog called the System Configuration Dialog appears on the system console screen. The System Configuration Dialog guides you through the configuration process.

The values shown in brackets next to each prompt are the current values.

You must go through the entire System Configuration Dialog until you come to the option that you want to change. To accept default settings for items that you do not want to change, press **Enter**.

To return to the EXEC prompt without making changes and without going through the entire System Configuration Dialog, press **Ctrl-C**.

The System Configuration Dialog also provides help text for each prompt. To access the help text, enter **?** at a prompt.

When you complete your changes, the System Configuration Dialog shows you the configuration that you created during the setup session. It also asks you if you want to use this configuration. If you enter **yes**, the configuration is saved. If you enter **no**, the configuration is not saved and the process begins again. There is no default for this prompt; you must enter either **yes** or **no**.

You can configure daylight savings time either in recurring mode or date mode. If you choose recurring mode, the start and end days are based on week, day, month, and time. If you choose date mode, the start and end days are based on month, day, year, and time. Choosing disable turns off daylight savings time.

Note You only need to set the date and time in the System Configuration Dialog if the system is an appliance and is NOT using NTP.

Note The System Configuration Dialog is an interactive dialog. The default settings are displayed.

Example 10-1 shows a sample System Configuration Dialog.

Example 10-1 Example System Configuration Dialog

```
    --- Basic Setup ---

    --- System Configuration Dialog ---

At any point you may enter a question mark '?' for help.
User ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.



Current time: Thu Jan 15 21:19:51 2009

Setup Configuration last modified:

Enter host name[sensor]:
Enter IP interface[192.168.1.2/24,192.168.1.1]:
```

```
Modify current access list?[no]:
Current access list entries:
  [1] 0.0.0.0/0
Delete:
Permit:
Use DNS server for Collaboration?[yes]:
  DNS server IP address[171.68.226.120]:
Use HTTP proxy server for Collaboration?[yes]:
  HTTP proxy server IP address[128.107.241.169]:
  HTTP proxy server Port number[8080]:
Modify system clock settings?[no]: yes
  Modify summer time settings?[no]:
    Use USA SummerTime Defaults?[yes]:
    Recurring, Date or Disable?[Recurring]:
    Start Month[march]:
    Start Week[second]:
    Start Day[sunday]:
    Start Time[02:00:00]:
    End Month[november]:
    End Week[first]:
    End Day[sunday]:
    End Time[02:00:00]:
    DST Zone[]:
    Offset[60]:
  Modify system timezone?[no]:
    Timezone[UTC]:
    UTC Offset[0]:
  Use NTP?[no]: yes
    NTP Server IP Address[]:
    Use NTP Authentication?[no]: yes
      NTP Key ID[]: 1
      NTP Key Value[]: 8675309
Participation in the SensorBase Network allows Cisco to collect aggregated statistics
about traffic sent to your IPS.
SensorBase Network Participation level?[off]: full

If you agree to participate in the SensorBase Network, Cisco will collect aggregated
statistics about traffic sent to your IPS.
This includes summary data on the Cisco IPS network traffic properties and how this
traffic was handled by the Cisco appliances.  We do not collect the data content of
traffic or other sensitive business or personal information.  All data is aggregated and
sent via secure HTTP to the Cisco SensorBase Network servers in periodic intervals.  All
data shared with Cisco will be anonymous and treated as strictly confidential.
The table below describes how the data will be used by Cisco.
Participation Level = "Partial":
  * Type of Data: Protocol Attributes (e.g. TCP max segment size and
    options string)
    Purpose: Track potential threats and understand threat exposure
  * Type of Data: Attack Type (e.g. Signature Fired and Risk Rating)
    Purpose: Used to understand current attacks and attack severity
  * Type of Data: Connecting IP Address and port
    Purpose: Identifies attack source
  * Type of Data: Summary IPS performance (CPU utilization memory usage,
    inline vs. promiscuous, etc)
    Purpose: Tracks product efficacy
Participation Level = "Full" additionally includes:
  * Type of Data: Victim IP Address and port
    Purpose: Detect threat behavioral patterns

Do you agree to participate in the SensorBase Network?[no]:
```

For More Information

For detailed information on the global correlation features, for IDM refer to Configuring Global Correlation, for IME refer to Configuring Global Correlation, and for the CLI, refer to Configuring Global Correlation.

Basic Sensor Setup

You can perform basic sensor setup using the **setup** command, and then finish setting up the sensor using the CLI, IDM, or IME.

To perform basic sensor setup using the **setup** command, follow these steps:

Step 1 Log in to the sensor using an account with administrator privileges.

Note Both the default username and password are `cisco`.

Step 2 The first time you log in to the sensor you are prompted to change the default password. Passwords must be at least eight characters long and be strong, that is, not be a dictionary word. After you change the password, basic setup begins.

Step 3 Enter the `setup` command. The System Configuration Dialog is displayed.

Step 4 Specify the hostname. The hostname is a case-sensitive character string up to 64 characters. Numbers, "_" and "-" are valid, but spaces are not acceptable. The default is sensor.

Step 5 Specify the IP interface. The IP interface is in the form of IP Address/Netmask,Gateway: *X.X.X.X/nn*,*Y.Y.Y.Y*, where *X.X.X.X* specifies the sensor IP address as a 32-bit address written as 4 octets separated by periods, *nn* specifies the number of bits in the netmask, and *Y.Y.Y.Y* specifies the default gateway as a 32-bit address written as 4 octets separated by periods.

Step 6 Enter `yes` to modify the network access list.

a. If you want to delete an entry, enter the number of the entry and press **Enter**, or press **Enter** to get to the Permit line.

b. Enter the IP address and netmask of the network you want to add to the access list.

   For example, 10.0.0.0/8 permits all IP addresses on the 10.0.0.0 network (10.0.0.0-10.255.255.255) and 10.1.1.0/24 permits only the IP addresses on the 10.1.1.0 subnet (10.1.1.0-10.1.1.255). If you want to permit access to a single IP address than the entire network, use a 32-bit netmask. For example, 10.1.1.1/32 permits just the 10.1.1.1 address.

c. Repeat Step b until you have added all networks that you want to add to the access list, and then press **Enter** at a blank permit line to go to the next step.

Step 7 You must configure a DNS server or an HTTP proxy server for Global Correlation to operate.

a. Enter `yes` to add a DNS server, and then enter the DNS server IP address.

b. Enter `yes` to add an HTTP proxy server, and then enter the HTTP proxy server IP address and port number.

Caution You must have a valid sensor license for Global Correlation features to function. You can still configure and display statistics for the Global Correlation features, but the Global Correlation databases are cleared and no updates are attempted. Once you install a valid license, the Global Correlation features are reactivated.

Step 8 Enter **yes** to modify the system clock settings.

a. Enter **yes** to modify summertime settings.

Note Summertime is also known as DST. If your location does not use Summertime, go to Step m.

b. Enter **yes** to choose the USA summertime defaults, or enter **no** and choose recurring, date, or disable to specify how you want to configure summertime settings. The default is recurring.

c. If you chose recurring, specify the month you want to start summertime settings. Valid entries are january, february, march, april, may, june, july, august, september, october, november, and december. The default is march.

d. Specify the week you want to start summertime settings. Valid entries are first, second, third, fourth, fifth, and last. The default is second.

e. Specify the day you want to start summertime settings. Valid entries are sunday, monday, tuesday, wednesday, thursday, friday, and saturday. The default is sunday.

f. Specify the time you want to start summertime settings. The default is 02:00:00.

Note The default recurring summertime parameters are correct for time zones in the United States. The default values specify a start time of 2:00 a.m. on the second Sunday in March, and a stop time of 2:00 a.m. on the first Sunday in November. The default summertime offset is 60 minutes.

g. Specify the month you want summertime settings to end. Valid entries are january, february, march, april, may, june, july, august, september, october, november, and december. The default is november.

h. Specify the week you want the summertime settings to end. Valid entries are first, second, third, fourth, fifth, and last. The default is first.

i. Specify the day you want the summertime settings to end. Valid entries are sunday, monday, tuesday, wednesday, thursday, friday, and saturday. The default is sunday.

j. Specify the time you want summertime settings to end. The default is 02:00:00.

k. Specify the DST zone. The zone name is a character string up to 24 characters long in the pattern [A-Za-z0-9()+:,_/-]+$.

l. Specify the summertime offset. Specify the summertime offset from UTC in minutes (negative numbers represent time zones west of the Prime Meridian). The default is 60.

m. Enter **yes** to modify the system time zone.

n. Specify the standard time zone name. The zone name is a character string up to 24 characters long.

o. Specify the standard time zone offset. Specify the standard time zone offset from UTC in minutes (negative numbers represent time zones west of the Prime Meridian). The default is 0.

p. Enter **yes** if you want to use NTP. To use authenticated NTP, you need the NTP server IP address, the NTP key ID, and the NTP key value. If you do not have those at this time, you can configure NTP later. Otherwise, you can choose unauthenticated NTP.

Step 9 Enter **off**, **partial**, or **full** to participate in the SensorBase Network Participation.

- Off—No data is contributed to the SensorBase Network.
- Partial—Data is contributed to the SensorBase Network, but data considered potentially sensitive is filtered out and never sent.
- Full—All data is contributed to the SensorBase Network.

The SensorBase Network Participation disclaimer appears. It explains what is involved in participating in the SensorBase Network.

Step 10 Enter **yes** to participate in the SensorBase Network.

```
The following configuration was entered.
service host
network-settings
host-ip 10.89.143.126/24,10.89.143.254
host-name sensor126
telnet-option disabled
access-list 10.0.0.0/8
ftp-timeout 300
no login-banner-text
exit
dns-primary-server enabled
address 171.68.226.120
exit
dns-secondary-server disabled
dns-tertiary-server disabled
http-proxy proxy-server
address 128.107.241.170
port 8080
exit
time-zone-settings
offset -360
standard-time-zone-name CST
exit
summertime-option recurring
offset 60
summertime-zone-name CDT
start-summertime
month march
week-of-month second
day-of-week sunday
time-of-day 02:00:00
exit
end-summertime
month november
week-of-month first
day-of-week sunday
time-of-day 02:00:00
exit
exit
ntp-option enabled
ntp-keys 1 md5-key 8675309
ntp-servers 10.89.143.92 key-id 1
exit
service global-correlation
network-participation full
exit
```

```
[0] Go to the command prompt without saving this config.
[1] Return to setup without saving this config.
[2] Save this configuration and exit setup.
[3] Continue to Advanced setup.
```

Step 11 Enter **2** to save the configuration (or **3** to continue with advanced setup using the CLI, IDM, or IME).

```
Enter your selection[2]: 2
Configuration Saved.
```

Step 12 Enter **yes** to reboot the sensor.

Step 13 After reboot, log in to the sensor, and display the self-signed X.509 certificate (needed by TLS).

```
sensor# show tls fingerprint
MD5: C4:BC:F2:92:C2:E2:4D:EB:92:0F:E4:86:53:6A:C6:01
SHA1: 64:9B:AC:DE:21:62:0C:D3:57:2E:9B:E5:3D:04:8F:A7:FD:CD:6F:27
```

Step 14 Write down the certificate fingerprints. You need the fingerprints to check the authenticity of the certificate when using HTTPS to connect to this appliance with a web browser.

Step 15 Apply the most recent service pack and signature update. You are now ready to configure your sensor for intrusion prevention.

For More Information

- For the procedure for obtaining the most recent IPS software, see Obtaining Cisco IPS Software, page 11-1.
- For the procedure for using HTTPS to log in to IDM, refer to Logging In to IDM.
- For the procedures for configuring intrusion prevention on your sensor, refer to the following guides:
  - *Installing and Using Cisco Intrusion Prevention System Device Manager 7.0*
  - *Installing and Using Cisco Intrusion Prevention System Manager Express 7.0*
  - *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 7.0*

Advanced Setup

This section describes how to continue with advanced setup in the CLI for the various Cisco IPS platforms. It contains the following sections:

- Advanced Setup for the IDSM2, page 10-20
- Advanced Setup for the NME IPS, page 10-25

Advanced Setup for the Appliance

The interfaces change according to the appliance model, but the prompts are the same for all models. Adding new subinterfaces is a two-step process. You first organize the interfaces when you edit the virtual sensor configuration. You then choose which interfaces and subinterfaces are assigned to which virtual sensors.

To continue with advanced setup for the appliance, follow these steps:

Step 1 Log in to the appliance using an account with administrator privileges.

Step 2 Enter the **setup** command. The System Configuration Dialog is displayed.

Step 3 Enter **3** to access advanced setup.

Step 4 Specify the Telnet server status. The default is disabled.

Step 5 Specify the web server port. The web server port is the TCP port used by the web server (1 to 65535). The default is 443.

Note The web server is configured to use TLS/SSL encryption by default. Setting the port to 80 does not disable the encryption.

Step 6 Enter **yes** to modify the interface and virtual sensor configuration and to see the current interface configuration.

```
Current interface configuration
 Command control: Management0/0
 Unassigned:
  Promiscuous:
   GigabitEthernet0/0
   GigabitEthernet0/1
   GigabitEthernet0/2
   GigabitEthernet0/3

 Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

 Virtual Sensor: vs1
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

 Virtual Sensor: vs2
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

  [1] Edit Interface Configuration
  [2] Edit Virtual Sensor Configuration
  [3] Display configuration
Option:
```

Step 7 Enter `1` to edit the interface configuration.

Note The following options let you create and delete interfaces. You assign the interfaces to virtual sensors in the virtual sensor configuration. If you are using promiscuous mode for your interfaces and are not subdividing them by VLAN, no additional configuration is necessary.

```
[1] Remove interface configurations.
  [2] Add/Modify Inline Vlan Pairs.
  [3] Add/Modify Promiscuous Vlan Groups.
  [4] Add/Modify Inline Interface Pairs.
  [5] Add/Modify Inline Interface Pair Vlan Groups.
  [6] Modify interface default-vlan.
Option:
```

Step 8 Enter `2` to add inline VLAN pairs and display the list of available interfaces.

Caution The new VLAN pair is not automatically added to a virtual sensor.

```
Available Interfaces
  [1] GigabitEthernet0/0
  [2] GigabitEthernet0/1
  [3] GigabitEthernet0/2
  [4] GigabitEthernet0/3
Option:
```

Step 9 Enter `1` to add an inline VLAN pair to GigabitEthernet0/0, for example.

```
Inline Vlan Pairs for GigabitEthernet0/0
   None
```

Step 10 Enter a subinterface number and description.

```
Subinterface Number:
Description[Created via setup by user asmith]:
```

Step 11 Enter numbers for VLAN 1 and 2.

```
Vlan1[]: 200
Vlan2[]: 300
```

Step 12 Press **Enter** to return to the available interfaces menu.

Note Entering a carriage return at a prompt without a value returns you to the previous menu.

```
  [1] GigabitEthernet0/0
  [2] GigabitEthernet0/1
  [3] GigabitEthernet0/2
  [4] GigabitEthernet0/3
Option:
```

Note At this point, you can configure another interface, for example, GigabitEthernet0/1, for inline VLAN pair.

Step 13 Press **Enter** to return to the top-level interface editing menu.

```
[1] Remove interface configurations.
```

```
  [2] Add/Modify Inline Vlan Pairs.
  [3] Add/Modify Promiscuous Vlan Groups.
  [4] Add/Modify Inline Interface Pairs.
  [5] Add/Modify Inline Interface Pair Vlan Groups.
  [6] Modify interface default-vlan.
Option:
```

Step 14 Enter **4** to add an inline interface pair and see these options.

```
Available Interfaces
   GigabitEthernet0/1
   GigabitEthernet0/2
   GigabitEthernet0/3
```

Step 15 Enter the pair name, description, and which interfaces you want to pair.

```
Pair name: newPair
Description[Created via setup by user asmith:
Interface1[]: GigabitEthernet0/1
Interface2[]: GigabitEthernet0/2
Pair name:
```

Step 16 Press **Enter** to return to the top-level interface editing menu.

```
  [1] Remove interface configurations.
  [2] Add/Modify Inline Vlan Pairs.
  [3] Add/Modify Promiscuous Vlan Groups.
  [4] Add/Modify Inline Interface Pairs.
  [5] Add/Modify Inline Interface Pair Vlan Groups.
  [6] Modify interface default-vlan.
Option:
```

Step 17 Press **Enter** to return to the top-level editing menu.

```
  [1] Edit Interface Configuration
  [2] Edit Virtual Sensor Configuration
  [3] Display configuration
Option:
```

Step 18 Enter **2** to edit the virtual sensor configuration.

```
  [1] Remove virtual sensor.
  [2] Modify "vs0" virtual sensor configuration.
  [3] Create new virtual sensor.
Option:
```

Step 19 Enter **2** to modify the virtual sensor configuration, vs0.

```
Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

No Interfaces to remove.

 Unassigned:
  Promiscuous:
   [1] GigabitEthernet0/3
   [2] GigabitEthernet0/0
  Inline Vlan Pair:
   [3] GigabitEthernet0/0:1  (Vlans: 200, 300)
  Inline Interface Pair:
   [4] newPair (GigabitEthernet0/1, GigabitEthernet0/2)
Add Interface:
```

Step 20 Enter **3** to add inline VLAN pair GigabitEthernet0/0:1.

Step 21 Enter **4** to add inline interface pair NewPair.

Step 22 Press **Enter** to return to the top-level virtual sensor menu.

```
Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0
  Inline Vlan Pair:
   GigabitEthernet0/0:1  (Vlans: 200, 300)
  Inline Interface Pair:
   newPair (GigabitEthernet0/1, GigabitEthernet0/2)

  [1] Remove virtual sensor.
  [2] Modify "vs0" virtual sensor configuration.
  [3] Create new virtual sensor.
Option: GigabitEthernet0/1, GigabitEthernet0/2)
Add Interface:
```

Step 23 Press **Enter** to return to the top-level interface and virtual sensor configuration menu.

```
  [1] Edit Interface Configuration
  [2] Edit Virtual Sensor Configuration
  [3] Display configuration
Option:
```

Step 24 Enter **yes** if you want to modify the default threat prevention settings.

Note The sensor comes with a built-in override to add the deny packet event action to high risk rating alerts. If you do not want this protection, disable automatic threat prevention.

```
Virtual sensor newVs is configured to prevent high risk threats in inline mode. (Risk
Rating 90-100)
Virtual sensor vs0 is configured to prevent high risk threats in inline mode.(Risk Rating
90-100)
Do you want to disable automatic threat prevention on all virtual sensors?[no]:
```

Step 25 Enter **yes** to disable automatic threat prevention on all virtual sensors.

Step 26 Press **Enter** to exit the interface and virtual sensor configuration.

```
The following configuration was entered.
service host
network-settings
host-ip 10.1.9.201/24,10.1.9.1
host-name sensor
telnet-option disabled
ftp-timeout 300
no login-banner-text
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
summertime-option disabled
ntp-option disabled
exit
service web-server
port 342
exit
service interface
```

```
physical-interfaces GigabitEthernet0/0
admin-state enabled
subinterface-type inline-vlan-pair
subinterface 1
description Created via setup by user asmith
vlan1 200
vlan2 300
exit
exit
exit
physical-interfaces GigabitEthernet0/1
admin-state enabled
exit
physical-interfaces GigabitEthernet0/2
admin-state enabled
exit
physical-interfaces GigabitEthernet0/0
admin-state enabled
exit
inline-interfaces newPair
description Created via setup by user asmith
interface1 GigabitEthernet0/1
interface2 GigabitEthernet0/2
exit
exit
service analysis-engine
virtual-sensor newVs
description Created via setup by user cisco
signature-definition newSig
event-action-rules rules0
anomaly-detection
anomaly-detection-name ad0
operational-mode inactive
exit
physical-interface GigabitEthernet0/0
exit
virtual-sensor vs0
physical-interface GigabitEthernet0/0 subinterface-number 1
logical-interface newPair
service event-action-rules rules0
overrides deny-packet-inline
override-item-status Disabled
risk-rating-range 90-100
exit
exit

[0] Go to the command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration and exit setup.
```

Step 27 Enter **2** to save the configuration.

```
Enter your selection[2]: 2
Configuration Saved.
```

Step 28 Reboot the appliance.

```
sensor# reset
Warning: Executing this command will stop all applications and reboot the node.
Continue with reset? []:
```

Step 29 Enter **yes** to continue the reboot.

Step 30 Apply the most recent service pack and signature update. You are now ready to configure your appliance for intrusion prevention.

For More Information

- For the procedure for obtaining the most recent IPS software, see Obtaining Cisco IPS Software, page 11-1
- For the procedure for using HTTPS to log in to IDM, refer to Logging In to IDM.
- For the procedures for configuring intrusion prevention on your sensor, refer to the following guides:
  - *Installing and Using Cisco Intrusion Prevention System Device Manager 7.0*
  - *Installing and Using Cisco Intrusion Prevention System Manager Express 7.0*
  - *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 7.0*

Advanced Setup for the AIM IPS

To continue with advanced setup for the AIM IPS, follow these steps:

Step 1 Session in to the AIM IPS using an account with administrator privileges.

```
router# service-module ids-sensor 0/0 session
Trying 10.1.9.1, 2322 ... Open


sensor login: cisco
Password: ********
```

Step 2 Enter the **setup** command. The System Configuration Dialog is displayed.

Step 3 Enter **3** to access advanced setup.

Step 4 Specify the Telnet server status. You can disable or enable Telnet services. The default is disabled.

Step 5 Specify the web server port. The web server port is the TCP port used by the web server (1 to 65535). The default is 443.

Note The web server is configured to use TLS/SSL encryption by default. Setting the port to 80 does not disable the encryption.

Step 6 Enter **yes** to modify the interface and virtual sensor configuration.

You may receive a warning that Analysis Engine is initializing and you cannot modify the virtual sensor configuration at this time. Press the space bar to receive this menu.

```
[0] Go to the command prompt without saving this config.
[1] Return back to the setup without saving this config.
```

```
[2] Save this configuration and exit setup.

Enter your selection[2]:
```

If you receive the warning that Analysis Engine is initializing, enter **2** to save your configuration thus far and exit setup. You can then reenter setup and press **Enter** until you are back to the interface and virtual sensor menu.

Step 7 Enter **2** to modify the virtual sensor configuration.

```
Modify interface/virtual sensor configuration?[no]: yes
Current interface configuration
 Command control: Management0/0
 Unassigned:
  Monitored:
   GigabitEthernet0/1

 Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

  [1] Edit Interface Configuration
  [2] Edit Virtual Sensor Configuration
  [3] Display configuration
Option:
```

Step 8 Enter **2** to edit the virtual sensor vs0 configuration.

```
Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

No Interfaces to remove.

Unassigned:
  Monitored:
   [1] GigabitEthernet0/1
Add Interface:
```

Step 9 Enter **1** to add GigabitEthernet0/1 to virtual sensor vs0.

```
Add Interface: 1

 Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0
  Monitored:
   GigabitEthernet0/1

  [1] Edit Interface Configuration
  [2] Edit Virtual Sensor Configuration
  [3] Display configuration
Option:
```

Step 10 Press **Enter** to exit the interface and virtual sensor configuration menu.

```
Modify default threat prevention settings?[no]:
```

Step 11 Enter **yes** if you want to modify the default threat prevention settings.

Note The sensor comes with a built-in override to add the deny packet event action to high risk rating alerts. If you do not want this protection, disable automatic threat prevention.

```
Virtual sensor newVs is configured to prevent high risk threats in inline mode. (Risk
Rating 90-100)
Virtual sensor vs0 is configured to prevent high risk threats in inline mode.(Risk Rating
90-100)
Do you want to disable automatic threat prevention on all virtual sensors?[no]:
```

Step 12 Enter **yes** to disable automatic threat prevention on all virtual sensors.

```
The following configuration was entered.

service host
network-settings
host-ip 10.1.9.201/24,10.1.9.1
host-name AIM IPS
telnet-option disabled
access-list 10.0.0.0/8
access-list 64.0.0.0/8
ftp-timeout 300
no login-banner-text
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
summertime-option disabled
ntp-option disabled
exit
service web-server
port 443
exit
service analysis-engine
virtual-sensor vs0
physical-interface GigabitEthernet0/1
exit
exit
service event-action-rules rules0
overrides deny-packet-inline
override-item-status Disabled
risk-rating-range 90-100
exit
exit

[0] Go to the command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration and exit setup.
```

Step 13 Enter **2** to save the configuration.

```
Enter your selection[2]: 2
Configuration Saved.
```

Step 14 Reboot the AIM IPS.

```
AIM IPS# reset
Warning: Executing this command will stop all applications and reboot the node.
Continue with reset? []:
```

Step 15 Enter **yes** to continue the reboot.

Step 16 Apply the most recent service pack and signature update. You are now ready to configure the AIM IPS for intrusion prevention.

For More Information

- For the procedure for obtaining the most recent IPS software, see Obtaining Cisco IPS Software, page 11-1.
- For the procedure for using HTTPS to log in to IDM, refer to Logging In to IDM.
- For the procedures for configuring intrusion prevention on your sensor, refer to the following guides:
  - *Installing and Using Cisco Intrusion Prevention System Device Manager 7.0*
  - *Installing and Using Cisco Intrusion Prevention System Manager Express 7.0*
  - *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 7.0*

Advanced Setup for the AIP SSM

To continue with advanced setup for the AIP SSM, follow these steps:

Step 1 Session in to the AIP SSM using an account with administrator privileges.

```
asa# session 1
```

Step 2 Enter the **setup** command. The System Configuration Dialog is displayed.

Step 3 Enter **3** to access advanced setup.

Step 4 Specify the Telnet server status. You can disable or enable Telnet services. The default is disabled.

Step 5 Specify the web server port. The web server port is the TCP port used by the web server (1 to 65535). The default is 443.

Note The web server is configured to use TLS/SSL encryption by default. Setting the port to 80 does not disable the encryption.

Step 6 Enter **yes** to modify the interface and virtual sensor configuration.

```
Current interface configuration
 Command control: GigabitEthernet0/0
 Unassigned:
  Monitored:
   GigabitEthernet0/1

 Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

  [1] Edit Interface Configuration
  [2] Edit Virtual Sensor Configuration
  [3] Display configuration
Option:
```

Step 7 Enter **1** to edit the interface configuration.

Note You do not need to configure interfaces on the AIP SSM. You should ignore the Modify interface default-vlan setting. The separation of traffic across virtual sensors is configured differently for the AIP SSM than for other sensors.

```
  [1] Modify interface default-vlan.
Option:
```

Step 8 Press **Enter** to return to the top-level interface and virtual sensor configuration menu.

```
  [1] Edit Interface Configuration
  [2] Edit Virtual Sensor Configuration
  [3] Display configuration
Option:
```

Step 9 Enter **2** to edit the virtual sensor configuration.

```
  [1] Remove virtual sensor.
  [2] Modify "vs0" virtual sensor configuration.
  [3] Create new virtual sensor.
Option:
```

Step 10 Enter **2** to modify the virtual sensor vs0 configuration.

```
Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

No Interfaces to remove.

 Unassigned:
  Monitored:
   [1] GigabitEthernet0/1
Add Interface:
```

Step 11 Enter **1** to add GigabitEthernet0/1 to virtual sensor vs0.

Note With ASA 7.2 and earlier, one virtual sensor is supported. The virtual sensor to which GigabitEthernet0/1 is assigned is used for monitoring packets coming from the adaptive security appliance. We recommend that you assign GigabitEthernet0/1 to vs0, but you can assign it to another virtual sensor if you want to.

Note With ASA 7.2.3 and later running IPS 6.0 or later, multiple virtual sensors are supported. The ASA 7.2.3 can direct packets to specific virtual sensors or can send packets to be monitored by a default virtual sensor. The default virtual sensor is the virtual sensor to which you assign GigabitEthernet0/1. We recommend that you assign GigabitEthernet0/1 to vs0, but you can assign it to another virtual sensor if you want to.

Step 12 Press **Enter** to return to the main virtual sensor menu.

Step 13 Enter **3** to create a virtual sensor.

```
Name[]:
```

Step 14 Enter a name and description for your virtual sensor.

```
Name[]: newVs
```

```
Description[Created via setup by user cisco]: New Sensor
Anomaly Detection Configuration
  [1] ad0
  [2] Create a new anomaly detection configuration
Option[2]:
```

Step 15 Enter **1** to use the existing anomaly-detection configuration, ad0.

```
Signature Definition Configuration
  [1] sig0
  [2] Create a new signature definition configuration
Option[2]:
```

Step 16 Enter **2** to create a signature-definition configuration file.

Step 17 Enter the signature-definition configuration name, **newSig**.

```
Event Action Rules Configuration
  [1] rules0
  [2] Create a new event action rules configuration
Option[2]:
```

Step 18 Enter **1** to use the existing event-action-rules configuration, rules0.

Note If GigabitEthernet0/1 has not been assigned to vs0, you are prompted to assign it to the new virtual sensor.

Note With ASA 7.2 and earlier, one virtual sensor is supported. The virtual sensor to which GigabitEthernet0/1 is assigned is used for monitoring packets coming from the adaptive security appliance. We recommend that you assign GigabitEthernet0/1 to vs0, but you can assign it to another virtual sensor if you want to.

Note With ASA 7.2.3 and later with IPS 6.0, multiple virtual sensors are supported. The ASA 7.2.3 can direct packets to specific virtual sensors or can send packets to be monitored by a default virtual sensor. The default virtual sensor is the virtual sensor to which you assign GigabitEthernet0/1. We recommend that you assign GigabitEthernet0/1 to vs0, but you can assign it to another virtual sensor if you want to.

```
Virtual Sensor: newVs
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: newSig
  Monitored:
   GigabitEthernet0/1

  [1] Remove virtual sensor.
  [2] Modify "newVs" virtual sensor configuration.
  [3] Modify "vs0" virtual sensor configuration.
  [4] Create new virtual sensor.
Option:
```

Step 19 Press **Enter** to exit the interface and virtual sensor configuration menu.

```
Modify default threat prevention settings?[no]:
```

Step 20 Enter **yes** if you want to modify the default threat prevention settings.

Note The sensor comes with a built-in override to add the deny packet event action to high risk rating alerts. If you do not want this protection, disable automatic threat prevention.

```
Virtual sensor newVs is configured to prevent high risk threats in inline mode. (Risk
Rating 90-100)
Virtual sensor vs0 is configured to prevent high risk threats in inline mode.(Risk Rating
90-100)
Do you want to disable automatic threat prevention on all virtual sensors?[no]:
```

Step 21 Enter **yes** to disable automatic threat prevention on all virtual sensors.

```
The following configuration was entered.

service host
network-settings
host-ip 10.1.9.201/24,10.1.9.1
host-name AIP SSM
telnet-option disabled
access-list 10.0.0.0/8
access-list 64.0.0.0/8
ftp-timeout 300
no login-banner-text
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
summertime-option disabled
ntp-option disabled
exit
service web-server
port 342
exit
service analysis-engine
virtual-sensor newVs
description New Sensor
signature-definition newSig
event-action-rules rules0
anomaly-detection
anomaly-detection-name ad0
exit
physical-interfaces GigabitEthernet0/1
exit
exit
service event-action-rules rules0
overrides deny-packet-inline
override-item-status Disabled
risk-rating-range 90-100
exit
exit

[0] Go to the command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration and exit setup.
```

Step 22 Enter **2** to save the configuration.

```
Enter your selection[2]: 2
Configuration Saved.
```

Step 23 Reboot the AIP SSM.

```
AIP SSM# reset
Warning: Executing this command will stop all applications and reboot the node.
Continue with reset? []:
```

Step 24 Enter **yes** to continue the reboot.

Step 25 Apply the most recent service pack and signature update. You are now ready to configure your AIP SSM for intrusion prevention.

For More Information

- For the procedure for obtaining the most recent IPS software, see Obtaining Cisco IPS Software, page 11-1.
- For the procedure for using HTTPS to log in to IDM, refer to Logging In to IDM.
- For the procedures for configuring intrusion prevention on your sensor, refer to the following guides:
  - *Installing and Using Cisco Intrusion Prevention System Device Manager 7.0*
  - *Installing and Using Cisco Intrusion Prevention System Manager Express 7.0*
  - *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 7.0*

Advanced Setup for the IDSM2

To continue with advanced setup for the IDSM2, follow these steps:

Step 1 Session in to the IDSM2 using an account with administrator privileges.

- Catalyst software

```
console> enable
console> (enable) session module_number
```

- Cisco IOS software

```
router# session slot slot_number processor 1
```

Step 2 Enter the **setup** command. The System Configuration Dialog is displayed.

Step 3 Enter **3** to access advanced setup.

Step 4 Specify the Telnet server status.

You can disable or enable Telnet services. The default is disabled.

Step 5 Specify the web server port.

The web server port is the TCP port used by the web server (1 to 65535). The default is 443.

Note The web server is configured to use TLS/SSL encryption by default. Setting the port to 80 does not disable the encryption.

Step 6 Enter **yes** to modify the interface and virtual sensor configuration.

```
Current interface configuration
 Command control: GigabitEthernet0/2
 Unassigned:
```

```
  Promiscuous:
   GigabitEthernet0/7
   GigabitEthernet0/8

 Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

  [1] Edit Interface Configuration
  [2] Edit Virtual Sensor Configuration
  [3] Display configuration
Option:
```

Step 7 Enter **1** to edit the interface configuration.

Note The following options let you create and delete interfaces. You assign the interfaces to virtual sensors in the virtual sensor configuration. If you are using promiscuous mode for your interfaces and are not subdividing them by VLAN, no additional configuration is necessary.

Note The IDSM2 does not support the Add/Modify Inline Interface Pair Vlan Groups option. When running an inline interface pair the two IDSM2 data ports are configured as access ports or a trunk port carrying only the native VLAN. The packets do not have 802.1q headers and cannot be separated by VLAN. To monitor multiple VLANs inline, use inline VLAN pairs.

```
  [1] Remove interface configurations.
  [2] Add/Modify Inline Vlan Pairs.
  [3] Add/Modify Promiscuous Vlan Groups.
  [4] Add/Modify Inline Interface Pairs.
  [5] Modify interface default-vlan.
Option:
```

Step 8 Enter **3** to add promiscuous VLAN groups.

```
Available Interfaces
  [1] GigabitEthernet0/7
  [2] GigabitEthernet0/8
Option:
```

Step 9 Enter **2** to add VLAN groups to GigabitEthernet0/8.

```
Promiscuous Vlan Groups for GigabitEthernet0/8
   None
Subinterface Number:
```

a. Enter **10** to add subinterface 10.

```
Subinterface Number: 10
Description[Created via setup by user asmith]:
Select vlans:
  [1] All unassigned vlans.
  [2] Enter vlans range.
Option:
```

b. Enter **1** to assign all unassigned VLANs to subinterface 10.

```
Subinterface Number:
```

c. Enter **9** to add subinterface 9.

```
Subinterface Number: 9
Description[Created via setup by user asmith]:
Vlans[]:
```

d. Enter **1-100** to assign VLANs 1-100 to subinterface 9.

Note This removes VLANs 1-100 from the unassigned VLANs contained in subinterface 10.

e. Repeat Steps c and d until you have added all VLAN groups.

f. Press **Enter** at a blank subinterface line to return to list of interfaces available for VLAN groups.

```
  [1] GigabitEthernet0/7
  [2] GigabitEthernet0/8
Option:
```

Step 10 Press **Enter** to return to the top-level interface configuration menu.

```
  [1] Remove interface configurations.
  [2] Add/Modify Inline Vlan Pairs.
  [3] Add/Modify Promiscuous Vlan Groups.
  [4] Add/Modify Inline Interface Pairs.
  [5] Modify interface default-vlan.
Option:
```

Step 11 Press **Enter** to return to the top-level menu.

```
  [1] Edit Interface Configuration
  [2] Edit Virtual Sensor Configuration
  [3] Display configuration
Option:
```

Step 12 Enter **2** to edit the virtual sensor configuration.

```
  [1] Remove vs
  [2] Modify "vs0"
  [3] Create new vs
Option:
```

Step 13 Enter **2** to modify the virtual sensor vs0 configuration.

```
Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

No Interfaces to remove.

Unassigned:
  Promiscuous:
   [1] GigabitEthernet0/7
```

Step 14 Enter **2** to add VLAN group GigabitEthernet0/8:10 to the virtual sensor vs0.

```
Promiscuous Vlan Groups:
   [2] GigabitEthernet0/8:10  (Vlans: unassigned)
   [3] GigabitEthernet0/8:9  (Vlans: 1-100)
Add Interface:
```

Step 15 Press **Enter** to return to the top-level virtual sensor configuration menu.

```
Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
```

```
  Signature Definitions: sig0
  Promiscuous Vlan Groups:
   GigabitEthernet0/8:10  (Vlans: unassigned)
   GigabitEthernet0/8:9  (Vlans: 1-100)

  [1] Remove vs
  [2] Modify "vs0"
  [3] Create new vs
Option:
```

Step 16 Press **Enter** to return to the top-level interface and virtual sensor configuration menu.

```
  [1] Edit Interface Configuration
  [2] Edit Virtual Sensor Configuration
  [3] Display configuration
Option:
```

Step 17 Press **Enter** to exit the interface and virtual sensor configuration menu.

Step 18 Enter **yes** if you want to modify the default threat prevention settings.

Note The sensor comes with a built-in override to add the deny packet event action to high risk rating alerts. If you do not want this protection, disable automatic threat prevention.

```
Virtual sensor vs0 is configured to prevent high risk threats in inline mode.(Risk Rating
90-100)
Do you want to disable automatic threat prevention on all virtual sensors?[no]:
```

Step 19 Enter **yes** to disable automatic threat prevention on all virtual sensors.

```
The following configuration was entered.
service host
network-settings
host-ip 10.1.9.201/24,10.1.9.1
host-name IDSM2
telnet-option disabled
ftp-timeout 300
no login-banner-text
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
summertime-option disabled
ntp-option disabled
exit
service web-server
port 342
exit
service interface
physical-interfaces GigabitEthernet0/8
admin-state enabled
subinterface-type vlan-group
subinterface 9
description Created via setup by user asmith
vlans range 1-100
exit
subinterface 10
description Created via setup by user asmith
vlans unassigned
exit
exit
```

```
exit
exit
service analysis-engine
virtual-sensor vs0
description Created via setup by user cisco
signature-definition sig0
event-action-rules rules0
anomaly-detection
anomaly-detection-name ad0
operational-mode inactive
exit
physical-interface GigabitEthernet0/8 subinterface-number 9
physical-interface GigabitEthernet0/8 subinterface-number 10
service event-action-rules rules0
overrides deny-packet-inline
override-item-status Disabled
risk-rating-range 90-100
exit

[0] Go to the command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration and exit setup.
```

Step 20 Enter **2** to save the configuration.

```
Enter your selection[2]: 2
Configuration Saved.
```

Step 21 Reboot the IDSM2.

```
IDSM2# reset
Warning: Executing this command will stop all applications and reboot the node.
Continue with reset? []:
```

Step 22 Enter **yes** to continue the reboot.

Step 23 Apply the most recent service pack and signature update. You are now ready to configure the IDSM2 for intrusion prevention.

For More Information

- For the procedure for obtaining the most recent IPS software, see Obtaining Cisco IPS Software, page 11-1.
- For the procedure for using HTTPS to log in to IDM, refer to Logging In to IDM.
- For the procedures for configuring intrusion prevention on your sensor, refer to the following guides:
  - *Installing and Using Cisco Intrusion Prevention System Device Manager 7.0*
  - *Installing and Using Cisco Intrusion Prevention System Manager Express 7.0*
  - *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 7.0*

Advanced Setup for the NME IPS

To continue with advanced setup for the NME IPS, follow these steps:

Step 1 Session in to the NME IPS using an account with administrator privileges.

```
router# service-module ids-sensor 1/0 session
Trying 10.1.9.1, 2322 ... Open


sensor login: cisco
Password: ********
```

Step 2 Enter the **setup** command. The System Configuration Dialog is displayed.

Step 3 Enter **3** to access advanced setup.

Step 4 Specify the Telnet server status. You can disable or enable Telnet services. The default is disabled.

Step 5 Specify the web server port. The web server port is the TCP port used by the web server (1 to 65535). The default is 443.

Note The web server is configured to use TLS/SSL encryption by default. Setting the port to 80 does not disable the encryption.

Step 6 Enter **yes** to modify the interface and virtual sensor configuration.

You may receive a warning that Analysis Engine is initializing and you cannot modify the virtual sensor configuration at this time. Press the space bar to receive this menu.

```
[0] Go to the command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration and exit setup.

Enter your selection[2]:
```

If you receive the warning that Analysis Engine is initializing, enter **2** to save your configuration thus far and exit setup. You can then reenter setup and press **Enter** until you are back to the interface and virtual sensor menu.

Step 7 Enter **2** to modify the virtual sensor configuration.

```
Modify interface/virtual sensor configuration?[no]: yes
Current interface configuration
 Command control: Management0/1
 Unassigned:
  Monitored:
   GigabitEthernet0/1

 Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

  [1] Edit Interface Configuration
  [2] Edit Virtual Sensor Configuration
  [3] Display configuration
Option:
```

Step 8 Enter **2** to edit the virtual sensor vs0 configuration.

```
Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

No Interfaces to remove.

Unassigned:
  Monitored:
   [1] GigabitEthernet0/1
Add Interface:
```

Step 9 Enter **1** to add GigabitEthernet0/1 to virtual sensor vs0.

```
Add Interface: 1

 Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0
  Monitored:
   GigabitEthernet0/1

  [1] Edit Interface Configuration
  [2] Edit Virtual Sensor Configuration
  [3] Display configuration
Option:
```

Step 10 Press **Enter** to exit the interface and virtual sensor configuration menu.

```
Modify default threat prevention settings?[no]:
```

Step 11 Enter **yes** if you want to modify the default threat prevention settings.

Note The sensor comes with a built-in override to add the deny packet event action to high risk rating alerts. If you do not want this protection, disable automatic threat prevention.

```
Virtual sensor vs0 is configured to prevent high risk threats in inline mode.(Risk Rating
90-100)
Do you want to disable automatic threat prevention on all virtual sensors?[no]:
```

Step 12 Enter **yes** if you want to disable automatic threat prevention on all virtual sensors; otherwise, press **Enter** to accept the default of no.

```
The following configuration was entered.

service host
network-settings
host-ip 192.168.1.2/24,192.168.1.1
host-name NME IPS
telnet-option enabled
access-list 10.0.0.0/8
access-list 64.0.0.0/8
ftp-timeout 300
no login-banner-text
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
summertime-option disabled
ntp-option disabled
```

```
exit
service web-server
port 443
exit
service analysis-engine
virtual-sensor vs0
physical-interface GigabitEthernet0/1
exit
exit
service event-action-rules rules0
overrides
override-item-status Enabled
risk-rating-range 90-100
exit
exit

[0] Go to the command prompt without saving this config.
[1] Return to Advanced setup without saving this config.
[2] Save this configuration and exit setup.
```

Step 13 Enter **2** to save the configuration.

```
Enter your selection[2]: 2
Configuration Saved.
```

Step 14 Reboot the NME IPS.

```
NME IPS# reset
Warning: Executing this command will stop all applications and reboot the node.
Continue with reset? []:
```

Step 15 Enter **yes** to continue the reboot.

Step 16 Apply the most recent service pack and signature update. You are now ready to configure the NME IPS for intrusion prevention.

For More Information

- For the procedure for obtaining the most recent IPS software, see Obtaining Cisco IPS Software, page 11-1.
- For the procedure for using HTTPS to log in to IDM, refer to Logging In to IDM.
- For the procedures for configuring intrusion prevention on your sensor, refer to the following guides:
  - *Installing and Using Cisco Intrusion Prevention System Device Manager 7.0*
  - *Installing and Using Cisco Intrusion Prevention System Manager Express 7.0*
  - *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 7.0*

Verifying Initialization

To verify that you initialized your sensor, follow these steps:

Step 1 Log in to the sensor.

Step 2 View your configuration.

```
sensor# show configuration
! ------------------------------
! Current configuration last modified Mon Feb 09 12:03:44 2009
! ------------------------------
! Version 7.0(1)
! Host:
!     Realm Keys          key1.0
! Signature Definition:
!     Signature Update    S365.0   2008-10-31
!     Virus Update        V1.4     2007-03-02
! ------------------------------
service interface
exit
! ------------------------------
service authentication
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
service host
network-settings
host-ip 172.23.204.84/24,172.23.204.1
host-name sensor
telnet-option enabled
access-list 0.0.0.0/0
dns-primary-server enabled
address 1.1.1.1
exit
dns-secondary-server enabled
address 2.2.2.2
exit
http-proxy proxy-server
address 1.1.1.1
port 1
exit
exit
time-zone-settings
offset -480
standard-time-zone-name PST
exit
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
exit
! ------------------------------
service notification
exit
! ------------------------------
service signature-definition sig0
exit
```

```
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
service trusted-certificates
exit
! ------------------------------
service web-server
exit
! ------------------------------
service anomaly-detection ad0
exit
! ------------------------------
service external-product-interface
exit
! ------------------------------
service health-monitor
exit
! ------------------------------
service global-correlation
exit
! ------------------------------
service analysis-engine
exit
sensor#
```

Note You can also use the **more current-config** command to view your configuration.

Step 3 Display the self-signed X.509 certificate (needed by TLS).

```
sensor# show tls fingerprint
MD5: C4:BC:F2:92:C2:E2:4D:EB:92:0F:E4:86:53:6A:C6:01
SHA1: 64:9B:AC:DE:21:62:0C:D3:57:2E:9B:E5:3D:04:8F:A7:FD:CD:6F:27
```

Step 4 Write down the certificate fingerprints. You need the fingerprints to check the authenticity of the certificate when connecting to this sensor with a web browser.

For More Information

For the procedure for using HTTPS to log in to IDM, refer to Logging In to IDM.

CHAPTER 11

Obtaining Software

This chapter provides information on obtaining Cisco IPS software for the sensor. It contains the following sections:

Caution The BIOS on Cisco IPS sensors is specific to Cisco IPS sensors and must only be upgraded under instructions from Cisco with BIOS files obtained from the Cisco website. Installing a non-Cisco or third-party BIOS on Cisco IPS sensors voids the warranty.

Obtaining Cisco IPS Software

Note You must be logged in to Cisco.com and have an IPS subscription service license to download software. You must have a sensor license to apply signature updates.

You can find major and minor updates, service packs, signature and signature engine updates, system and recovery files, firmware upgrades, and readmes on the Download Software download site on Cisco.com. Signature updates are posted to Cisco.com approximately every week, more often if needed. Service packs are posted to Cisco.com as needed. Major and minor updates are also posted periodically. You must have an active IPS maintenance contract and a Cisco.com password to download software. Check Cisco.com regularly for the latest IPS software.

To download software on Cisco.com, follow these steps:

Step 1 Log in to Cisco.com.

Step 2 From the Support drop-down menu, choose **Download Software**.

Step 3 Under Select a Software Product Category, choose **Security Software**.

Step 4 Choose **Intrusion Prevention System (IPS)**.

Step 5 Enter your username and password.

Step 6 In the Download Software window, choose **IPS Appliances > Cisco Intrusion Prevention System** and then click the version you want to download.

Step 7 Click the type of software file you need. The available files appear in a list in the right side of the window. You can sort by file name, file size, memory, and release date. And you can access the Release Notes and other product documentation.

Step 8 Click the file you want to download. The file details appear.

Step 9 Verify that it is the correct file, and click **Download**.

Step 10 Click **Agree** to accept the software download rules. The first time you download a file from Cisco.com, you must fill in the Encryption Software Export Distribution Authorization form before you can download the software.

- Fill out the form and click **Submit**. The Cisco Systems Inc. Encryption Software Usage Handling and Distribution Policy appears.
- Read the policy and click **I Accept**. The Encryption Software Export/Distribution Form appears.

If you previously filled out the Encryption Software Export Distribution Authorization form, and read and accepted the Cisco Systems Inc. Encryption Software Usage Handling and Distribution Policy, these forms are not displayed again. The File Download dialog box appears.

Step 11 Open the file or save it to your computer.

Step 12 Follow the instructions in the Readme to install the update.

Note Major and minor updates, service packs, recovery files, signature and signature engine updates are the same for all sensors. System image files are unique per platform.

For More Information

- For the procedure for obtaining and installing the license key, see Obtaining a License Key From Cisco.com, page 11-10.
- For an explanation of the IPS file versioning scheme, see IPS Software Versioning, page 11-2.

IPS Software Versioning

When you download IPS software images from Cisco.com, you should understand the versioning scheme so that you know which files are base files, which are cumulative, and which are incremental.

Major Update

A major update contains new functionality or an architectural change in the product. For example, the Cisco IPS 7.0 base version includes everything (except deprecated features) since the previous major release (the minor update features, service pack fixes, and signature updates) plus any new changes. Major update 7.0(1) requires 5.1(6) and later. With each major update there are corresponding system and recovery packages.

Note The 7.0(1) major update is used to upgrade 5.1(6) and later sensors to 7.0(1) If you are reinstalling 7.0(1) on a sensor that already has 7.0(1) installed, use the system image or recovery procedures rather than the major update.

Minor Update

A minor update is incremental to the major version. Minor updates are also base versions for service packs. The first minor update for 7.0 is 7.1(1). Minor updates are released for minor enhancements to the product. Minor updates contain all previous minor features (except deprecated features), service pack fixes, signature updates since the last major version, and the new minor features being released. You can install the minor updates on the previous major or minor version (and often even on earlier versions). The minimum supported version needed to upgrade to the newest minor version is listed in the Readme that accompanies the minor update. With each minor update there are corresponding system and recovery packages.

Service Pack

A service pack is cumulative following a base version release (minor or major). Service packs are used for the release of defect fixes with no new enhancements. Service packs contain all service pack fixes since the last base version (minor or major) and the new defect fixes being released. Service packs require the minor version. The minimum supported version needed to upgrade to the newest service pack is listed in the Readme that accompanies the service pack. Service packs also include the latest engine update. For example, if service pack 7.0(3) is released, and E3 is the latest engine level, the service pack is released as 7.0(3)E3.

Patch Release

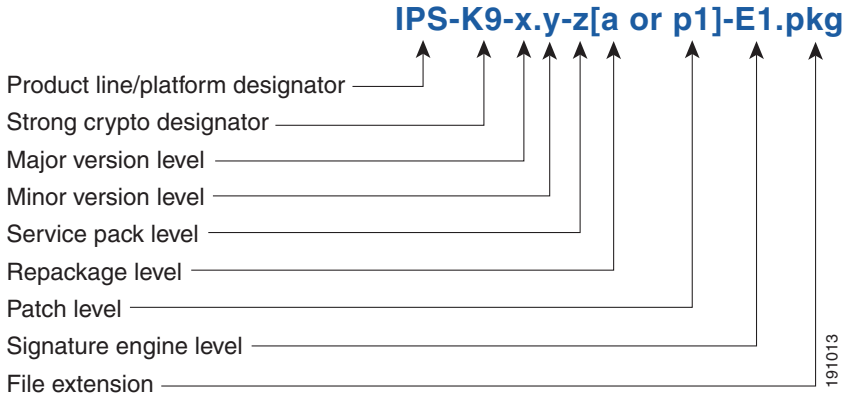
A patch release is used to address defects that are identified in the upgrade binaries after a software release. Rather than waiting until the next major or minor update, or service pack to address these defects, a patch can be posted. Patches include all prior patch releases within the associated service pack level. The patches roll into the next official major or minor update, or service pack.

Before you can install a patch release, the most recent major or minor update, or service pack must be installed. For example, patch release 7.0(1p1) requires 7.0(1).

Note Upgrading to a newer patch does not require you to uninstall the old patch. For example, you can upgrade from patch 7.0(1p1) to 7.0(1p2) without first uninstalling 7.0(1p1).

Figure 11-1 illustrates what each part of the IPS software file represents for major and minor updates, service packs, and patch releases.

Figure 11-1 IPS Software File Name for Major and Minor Updates, Service Packs, and Patch Releases

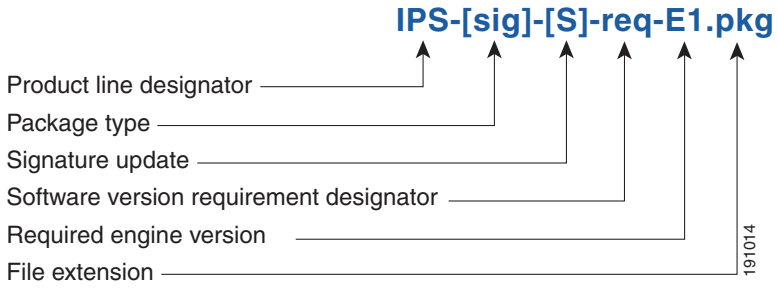


Signature Updates

A signature update is a package file containing a set of rules designed to recognize malicious network activities. Signature updates are released independently from other software updates. Each time a major or minor update is released, you can install signature updates on the new version and the next oldest version for a period of at least six months. Signature updates are dependent on a required signature engine version. Because of this, a *req* designator lists the signature engine required to support a particular signature update.

Figure 11-2 illustrates what each part of the IPS software file represents for signature updates.

Figure 11-2 IPS Software File Name for Signature/Virus Updates,

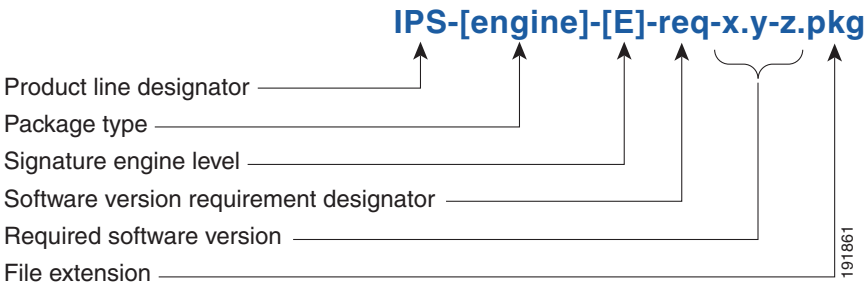


Signature Engine Update

A signature engine update is an xecutable file containing binary code to support new signature updates. Signature engine files require a specific service pack, which is also identified by the *req* designator.

Figure 11-3 illustrates what each part of the IPS software file represents for signature engine updates.

Figure 11-3 IPS Software File Name for Signature Engine Updates



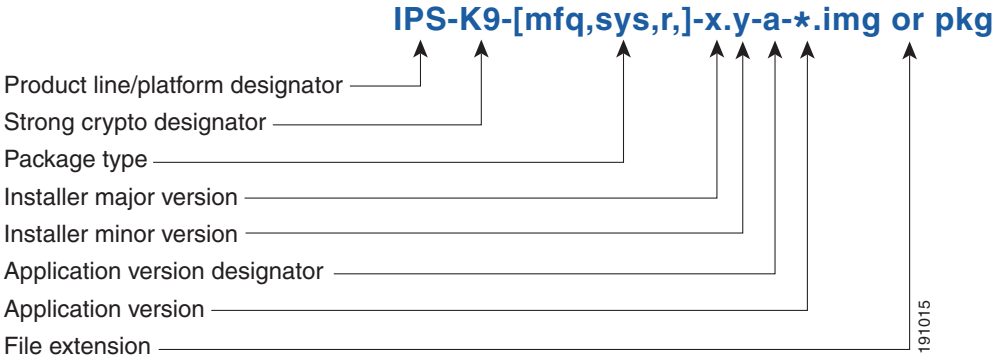
Recovery and System Image Files

Recovery and system image files contain separate versions for the installer and the underlying application. The installer version contains a major and minor version field. The major version is incremented by one of any major changes to the image installer, for example, switching from .tar to rpm or changing kernels. The minor version can be incremented by any one of the following:

- Minor change to the installer, for example, a user prompt added.
- Repackages require the installer minor version to be incremented by one if the image file must be repackaged to address a defect or problem with the installer.

Figure 11-4 illustrates what each part of the IPS software file represents for recovery and system image files.

Figure 11-4 IPS Software File Name for Recovery and System Image Files



Software Release Examples

Table 11-1 lists platform-independent Cisco IPS 7.*x* software release examples. Refer to the Readmes that accompany the software files for detailed instructions on how to install the files.

Table 11-1 Platform-Independent Release Examples

Release	Target Frequency	Identifier	Example Version	Example Filename
Signature update[1]	Weekly	sig	S353	IPS-sig-S353-req-E3.pkg
Signature engine update[2]	As needed	engine	E3	IPS-engine-E3-req-7.0-1.pkg
Service packs[3]	Semi-annually or as needed	—	7.0(3)	IPS-K9-7.0-3-E3.pkg
Minor version update[4]	Annually	—	7.1(1)	IPS-K9-7.1-1-E3.pkg **Note** IPS-AIM-K9-7.1-1-E3.pkg is the minor version update for the AIM IPS. IPS-NME-K-9-7.1-1-E3.pkg is the minor version update for the NME IPS.
Major version update[5]	Annually	—	7.0(1)	IPS-K9-7.0-1-E3.pkg
Patch release[6]	As needed	patch	7.0(1p1)	IPS-K9-patch-67.0-1pl-E3.pkg
Recovery package[7]	Annually or as needed	r	1.1-7.0(1)	IPS-K9-r-1.1-a-7.0-1-E3.pkg

1. Signature updates include the latest cumulative IPS signatures.
2. Signature engine updates add new engines or engine parameters that are used by new signatures in later signature updates.
3. Service packs include defect fixes.
4. Minor versions include new minor version features and/or minor version functionality.
5. Major versions include new major version functionality or new architecture.
6. Patch releases are for interim fixes.
7. The r 1.1 can be revised to r 1.2 if it is necessary to release a new recovery package that contains the same underlying application image. If there are defect fixes for the installer, for example, the underlying application version may still be 7.0(1), but the recovery partition image will be r 1.2.

Table 11-2 describes platform-dependent software release examples.

Table 11-2 Platform-Dependent Release Examples

Release	Target Frequency	Identifier	Supported Platform	Example Filename
System image[1]	Annually	sys	Separate file for each sensor platform	IPS 4240-K9-sys-1.1-a-7.0-1-E3.img
Maintenance partition image[2]	Annually	mp	IDSM2	c6svc-mp.2-1-2.bin.gz

Table 11-2 Platform-Dependent Release Examples (continued)

Release	Target Frequency	Identifier	Supported Platform	Example Filename
Bootloader	As needed	bl	AIM IPS NME IPS	pse_aim_x.y.z.bin pse_nm_x.y.z.bin (where x, y, z is the release number)
Mini-kernel	As needed	mini-kernel	AIM IPS NME IPS	pse_mini_kernel_1.1.10.64.bz2

1. The system image includes the combined recovery and application image used to reimage an entire sensor.
2. The maintenance partition image includes the full image for the IDSM2 maintenance partition. The file is installed from but does not affect the IDSM2 application partition.

Table 11-3 describes the platform identifiers used in platform-specific names.

Table 11-3 Platform Identifiers

Sensor Family	Identifier
IPS 4240 series	4240
IPS 4255 series	4255
IPS 4260 series	4260
IPS 4270-20 series	4270_20
IDS module for Catalyst 6K	IDSM2
IPS network module	AIM NME
adaptive security appliance modules	SSM_10 SSM_20 SSM_40

For More Information

For instructions on how to access these files on Cisco.com, see Obtaining Cisco IPS Software, page 11-1.

Upgrading Cisco IPS Software to 7.0

The following notes and caveats apply to upgrading your sensor to IPS 7.0:

- The minimum required version for upgrading to 7.0 is 5.1(6) or later.
- Use IPS-AIM-K9-7.0-1-E3.pkg to upgrade the AIM IPS and IPS-NME-K9-7.0-1-E3 to upgrade the NME IPS. For all other supported sensors, use the IPS-K9-7.0-1-E3.pkg upgrade file.
- After you upgrade any IPS software on your sensor, you must restart the IDM to see the latest software features.
- If you configured automatic update for your sensor, copy the 7.0(1)E3 update files to the directory on the server that your sensor polls for updates.
- If you are using automatic update with a mixture of AIM IPS, NME IPS, and other IPS appliances or modules, make sure you put both the 7.0(1)E3 upgrade file (IPS-K9-7.0-1-E3.pkg), the AIM IPS upgrade file (IPS-AIM-K9-7.0-1-E3.pkg), and the NME IPS upgrade file (IPS-NME-K9-7.0-1-E3)

on the automatic update server so that the AIM IPS and the NME IPS can correctly detect which file needs to be automatically downloaded and installed. If you only put the 7.0(1)E3 upgrade file (IPS-K9-7.0-1-E3.pkg) on the server, the AIM IPS and the NME IPS will download and try to install the wrong file.

- If you install an update on your sensor and the sensor is unusable after it reboots, you must reimage your sensor. You can reimage your sensor in the following ways:
  - For all sensors, use the **recover** command.
  - For the IPS 4240, IPS 4255, IPS 4260, and IPS 4270-20, use the ROMMON to restore the system image.
  - For the AIM IPS and the NME IPS, use the bootloader.
  - For the IDSM2, reimage the application partition from the maintenance partition.
  - For the AIP SSM, reimage from the adaptive security appliance using the **hw-module module 1 recover configure/boot** command.

Caution When you install the system image for your sensor, all accounts are removed and the default account and password are reset to **cisco**.

For More Information

- For the procedure for accessing downloads on Cisco.com, see Obtaining Cisco IPS Software, page 11-1.
- For the procedure for using the **upgrade** command to upgrade the sensor, see Upgrading the Sensor, page 12-2.
- For the procedure for configuring automatic upgrades on the sensor, see Configuring Automatic Upgrades, page 12-6.
- For the procedure for using the **recover** command, see Recovering the Application Partition, page 12-11.
- For the procedures for using ROMMON to restore the system image, see Installing the IPS 4240 and IPS 4255 System Images, page 12-14, Installing the IPS 4260 System Image, page 12-17, and Installing the IPS 4270-20 System Image, page 12-19.
- For the procedure for restoring the AIM IPS system image, see Installing the AIM IPS System Image, page 12-22.
- For the procedure for using the **hw-module module 1 recover configure/boot** command to reimage the AIP SSM, see Installing the AIP SSM System Image, page 12-24.
- For the procedure for reimaging the IDSM2 application partition from the maintenance partition, see Installing the IDSM2 System Image, page 12-27.
- For the procedure for restoring the NME IPS system image, see Installing the NME IPS System Image, page 12-39.

Accessing IPS Documentation

You can find IPS documentation at this URL:

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

Or to access IPS documentation from Cisco.com, follow these steps:

Step 1 Log in to Cisco.com.

Step 2 Click **Support**.

Step 3 Under Support at the bottom of the page, click **Documentation**.

Step 4 Choose **Products > Security > Intrusion Prevention System (IPS) > IPS Appliances > Cisco IPS 4200 Series Sensors**. The Cisco IPS 4200 Series Sensors page appears. All of the most up-to-date IPS documentation is on this page.

Note Although you will see references to other IPS documentation sites on Cisco.com, this is the site with the most complete and up-to-date IPS documentation.

Step 5 Click one of the following categories to access Cisco IPS documentation:

- **Download Software**—Takes you to the Download Software site.

  Note You must be logged into Cisco.com to access the software download site.

- **Release and General Information**—Contains documentation roadmaps and release notes.
- **Reference Guides**—Contains command references and technical references.
- **Design**—Contains design guide and design tech notes.
- **Install and Upgrade**—Contains hardware installation and regulatory guides.
- **Configure**—Contains configuration guides for IPS CLI, IDM, and IME.
- **Troubleshoot and Alerts**—Contains TAC tech notes and field notices.

Cisco Security Intelligence Operations

The Cisco Security Intelligence Operations site on Cisco.com provides intelligence reports about current vulnerabilities and security threats. It also has reports on other security topics that help you protect your network and deploy your security systems to reduce organizational risk.

You should be aware of the most recent security threats so that you can most effectively secure and manage your network. Cisco Security Intelligence Operations contains the top ten intelligence reports listed by date, severity, urgency, and whether there is a new signature available to deal with the threat.

Cisco Security Intelligence Operations contains a Security News section that lists security articles of interest. There are related security tools and links.

You can access Cisco Security Intelligence Operations at this URL:

http://tools.cisco.com/security/center/home.x

Cisco Security Intelligence Operations is also a repository of information for individual signatures, including signature ID, type, structure, and description.

You can search for security alerts and signatures at this URL:

http://tools.cisco.com/security/center/search.x

Obtaining a License Key From Cisco.com

This section describes how to obtain a license key from Cisco.com and how to install it using the CLI, IDM, or IME. It contains the following topics:

Understanding Licensing

Although the sensor functions without the license key, you must have a license key to obtain signature updates and use the global correlation features. To obtain a license key, you must have the following:

- Cisco Service for IPS service contract—Contact your reseller, Cisco service or product sales to purchase a contract.
- Your IPS device serial number—To find the IPS device serial number in IDM or IME, for IDM choose **Configuration > Sensor Management > Licensing**, and for IME choose **Configuration > *sensor_name* > Sensor Management > Licensing**, or in the CLI use the **show version** command.
- Valid Cisco.com username and password

Trial license keys are also available. If you cannot get your sensor licensed because of problems with your contract, you can obtain a 60-day trial license that supports signature updates that require licensing.

You can obtain a license key from the Cisco.com licensing server, which is then delivered to the sensor. Or, you can update the license key from a license key provided in a local file. Go to http://www.cisco.com/go/license and click **IPS Signature Subscription Service** to apply for a license key.

You can view the status of the license key in these places:

- IDM Home window Licensing section on the Health tab
- IDM Licensing pane (**Configuration > Licensing**)
- IME Home page in the Device Details section on the Licensing tab
- License Notice at CLI login

Whenever you start IDM, IME, or the CLI, you are informed of your license status—whether you have a trial, invalid, or expired license key. With no license key, an invalid license key, or an expired license key, you can continue to use IDM, IME, and the CLI, but you cannot download signature updates.

If you already have a valid license on the sensor, you can click **Download** on the License pane to download a copy of your license key to the computer that IDM or IME is running on and save it to a local file. You can then replace a lost or corrupted license, or reinstall your license after you have reimaged the sensor.

Service Programs for IPS Products

You must have a Cisco Services for IPS service contract for any IPS product so that you can download a license key and obtain the latest IPS signature updates. If you have a direct relationship with Cisco Systems, contact your account manager or service account manager to purchase the Cisco Services for IPS service contract. If you do not have a direct relationship with Cisco Systems, you can purchase the service account from a one-tier or two-tier partner.

When you purchase the following IPS products you must also purchase a Cisco Services for IPS service contract:

- IPS 4240
- IPS 4255
- IPS 4260
- IPS 4270-20
- AIM IPS
- IDSM2
- NME IPS

When you purchase an ASA 5500 series adaptive security appliance product that does not contain IPS, you must purchase a SMARTnet contract.

Note SMARTnet provides operating system updates, access to Cisco.com, access to TAC, and hardware replacement NBD on site.

When you purchase an ASA 5500 series adaptive security appliance product that ships with the AIP SSM installed or if you purchase to add to your ASA 5500 series adaptive security appliance product, you must purchase the Cisco Services for IPS service contract.

Note Cisco Services for IPS provides IPS signature updates, operating system updates, access to Cisco.com, access to TAC, and hardware replacement NBD on site.

For example, if you purchased an ASA 5510 and then later wanted to add IPS and purchased an ASA-SSM-AIP-10-K9, you must now purchase the Cisco Services for IPS service contract. After you have the Cisco Services for IPS service contract, you must also have your product serial number to apply for the license key.

Caution If you ever send your product for RMA, the serial number will change. You must then get a new license key for the new serial number.

Obtaining and Installing the License Key Using IDM or IME

Note In addition to a valid Cisco.com username and password, you must also have a Cisco Services for IPS service contract before you can apply for a license key.

To obtain and install the license key, follow these steps:

Step 1 Log in to IDM or IME using an account with administrator privileges.

Step 2 For IDM choose **Configuration > Sensor Management > Licensing**. For IME choose **Configuration > *sensor_name* > Sensor Management > Licensing**. The Licensing pane displays the status of the current license. If you have already installed your license, you can click **Download** to save it if needed.

Step 3 Obtain a license key by doing one of the following:

- Click the **Cisco.com** radio button to obtain the license from Cisco.com. IDM or IME contacts the license server on Cisco.com and sends the server the serial number to obtain the license key. This is the default method. Go to Step 4.
- Click the **License File** radio button to use a license file. To use this option, you must apply for a license key at this URL: www.cisco.com/go/license. The license key is sent to you in e-mail and you save it to a drive that IDM or IME can access. This option is useful if your computer cannot access Cisco.com. Go to Step 7.

Step 4 Click **Update License**, and in the Licensing dialog box, click **Yes** to continue. The Status dialog box informs you that the sensor is trying to connect to Cisco.com. An Information dialog box confirms that the license key has been updated.

Step 5 Click **OK**.

Step 6 Go to www.cisco.com/go/license.

Step 7 Fill in the required fields. Your license key will be sent to the e-mail address you specified.

Caution You must have the correct IPS device serial number because the license key only functions on the device with that number.

Step 8 Save the license key to a hard-disk drive or a network drive that the client running IDM or IME can access.

Step 9 Log in to IDM or IME.

Step 10 For IDM choose **Configuration > Sensor Management > Licensing**. For IME choose **Configuration > *sensor_name* > Sensor Management > Licensing**.

Step 11 Under Update License, click the **License File** radio button.

Step 12 In the Local File Path field, specify the path to the license file or click **Browse Local** to browse to the file.

Step 13 Browse to the license file and click **Open**.

Step 14 Click **Update License**.

For More Information

For more information about obtaining a Cisco Services for IPS service contract, see Service Programs for IPS Products, page 11-11.

Obtaining and Installing the License Key Using the CLI

Note You cannot install an older license key over a newer license key.

Use the **copy** *source-url license_file_name* **license-key** command to copy the license key to your sensor.

The following options apply:

- *source-url*—The location of the source file to be copied. It can be a URL or keyword.
- *destination-url*—The location of the destination file to be copied. It can be a URL or a keyword.
- **license-key**—The subscription license file.
- *license_file_name*—The name of the license file you receive.

The exact format of the source and destination URLs varies according to the file. Here are the valid types:

- ftp:—Source or destination URL for an FTP network server. The syntax for this prefix is:

  ftp:[//[username@] location]/relativeDirectory]/filename

  ftp:[//[username@]location]//absoluteDirectory]/filename
- scp:—Source or destination URL for the SCP network server. The syntax for this prefix is:

  scp:[//[username@] location]/relativeDirectory]/filename

  scp:[//[username@] location]//absoluteDirectory]/filename

  Note If you use FTP or SCP protocol, you are prompted for a password. If you use SCP protocol, you must add the remote host to the SSH known hosts list.
- http:—Source URL for the web server. The syntax for this prefix is:

  http:[[/[username@]location]/directory]/filename
- https:—Source URL for the web server. The syntax for this prefix is:

  https:[[/[username@]location]/directory]/filename

  Note If you use HTTPS protocol, the remote host must be a TLS trusted host.

Installing the License Key

To install the license key, follow these steps:

Step 1 Apply for the license key at this URL: www.cisco.com/go/license.

Note In addition to a valid Cisco.com username and password, you must also have a Cisco Services for IPS service contract before you can apply for a license key.

Step 2 Fill in the required fields. Your Cisco IPS Signature Subscription Service license key will be sent by e-mail to the e-mail address you specified.

Note You must have the correct IPS device serial number because the license key only functions on the device with that number.

Step 3 Save the license key to a system that has a web server, FTP server, or SCP server.

Step 4 Log in to the CLI using an account with administrator privileges.

Step 5 Copy the license key to the sensor.

```
sensor# copy scp://user@10.89.147.3://tftpboot/dev.lic license-key
Password: *******
```

Step 6 Verify the sensor is licensed.

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.0(1)E3

Host:
    Realm Keys          key1.0
Signature Definition:
    Signature Update    S391.0                  2008-04-16
    Virus Update        V1.2                    2005-11-24
OS Version:             2.4.30-IDS-smp-bigphys
Platform:               ASA-SSM-20
Serial Number:          P300000220
Sensor up-time is 3 days.
Using 1031888896 out of 2093682688 bytes of available memory (49% usage)
system is using 17.8M out of 29.0M bytes of available disk space (61% usage)
application-data is using 52.4M out of 166.6M bytes of available disk space (33% usage)
boot is using 37.8M out of 68.5M bytes of available disk space (58% usage)


MainApp          N-2007_JUN_19_16_45   (Release)   2007-06-19T17:10:20-0500   Running
AnalysisEngine   N-2007_JUN_19_16_45   (Release)   2007-06-19T17:10:20-0500   Running
CLI              N-2007_JUN_19_16_45   (Release)   2007-06-19T17:10:20-0500


Upgrade History:

  IPS-K9-7.0-1-E3 15:36:05 UTC Thu Apr 24 2008

Recovery Partition Version 1.1 - 7.0(1)E3

Host Certificate Valid from: 25-Apr-2008 to 26-Apr-2010

sensor#
```

Step 7 Copy your license key from a sensor to a server to keep a backup copy of the license.

```
sensor# copy license-key scp://user@10.89.147.3://tftpboot/dev.lic
Password: *******
sensor#
```

For More Information

- For the procedure for adding a remote host to the SSH known hosts list, for IDM refer to Defining Known Hosts Keys, for IME refer to Defining Known Host Keys, and for the CLI refer to Adding Hosts to the SSH Known Hosts List.
- For the procedure for adding a remote host to the trusted hosts list, for IDM refer to Adding Trusted Hosts, for IME refer to Adding Trusted Hosts, and for the CLI refer to Adding TLS Trusted Hosts
- For more information about obtaining a Cisco Services for IPS service contract, see Service Programs for IPS Products, page 11-11.

CHAPTER 12

Upgrading, Downgrading, and Installing System Images

This chapter describes how to upgrade, downgrade, and install system images. It contains the following sections:

Upgrades, Downgrades, and System Images

Note After you upgrade any IPS software on your sensor, you must restart the IDM to see the latest software features.

You can upgrade and downgrade the software on the sensor. Upgrading applies a service pack, signature update, signature engine update, minor version, major version, or recovery partition file. Downgrading removes the last applied service pack or signature update from the sensor.

Caution You cannot use the **downgrade** command to revert to a previous major or minor version, for example, from Cisco IPS 7.0 to 6.2. You can only use the **downgrade** command to downgrade from the latest signature update or signature engine update. To revert to 6.2, you must reimage the sensor.

You can recover the application partition image on your sensor if it becomes unusable. Using the **recover** command lets you retain your host settings while other settings revert to the factory defaults.

To install a new system image on the sensor, use ROMMON, the bootloader file, or the maintenance partition depending on which platform you have.

When you install a new system image on your sensor, all accounts are removed and the default cisco account is reset to use the default password **cisco**. After installing the system image, you must initialize the sensor again.

After you reimage and initialize your sensor, upgrade your sensor with the most recent service pack, signature update, signature engine update, minor update, major update, and recovery partition file.

For More Information

- For the procedure for initializing the sensor, see Chapter 10, "Initializing the Sensor."
- For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software, page 11-1.

Supported FTP and HTTP/HTTPS Servers

The following FTP servers are supported for IPS software updates:

- WU-FTPD 2.6.2 (Linux)
- Solaris 2.8
- Sambar 6.0 (Windows 2000)
- Serv-U 5.0 (Windows 2000)
- MS IIS 5.0 (Windows 2000)

The following HTTP/HTTPS servers are supported for IPS software updates:

- CMS - Apache Server (Tomcat)
- CMS - Apache Server (JRun)

For More Information

- For the procedure for downloading IPS software updates from Cisco.com, see Obtaining Cisco IPS Software, page 11-1.
- For the procedure for configuring automatic updates, see Configuring Automatic Upgrades, page 12-6.

Upgrading the Sensor

This section explains how to use the **upgrade** command to upgrade the software on the sensor. It contains the following topics:

IPS 7.0 Upgrade Files

The following files are part of Cisco IPS 7.0(1)E3:

- Readme
  - IPS-7.0-1-E3.readme.txt
- Major Version Upgrade File
  - IPS-K9-7.0-1-E3.pkg
  - IPS-AIM-K9-7.0-1-E3.pkg
  - IPS-NME-K9-7.0-1-E3.pkg
- System Image Files
  - IPS 4240-K9-sys-1.1-a-7.0-1-E3.img
  - IPS 4255-K9-sys-1.1-a-7.0-1-E3.img
  - IPS 4260-K9-sys-1.1-a-7.0-1-E3.img
  - IPS-4270_20-K9-sys-1.1-a-7.0-1-E3.img
  - IPS-IDSM2-K9-sys-1.1-a-7.0-1-E3.bin.gz
  - IPS-SSM_10-K9-sys-1.1-a-7.0-1-E3.img
  - IPS-SSM_20-K9-sys-1.1-a-7.0-1-E3.img
  - IPS-SSM_40-K9-sys-1.1-a-7.0-1-E3.img
  - IPS-AIM-K9-sys-1.1-a-7.0-1-E3.img
  - IPS-NME-K9-sys-1.1-a-7.0-1-E3.img
- Recovery Image Files
  - IPS-K9-r-1.1-a-7.0-1-E3.pkg
  - IPS-AIM-K9-r-1.1-a-7.0-1-E3.pkg
  - IPS-NME-K9-r-1.1-a-7.0-1-E3.pkg

For More Information

For the procedure for obtaining these files on Cisco.com, see Obtaining Cisco IPS Software, page 11-1.

upgrade Command and Options

Use the **upgrade** *source-url* command to apply service pack, signature update, engine update, minor version, major version, or recovery partition file upgrades.

The following options apply:

- *source-url*—The location of the source file to be copied.
  - ftp:—Source URL for an FTP network server. The syntax for this prefix is:

    ftp:[//[username@] location]/relativeDirectory]/filename

    ftp:[//[username@]location]//absoluteDirectory]/filename

    Note You are prompted for a password.

– scp:—Source URL for the SCP network server. The syntax for this prefix is:

scp:[//[username@] location]/relativeDirectory]/filename

scp:[//[username@] location]//absoluteDirectory]/filename

Note You are prompted for a password.

– http:—Source URL for the web server. The syntax for this prefix is:

http:[[//username@] location]/directory] filename

Note The directory specification should be an absolute path to the desired file.

– https:—Source URL for the web server. The syntax for this prefix is:

https:[[//username@] location]/directory] filename

Note The directory specification should be an absolute path to the desired file.

Using the upgrade Command

Caution You must log in to Cisco.com using an account with cryptographic privileges to download software. The first time you download software on Cisco.com, you receive instructions for setting up an account with cryptographic privileges.

Caution Do not change the filename. You must preserve the original filename for the sensor to accept the update.

Caution When you upgrade the AIM IPS or the NME IPS using manual upgrade, you must disable heartbeat reset on the router before installing the upgrade. You can reenable heartbeat reset after you complete the upgrade. If you do not disable heartbeat reset, the upgrade can fail and leave the AIM IPS or the NME IPS in an unknown state, which can require a system reimage to recover.

To upgrade the sensor, follow these steps:

Step 1 Download the appropriate file (for example, IPS-K9-7.0-1-E3.pkg) to an FTP, SCP, HTTP, or HTTPS server that is accessible from your sensor.

Step 2 Log in to the CLI using an account with administrator privileges.

Step 3 Enter configuration mode.

```
sensor# configure terminal
```

Step 4 Upgrade the sensor.

```
sensor(config)# upgrade url/IPS-K9-7.0-1-E3.pkg
```

The URL points to where the update file is located, for example, to retrieve the update using FTP, enter the following:

```
sensor(config)# upgrade ftp://username@ip_address//directory/IPS-K9-7.0-1-E3.pkg
```

Step 5 Enter the password when prompted.

```
Enter password: ********
```

Step 6 Enter **yes** to complete the upgrade.

Note Major updates, minor updates, and service packs may force a restart of the IPS processes or even force a reboot of the sensor to complete installation.

Note The operating system is reimaged and all files that have been placed on the sensor through the service account are removed.

For More Information

- For a list of supported FTP and HTTP/HTTPS servers, see Supported FTP and HTTP/HTTPS Servers, page 12-2.
- For the procedure for locating software on Cisco.com and obtaining an account with cryptographic privileges, see Obtaining Cisco IPS Software, page 11-1.
- For the procedure for disabling heartbeat reset on the AIM IPS, refer to Disabling and Enabling Heartbeat Reset; for the NME IPS, refer to Disabling and Enabling Heartbeat Reset.

Upgrading the Recovery Partition

Use the **upgrade** command to upgrade the recovery partition with the most recent version so that it is ready if you need to recover the application partition on your sensor.

Note Recovery partition images are generated for major and minor updates and only in rare situations for service packs or signature updates.

Note The AIM IPS and the NME IPS have unique recovery images that you must use to upgrade the recovery partition:
AIM IPS—IPS-AIM-K9-r-1.1-a-7.0-1-E3.pkg
NME IPS—IPS-NME-K9-r-1.1-a-7.0-1-E3.pkg

To upgrade the recovery partition on your sensor, follow these steps:

Step 1 Download the recovery partition image file (IPS-K9-r-1.1-a-7.0-1-E3.pkg) to an FTP, SCP, HTTP, or HTTPS server that is accessible from your sensor.

Caution Some browsers add an extension to the filename. The filename of the saved file must match what is displayed on the download page or you cannot use it to upgrade the recovery partition.

Step 2 Log in to the CLI using an account with administrator privileges.

Step 3 Enter configuration mode.

```
sensor# configure terminal
```

Step 4 Upgrade the recovery partition.

```
sensor(config)#
upgrade scp://user@server_ipaddress//upgrade_path/IPS-K9-r-1.1-a-7.0-1-E3.pkg

sensor(config)#
upgrade ftp://user@server_ipaddress//upgrade_path/IPS-K9-r-1.1-a-7.0-1-E3.pkg
```

Step 5 Enter the server password.

The upgrade process begins.

Note This procedure only reimages the recovery partition. The application partition is not modified by this upgrade. To reimage the application partition after the recovery partition, use the **recover application-partition** command.

For More Information

- For a list of supported FTP and HTTP/HTTPS servers, see Supported FTP and HTTP/HTTPS Servers, page 12-2.
- For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software, page 11-1.
- For the procedure for using the **recover** command, see Using the recover Command, page 12-11.

Configuring Automatic Upgrades

This section describes how to configure the sensor to automatically look for upgrades in the upgrade directory. It contains the following topics:

- Using the auto-upgrade Command, page 12-8

Automatic Upgrades

You can configure the sensor to look for new upgrade files in your upgrade directory automatically. For example, several sensors can point to the same remote FTP server directory with different update schedules, such as every 24 hours, or Monday, Wednesday, and Friday at 11:00 pm.

You specify the following information to schedule automatic upgrades:

- Server IP address
- Path of the directory on the file server where the sensor checks for upgrade files
- File copy protocol (SCP or FTP)
- Username and password
- Upgrade schedule

You must download the software upgrade from Cisco.com and copy it to the upgrade directory before the sensor can poll for automatic upgrades.

For More Information

For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software, page 11-1.

auto-upgrade Command and Options

Use the **auto-upgrade-option enabled** command in the service host submode to configure automatic upgrades.

The following options apply:

- **cisco-server**—Enables automatic signature and engine updates from Cisco.com.
- **cisco-url**—The Cisco server locator service.

  You do not need to change this unless the www.cisco.com IP address changes.
- **default**— Sets the value back to the system default setting.
- **directory**— Directory where upgrade files are located on the file server.

  A leading '/' indicates an absolute path.
- **file-copy-protocol**— File copy protocol used to download files from the file server. The valid values are **ftp** or **scp**.

  Note If you use SCP, you must use the **ssh host-key** command to add the server to the SSH known hosts list so the sensor can communicate with it through SSH.
- **ip-address**— IP address of the file server.
- **password**— User password for Cisco server authentication.

- **schedule-option**—Schedules when Cisco server automatic upgrades occur. Calendar scheduling starts upgrades at specific times on specific days. Periodic scheduling starts upgrades at specific periodic intervals.
  - **calendar-schedule**—Configure the days of the week and times of day that automatic upgrades will be performed.
  - **days-of-week**—Days of the week on which auto-upgrades will be performed. You can select multiple days: *sunday* through *saturday* are the valid values.
  - **no**—Removes an entry or selection setting.
  - **times-of-day**—Times of day at which auto-upgrades will begin. You can select multiple times. The valid value is *hh:mm[:ss]*.
  - **periodic-schedule**—Configure the time that the first automatic upgrade should occur, and how long to wait between automatic upgrades.
  - **interval**—The number of hours to wait between automatic upgrades. Valid values are 0 to 8760.
  - **start-time**—The time of day to start the first automatic upgrade. The valid value is *hh:mm[:ss]*.
- **user-name**—Username for server authentication.
- **user-server**—Enables automatic upgrades from a user-defined server.

For More Information

For the procedure for adding a remote host to the SSH known hosts list, for IDM refer to Defining Known Hosts Keys, for IME refer to Defining Known Host Keys, and for the CLI, refer to Adding Hosts to the SSH Known Hosts List.

Using the auto-upgrade Command

Note If you get an unauthorized error message while configuring an automatic update, make sure you have the correct ports open on any firewalls between the sensor and Cisco.com. For example, you need 198.133.219.25 port 443 for the initial automatic update connection to www.cisco.com, and you need 198.133.219.243 port 80 to download the chosen package from a Cisco file server. The IP address may change for the Cisco file server, but you can find it in the lastDownloadAttempt section in the output of the **show statistics host** command.

Note To check the status of the last automatic update or the next scheduled automatic update, run the **show statistics host** command and check the Auto Update Statistics section.

To schedule automatic upgrades, follow these steps:

Step 1 Log in to the CLI using an account with administrator privileges.

Step 2 Enter automatic upgrade submode.

```
sensor# configure terminal
sensor(config)# service host
sensor(config-hos)# auto-upgrade
sensor(config-hos-aut)#
```

Step 3 Configure the sensor to automatically look for new upgrades either on Cisco.com or on your file server.

a. On Cisco.com.

```
sensor(config-hos-aut)# cisco-server enabled
```

Continue with Step 4.

b. From your server.

```
sensor(config-hos-aut)# user-server enabled
```

c. Specify the IP address of the file server.

```
sensor(config-hos-ena)# ip-address 10.1.1.1
```

d. Specify the directory where the upgrade files are located on the file server.

```
sensor(config-hos-ena)# directory /tftpboot/sensor_updates
```

e. Specify the file server protocol.

```
sensor(config-hos-ena)# file-copy-protocol ftp
```

Note If you use SCP, you must use the **ssh host-key** command to add the server to the SSH known hosts list so the sensor can communicate with it through SSH.

Step 4 Specify the username for authentication.

```
sensor(config-hos-ena)# user-name tester
```

Step 5 Specify the password of the user.

```
sensor(config-hos-ena)# password
Enter password[]: ******
Re-enter password: ******
```

Step 6 Specify the scheduling.

a. For calendar scheduling, which starts upgrades at specific times on specific day.

```
sensor(config-hos-ena)# schedule-option calendar-schedule
sensor(config-hos-ena-cal)# days-of-week sunday
sensor(config-hos-ena-cal)# times-of-day 12:00:00
```

b. For periodic scheduling, which starts upgrades at specific periodic intervals.

```
sensor(config-hos-ena)# schedule-option periodic-schedule
sensor(config-hos-ena-per)# interval 24
sensor(config-hos-ena-per)# start-time 13:00:00
```

Step 7 Verify the settings.

```
sensor(config-hos-ena)# show settings
   enabled
   ----------------------------------------------
      schedule-option
      ----------------------------------------------
         periodic-schedule
         ----------------------------------------------
            start-time: 13:00:00
            interval: 24 hours
         ----------------------------------------------
      ----------------------------------------------
```

```
      ip-address: 10.1.1.1
      directory: /tftpboot/update/6.1_dummy_updates
      user-name: tester
      password: <hidden>
      file-copy-protocol: ftp default: scp
   ----------------------------------------------
sensor(config-hos-ena)#
```

Step 8 Exit automatic upgrade submode.

```
sensor(config-hos-ena)# exit
sensor(config-hos)# exit
Apply Changes:?[yes]:
```

Step 9 Press **Enter** to apply the changes or type **no** to discard them.

For More Information

- For a list of supported FTP and HTTP/HTTPS servers, see Supported FTP and HTTP/HTTPS Servers, page 12-2.
- For the procedure for adding a remote host to the trusted hosts list, for IDM refer to Defining Known Hosts Keys, for IME refer to Defining Known Host Keys, and for the CLI, refer to Adding Hosts to the SSH Known Hosts List.

Downgrading the Sensor

Caution You cannot use the **downgrade** command to revert to a previous major or minor version, for example, from Cisco IPS 7.0 to 6.2. You can only use the **downgrade** command to downgrade from the latest signature update or signature engine update. To revert to 6.2, you must reimage the sensor.

Use the **downgrade** command to remove the last applied signature upgrade or signature engine upgrade from the sensor.

To remove the last applied signature update or signature engine update from the sensor, follow these steps:

Step 1 Log in to the sensor using an account with administrator privileges.

Step 2 Enter global configuration mode.

```
sensor# configure terminal
```

Step 3 If there is no recently applied service pack or signature update, the **downgrade** command is not available.

```
sensor(config)# downgrade
No downgrade available.
sensor(config)#
```

Recovering the Application Partition

This section explains how to recover the application partition, and contains the following topics:

Application Partition

You can recover the application partition image for the sensor if it becomes unusable. Some network configuration information is retained when you use this method, which lets you have network access after the recovery is performed.

Use the **recover application-partition** command to boot to the recovery partition, which automatically recovers the application partition on your sensor.

Note If you have upgraded your recovery partition to the most recent version before you recover the application partition image, you can install the most up-to-date software image.

Because you can execute the **recover application-partition** command through a Telnet or SSH connection, we recommend using this command to recover sensors that are installed at remote locations.

Note When you reconnect to the sensor after recovery, you must log in with the default username and password **cisco**.

For More Information

For the procedure for upgrading the recovery partition to the most recent version, see Upgrading the Recovery Partition, page 12-5.

Using the recover Command

Note To upgrade the recovery partition the sensor must already be running IPS 7.0(1).

To recover the application partition image, follow these steps:

Step 1 Download the recovery partition image file (IPS-K9-r-1.1-a-7.0-1-E3.pkg) to an FTP, HTTP, or HTTPS server that is accessible from your sensor.

Step 2 Log in to the CLI using an account with administrator privileges.

Step 3 Enter configuration mode.

```
sensor# configure terminal
```

Step 4 Recover the application partition image.

```
sensor(config)# recover application-partition
```

```
Warning: Executing this command will stop all applications and re-image the node to
version 6.2(1)E3. All configuration changes except for network settings will be reset to
default.
Continue with recovery? []:
```

Step 5 Enter **yes** to continue. Shutdown begins immediately after you execute the **recover** command. Shutdown can take a while, and you will still have access to the CLI, but access will be terminated without warning.

The application partition is reimaged using the image stored on the recovery partition. You must now initialize the sensor with the **setup** command.The IP address, netmask, access lists, time zone, and offset are saved and applied to the reimaged application partition. If you executed the **recover application-partition** command remotely, you can SSH to the sensor with the default username and password (**cisco/cisco**) and then initialize the sensor again with the **setup** command. You cannot use Telnet until you initialize the sensor because Telnet is disabled by default.

For More Information

- For a list of supported TFTP servers, see Supported TFTP Servers, page 12-13.
- For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software, page 11-1.
- For the procedure for using the **setup** command, see Initializing the Sensor, page 10-1.

Installing System Images

This section contains the procedures for installing system images on the appliances and modules. It contains the following topics:

Caution All user configuration settings are lost when you install the system image. Before trying to recover the sensor by installing the system image, try to recover by using the **recover application-partition** command or by selecting the recovery partition during sensor bootup.

Understanding ROMMON

Some Cisco sensors include a preboot CLI called ROMMON, which lets you boot images on sensors where the image on the primary device is missing, corrupt, or otherwise unable to boot the normal application. ROMMON is particularly useful for recovering remote sensors as long as the serial console port is available.

Access to ROMMON is available only through the serial console port, a Cisco-standard asynchronous RS-232C DTE available in an RJ-45F connector on the sensor chassis. The serial port is configured for 9600 baud, 8 data bits, 1 stop bit, no parity, and no flow control.

For More Information

For the procedure for using a terminal server, see Connecting an Appliance to a Terminal Server, page 12-13.

Supported TFTP Servers

ROMMON uses TFTP to download an image and launch it. TFTP does not address network issues such as latency or error recovery. It does implement a limited packet integrity check so that packets arriving in sequence with the correct integrity value have an extremely low probability of error. But TFTP does not offer pipelining so the total transfer time is equal to the number of packets to be transferred times the network average RTT. Because of this limitation, we recommend that the TFTP server be located on the same LAN segment as the sensor. Any network with an RTT less than a 100 milliseconds should provide reliable delivery of the image.

Some TFTP servers limit the maximum file size that can be transferred to ~32 MB. Therefore, we recommend the following TFTP servers:

- For Windows:

  Tftpd32 version 2.0, available at:

  http://tftpd32.jounin.net/

- For UNIX:

  Tftp-hpa series, available at:

  http://www.kernel.org/pub/software/network/tftp/

Connecting an Appliance to a Terminal Server

A terminal server is a router with multiple, low speed, asynchronous ports that are connected to other serial devices. You can use terminal servers to remotely manage network equipment, including appliances.

To set up a Cisco terminal server with RJ-45 or hydra cable assembly connections, follow these steps:

Step 1 Connect to a terminal server using one of the following methods:

- For terminal servers with RJ-45 connections, connect a 180 rollover cable from the console port on the appliance to a port on the terminal server.
- For hydra cable assemblies, connect a straight-through patch cable from the console port on the appliance to a port on the terminal server.

Step 2 Configure the line and port on the terminal server. In enable mode, enter the following configuration, where # is the line number of the port to be configured.

```
config t
line #
login
transport input all
stopbits 1
flowcontrol hardware
speed 9600
exit
exit
wr mem
```

Step 3 Be sure to properly close a terminal session to avoid unauthorized access to the appliance.

If a terminal session is not stopped properly, that is, if it does not receive an exit(0) signal from the application that initiated the session, the terminal session can remain open. When terminal sessions are not stopped properly, authentication is not performed on the next session that is opened on the serial port.

Caution Always exit your session and return to a login prompt before terminating the application used to establish the connection.

Caution If a connection is dropped or terminated by accident, you should reestablish the connection and exit normally to prevent unauthorized access to the appliance.

Installing the IPS 4240 and IPS 4255 System Images

Note This procedure is for the IPS 4240, but is also applicable to the IPS 4255. The system image for the IPS 4255 has “4255” in the filename.

You can install the IPS 4240 and IPS 4255 system image by using the ROMMON on the appliance to TFTP the system image onto the compact flash device.

To install the IPS 4240 and IPS 4255 system image, follow these steps:

Step 1 Download the IPS 4240 system image file (IPS 4240-K9-sys-1.1-a-6.27.0-1-E3.img) to the tftp root directory of a TFTP server that is accessible from your IPS 4240.

Note Make sure you can access the TFTP server location from the network connected to the Ethernet port of your IPS 4240.

Step 2 Boot the IPS 4240.

```
Booting system, please wait...

CISCO SYSTEMS
Embedded BIOS Version 1.0(5)0 09/14/04 12:23:35.90
```

```
Low Memory: 631 KB
High Memory: 2048 MB
PCI Device Table.
Bus Dev Func VendID DevID Class              Irq
00  00  00   8086   2578  Host Bridge
00  01  00   8086   2579  PCI-to-PCI Bridge
00  03  00   8086   257B  PCI-to-PCI Bridge
00  1C  00   8086   25AE  PCI-to-PCI Bridge
00  1D  00   8086   25A9  Serial Bus         11
00  1D  01   8086   25AA  Serial Bus         10
00  1D  04   8086   25AB  System
00  1D  05   8086   25AC  IRQ Controller
00  1D  07   8086   25AD  Serial Bus         9
00  1E  00   8086   244E  PCI-to-PCI Bridge
00  1F  00   8086   25A1  ISA Bridge
00  1F  02   8086   25A3  IDE Controller     11
00  1F  03   8086   25A4  Serial Bus         5
00  1F  05   8086   25A6  Audio              5
02  01  00   8086   1075  Ethernet           11
03  01  00   177D   0003  Encrypt/Decrypt    9
03  02  00   8086   1079  Ethernet           9
03  02  01   8086   1079  Ethernet           9
03  03  00   8086   1079  Ethernet           9
03  03  01   8086   1079  Ethernet           9
04  02  00   8086   1209  Ethernet           11
04  03  00   8086   1209  Ethernet           5

Evaluating BIOS Options ...
Launch BIOS Extension to setup ROMMON

Cisco Systems ROMMON Version (1.0(5)0) #1: Tue Sep 14 12:20:30 PDT 2004

Platform IPS 4240-K9
Management0/0

MAC Address: 0000.c0ff.ee01
```

Step 3 Press **Break** or **Esc** at the following prompt while the system is booting to interrupt boot. Press the spacebar to begin boot immediately.

Note You have ten seconds to press **Break** or **Esc**.

```
Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
```

The system enters ROMMON mode. The `rommon>` prompt appears.

Step 4 Check the current network settings.

```
rommon> set

ROMMON Variable Settings:
      ADDRESS=0.0.0.0
      SERVER=0.0.0.0
      GATEWAY=0.0.0.0
      PORT=Management0/0
      VLAN=untagged
      IMAGE=
      CONFIG=
```

The variables have the following definitions:

- Address—Local IP address of the IPS 4240
- Server—TFTP server IP address where the application image is stored
- Gateway—Gateway IP address used by the IPS 4240
- Port—Ethernet interface used for the IPS 4240 management
- VLAN—VLAN ID number (leave as untagged)
- Image—System image file/path name
- Config—Unused by these platforms

Note Not all values are required to establish network connectivity. The address, server, gateway, and image values are required. If you are not sure of the settings needed for your local environment, contact your system administrator.

Step 5 If necessary, change the interface used for the TFTP download.

Note The default interface used for TFTP downloads is Management0/0, which corresponds to the MGMT interface of the IPS 4240.

```
rommon> PORT=interface_name
```

Step 6 If necessary, assign an IP address for the local port on the IPS 4240.

```
rommon> ADDRESS=ip_address
```

Note Use the same IP address that is assigned to the IPS 4240.

Step 7 If necessary, assign the TFTP server IP address.

```
rommon> SERVER=ip_address
```

Step 8 If necessary, assign the gateway IP address.

```
rommon> GATEWAY=ip_address
```

Step 9 Verify that you have access to the TFTP server by pinging it from your local Ethernet port with one of the following commands.

```
rommon> ping server_ip_address
rommon> ping server
```

Step 10 If necessary define the path and filename on the TFTP file server from which you are downloading the image.

```
rommon> IMAGE=path/file_name
```

Caution Make sure that you enter the **IMAGE** command in all uppercase. You can enter the other ROMMON commands in either lower case or upper case, but the **IMAGE** command specifically must be all uppercase.

UNIX Example

```
rommon> IMAGE=/system_images/IPS 4240-K9-sys-1.1-a-7.0-1-E3.img
```

Note The path is relative to the default tftpboot directory of the UNIX TFTP server. Images located in the default tftpboot directory do not have any directory names or slashes in the IMAGE specification.

Windows Example

```
rommon> IMAGE=\system_images\IPS 4240-K9-sys-1.1-a-7.0-1-E3.img
```

Step 11 Enter **set** and press **Enter** to verify the network settings.

Note You can use the **sync** command to store these settings in NVRAM so they are maintained across boots. Otherwise, you must enter this information each time you want to boot an image from ROMMON.

Step 12 Download and install the system image.

```
rommon> tftp
```

Caution To avoid corrupting the system image, do not remove power from the IPS 4240 while the system image is being installed.

Note If the network settings are correct, the system downloads and boots the specified image on the IPS 4240. Be sure to use the IPS 4240 image.

For More Information

- For a list of supported TFTP servers, see Supported TFTP Servers, page 12-13.
- For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software, page 11-1.

Installing the IPS 4260 System Image

You can install the IPS 4260 system image by using the ROMMON on the appliance to TFTP the system image onto the flash device.

To install the IPS 4260 system image, follow these steps:

Step 1 Download the IPS 4260 system image file (IPS 4260-K9-sys-1.1-a-7.0-1-E3.img) to the tftp root directory of a TFTP server that is accessible from your IPS 4260.

Make sure you can access the TFTP server location from the network connected to your IPS 4260 Ethernet port.

Step 2 Boot the IPS 4260.

Step 3 Press **Ctrl-R** at the following prompt while the system is booting.

```
Evaluating Run Options...
```

Note You have five seconds to press **Ctrl-R**.

```
Assuming IPS 4260-K9 Platform
 2 Ethernet Interfaces detected

Cisco Systems ROMMON Version (1.0(11)1c) #26: Mon Mar 13 18:05:54 CST 2006

Platform IPS 4260-K9
Management0/0
Link is UP
MAC Address: 0004.23cc.6047


Use ? for help.
rommon #0>
```

Step 4 If necessary, change the port used for the TFTP download.

```
rommon #1> interface name
```

The port in use is listed just after the platform identification. In the example, port Management0/0 is being used.

Note The default port used for TFTP downloads is Management0/0, which corresponds with the command and control (MGMT) interface of the IPS 4260.

Note Ports Management0/0 (MGMT) and GigabitEthernet0/1 (GE 0/1) are labeled on the back of the chassis.

Step 5 Specify an IP address for the local port on the IPS 4260.

```
rommon> address ip_address
```

Note Use the same IP address that is assigned to the IPS 4260.

Step 6 Specify the TFTP server IP address.

```
rommon> server ip_address
```

Step 7 Specify the gateway IP address.

```
rommon> gateway ip_address
```

Step 8 Verify that you have access to the TFTP server by pinging it from the local Ethernet port.

```
rommon> ping server_ip_address
rommon> ping server
```

Step 9 Specify the path and filename on the TFTP file server from which you are downloading the image.

```
rommon> file path/filename
```

UNIX Example

```
rommon> file /system_images/IPS 4260-K9-sys-1.1-a-7.0-1-E3.img
```

Note The path is relative to the default tftpboot directory of the UNIX TFTP server. Images located in the default tftpboot directory do not have any directory names or slashes in the file location.

Windows example

```
rommon> file <tftpboot_directory>IPS 4260-K9-sys-1.1-a-7.0-1-E3.img
```

Step 10 Download and install the system image.

```
rommon> tftp
```

Note The IPS 4260 reboots once during the reimaging process. Do not remove power from the IPS 4260 during the update process or the upgrade can become corrupted.

For More Information

- For a list of supported TFTP servers, see Supported TFTP Servers, page 12-13.
- For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software, page 11-1.

Installing the IPS 4270-20 System Image

You can install the IPS 4270-20 system image by using the ROMMON on the appliance to TFTP the system image onto the compact flash device.

To install the IPS 4270-20 system image, follow these steps:

Step 1 Download the IPS 4270-20 system image file (IPS-4270_20-K9-sys-1.1-a-7.0-1-E3.img) to the tftp root directory of a TFTP server that is accessible from your IPS 4270-20.

Note Make sure you can access the TFTP server location from the network connected to the Ethernet port of your IPS 4270-20.

Step 2 Boot the IPS 4270-20.

```
Booting system, please wait...
Cisco Systems ROMMON Version (1.0(12)10) #7: Thu Jun 21 13:50:04 CDT 2007

ft_id_update: Invalid ID-PROM Controller Type (0x5df)

ft_id_update: Defaulting to Controller Type (0x5c2)
```

Note The controller type errors are a known issue and can be disregarded.

Step 3 Press **Break** or **Esc** at the following prompt while the system is booting to interrupt boot. Press the spacebar to begin boot immediately.

Note You have ten seconds to press **Break** or **Esc**.

```
Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
```

The system enters ROMMON mode. The `rommon>` prompt appears.

Step 4 Check the current network settings.

```
rommon> set

ROMMON Variable Settings:
  ADDRESS=0.0.0.0
  SERVER=0.0.0.0
  GATEWAY=0.0.0.0
  PORT=Management0/0
  VLAN=untagged
  IMAGE=
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=2
  RETRY=20
```

The variables have the following definitions:

- Address—Local IP address of the IPS 4270-20
- Server—TFTP server IP address where the application image is stored
- Gateway—Gateway IP address used by the IPS 4270-20
- Port—Ethernet interface used for the IPS 4270-20 management
- VLAN—VLAN ID number (leave as untagged)
- Image—System image file/path name
- Config—Unused by these platforms

Note Not all values are required to establish network connectivity. The address, server, gateway, and image values are required. If you are not sure of the settings needed for your local environment, contact your system administrator.

Step 5 If necessary, assign an IP address for the local port on the IPS 4270-20.

```
rommon> ADDRESS=ip_address
```

Note Use the same IP address that is assigned to the IPS 4270-20.

Step 6 If necessary, assign the TFTP server IP address.

```
rommon> SERVER=ip_address
```

Step 7 If necessary, assign the gateway IP address.

```
rommon> GATEWAY=ip_address
```

Step 8 Verify that you have access to the TFTP server by pinging it from your local Ethernet port with one of the following commands:

```
rommon> ping server_ip_address
rommon> ping server
```

Step 9 If necessary define the path and filename on the TFTP file server from which you are downloading the image.

```
rommon> IMAGE=path/file_name
```

UNIX Example0

```
rommon> IMAGE=/system_images/IPS-4270_20-K9-sys-1.1-a-7.0-1-E3.img
```

Note The path is relative to the UNIX TFTP server default tftpboot directory. Images located in the default tftpboot directory do not have any directory names or slashes in the IMAGE specification.

Windows Example

```
rommon> IMAGE=\system_images\IPS-4270_20-K9-sys-1.1-a-7.0-1-E3.img
```

Step 10 Enter **set** and press **Enter** to verify the network settings.

Note You can use the **sync** command to store these settings in NVRAM so they are maintained across boots. Otherwise, you must enter this information each time you want to boot an image from ROMMON.

Step 11 Download and install the system image.

```
rommon> tftp
```

Caution To avoid corrupting the system image, do not remove power from the IPS 4270-20 while the system image is being installed.

Note If the network settings are correct, the system downloads and boots the specified image on the IPS 4270-20. Be sure to use the IPS 4270-20 image.

For More Information

- For a list of supported TFTP servers, see Supported TFTP Servers, page 12-13.
- For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software, page 11-1.

Installing the AIM IPS System Image

To install the AIM IPS system image, follow these steps:

Step 1 Download the AIM IPS system image file (IPS-AIM-K9-sys-1.1-7.0-1-E3.img), and place it on a TFTP server relative to the tftp root directory.

Note Make sure the network is configured so that the AIM IPS can access the TFTP server.

If no TFTP server is available, you can configure the router to operate as a TFTP server.

```
router# copy tftp: flash:
router# configure terminal
router(config)# tftp-server flash:IPS-AIM-K9-sys-1.1-7.0-1-E3.img
router(config)# exit
router#
```

Step 2 Disable the heartbeat reset.

```
router# service-module IDS-Sensor 0/slot_number heartbeat-reset disable
```

Note Disabling the heartbeat reset prevents the router from resetting the module during system image installation if the process takes too long.

Step 3 Session to the AIM IPS.

```
router# service-module IDS-Sensor 0/slot_number session
```

Note Use the **show configuration | include interface IDS-Sensor** command to determine the AIM IPS slot number.

Step 4 Suspend the session by pressing **Shift-Ctrl-6 X**. You should see the `router#` prompt. If you do not see this prompt, try **Ctrl-6 X**.

Step 5 Reset the AIM IPS. You are prompted to confirm the **reset** command.

```
router# service-module IDS-Sensor 0/slot_number reset
```

Step 6 Press **Enter** to confirm.

Step 7 Press **Enter** to resume the suspended session. After displaying its version, the bootloader displays this prompt for 15 seconds.

```
Please enter '***' to change boot configuration:
```

Step 8 Enter `***` during the 15-second delay. The bootloader prompt appears.

Step 9 Press **Enter** to session back to the AIM IPS.

Step 10 Configure the bootloader.

```
ServicesEngine bootloader> config

IP Address [10.89.148.188]>
Subnet mask [255.255.255.0]>
TFTP server [10.89.150.74]>
Gateway [10.89.148.254]>
```

```
Default boot [disk]>
Number cores [2]>
ServicesEngine boot-loader >
```

For each prompt, enter a value or accept the previously stored input that appears inside square brackets by pressing **Enter**.

Note The gateway IP address must match the IP address of the IDS-Sensor *slot/port* interface.

Note If you set up the module interfaces using the **unnumbered** command, the gateway IP address should be the IP address of the other router interface being used as part of the unnumbered command.

Caution The pathname for the AIM IPS image is full but relative to the tftp server root directory (typically /tftpboot).

Step 11 Start the bootloader.

```
ServicesEngine bootloader> upgrade
```

Step 12 Follow the bootloader instructions to install the software (choose option 1 and follow the wizard instructions).

Note In the following example, the AIM IPS IP address is 10.1.9.201. The imaging process accesses the AIM IPS image from the router TFTP server at IP address 10.1.9.1.

Example

```
Booting from flash...please wait.
Please enter '***' to change boot configuration:
11 ***
ServicesEngine boot-loader Version : 1.1.0
ServicesEngine boot-loader > config

IP Address [10.1.9.201]>
Subnet mask [255.255.255.0]>
TFTP server [10.1.9.1]>
Gateway [10.1.9.1]>
Default boot [disk]>
Number cores [2]>
ServicesEngine boot-loader > upgrade

Cisco Systems, Inc.
Services engine upgrade utility for AIM IPS
-----
Main menu
1 - Download application image and write to USB Drive
2 - Download bootloader and write to flash
3 - Download minikernel and write to flash
r - Exit and reset card
x - Exit
Selection [123rx]
Download recovery image via tftp and install on USB Drive
TFTP server [10.1.9.1]>
full pathname of recovery image []:IPS-AIM-K9-sys-1.1-7.0-1-E3.img
```

```
Ready to begin
Are you sure [Y/N]
Returning TRUE
Press <CTRL-C> to abort.
octeth1:        Up     1Gbs Full duplex, (port  1)
octeth0:        Down  10Mbs Half duplex, (port  0)
Using octeth1 device
TFTP from server 10.1.9.1; our IP address is 10.1.9.201
Filename 'IPS-AIM-K9-sys-1.1-7.0-1-E3.img'.
Load address: 0x21000000
Loading: ##################################################################
         ##################################################################
         ##################################################################
         ##################################################################
         ##################################################################
         ##################################################################
         ##################################################################
         ##################################################################
         ##################################################################
         ##################################################################
         ######
         32 MB received
         ##################################################################
         ########################
done
```

Step 13 Suspend the session by pressing **Shift-Ctrl-6 X**. You should see the `router#` prompt. If you do not see this prompt, try **Ctrl-6 X**.

Step 14 From the router CLI, clear the session.

```
router# service-module interface ids-sensor 0/slot_number session clear
```

Step 15 Enable the heartbeat reset.

```
router# service-module IDS-sensor 0/slot_number heartbeat-reset enable
```

For More Information

- For a list of supported TFTP servers, see Supported TFTP Servers, page 12-13.
- For the procedure for obtaining the most recent IPS software, see Obtaining Cisco IPS Software, page 11-1.
- For the procedure for setting up an unnumbered IP address, refer to Using an Unnumbered IP Address Interface.

Installing the AIP SSM System Image

This section describes how to install the AIP SSM system image, and contains the following topics:

Reimaging the AIP SSM

You can reimage the AIP SSM in one of the following ways:

- From ASA using the **hw-module module 1 recover configure/boot** command.
- Recovering the application image from the sensor CLI using the **recover application-partition** command.
- Upgrading the recovery image from the sensor CLI using the **upgrade** command.

For More Information

- For the procedure for using the **hw-module module 1 recover configure/boot** command, see Reimaging the AIP SSM Using the recover configure/boot Command, page 12-25.
- For the procedure for recovering the application partition, see Recovering the Application Partition, page 12-11.
- For the procedure for upgrading the recovery image, see Upgrading the Recovery Partition, page 12-5.

Reimaging the AIP SSM Using the recover configure/boot Command

If the AIP SSM suffers a failure and the module application image cannot run, you can transfer application images from a TFTP server to the module using the adaptive security appliance CLI. The adaptive security appliance can communicate with the module ROMMON application to transfer the image.

Note Be sure the TFTP server that you specify can transfer files up to 60 MB in size.

Note This process can take approximately 15 minutes to complete, depending on your network and the size of the image.

To install the AIP SSM system image, follow these steps:

Step 1 Log in to the adaptive security appliance.

Step 2 Enter enable mode.

```
asa# enable
```

Step 3 Configure the recovery settings for the AIP SSM.

```
asa (enable)# hw-module module 1 recover configure
```

Note If you make an error in the recovery configuration, use the **hw-module module 1 recover stop** command to stop the system reimaging and then you can correct the configuration.

Step 4 Specify the TFTP URL for the system image.

```
Image URL [tftp://0.0.0.0/]:
```

Example

```
Image URL [tftp://0.0.0.0/]: tftp://10.89.146.1/IPS-SSM-K9-sys-1.1-a-7.0-1-E3.img
```

Step 5 Specify the command and control interface of the AIP SSM.

Note The port IP address is the management IP address of the AIP SSM.

```
Port IP Address [0.0.0.0]:
```

Example

```
Port IP Address [0.0.0.0]: 10.89.149.231
```

Step 6 Leave the VLAN ID at 0.

```
VLAN ID [0]:
```

Step 7 Specify the default gateway of the AIP SSM.

```
Gateway IP Address [0.0.0.0]:
```

Example

```
Gateway IP Address [0.0.0.0]: 10.89.149.254
```

Step 8 Execute the recovery.

```
asa# hw-module module 1 recover boot
```

This transfers the image from the TFTP server to the AIP SSM and restarts it.

Step 9 Periodically check the recovery until it is complete.

Note The status reads `Recovery` during recovery and reads `Up` when reimaging is complete.

```
asa# show module 1

Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  0 ASA 5540 Adaptive Security Appliance         ASA5540            P2B00000019
  1 ASA 5500 Series Security Services Module-20  ASA-SSM-20         P1D000004F4

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  0 000b.fcf8.7b1c to 000b.fcf8.7b20  0.2          1.0(7)2      7.0(0)82
  1 000b.fcf8.011e to 000b.fcf8.011e  0.1          1.0(7)2      5.0(0.22)S129.0

Mod Status
--- ------------------
  0 Up Sys
  1 Up
asa#
```

Note The Status field in the output indicates the operational status of the AIP SSM. An AIP SSM operating normally shows a status of "Up." While the adaptive security appliance transfers an application image to the AIP SSM, the Status field in the output reads "Recover." When the adaptive security appliance completes the image transfer and restarts the AIP SSM, the newly transferred image is running.

Note To debug any errors that may happen in the recovery process, use the **debug module-boot** command to enable debugging of the system reimaging process.

Step 10 Session to the AIP SSM and initialize it with the **setup** command.

For More Information

- For a list of recommended TFTP servers, see Supported TFTP Servers, page 12-13.
- For the procedure for initializing the AIP SSM with the **setup** command, see Advanced Setup for the AIP SSM, page 10-16.

Installing the IDSM2 System Image

This section describes how to install the IDSM2 system image, and contains the following topics:

Understanding the IDSM2 System Image

If the IDSM2 application partition becomes unusable, you can reimage it from the maintenance partition. After you reimage the application partition of the IDSM2, you must initialize the IDSM2 using the **setup** command.

When there is a new maintenance partition image file, you can reimage the maintenance partition from the application partition.

For More Information

For the procedure to use the **setup** command to initialize the IDSM2, see Advanced Setup for the IDSM2, page 10-20.

Installing the IDSM2 System Image for Catalyst Software

To install the system image, follow these steps:

Step 1 Download the IDSM2 system image file (IPS-IDSM2-K9-sys-1.1-a-7.0-1-E3.bin.gz) to the FTP root directory of an FTP server that is accessible from your IDSM2.

Step 2 Log in to the switch CLI.

Step 3 Boot the IDSM2 to the maintenance partition.

```
console> (enable) reset module_number cf:1
```

Step 4 Log in to the maintenance partition CLI.

```
login: guest
Password: cisco
```

Note You must configure the maintenance partition on the IDSM2.

Step 5 Install the system image.

```
guest@hostname.localdomain# upgrade ftp://user@ftp server IP/directory
path/IPS-IDSM2-K9-sys-1.1-a-7.0-1-E3.bin.gz
```

Step 6 Specify the FTP server password. After the application partition file has been downloaded, you are asked if you want to proceed:

```
Upgrading will wipe out the contents on the hard disk. Do you want to proceed installing
it [y|n]:
```

Step 7 Enter **y** to continue. When the application partition file has been installed, you are returned to the maintenance partition CLI.

Step 8 Exit the maintenance partition CLI and return to the switch CLI.

Step 9 Reboot the IDSM2 to the application partition.

```
console> (enable) reset module_number hdd:1
```

Step 10 When the IDSM2 has rebooted, check the software version.

Step 11 Log in to the application partition CLI and initialize the IDSM2 using the **setup** command.

For More Information

- For a list of supported FTP and HTTP/HTTPS servers, see Supported FTP and HTTP/HTTPS Servers, page 12-2.
- For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software, page 11-1.

- For the procedure for configuration the maintenance partition on IDMS-2, see Configuring the IDSM2 Maintenance Partition for Catalyst Software, page 12-30 and Configuring the IDSM2 Maintenance Partition for Cisco IOS Software, page 12-34.
- For the procedure for initializing the IDSM2, see Advanced Setup for the IDSM2, page 10-20.

Installing the IDSM2 System Image for Cisco IOS Software

To install the system image, follow these steps:

Step 1 Download the IDSM2 system image file (IPS-IDSM2-K9-sys-1.1-a-7.0-1-E3.bin.gz) to the FTP root directory of an FTP server that is accessible from your IDSM2.

Step 2 Log in to the switch CLI.

Step 3 Boot the IDSM2 to the maintenance partition.

```
router# hw-module module module_number reset cf:1
```

Step 4 Session to the maintenance partition CLI.

```
router# session slot slot_number processor 1
```

Step 5 Log in to the maintenance partition CLI.

```
login: guest
Password: cisco
```

Step 6 Configure the maintenance partition interface IP address.

```
guest@localhost.localdomain# ip address ip_address netmask
```

Note Choose an address that is appropriate for the VLAN on which the IDSM2 management interface is located based on the switch configuration.

Step 7 Configure the maintenance partition default gateway address.

```
guest@localhost.localdomain# ip gateway gateway_address
```

Step 8 Install the system image.

```
guest@hostname.localdomain# upgrade
ftp://user@ftp_server_ip_address/directory_path/IPS-IDSM2-K9-sys-1.1-a-7.0-1-E3.bin.gz
–install
```

Step 9 Specify the FTP server password. After the application partition file has been downloaded, you are asked if you want to proceed:

```
Upgrading will wipe out the contents on the hard disk.
Do you want to proceed installing it [y|n]:
```

Step 10 Enter **y** to continue. When the application partition file has been installed, you are returned to the maintenance partition CLI.

Step 11 Exit the maintenance partition CLI and return to the switch CLI.

Step 12 Reboot the IDSM2 to the application partition.

```
router# hw-module module module_number reset hdd:1
```

Step 13 Verify that the IDSM2 is online and that the software version is correct and that the status is `ok`.

```
router# show module module_number
```

Step 14 Session to the IDSM2 application partition CLI.

```
router# session slot slot_number processor 1
```

Step 15 Initialize the IDSM2 using the **setup** command.

For More Information

- For a list of supported FTP and HTTP/HTTPS servers, see Supported FTP and HTTP/HTTPS Servers, page 12-2.
- For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software, page 11-1.
- For the procedure for configuration the maintenance partition on IDMS-2, see Configuring the IDSM2 Maintenance Partition for Catalyst Software, page 12-30 and Configuring the IDSM2 Maintenance Partition for Cisco IOS Software, page 12-34.
- For the procedure for initializing the IDSM2, see Advanced Setup for the IDSM2, page 10-20.

Configuring the IDSM2 Maintenance Partition for Catalyst Software

To configure the IDSM2 maintenance partition, follow these steps:

Step 1 Log in to the switch CLI.

Step 2 Enter privileged mode.

```
console# enable
console(enable)#
```

Step 3 Reload the IDSM2.

```
console> (enable) reset module_number cf:1
```

Step 4 Session to the IDSM2.

```
console# session 9
Trying IDS-9...
Connected to IDS-9.
Escape character is '^]'.

Cisco Maintenance image
```

Note You cannot Telnet or SSH to the IDSM2 maintenance partition.You must session to it from the switch CLI.

Step 5 Log in as user **guest** and password **cisco**.

Note You can change the guest password, but we do not recommend it. If you forget the maintenance partition guest password, and you cannot log in to the IDSM2 application partition for some reason, the IDSM2 requires an RMA.

```
login: guest
Password: cisco

Maintenance image version: 2.1(2)

guest@idsm2.localdomain#
```

Step 6 View the IDSM2 maintenance partition host configuration.

```
guest@idsm2.localdomain# show ip

IP address      : 10.89.149.74
Subnet Mask     : 255.255.255.128
IP Broadcast    : 10.255.255.255
DNS Name        : idsm2.localdomain
Default Gateway : 10.89.149.126
Nameserver(s)   :

guest@idsm2.localdomain#
```

Step 7 Clear the IDSM2 maintenance partition host configuration (ip address, gateway, hostname).

```
guest@idsm2.localdomain# clear ip
guest@localhost.localdomain# show ip

IP address      : 0.0.0.0
Subnet Mask     : 0.0.0.0
IP Broadcast    : 0.0.0.0
DNS Name        : localhost.localdomain
Default Gateway : 0.0.0.0
Nameserver(s)   :

guest@localhost.localdomain#
```

Step 8 Configure the maintenance partition host configuration.

a. Specify the IP address.

```
guest@localhost.localdomain# ip address ip_address netmask
```

b. Specify the default gateway.

```
guest@localhost.localdomain# ip gateway gateway_ip_address
```

c. Specify the hostname.

```
guest@localhost.localdomain# ip host hostname
```

Step 9 View the maintenance partition host configuration.

```
guest@idsm2.localdomain# show ip

IP address      : 10.89.149.74
Subnet Mask     : 255.255.255.128
IP Broadcast    : 10.255.255.255
DNS Name        : idsm2.localdomain
Default Gateway : 10.89.149.126
Nameserver(s)   :

guest@idsm2.localdomain#
```

Step 10 Verify the image installed on the application partition.

```
guest@idsm2.localdomain# show images
Device name             Partition#              Image name
-----------             ----------               ----------
```

```
Hard disk(hdd)          1                       6.1(1)
guest@idsm2.localdomain#
```

Step 11 Verify the maintenance partition version (including the BIOS version).

```
guest@idsm2.localdomain# show version

Maintenance image version: 2.1(2)
mp.2-1-2.bin : Thu Nov 18 11:41:36 PST 2004 :
integ@kplus-build-lx.cisco.com

Line Card Number :WS-SVC-IDSM2-XL
Number of Pentium-class Processors : 2
BIOS Vendor: Phoenix Technologies Ltd.
BIOS Version: 4.0-Rel 6.0.9

Total available memory: 2012 MB
Size of compact flash: 61 MB
Size of hard disk: 19077 MB
Daughter Card Info: Falcon rev 3, FW ver 2.0.3.0 (IDS), SRAM  8 MB, SDRAM  256 MB

guest@idsm2.localdomain#
```

Step 12 Upgrade the application partition.

```
guest@idsm2.localdomain# upgrade
ftp://jsmith@10.89.146.11//RELEASES/Latest/6.2-1/WS-SVC-IDSM2-K9-sys-1.1-a-6.1-1.190-E0.
1.bin.gz
Downloading the image. This may take several minutes...
Password for jsmith@10.89.146.114:
500 'IPS-IDSM2-K9-sys-1.1-a-6.2-1-E3.bin.gz': command not understood.

ftp://jsmith@10.89.146.11//RELEASES/Latest/6.2-1/IPS-IDSM2-K9-sys-1.1-a-6.2-1-E3.bin.gz
(unknown size)
/tmp/upgrade.gz           [|]   28616K
29303086 bytes transferred in 5.34 sec (5359.02k/sec)

Upgrade file
ftp://jsmith@10.89.146.114//RELEASES/Latest/6.2-1/IPS-IDSM2-K9-sys-1.1-a-6.2-1-E3.bin.gz
is downloaded.
Upgrading will wipe out the contents on the storage media.
Do you want to proceed installing it [y|N]:
```

Step 13 Enter **y** to proceed with the upgrade.

```
Proceeding with upgrade. Please do not interrupt.
If the upgrade is interrupted or fails, boot into maintenance image again and restart
upgrade.

Creating IDS application image file...

Initializing the hard disk...
Applying the image, this process may take several minutes...
Performing post install, please wait...
Application image upgrade complete. You can boot the image now.
guest@idsm3.localdomain#
```

Step 14 Display the upgrade log.

```
guest@idsm3.localdomain# show log upgrade

Upgrading the line card on Fri Mar 11 21:21:53 UTC 2005
Downloaded upgrade image
ftp://jsmith@10.89.146.114//RELEASES/Latest/6.2-1/WS-SVC-IDSM2-K9-sys-1.1-a-6.2-1-E3.bin.g
z
```

```
Extracted the downloaded file
Proceeding with image upgrade.
Fri Mar 11 21:22:06 2005 : argv1 = 0, argv2 = 0, argv3 = 3, argv4 = 1
Fri Mar 11 21:22:06 2005 : Creating IDS application image file...
Fri Mar 11 21:22:06 2005 : footer: XXXXXXXXXXXXXXXX
Fri Mar 11 21:22:06 2005 : exeoff: 0000000000031729
Fri Mar 11 21:22:06 2005 : image: 0000000029323770
Fri Mar 11 21:22:06 2005 : T: 29323818, E: 31729, I: 29323770
Fri Mar 11 21:22:07 2005 : partition: /dev/hdc1
Fri Mar 11 21:22:07 2005 : startIDSAppUpgrade:Image: /tmp/cdisk.gz
Fri Mar 11 21:22:07 2005 : startIDSAppUpgrade:Device: /dev/hdc1
Fri Mar 11 21:22:07 2005 : startIDSAppUpgrade:Install type: 1
Fri Mar 11 21:22:07 2005 : Initializing the hard disk...
Fri Mar 11 21:22:07 2005 : Required disk size: 524288 Kb (blocks)
Fri Mar 11 21:22:07 2005 : Available disk size: 19535040 Kb (blocks)
Fri Mar 11 21:22:13 2005 : Partitions created on '/dev/hdc'.
Fri Mar 11 21:22:13 2005 : Device '/dev/hdc' verified for OK.
Fri Mar 11 21:22:19 2005 : Created ext2 fileSystem on '/dev/hdc1'.
Fri Mar 11 21:22:19 2005 : Directory '/mnt/hd/' created.
Fri Mar 11 21:22:19 2005 : Partition '/dev/hdc1' mounted.
Fri Mar 11 21:22:19 2005 : Finished initializing the hard disk.
Fri Mar 11 21:22:19 2005 : Applying the image, this process may take several minutes...
Fri Mar 11 21:22:19 2005 : Directory changed to '/mnt/hd'.
Fri Mar 11 21:22:20 2005 : Performing post install, please wait...
Fri Mar 11 21:22:20 2005 : File /mnt/hd/post-install copied to /tmp/post-install.
Fri Mar 11 21:22:20 2005 : Directory changed to '/tmp'.
Fri Mar 11 21:22:28 2005 : Partition '/dev/hdc1' unmounted.
Fri Mar 11 21:22:28 2005 : Directory changed to '/tmp'.
Application image upgrade complete. You can boot the image now.
Partition upgraded successfully
guest@idsm2.localdomain#
```

Step 15 Clear the upgrade log.

```
guest@idsm2.localdomain# clear log upgrade
Cleared log file successfully
```

Step 16 Display the upgrade log.

```
guest@idsm2.localdomain# show log upgrade
guest@idsm2.localdomain#
```

Step 17 Ping another computer.

```
guest@idsm2.localdomain# ping 10.89.146.114
PING 10.89.146.114 (10.89.146.114) from 10.89.149.74 : 56(84) bytes of data.
64 bytes from 10.89.146.114: icmp_seq=0 ttl=254 time=381 usec
64 bytes from 10.89.146.114: icmp_seq=1 ttl=254 time=133 usec
64 bytes from 10.89.146.114: icmp_seq=2 ttl=254 time=129 usec
64 bytes from 10.89.146.114: icmp_seq=3 ttl=254 time=141 usec
64 bytes from 10.89.146.114: icmp_seq=4 ttl=254 time=127 usec

--- 10.89.146.114 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/mdev = 0.127/0.182/0.381/0.099 ms
guest@idsm2.localdomain#
```

Step 18 Reset the IDSM2.

Note You cannot specify a partition when issuing the **reset** command from the maintenance partition. The IDSM2 boots to whichever partition is specified in the boot device variable. If the boot device variable is blank, the IDSM2 boots to the application partition.

```
guest@idsm2.localdomain# reset
guest@idsm2.localdomain#
2005 Mar 11 21:55:46 CST -06:00 %SYS-4-MOD_SHUTDOWNSTART:Module 9 shutdown in progress. Do
not remove module until shutdown completes

Broadcast message from root Fri Mar 11 21:55:47 2005...

The system is going down for system halt NOW !!
console> (enable)#
```

For More Information

For a list of supported FTP and HTTP/HTTPS servers, see Supported FTP and HTTP/HTTPS Servers, page 12-2.

Configuring the IDSM2 Maintenance Partition for Cisco IOS Software

To configure the IDSM2 maintenance partition, follow these steps:

Step 1 Log in to the switch CLI.

Step 2 Session to the IDSM2.

```
router# session slot 11 processor 1
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.111 ... Open

Cisco Maintenance image
```

Note You cannot Telnet or SSH to the IDSM2 maintenance partition.You must session to it from the switch CLI.

Step 3 Log in as user **guest** and password **cisco**.

Note You can change the guest password, but we do not recommend it. If you forget the maintenance partition guest password, and you cannot log in to the IDSM2 application partition for some reason, you will have to RMA the IDSM2.

```
login: guest
password: cisco

Maintenance image version: 2.1(2)

guest@idsm2.localdomain#
```

Step 4 View the maintenance partition host configuration.

```
guest@idsm2.localdomain# show ip

IP address      : 10.89.149.74
Subnet Mask     : 255.255.255.128
IP Broadcast    : 10.255.255.255
DNS Name        : idsm2.localdomain
Default Gateway : 10.89.149.126
```

```
Nameserver(s)   :

guest@idsm2.localdomain#
```

Step 5 Clear the maintenance partition host configuration (ip address, gateway, hostname).

```
guest@idsm2.localdomain# clear ip
guest@localhost.localdomain# show ip

IP address      : 0.0.0.0
Subnet Mask     : 0.0.0.0
IP Broadcast    : 0.0.0.0
DNS Name        : localhost.localdomain
Default Gateway : 0.0.0.0
Nameserver(s)   :

guest@localhost.localdomain#
```

Step 6 Configure the maintenance partition host configuration.

a. Specify the IP address.

```
guest@localhost.localdomain# ip address ip_address netmask
```

b. Specify the default gateway.

```
guest@localhost.localdomain# ip gateway gateway_ip_address
```

c. Specify the hostname.

```
guest@localhost.localdomain# ip host hostname
```

Step 7 View the maintenance partition host configuration.

```
guest@idsm2.localdomain# show ip

IP address      : 10.89.149.74
Subnet Mask     : 255.255.255.128
IP Broadcast    : 10.255.255.255
DNS Name        : idsm2.localdomain
Default Gateway : 10.89.149.126
Nameserver(s)   :

guest@idsm2.localdomain#
```

Step 8 Verify the image installed on the application partition.

```
guest@idsm2.localdomain# show images
Device name             Partition#              Image name
-----------             ----------               ----------
Hard disk(hdd)          1                       6.1(1)
guest@idsm2.localdomain#
```

Step 9 Verify the maintenance partition version (including the BIOS version).

```
guest@idsm2.localdomain# show version

Maintenance image version: 2.1(2)
mp.2-1-2.bin : Thu Nov 18 11:41:36 PST 2004 :
integ@kplus-build-lx.cisco.com

Line Card Number :WS-SVC-IDSM2-XL
Number of Pentium-class Processors : 2
BIOS Vendor: Phoenix Technologies Ltd.
BIOS Version: 4.0-Rel 6.0.9
```

```
Total available memory: 2012 MB
Size of compact flash: 61 MB
Size of hard disk: 19077 MB
Daughter Card Info: Falcon rev 3, FW ver 2.0.3.0 (IDS), SRAM  8 MB, SDRAM  256 MB

guest@idsm2.localdomain#
```

Step 10 Upgrade the application partition.

```
guest@idsm2.localdomain# upgrade
ftp://jsmith@10.89.146.11//RELEASES/Latest/6.2-1/IPS-IDSM2-K9-sys-1.1-a-6.2-1-E3.img
Downloading the image. This may take several minutes...
Password for jsmith@10.89.146.114:
500 'SIZE IPS-IDSM2-K9-sys-1.1-a-6.2-1.bin.gz': command not understood.

ftp://jsmith@10.89.146.11//RELEASES/Latest/6.1-1/IPS-IDSM2-K9-sys-1.1-a-6.2-1-E3.img
(unknown size)
/tmp/upgrade.gz           [|]   28616K
29303086 bytes transferred in 5.34 sec (5359.02k/sec)

Upgrade file
ftp://jsmith@10.89.146.114//RELEASES/Latest/6.2-1/IPS-IDSM2-K9-sys-1.1-a-6.2-1-E3.img is
downloaded.
Upgrading will wipe out the contents on the storage media.
Do you want to proceed installing it [y|N]:
```

Step 11 Enter **y** to proceed with the upgrade.

```
Proceeding with upgrade. Please do not interrupt.
If the upgrade is interrupted or fails, boot into maintenance image again and restart
upgrade.

Creating IDS application image file...

Initializing the hard disk...
Applying the image, this process may take several minutes...
Performing post install, please wait...
Application image upgrade complete. You can boot the image now.
guest@idsm3.localdomain#
```

Step 12 Display the upgrade log.

```
guest@idsm3.localdomain# show log upgrade

Upgrading the line card on Fri Mar 11 21:21:53 UTC 2005
Downloaded upgrade image
ftp://jsmith@10.89.146.114//RELEASES/Latest/6.2-1/IPS-IDSM2-K9-sys-1.1-a-6.2-1-E3.img
Extracted the downloaded file
Proceeding with image upgrade.
Fri Mar 11 21:22:06 2005 : argv1 = 0, argv2 = 0, argv3 = 3, argv4 = 1
Fri Mar 11 21:22:06 2005 : Creating IDS application image file...
Fri Mar 11 21:22:06 2005 : footer: XXXXXXXXXXXXXXXX
Fri Mar 11 21:22:06 2005 : exeoff: 0000000000031729
Fri Mar 11 21:22:06 2005 : image: 0000000029323770
Fri Mar 11 21:22:06 2005 : T: 29323818, E: 31729, I: 29323770
Fri Mar 11 21:22:07 2005 : partition: /dev/hdc1
Fri Mar 11 21:22:07 2005 : startIDSAppUpgrade:Image: /tmp/cdisk.gz
Fri Mar 11 21:22:07 2005 : startIDSAppUpgrade:Device: /dev/hdc1
Fri Mar 11 21:22:07 2005 : startIDSAppUpgrade:Install type: 1
Fri Mar 11 21:22:07 2005 : Initializing the hard disk...
Fri Mar 11 21:22:07 2005 : Required disk size: 524288 Kb (blocks)
Fri Mar 11 21:22:07 2005 : Available disk size: 19535040 Kb (blocks)
Fri Mar 11 21:22:13 2005 : Partitions created on '/dev/hdc'.
Fri Mar 11 21:22:13 2005 : Device '/dev/hdc' verified for OK.
Fri Mar 11 21:22:19 2005 : Created ext2 fileSystem on '/dev/hdc1'.
```

```
Fri Mar 11 21:22:19 2005 : Directory '/mnt/hd/' created.
Fri Mar 11 21:22:19 2005 : Partition '/dev/hdc1' mounted.
Fri Mar 11 21:22:19 2005 : Finished initializing the hard disk.
Fri Mar 11 21:22:19 2005 : Applying the image, this process may take several minutes...
Fri Mar 11 21:22:19 2005 : Directory changed to '/mnt/hd'.
Fri Mar 11 21:22:20 2005 : Performing post install, please wait...
Fri Mar 11 21:22:20 2005 : File /mnt/hd/post-install copied to /tmp/post-install.
Fri Mar 11 21:22:20 2005 : Directory changed to '/tmp'.
Fri Mar 11 21:22:28 2005 : Partition '/dev/hdc1' unmounted.
Fri Mar 11 21:22:28 2005 : Directory changed to '/tmp'.
Application image upgrade complete. You can boot the image now.
Partition upgraded successfully
guest@idsm2.localdomain#
```

Step 13 Clear the upgrade log.

```
guest@idsm2.localdomain# clear log upgrade
Cleared log file successfully
```

Step 14 Display the upgrade log.

```
guest@idsm2.localdomain# show log upgrade
guest@idsm2.localdomain#
```

Step 15 Ping another computer.

```
guest@idsm2.localdomain# ping 10.89.146.114
PING 10.89.146.114 (10.89.146.114) from 10.89.149.74 : 56(84) bytes of data.
64 bytes from 10.89.146.114: icmp_seq=0 ttl=254 time=381 usec
64 bytes from 10.89.146.114: icmp_seq=1 ttl=254 time=133 usec
64 bytes from 10.89.146.114: icmp_seq=2 ttl=254 time=129 usec
64 bytes from 10.89.146.114: icmp_seq=3 ttl=254 time=141 usec
64 bytes from 10.89.146.114: icmp_seq=4 ttl=254 time=127 usec

--- 10.89.146.114 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/mdev = 0.127/0.182/0.381/0.099 ms
guest@idsm2.localdomain#
```

Step 16 Reset the IDSM2.

Note You cannot specify a partition when issuing the **reset** command from the maintenance partition. The IDSM2 boots to whichever partition is specified in the boot device variable. If the boot device variable is blank, the IDSM2 boots to the application partition.

```
guest@idsm2.localdomain# reset
guest@idsm2.localdomain#
Broadcast message from root Fri Mar 11 22:04:53 2005...

The system is going down for system halt NOW !!

[Connection to 127.0.0.111 closed by foreign host]
router#
```

For More Information

For a list of supported FTP and HTTP/HTTPS servers, see Supported FTP and HTTP/HTTPS Servers, page 12-2.

Upgrading the IDSM2 Maintenance Partition for Catalyst Software

To upgrade the maintenance partition, follow these steps:

Step 1 Download the IDSM2 maintenance partition file (c6svc-mp.2-1-2.bin.gz) to the FTP root directory of an FTP server that is accessible from your IDSM2.

Step 2 Session to the IDSM2 from the switch.

```
console>(enable) session slot_number
```

Step 3 Log in to the IDSM2 CLI.

Step 4 Enter configuration mode.

```
idsm2# configure terminal
```

Step 5 Upgrade the maintenance partition. You are asked whether you want continue.

```
idsm2(config)# upgrade
ftp://user@ftp_server_IP_address/directory_path/c6svc-mp.2-1-2.bin.gz
```

Step 6 Enter the FTP server password.

Step 7 Enter **y** to continue. The maintenance partition file is upgraded.

For More Information

- For a list of supported FTP and HTTP/HTTPS servers, see Supported FTP and HTTP/HTTPS Servers, page 12-2.
- For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software, page 11-1.

Upgrading the IDSM2 Maintenance Partition for Cisco IOS Software

To upgrade the maintenance partition, follow these steps:

Step 1 Download the IDSM2 maintenance partition file (c6svc-mp.2-1-2.bin.gz) to the FTP root directory of an FTP server that is accessible from your IDSM2.

Step 2 Log in to the switch CLI.

Step 3 Session in to the application partition CLI.

```
router# session slot slot_number processor 1
```

Step 4 Log in to the IDSM2.

Step 5 Enter configuration mode.

```
idsm2# configure terminal
```

Step 6 Upgrade the maintenance partition.

```
idsm2(config)# upgrade
ftp://user@ftp_server_IP_address/directory_path/c6svc-mp.2-1-2.bin.gz
```

Step 7 Specify the FTP server password.

```
Password: ********
```

You are prompted to continue.

```
Continue with upgrade?:
```

Step 8 Enter **yes** to continue.

For More Information

- For a list of supported FTP and HTTP/HTTPS servers, see Supported FTP and HTTP/HTTPS Servers, page 12-2.
- For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software, page 11-1.

Installing the NME IPS System Image

Note Use the **show configuration | include interface ids-sensor** command to determine the NME IPS slot number.

To install the NME IPS system image, follow these steps:

Step 1 Download the NME IPS system image file (IPS-NME-K9-sys-1.1-7.0-1-E3.img), and place it on a TFTP server relative to the tftp root directory.

Note Make sure the network is configured so that the NME IPS can access the TFTP server.

If no TFTP server is available, you can configure the router to operate as a TFTP server.

```
router# copy tftp: flash:
router# configure terminal
router(config)# tftp-server flash:IPS-NME-K9-sys-1.1-7.0-1-E3.img
router(config)# exit
router#
```

Step 2 Disable the heartbeat reset.

```
router# service-module ids-sensor 1/0 heartbeat-reset disable
```

Note Disabling the heartbeat reset prevents the router from resetting the module during system image installation if the process takes too long.

Step 3 Session to the NME IPS.

```
router# service-module ids-sensor 1/0 session
```

Step 4 Suspend the session by pressing **Shift-Ctrl-6 X**. You should see the `router#` prompt. If you do not see this prompt, try **Ctrl-6 X**.

Step 5 Reset the NME IPS. You are prompted to confirm the **reset** command.

```
router# service-module ids-sensor 1/0 reset
```

Step 6 Press **Enter** to confirm.

Step 7 Press **Enter** to resume the suspended session. After displaying its version, the bootloader displays this prompt for 15 seconds.

```
Please enter '***' to change boot configuration:
```

Step 8 Enter ******* during the 15-second delay. The bootloader prompt appears.

Step 9 Press **Enter** to session back to the NME IPS.

Step 10 Configure the bootloader.

```
ServicesEngine bootloader> config

IP Address [10.89.148.195]>
Subnet mask [255.255.255.0]>
TFTP server [10.89.150.74]>
Gateway [10.89.148.254]>
Default boot [disk]>
Number cores [2]>
ServicesEngine boot-loader >
```

For each prompt, enter a value or accept the previously stored input that appears inside square brackets by pressing **Enter**.

Caution The pathname for the NME IPS image is full but relative to the tftp server root directory (typically /tftpboot).

Step 11 Start the bootloader.

```
ServicesEngine bootloader> upgrade
```

Step 12 Follow the bootloader instructions to install the software (choose option 1 and follow the wizard instructions).

Example

```
Booting from flash...please wait.
Please enter '***' to change boot configuration:
12 ***
ServicesEngine boot-loader Version : 1.2.0
ServicesEngine boot-loader > config

IP Address [10.89.148.195]>
Subnet mask [255.255.255.0]>
TFTP server [10.89.150.74]>
Gateway [10.89.148.254]>
Default boot [disk]>
Number cores [2]>
ServicesEngine boot-loader > upgrade

Cisco Systems, Inc.
Services engine upgrade utility for NM-IPS
-----
Main menu
1 - Download application image and write to USB Drive
2 - Download bootloader and write to flash
3 - Download minikernel and write to flash
r - Exit and reset card
x - Exit
Selection [123rx]
Download recovery image via tftp and install on USB Drive
TFTP server [10.89.150.74]>
full pathname of recovery image
```

```
[]:test/sensor/6.1-1-E2/IPS-NME-K9-sys-1.1-a-7.0-1-E3.img
Ready to begin
Are you sure [Y/N]
Press <CTRL-C> to abort.
octeth0:        Up     1Gbs Full duplex, (port  0)
octeth1:        Up     1Gbs Full duplex, (port  1)
Using octeth0 device
TFTP from server 10.89.150.74; our IP address is 10.89.148.195; sending through gateway
10.89.148.254
Filename 'test/sensor/6.1-1-E2/IPS-NME-K9-sys-1.1-a-7.0-1-E3.img'.
Load address: 0x21000000
Loading: octeth0: Down   1Gbs Half duplex, (port  0)
octeth0: Down   1Gbs Full duplex, (port  0)
octeth0: Up     1Gbs Full duplex, (port  0)
T T T T T T T T T ##################################################################
         ##################################################################
         ##################################################################
         ##################################################################
         ##################################################################
         ##################################################################
         ##################################################################
         ##################################################################
         ##################################################################
         ##################################################################
         ######
         32 MB received
         ##################################################################
         ##################################################################
         ##################
done
```

Step 13 Suspend the session by pressing **Shift-Ctrl-6 X**. You should see the `router#` prompt. If you do not see this prompt, try **Ctrl-6 X**.

Step 14 From the router CLI, clear the session.

```
router# service-module interface ids-sensor 1/0 session clear
```

Step 15 Enable the heartbeat reset.

```
router# service-module IDS-sensor 1/0 heartbeat-reset enable
```

CHAPTER A

Troubleshooting

This appendix contains troubleshooting tips and procedures for sensors and software. It contains the following sections:

Bug Toolkit

For the most complete and up-to-date list of caveats, use the Bug Toolkit to refer to the caveat release note. You can use the Bug Toolkit to search for known bugs based on software version, feature set, and keywords. The resulting matrix shows when each bug was integrated, or fixed if applicable. It also lets you save the results of a search in Bug Groups, and also create persistent Alert Agents that can feed those groups with new defect alerts.

Note You must be logged in to Cisco.com to access the Bug Toolkit.

If you are a registered Cisco.com user, you can view the Bug Toolkit at this URL:

http://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs

To become a registered cisco.com user, go to this URL:

http://tools.cisco.com/RPF/register/register.do

Preventive Maintenance

This section describes how to perform preventive maintenance for your sensor, and contains the following topics:

Understanding Preventive Maintenance

The following actions will help you maintain your sensor:

- Back up a good configuration. If your current configuration becomes unusable, you can replace it with the backup version.
- Save your backup configuration to a remote system.
- Always back up your configuration before you do a manual upgrade. If you have auto upgrades configured, make sure you do periodic backups.
- Create a service account.

  A service account is needed for special debug situations directed by TAC.

Caution You should carefully consider whether you want to create a service account. The service account provides shell access to the system, which makes the system vulnerable. Analyze your situation to decide if you want a service account existing on the system.

For More Information

- For the procedure for backing up a configuration file, see Creating and Using a Backup Configuration File, page A-3.
- For the procedure for using a remote server to copy and restore the a configuration file, see Backing Up and Restoring the Configuration File Using a Remote Server, page A-3.
- For more information about the service account, see Creating the Service Account, page A-5.

Creating and Using a Backup Configuration File

To protect your configuration, you can back up the current configuration and then display it to confirm that is the configuration you want to save. If you need to restore this configuration, you can merge the backup configuration file with the current configuration or overwrite the current configuration file with the backup configuration file.

To back up your current configuration, follow these steps:

Step 1 Log in to the CLI using an account with administrator privileges.

Step 2 Save the current configuration.

```
sensor# copy current-config backup-config
```

The current configuration is saved in a backup file.

Step 3 Display the backup configuration file.

```
sensor# more backup-config
```

The backup configuration file is displayed.

Step 4 You can either merge the backup configuration with the current configuration, or you can overwrite the current configuration.

- Merge the backup configuration into the current configuration.

  ```
  sensor# copy backup-config current-config
  ```

- Overwrite the current configuration with the backup configuration.

  ```
  sensor# copy /erase backup-config current-config
  ```

Backing Up and Restoring the Configuration File Using a Remote Server

Note We recommend copying the current configuration file to a remote server before upgrading.

Use the **copy** [**/erase**] *source_url destination_url keyword* command to copy the configuration file to a remote server. You can then restore the current configuration from the remote server. You are prompted to back up the current configuration first.

Options

The following options apply:

- **/erase**—Erases the destination file before copying.

  This keyword only applies to the current-config; the backup-config is always overwritten. If this keyword is specified for destination current-config, the source configuration is applied to the system default configuration. If it is not specified for the destination current-config, the source configuration is merged with the current-config.

- *source_url*—The location of the source file to be copied. It can be a URL or keyword.
- *destination_url*—The location of the destination file to be copied. It can be a URL or a keyword.

- **current-config**—The current running configuration. The configuration becomes persistent as the commands are entered.
- **backup-config**—The storage location for the configuration backup.

The exact format of the source and destination URLs varies according to the file. Here are the valid types:

- ftp:—Source or destination URL for an FTP network server. The syntax for this prefix is:

  ftp:[//[username@] location]/relativeDirectory]/filename

  ftp:[//[username@]location]//absoluteDirectory]/filename
- scp:—Source or destination URL for the SCP network server. The syntax for this prefix is:

  scp:[//[username@] location]/relativeDirectory]/filename

  scp:[//[username@] location]//absoluteDirectory]/filename

Note If you use FTP or SCP protocol, you are prompted for a password. If you use SCP protocol, you must also add the remote host to the SSH known hosts list.

- http:—Source URL for the web server. The syntax for this prefix is:

  http:[[/[username@]location]/directory]/filename
- https:—Source URL for the web server. The syntax for this prefix is:

  https:[[/[username@]location]/directory]/filename

Note HTTP and HTTPS prompt for a password if a username is required to access the website. If you use HTTPS protocol, the remote host must be a TLS trusted host.

Caution Copying a configuration file from another sensor may result in errors if the sensing interfaces and virtual sensors are not configured the same.

Backing Up the Current Configuration to a Remote Server

To back up your current configuration to a remote server, follow these steps:

Step 1 Log in to the CLI using an account with administrator privileges.

Step 2 Back up the current configuration to the remote server.

```
sensor# copy current-config scp://user@192.0.2.0//configuration/cfg current-config
Password: ********
Warning: Copying over the current configuration may leave the box in an unstable state.
Would you like to copy current-config to backup-config before proceeding? [yes]:
```

Step 3 Enter **yes** to copy the current configuration to a backup configuration.

```
cfg           100% |***********************************************| 36124       00:00
```

Restoring the Current Configuration From a Backup File

To restore your current configuration from a backup file, follow these steps:

Step 1 Log in to the CLI using an account with administrator privileges.

Step 2 Back up the current configuration to the remote server.

```
sensor# copy scp://user@192.0.2.0//configuration/cfg current-config
Password: ********
Warning: Copying over the current configuration may leave the box in an unstable state.
Would you like to copy current-config to backup-config before proceeding? [yes]:
```

Step 3 Enter **yes** to copy the current configuration to a backup configuration.

```
cfg            100% |***********************************************| 36124       00:00

Warning: Replacing existing network-settings may leave the box in an unstable state.
Would you like to replace existing network settings
(host-ipaddress/netmask/gateway/access-list) on sensor before proceeding? [no]:
sensor#
```

Step 4 Enter **no** to retain the currently configured hostname, IP address, subnet mask, management interface, and access list. We recommend you retain this information to preserve access to your sensor after the rest of the configuration has been restored.

For More Information

For a list of supported HTTP/HTTPS servers, see Supported FTP and HTTP/HTTPS Servers, page 12-2.

Creating the Service Account

Caution Do not make modifications to the sensor through the service account except under the direction of TAC. If you use the service account to configure the sensor, your configuration is not supported by TAC. Adding services to the operating system through the service account affects proper performance and functioning of the other IPS services. TAC does not support a sensor on which additional services have been added.

You can create a service account for TAC to use during troubleshooting. Although more than one user can have access to the sensor, only one user can have service privileges on a sensor. The service account is for support purposes only.

Note The root user password is synchronized to the service account password when the service account is created. To gain root access you must log in with the service account and switch to user root with the **su - root** command.

Caution You should carefully consider whether you want to create a service account. The service account provides shell access to the system, which makes the system vulnerable. However, you can use the service account to create a password if the administrator password is lost. Analyze your situation to decide if you want a service account existing on the system.

Note For IPS 5.0 and later, you can no longer remove the **cisco** account. You can disable it using the **no password cisco** command, but you cannot remove it. To use the **no password cisco** command, there must be another administrator account on the sensor. Removing the **cisco** account through the service account is not supported. If you remove the **cisco** account through the service account, the sensor most likely will not boot up, so to recover the sensor you must reinstall the sensor system image.

To create the service account, follow these steps:

Step 1 Log in to the CLI using an account with administrator privileges.

Step 2 Enter configuration mode.

```
sensor# configure terminal
```

Step 3 Specify the parameters for the service account.

```
sensor(config)# user username privilege service
```

A valid username contains 1 to 64 alphanumeric characters. You can also use an underscore (_) or dash (-) in the username.

Step 4 Specify a password when prompted. If a service account already exists for this sensor, the following error is displayed and no service account is created.

```
Error: Only one service account may exist
```

Step 5 Exit configuration mode.

```
sensor(config)# exit
sensor#
```

When you use the service account to log in to the CLI, you receive this warning.

```
************************ WARNING ****************************************************
UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. This account is intended to be
used for support and troubleshooting purposes only. Unauthorized modifications are not
supported and will require this device to be reimaged to guarantee proper operation.
*****************************************************************************************
```

Disaster Recovery

This section provides recommendations and steps to take if you need to recover your sensor after a disaster.

Follow these recommendations so that you are ready in case of a disaster:

- If you are using the CLI, IDM, or IME for configuration, copy the current configuration from the sensor to an FTP or SCP server any time a change has been made.
- You should note the specific software version for that configuration. You can apply the copied configuration only to a sensor of the same version.
- You also need the list of user IDs that have been used on that sensor. The list of user IDs and passwords are not saved in the configuration.

When a disaster happens and you need to recover the sensor, try the following:

1. Reimage the sensor.
2. Log in to the sensor with the default user ID and password—**cisco**.

   Note You are prompted to change the **cisco** password.

3. Initialize the sensor.
4. Upgrade the sensor to the IPS software version it had when the configuration was last saved and copied.

Warning **Trying to copy the saved configuration without getting the sensor back to the same IPS software version it had before the disaster can cause configuration errors.**

5. Copy the last saved configuration to the sensor.
6. Update clients to use the new key and certificate of the sensor.

   Reimaging changes the sensor SSH keys and HTTPS certificate, so you must add the hosts back to the SSN known hosts list.

7. Create previous users.

For More Information

- For the procedure for backing up a configuration file, see Creating and Using a Backup Configuration File, page A-3.
- For the procedures for reimagine a sensor, see Chapter 12, "Upgrading, Downgrading, and Installing System Images."
- For the procedure for using the **setup** command to initialize the sensor, see Chapter 10, "Initializing the Sensor."
- For more information on obtaining IPS software and how to install it, see Obtaining Cisco IPS Software, page 11-1.
- For the procedure for using a remote server to copy and restore the a configuration file, see Backing Up and Restoring the Configuration File Using a Remote Server, page A-3.
- For the procedure for adding hosts to the SSH known hosts list, refer to Adding Hosts to the SSH Known Hosts Lists.
- For the procedure for adding users and obtaining a list of the current users on the sensor, refer to Configuring User Parameters.

Recovering the Password

For most IPS platforms, you can now recover the password on the sensor rather than using the service account or reimaging the sensor. This section describes how to recover the password for the various IPS platforms. It contains the following topics:

Understanding Password Recovery

Password recovery implementations vary according to IPS platform requirements. Password recovery is implemented only for the cisco administrative account and is enabled by default. The IPS administrator can then recover user passwords for other accounts using the CLI. The cisco user password reverts to **cisco** and must be changed after the next login.

Note Administrators may need to disable the password recovery feature for security reasons.

Table A-1 lists the password recovery methods according to platform.

Table A-1 Password Recovery Methods According to Platform

Platform	Description	Recovery Method
4200 series sensors	Standalone IPS appliances	GRUB prompt or ROMMON
AIM IPS NME IPS	Router IPS modules	Bootloader command
AIP SSM	ASA 5500 series adaptive security appliance modules	adaptive security appliance CLI command
IDSM2	Switch IPS module	Password recovery image file

Recovering the Appliance Password

This section describes the two ways to recover the password for appliances. It contains the following topics:

- Using the GRUB Menu, page A-8
- Using ROMMON, page A-9

Using the GRUB Menu

For the 4200 series appliances, the password recovery is found in the GRUB menu, which appears during bootup. When the GRUB menu appears, press any key to pause the boot process.

Note You must have a terminal server or direct serial connection to the appliance to use the GRUB menu to recover the password.

To recover the password on appliances, follow these steps:

Step 1 Reboot the appliance to see the GRUB menu.

```
GNU GRUB version 0.94 (632K lower / 523264K upper memory)
-------------------------------------------
0: Cisco IPS
1: Cisco IPS Recovery
2: Cisco IPS Clear Password (cisco)
-------------------------------------------

    Use the ^ and v keys to select which entry is highlighted.
    Press enter to boot the selected OS, 'e' to edit the
    Commands before booting, or 'c' for a command-line.

    Highlighted entry is 0:
```

Step 2 Press any key to pause the boot process.

Step 3 Choose **`2: Cisco IPS Clear Password (cisco)`**. The password is reset to **cisco**. You can change the password the next time you log in to the CLI.

Using ROMMON

For the IPS 4240 and the IPS 4255 you can use the ROMMON to recover the password. To access the ROMMON CLI, reboot the sensor from a terminal server or direct connection and interrupt the boot process.

To recover the password using the ROMMON CLI, follow these steps:

Step 1 Reboot the appliance.

Step 2 To interrupt the boot process, press **ESC** or **Control-R** (terminal server) or send a **BREAK** command (direct connection).

The boot code either pauses for 10 seconds or displays something similar to one of the following:

- `Evaluating boot options`
- `Use BREAK or ESC to interrupt boot`

Step 3 Enter the following commands to reset the password.

```
confreg 0x7
boot
```

Sample ROMMON session:

```
Booting system, please wait...
CISCO SYSTEMS
Embedded BIOS Version 1.0(11)2 01/25/06 13:21:26.17
...
Evaluating BIOS Options...
Launch BIOS Extension to setup ROMMON
Cisco Systems ROMMON Version (1.0(11)2) #0: Thu Jan 26 10:43:08 PST 2006
Platform IPS 4240-K9
Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot interrupted.
Management0/0
Link is UP
```

```
MAC Address:000b.fcfa.d155
Use ? for help.
rommon #0> confreg 0x7
Update Config Register (0x7) in NVRAM...
rommon #1> boot
```

Recovering the AIM IPS Password

To recover the password for the AIM IPS, use the **clear password** command. You must have console access to the AIM IPS and administrative access to the router. To recover the password for the AIM IPS, follow these steps:

Step 1 Log in to the router.

Step 2 Enter privileged EXEC mode on the router.

```
router> enable
```

Step 3 Confirm the module slot number in your router.

```
router# show run | include ids-sensor
interface IDS-Sensor0/0
router#
```

Step 4 Session in to the AIM IPS.

```
router# service-module ids-sensor slot/port session
```

Example:

```
router# service-module ids-sensor 0/0 session
```

Step 5 Press **Control-shift-6** followed by **x** to navigate to the router CLI.

Step 6 Reset the AIM IPS from the router console.

```
router# service-module ids-sensor 0/0 reset
```

Step 7 Press **Enter** to return to the router console.

Step 8 When prompted for boot options, enter ******* quickly. You are now in the bootloader.

Step 9 Clear the password.

```
ServicesEngine boot-loader# clear password
```

The AIM IPS reboots. The password is reset to **cisco**. Log in to the CLI with username **cisco** and password **cisco**. You can then change the password.

Recovering the AIP SSM Password

You can reset the password to the default (**cisco**) for the AIP SSM using the CLI or the ASDM. Resetting the password causes it to reboot. IPS services are not available during a reboot.

Note To reset the password, you must have ASA 7.2.2 or later.

Use the **hw-module module** *slot_number* **password-reset** command to reset the password to the default **cisco**. If the module in the specified slot has an IPS version that does not support password recovery, the following error message is displayed:

```
ERROR: the module in slot <n> does not support password recovery.
```

Resetting the Password Using the CLI

To reset the password on the AIP SSM, follow these steps:

Step 1 Log into the adaptive security appliance and enter the following command to verify the module slot number:

```
asa# show module
Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  0 ASA 5510 Adaptive Security Appliance         ASA5510            JMX1135L097
  1 ASA 5500 Series Security Services Module-40  ASA-SSM-40         JAF1214AMRL

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  0 001b.d5e8.e0c8 to 001b.d5e8.e0cc  2.0          1.0(11)2     8.4(3)
  1 001e.f737.205f to 001e.f737.205f  1.0          1.0(14)5     7.0(7)E4

Mod SSM Application Name           Status           SSM Application Version
--- ------------------------------ ---------------- --------------------------
  1 IPS                            Up               7.0(7)E4

Mod Status             Data Plane Status     Compatibility
--- ------------------ --------------------- -------------
  0 Up Sys             Not Applicable
  1 Up                 Up
```

Step 2 Reset the password for module 1.

```
asa# hw-module module 1 password-reset
Reset the password on module in slot 1? [confirm]
```

Step 3 Press **Enter** to confirm.

```
Password-Reset issued for slot 1.
```

Step 4 Verify the status of the module. Once the status reads Up, you can session to the AIP SSM.

```
asa# show module 1
Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  1 ASA 5500 Series Security Services Module-40  ASA-SSM-40         JAF1214AMRL

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  1 001e.f737.205f to 001e.f737.205f  1.0          1.0(14)5     7.0(7)E4

Mod SSM Application Name           Status           SSM Application Version
--- ------------------------------ ---------------- --------------------------
  1 IPS                            Up               7.0(7)E4

Mod Status             Data Plane Status     Compatibility
--- ------------------ --------------------- -------------
```

```
  1 Up                 Up
```

Step 5 Session to the AIP SSM.

```
asa# session 1
Opening command session with slot 1.
Connected to slot 1. Escape character sequence is 'CTRL-^X'.
```

Step 6 Enter the default username (**cisco**) and password (**cisco**) at the login prompt.

```
login: cisco
Password: cisco

You are required to change your password immediately (password aged)
Changing password for cisco.
(current) password: cisco
```

Step 7 Enter your new password twice.

```
New password: new password
Retype new password: new password

***NOTICE***
This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco cryptographic
products does not imply third-party authority to import, export, distribute or use
encryption. Importers, exporters, distributors and users are responsible for compliance
with U.S. and local country laws. By using this product you agree to comply with
applicable laws and regulations. If you are unable to comply with U.S. and local laws,
return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to export@cisco.com.

***LICENSE NOTICE***
There is no license key installed on this IPS platform. The system will continue to
operate with the currently installed signature set. A valid license must be obtained in
order to apply signature updates. Please go to http://www.cisco.com/go/license to obtain a
new license or install a license.
aip_ssm#
```

Using the ASDM

To reset the password in the ASDM, follow these steps:

Step 1 From the ASDM menu bar, choose **Tools > IPS Password Reset**.

Note This option does not appear in the menu if there is no IPS present.

Step 2 In the IPS Password Reset confirmation dialog box, click **OK** to reset the password to the default (**cisco**). A dialog box displays the success or failure of the password reset. If the reset fails, make sure you have the correct ASA and IPS software versions.

Step 3 Click **Close** to close the dialog box. The sensor reboots.

Recovering the IDSM2 Password

To recover the password for the IDSM2, you must install a special password recovery image file. This installation only resets the password, all other configuration remains intact. The password recovery image is version-dependent and can be found on the Cisco Download Software site. For IPS 6.*x*, download WS-SVC-IDSM2-K9-a-6.0-password-recovery.bin.gz. For IPS 7.*x*, download WS-SVC-IDSM2-K9-a-7.0-password-recovery.bin.gz.

FTP is the only supported protocol for image installations, so make sure you put the password recovery image file on an FTP server that is accessible to the switch. You must have administrative access to the Cisco 6500 series switch to recover the password on the IDSM2.

During the password recovery image installation, the following message appears:

```
Upgrading will wipe out the contents on the hard disk.
Do you want to proceed installing it [y|n]:
```

This message is in error. Installing the password recovery image does not remove any configuration, it only resets the login account.

Once you have downloaded the password recovery image file, follow the instructions to install the system image file but substitute the password recovery image file for the system image file. The IDSM2 should reboot into the primary partition after installing the recovery image file. If it does not, enter the following command from the switch:

```
hw-module module module_number reset hdd:1
```

Note The password is reset to **cisco**. Log in to the CLI with username **cisco** and password **cisco**. You can then change the password.

For More Information

- For the procedure for installing system images on the IDSM2, see Installing the IDSM2 System Image, page 12-27.
- For more information on downloading Cisco IPS software, see Obtaining Cisco IPS Software, page 11-1.

Recovering the NME IPS Password

To recover the password for the NME IPS, use the **clear password** command. You must have console access to the NME IPS and administrative access to the router. To recover the password for the NME IPS, follow these steps:

Step 1 Log in to the router.

Step 2 Enter privileged EXEC mode on the router.

```
router> enable
```

Step 3 Confirm the module slot number in your router.

```
router# show run | include ids-sensor
interface IDS-Sensor1/0
router#
```

Step 4 Session in to the NME IPS.

```
router# service-module ids-sensor slot/port session
```

Example

```
router# service-module ids-sensor 1/0 session
```

Step 5 Press **Control-shift-6** followed by **x** to navigate to the router CLI.

Step 6 Reset the NME IPS from the router console.

```
router# service-module ids-sensor 1/0 reset
```

Step 7 Press **Enter** to return to the router console.

Step 8 When prompted for boot options, enter ******* quickly. You are now in the bootloader.

Step 9 Clear the password.

```
ServicesEngine boot-loader# clear password
```

The NME IPS reboots. The password is reset to **cisco**. Log in to the CLI with username **cisco** and password **cisco**. You can then change the password.

Disabling Password Recovery

Caution If you try to recover the password on a sensor on which password recovery is disabled, the process proceeds with no errors or warnings; however, the password is not reset. If you cannot log in to the sensor because you have forgotten the password, and password recovery is set to disabled, you must reimage your sensor.

Password recovery is enabled by default. You can disable password recovery through the CLI, IDM, or IME.

Disabling Password Recovery Using the CLI

To disable password recovery in the CLI, follow these steps:

Step 1 Log in to the CLI using an account with administrator privileges.

Step 2 Enter global configuration mode.

```
sensor# configure terminal
```

Step 3 Enter host mode.

```
sensor(config)# service host
```

Step 4 Disable password recovery.

```
sensor(config-hos)# password-recovery disallowed
```

Disabling Password Recovery Using IDM or IME

To disable password recovery in IDM or IME, follow these steps:

Step 1 Log in to IDM or IME using an account with administrator privileges.

Step 2 Choose **Configuration > *sensor_name* > Sensor Setup > Network**.

Step 3 To disable password recovery, uncheck the **Allow Password Recovery** check box.

Verifying the State of Password Recovery

Use the **show settings | include password** command to verify whether password recovery is enabled.

To verify whether password recovery is enabled, follow these steps:

Step 1 Log in to the CLI.

Step 2 Enter service host submode.

```
sensor# configure terminal
sensor (config)# service host
sensor (config-hos)#
```

Step 3 Verify the state of password recovery by using the **include** keyword to show settings in a filtered output.

```
sensor(config-hos)# show settings | include password
   password-recovery: allowed <defaulted>
sensor(config-hos)#
```

Troubleshooting Password Recovery

When you troubleshoot password recovery, pay attention to the following:

- You cannot determine whether password recovery has been disabled in the sensor configuration from the ROMMON prompt, GRUB menu, switch CLI, or router CLI. If you attempt password recovery, it always appears to succeed. If it has been disabled, the password is not reset to **cisco**. The only option is to reimage the sensor.
- You can disable password recovery in the host configuration. For the platforms that use external mechanisms, such as the AIM IPS and the NME IPS bootloader, ROMMON, and the maintenance partition for the IDSM2, although you can run commands to clear the password, if password recovery is disabled in the IPS, the IPS detects that password recovery is not allowed and rejects the external request.
- To check the state of password recovery, use the **show settings | include password** command.
- When performing password recovery on the IDSM2, you see the following message: `Upgrading will wipe out the contents on the storage media`. You can ignore this message. Only the password is reset when you use the specified password recovery image.

Time and the Sensor

This section describes how to maintain accurate time on the sensor, and contains the following topics:

Time Sources and the Sensor

The sensor requires a reliable time source. All events (alerts) must have the correct UTC and local time stamp, otherwise, you cannot correctly analyze the logs after an attack. When you initialize the sensor, you set up the time zones and summertime settings. This section provides a summary of the various ways to set the time on sensors.

Note We recommend that you use an NTP server. You can use authenticated or unauthenticated NTP. For authenticated NTP, you must obtain the NTP server IP address, NTP server key ID, and the key value from the NTP server. You can set up NTP during initialization or you can configure NTP through the CLI, IDM, IME, or ASDM.

The Appliances

- Use the **clock set** command to set the time. This is the default.
- Configure the appliance to get its time from an NTP time synchronization source.

The IDSM2

- The IDSM2 can automatically synchronize its clock with the switch time. This is the default. The UTC time is synchronized between the switch and the IDSM2. The time zone and summertime settings are not synchronized between the switch and the IDSM2.

  Note Be sure to set the time zone and summertime settings on both the switch and the IDSM2 to ensure that the UTC time settings are correct. The local time of the IDSM2 could be incorrect if the time zone and/or summertime settings do not match between the IDSM2 and the switch.

- Configure the IDSM2 to get its time from an NTP time synchronization source.

The AIM IPS and the NME IPS

- The AIM IPS and the NME IPS can automatically synchronize their clock with the clock in the router chassis in which they are installed (parent router). This is the default. The UTC time is synchronized between the parent router and the AIM IPS and the NME IPS. The time zone and summertime settings are not synchronized between the parent router and the AIM IPS and the NME IPS.

Note Be sure to set the time zone and summertime settings on both the parent router and the AIM IPS and the NME IPS to ensure that the UTC time settings are correct. The local time of the AIM IPS and the NME IPS could be incorrect if the time zone and/or summertime settings do not match between the AIM IPS and the NME IPS and the router.

- Configure the AIM IPS and the NME IPS to get their time from an NTP time synchronization source, such as a Cisco router, other than the parent router.

The AIP SSM

- The AIP SSM automatically synchronizes its clock with the clock in the adaptive security appliance in which it is installed. This is the default.
- Configure the AIP SSM to get its time from an NTP time synchronization source, such as a Cisco router other than the parent router.

For More Information

For the procedure for configuring NTP, refer to Configuring NTP.

Synchronizing IPS Module Clocks with Parent Device Clocks

All IPS modules (AIM IPS, AIP SSM, IDSM2, and NME IPS) synchronize their system clocks to the parent chassis clock (switch, router, or security appliance) each time the module boots up and any time the parent chassis clock is set. The module clock and parent chassis clock tend to drift apart over time. The difference can be as much as several seconds per day. To avoid this problem, make sure that both the module clock and the parent clock are synchronized to an external NTP server. If only the module clock or only the parent chassis clock is synchronized to an NTP server, the time drift occurs.

Verifying the Sensor is Synchronized with the NTP Server

In IPS, you cannot apply an incorrect NTP configuration, such as an invalid NTP key value or ID, to the sensor. If you try to apply an incorrect configuration, you receive an error message. To verify the NTP configuration, use the **show statistics host** command to gather sensor statistics. The NTP statistics section provides NTP statistics including feedback on sensor synchronization with the NTP server.

To verify the NTP configuration, follow these steps:

Step 1 Log in to the sensor.

Step 2 Generate the host statistics.

```
sensor# show statistics host
     ...
     NTP Statistics
             remote           refid      st t when poll reach   delay   offset  jitter
         11.22.33.44     CHU_AUDIO(1)     8 u   36   64    1    0.536    0.069   0.001
         LOCAL(0)        73.78.73.84      5 l   35   64    1    0.000    0.000   0.001
        ind assID status  conf reach auth condition  last_event cnt
          1 10372  f014   yes   yes   ok     reject   reachable  1
          2 10373  9014   yes   yes  none    reject   reachable  1
        status = Not Synchronized
     ...
```

Step 3 Generate the hosts statistics again after a few minutes.

```
sensor# show statistics host
   ...
   NTP Statistics
           remote           refid      st t when poll reach   delay   offset  jitter
      *11.22.33.44     CHU_AUDIO(1)     8 u   22   64  377    0.518   37.975  33.465
       LOCAL(0)        73.78.73.84      5 l   22   64  377    0.000    0.000   0.001
      ind assID status  conf reach auth condition  last_event cnt
        1 10372  f624   yes   yes   ok   sys.peer   reachable  2
        2 10373  9024   yes   yes  none    reject   reachable  2
      status = Synchronized
```

Step 4 If the status continues to read `Not Synchronized`, check with the NTP server administrator to make sure the NTP server is configured correctly.

Correcting Time on the Sensor

If you set the time incorrectly, your stored events will have the incorrect time because they are stamped with the time the event was created.

The Event Store time stamp is always based on UTC time. If during the original sensor setup, you set the time incorrectly by specifying 8:00 p.m. rather than 8:00 a.m., when you do correct the error, the corrected time will be set backwards. New events might have times older than old events.

For example, if during the initial setup, you configure the sensor as central time with daylight saving time enabled and the local time is 8:04 p.m., the time is displayed as 20:04:37 CDT and has an offset from UTC of -5 hours (01:04:37 UTC, the next day). A week later at 9:00 a.m., you discover the error: the clock shows 21:00:23 CDT. You then change the time to 9:00 a.m. and now the clock shows 09:01:33 CDT. Because the offset from UTC has not changed, it requires that the UTC time now be 14:01:33 UTC, which creates the time stamp problem.

To ensure the integrity of the time stamp on the event records, you must clear the event archive of the older events by using the **clear events** command.

Note You cannot remove individual events.

For More Information

For the procedure for clearing events, see Clearing Events, page A-95.

Advantages and Restrictions of Virtualization

To avoid configuration problems on your sensor, make sure you understand the advantages and restrictions of virtualization on your sensor.

Note The AIM IPS and the NME IPS do not support virtualization.

Virtualization has the following advantages:

- You can apply different configurations to different sets of traffic.
- You can monitor two networks with overlapping IP spaces with one sensor.
- You can monitor both inside and outside of a firewall or NAT device.

Virtualization has the following restrictions:

- You must assign both sides of asymmetric traffic to the same virtual sensor.
- Using VACL capture or SPAN (promiscuous monitoring) is inconsistent with regard to VLAN tagging, which causes problems with VLAN groups.
  - When using Cisco IOS software, a VACL capture port or a SPAN target does not always receive tagged packets even if it is configured for trunking.
  - When using the MSFC, fast path switching of learned routes changes the behavior of VACL captures and SPAN.
- Persistent store is limited.

Virtualization has the following traffic capture requirements:

- The virtual sensor must receive traffic that has 802.1q headers (other than traffic on the native VLAN of the capture port).
- The sensor must see both directions of traffic in the same VLAN group in the same virtual sensor for any given sensor.

The following sensors support virtualization:

- IPS 4240
- IPS 4255
- IPS 4260
- IPS 4270-20
- AIP SSM
- IDSM2 (with the exception of VLAN groups on inline interface pairs)

Supported MIBs

To avoid problems with configuring SNMP, be aware of the MIBs that are supported on the sensor.

The following private MIBs are supported on the sensor:

- CISCO-CIDS-MIB
- CISCO-ENHANCED-MEMPOOL-MIB
- CISCO-ENTITY-ALARM-MIB

You can obtain these private Cisco MIBs under the heading SNMP v2 MIBs at this URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Note MIB II is available on the sensor, but we do not support it. We know that some elements are not correct (for example, the packet counts from the IF MIB on the sensing interfaces). While you can use elements from MIB II, we do not guarantee that they all provide correct information. We fully support the other listed MIBs and their output is correct.

Note CISCO-PROCESS-MIB is available on the sensor, but we do not support it. We know that some elements are not available. While you can use elements from CISCO-PROCESS-MIB, we do not guarantee that they all provide correct information. We fully support the other listed MIBs and their output is correct.

When to Disable Anomaly Detection

If you have your sensor configured to see only one direction of traffic, you should disable anomaly detection. Otherwise, you will receive many alerts, because anomaly detection sees asymmetric traffic as having incomplete connections, that is, like worm scanners, and fires alerts.

To disable anomaly detection, follow these steps:

Step 1 Log in to the CLI using an account with administrator privileges.

Step 2 Enter analysis engine submode.

```
sensor# configure terminal
sensor(config)# service analysis-engine
sensor(config-ana)#
```

Step 3 Enter the virtual sensor name that contains the anomaly detection policy you want to disable.

```
sensor(config-ana)# virtual-sensor vs0
sensor(config-ana-vir)#
```

Step 4 Disable anomaly detection operational mode.

```
sensor(config-ana-vir)# anomaly-detection
sensor(config-ana-vir-ano)# operational-mode inactive
sensor(config-ana-vir-ano)#
```

Step 5 Exit analysis engine submode.

```
sensor(config-ana-vir-ano)# exit
sensor(config-ana-vir)# exit
sensor(config-ana-)# exit
Apply Changes:?[yes]:
```

Step 6 Press **Enter** to apply your changes or enter **no** to discard them.

For More Information

For more information about Worms, refer to Worms.

Troubleshooting Global Correlation

Make sure you observe the following when configuring global correlation:

- Because global correlation updates occur through the sensor management interface, firewalls must allow port 443/80 traffic.
- You must have an HTTP proxy server or a DNS server configured to allow global correlation features to function.

- You must have a valid IPS license to allow global correlation features to function.
- Global correlation features only contain external IP addresses, so if you position a sensor in an internal lab, you may never receive global correlation information.
- Make sure your sensor supports the global correlation features
- Make sure your IPS version supports the global correlation features.

For More Information

- For detailed information about global correlation features and how to configure them, for IDM refer to Configuring Global Correlation, for IME refer to Configuring Global Correlation, and for the CLI refer to Configuring Global Correlation.
- For the procedure for adding a DNS or HTTP Proxy server to support global correlation, for IDM refer to Configuring Network Settings, for IME refer to Configuring Network Settings, and for the CLI, refer to Configuring the DNS and Proxy Servers for Global Correlation.
- For the procedure for obtaining and installing the IPS license key, for IDM refer to Configuring Licensing, for IME refer to Configuring Licensing, and for the CLI, refer to Installing the License Key.

Analysis Engine Not Responding

Error Message `Output from show statistics analysis-engine`

```
Error: getAnalysisEngineStatistics : ct-sensorApp.424 not responding, please
check system processes - The connect to the specified Io::ClientPipe failed.
```

Error Message `Output from show statistics anomaly-detection`

```
Error: getAnomalyDetectionStatistics : ct-sensorApp.424 not responding, please
check system processes - The connect to the specified Io::ClientPipe failed.
```

Error Message `Output from show statistics denied-attackers`

```
Error: getDeniedAttackersStatistics : ct-sensorApp.424 not responding, please
check system processes - The connect to the specified Io::ClientPipe failed.
```

Possible Cause These error messages appear when you run the **show tech support** command and Analysis Engine is not running.

Recommended Action Verify Analysis Engine is running and monitor it to see if the issue is resolved.

To verify Analysis Engine is running and to monitor the issue, follow these steps:

Step 1 Log in to the sensor.

Step 2 Verify that Analysis Engine is not running:

```
sensor# show version

-----
MainApp N-2007_JUN_19_16_45 (Release) 2007-06-19T17:10:20-0500 Running
AnalysisEngine N-2007_JUN_19_16_45 (Release) 2007-06-19T17:10:20-0500 Not Running
CLI N-2007_JUN_19_16_45 (Release) 2007-06-19T17:10:20-0500
```

Check to see if Analysis Engine reads `Not Running`.

Step 3 Enter **`show tech-support`** and save the output.

Step 4 Reboot the sensor.

Step 5 Enter **`show version`** after the sensor has stabilized to see if the issue is resolved.

Step 6 If Analysis Engine still reads `Not Running`, contact TAC with the original **show tech support** command output.

Troubleshooting External Product Interfaces

This section lists issues that can occur with external product interfaces and provides troubleshooting tips. It contains the following topics:

- External Product Interfaces Issues, page A-22
- External Product Interfaces Troubleshooting Tips, page A-23

External Product Interfaces Issues

When the external product interface receives host posture and quarantine events, the following issues can arise:

- The sensor can store only a certain number of host records.
  - If the number of records exceeds 10,000, subsequent records are dropped.
  - If the 10,000 limit is reached and then it drops to below 9900, new records are no longer dropped.
- Hosts can change an IP address or appear to use another host IP address, for example, because of DHCP lease expiration or movement in a wireless network. In the case of an IP address conflict, the sensor presumes the most recent host posture event to be the most accurate.
- A network can include overlapping IP address ranges in different VLANs, but host postures do not include VLAN ID information. You can configure the sensor to ignore specified address ranges.
- A host can be unreachable from the CSA MC because it is behind a firewall. You can exclude unreachable hosts.
- The CSA MC event server allows up to ten open subscriptions by default. You can change this value. You must have an administrative account and password to open subscriptions.
- CSA data is not virtualized; it is treated globally by the sensor.
- Host posture OS and IP addresses are integrated into passive OS fingerprinting storage. You can view them as imported OS profiles.
- You cannot see the quarantined hosts.
- The sensor must recognize each CSA MC host X.509 certificate. You must add them as a trusted host.
- You can configure a maximum of two external product devices.

For More Information

- For more information on external product interfaces, refer to Configuring External Product Interfaces.
- For more information on working with OS maps and identifications, refer to Adding, Editing, Deleting, and Moving Configured OS Maps and Adding, Editing, Deleting, and Moving Configured OS Maps.
- For the procedure for adding trusted hosts, refer to Adding TLS Trusted Hosts.

External Product Interfaces Troubleshooting Tips

To troubleshoot external product interfaces, check the following:

- Make sure the interface is active by checking the output from the **show statistics external-product-interface** command in the CLI, or choose **Monitoring > Sensor Monitoring > Support Information > Statistics** in IDM and check the Interface state line in the response, or choose **Configuration >** ***sensor_name*** **> Sensor Monitoring > Support Information > Statistics** in IME, and check the Interface state line in the response.
- Make sure you have added the CSA MC IP address to the trusted hosts. If you forgot to add it, add it, wait a few minutes and then check again.
- Confirm subscription login information by opening and closing a subscription on CSA MC using the browser.
- Check Event Store for CSA MC subscription errors.

For More Information

- For the procedure for adding trusted hosts, refer to Adding TLS Trusted Hosts.
- For the procedure for displaying events, refer to Displaying Events.

Troubleshooting the Appliance

This section contains information to troubleshoot the appliance. It contains the following topics:

The Sensor and Jumbo Packet Frame Size

For IPS standalone appliances with 1 G and 10 G fixed or add-on interfaces, the maximum jumbo frame size is 9216 bytes.

Note A jumbo frame is an Ethernet packet that is larger than the standard maximum of 1518 bytes (including Layer 2 header and FCS).

Hardware Bypass and Link Changes and Drops

Note Hardware bypass is available on the 4GE bypass interface card, which is supported on IPS 4260 and IPS 4270-20.

Properly configuring and deploying hardware bypass protects against complete link failure if the IPS appliance experiences a power loss, critical hardware failure, or is rebooted; however, a link status change still occurs when hardware bypass engages (and again when it disengages).

During engagement, the interface card disconnects both physical connections from itself and bridges them together. The interfaces of the connected devices can then negotiate the link and traffic forwarding can resume. Once the appliance is back online, hardware bypass disengages and the interface card interrupts the bypass and reconnects the links back to itself. The interface card then negotiates both links and traffic resumes.

There is no built-in way to completely avoid link status changes and drops. However, you can greatly reduce the interruption time (in some cases to sub-second times) by doing the following:

- Make sure you use CAT 5e/6-certified cabling for all connections.
- Make sure the interfaces of the connected devices are configured to match the interfaces of the appliance for speed/duplex negotiation (auto/auto).
- Enable portfast on connected switchports to reduce spanning-tree forwarding delays.

For More Information

- For more information on hardware bypass and the IPS 4260, see Hardware Bypass, page 3-4.
- For more information on hardware bypass and the IPS 4270-20, see Hardware Bypass, page 4-5.

Troubleshooting Loose Connections

Perform the following actions to troubleshoot loose connections on a sensor:

- Make sure all power cords are securely connected.
- Make sure all cables are properly aligned and securely connected for all external and internal components.
- Remove and check all data and power cables for damage. Make sure no cables have bent pins or damaged connectors.
- Make sure each device is properly seated.
- If a device has latches, make sure they are completely closed and locked.

- Check any interlock or interconnect indicators that indicate a component is not connected properly.
- If problems continue, remove and reinstall each device, checking the connectors and sockets for bent pins or other damage.

Analysis Engine is Busy

After you reimage a sensor, Analysis Engine is busy rebuilding Regex tables and does not respond to new configurations. You can check whether Analysis Engine is busy by using the **show statistics virtual-sensor** command. You receive the following error message if Analysis Engine is busy:

```
sensor# show statistics virtual-sensor
Error: getVirtualSensorStatistics : Analysis Engine is busy rebuilding regex tables. This
may take a while.
sensor#
```

When Analysis Engine is busy rebuilding Regex tables, you receive an error message if you try to update a configuration, for example, enabling or retiring a signature:

```
sensor# configure terminal
sensor(config)# service sig sig0
sensor(config-sig)# sig 2000 0
sensor(config-sig-sig)# status enabled
sensor(config-sig-sig)# status
sensor(config-sig-sig-sta)# enabled true
sensor(config-sig-sig-sta)# retired false
sensor(config-sig-sig-sta)# exit
sensor(config-sig-sig)# exit
sensor(config-sig)# exit
Apply Changes?[yes]:
Error: editConfigDeltaSignatureDefinition : Analysis Engine is busy rebuilding regex
tables. This may take a while.
The configuration changes failed validation, no changes were applied.
Would you like to return to edit mode to correct the errors? [yes]: no
No changes were made to the configuration.
sensor(config)#
```

If you try to get the virtual sensor statistics immediately after you boot a sensor, you receive an error message. Although the sensor has rebuilt the cache files, the virtual sensor is not finished initializing.

```
sensor# show statistics virtual-sensor
Error: getVirtualSensorStatistics : Analysis Engine is busy.
sensor#
```

When you receive the errors that Analysis Engine is busy, wait a while before trying to make configuration changes. Use the **show statistics virtual-sensor** command to find out when Analysis Engine is available again.

Connecting the IPS 4240 to a Cisco 7200 Series Router

When an IPS 4240 is connected directly to a 7200 series router and both the IPS 4240 and the router interfaces are hard-coded to speed 100 with duplex Full, the connection does not work. If you set the IPS 4240 to speed Auto and duplex Auto, it connects to the router but only at speed 100 and duplex Half.

To connect correctly at speed 100 and duplex Full, set the interfaces of both the IPS 4240 and the router to speed Auto and duplex Auto. Also, if either interface is hard-coded, you must make the connection using a crossover cable.

Communication Problems

This section helps you troubleshoot communication problems with the 4200 series sensor. It contains the following topics:

Cannot Access the Sensor CLI Through Telnet or SSH

If you cannot access the sensor CLI through Telnet (if you already have it enabled) or SSH, follow these steps:

Step 1 Log in to the sensor CLI through a console, terminal, or module session.

Step 2 Make sure that the sensor management interface is enabled.

```
sensor# show interfaces
Interface Statistics
   Total Packets Received = 0
   Total Bytes Received = 0
   Missed Packet Percentage = 0
   Current Bypass Mode = Auto_off
MAC statistics from interface GigabitEthernet0/1
   Media Type = backplane
   Missed Packet Percentage = 0
   Inline Mode = Unpaired
   Pair Status = N/A
   Link Status = Up
   Link Speed = Auto_1000
   Link Duplex = Auto_Full
   Total Packets Received = 0
   Total Bytes Received = 0
   Total Multicast Packets Received = 0
   Total Broadcast Packets Received = 0
   Total Jumbo Packets Received = 0
   Total Undersize Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 0
   Total Bytes Transmitted = 0
   Total Multicast Packets Transmitted = 0
   Total Broadcast Packets Transmitted = 0
   Total Jumbo Packets Transmitted = 0
   Total Undersize Packets Transmitted = 0
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
MAC statistics from interface GigabitEthernet0/0
   Media Type = TX
   Link Status = Up
   Link Speed = Auto_100
   Link Duplex = Auto_Full
   Total Packets Received = 944333
   Total Bytes Received = 83118358
   Total Multicast Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 397633
```

```
   Total Bytes Transmitted = 435730956
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
sensor#
```

The management interface is the interface in the list with the status line `Media Type = TX`. If the Link Status is `Down`, go to Step 3. If the Link Status is `Up`, go to Step 5.

Step 3 Make sure the sensor IP address is unique.

```
sensor# setup
--- System Configuration Dialog ---

At any point you may enter a question mark '?' for help.
User ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.


Current Configuration:


service host
network-settings
host-ip 10.89.130.108/23,10.89.130.1
host-name sensor
telnet-option enabled
access-list 0.0.0.0/0
ftp-timeout 300
no login-banner-text
exit
--MORE--
```

If the management interface detects that another device on the network has the same IP address, it does not come up.

Step 4 Make sure the management port is connected to an active network connection. If the management port is not connected to an active network connection, the management interface does not come up.

Step 5 Make sure the IP address of the workstation that is trying to connect to the sensor is permitted in the sensor access list.

```
sensor# setup
--- System Configuration Dialog ---

At any point you may enter a question mark '?' for help.
User ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.


Current Configuration:


service host
network-settings
host-ip 10.89.130.108/23,10.89.130.1
host-name sensor
telnet-option enabled
access-list 0.0.0.0/0
ftp-timeout 300
no login-banner-text
exit
--MORE--
```

If the workstation network address is permitted in the sensor access list, go to Step 6.

Step 6 Add a permit entry for the workstation network address, save the configuration, and try to connect again.

Step 7 Make sure the network configuration allows the workstation to connect to the sensor.

If the sensor is protected behind a firewall and the workstation is in front of the firewall, make sure the firewall is configured to allow the workstation to access the sensor. Or if the workstation is behind a firewall that is performing network address translation on the workstation IP address, and the sensor is in front of the firewall, make sure that the sensor access list contains a permit entry for the workstation translated address.

For More Information

- For the procedures for changing the IP address, changing the access list, and enabling and disabling Telnet, refer to Configuring Network Settings.
- For the various ways to open a CLI session directly on the sensor, see Chapter 9, "Logging In to the Sensor."

Correcting a Misconfigured Access List

To correct a misconfigured access list, follow these steps:

Step 1 Log in to the CLI.

Step 2 View your configuration to see the access list.

```
sensor# show configuration | include access-list
access-list 10.0.0.0/8
access-list 64.0.0.0/8
sensor#
```

Step 3 Verify that the client IP address is listed in the allowed networks. If it is not, add it.

```
sensor# configure terminal
sensor(config)# service host
sensor(config-hos)# network-settings
sensor(config-hos-net)# access-list 171.69.70.0/24
```

Step 4 Verify the settings.

```
sensor(config-hos-net)# show settings
   network-settings
   ----------------------------------------------
      host-ip: 10.89.149.238/25,10.89.149.254 default: 10.1.9.201/24,10.1.9.1
      host-name: sensor-238 default: sensor
      telnet-option: enabled default: disabled
      access-list (min: 0, max: 512, current: 3)
      ---------------------------------------------
         network-address: 10.0.0.0/8
         ---------------------------------------------
         network-address: 64.0.0.0/8
         ---------------------------------------------
         network-address: 171.69.70.0/24
         ---------------------------------------------
```

```
      ----------------------------------------------
      ftp-timeout: 300 seconds <defaulted>
      login-banner-text: <defaulted>
   ----------------------------------------------
sensor(config-hos-net)#
```

Duplicate IP Address Shuts Interface Down

If you have two newly imaged sensors with the same IP address that come up on the same network at the same time, the interface shuts down. Linux prevents the command and control interface from activating if it detects an address conflict with another host.

To verify that the sensor in question does not have an IP address conflict with another host on the network, follow these steps:

Step 1 Log in to the CLI.

Step 2 Determine whether the interface is up.

```
sensor# show interfaces
Interface Statistics
   Total Packets Received = 0
   Total Bytes Received = 0
   Missed Packet Percentage = 0
   Current Bypass Mode = Auto_off
MAC statistics from interface GigabitEthernet0/1
   Media Type = backplane
   Missed Packet Percentage = 0
   Inline Mode = Unpaired
   Pair Status = N/A
   Link Status = Up
   Link Speed = Auto_1000
   Link Duplex = Auto_Full
   Total Packets Received = 0
   Total Bytes Received = 0
   Total Multicast Packets Received = 0
   Total Broadcast Packets Received = 0
   Total Jumbo Packets Received = 0
   Total Undersize Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 0
   Total Bytes Transmitted = 0
   Total Multicast Packets Transmitted = 0
   Total Broadcast Packets Transmitted = 0
   Total Jumbo Packets Transmitted = 0
   Total Undersize Packets Transmitted = 0
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
MAC statistics from interface GigabitEthernet0/0
   Media Type = TX
   Link Status = Up
   Link Speed = Auto_100
   Link Duplex = Auto_Full
   Total Packets Received = 1822323
   Total Bytes Received = 131098876
   Total Multicast Packets Received = 20
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
```

```
   Total Packets Transmitted = 219260
   Total Bytes Transmitted = 103668610
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
sensor#
```

If the output says the command and control interface link status is down, there is a hardware issue or an IP address conflict.

Step 3 Make sure the sensor cabling is correct.

Step 4 Make sure the IP address is correct.

For More Information

- To make sure the sensor cabling is correct, refer to the chapter for your sensor in this document.
- For the procedure for making sure the IP address is correct, refer to Configuring Network Settings.

SensorApp and Alerting

This section helps you troubleshoot issues with SensorApp and alerting. It contains the following topics:

SensorApp Not Running

The sensing process, SensorApp, should always be running. If it is not, you do not receive any alerts. SensorApp is part of Analysis Engine, so you must make sure the Analysis Engine is running. To make sure Analysis Engine is running, follow these steps:

Step 1 Log in to the CLI.

Step 2 Determine the status of the Analysis Engine service.

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.0(1)E3

Host:
    Realm Keys          key1.0
Signature Definition:
    Signature Update    S329.0                  2008-04-16
    Virus Update        V1.2                    2005-11-24
OS Version:             2.4.30-IDS-smp-bigphys
Platform:               ASA-SSM-20
Serial Number:          JAB0948035P
License expired:        11-Apr-2008 UTC
Sensor up-time is 7 days.
Using 1018015744 out of 2093600768 bytes of available memory (48% usage)
```

```
system is using 17.7M out of 29.0M bytes of available disk space (61% usage)
application-data is using 39.7M out of 166.6M bytes of available disk space (25% usage)
boot is using 40.5M out of 68.5M bytes of available disk space (62% usage)


MainApp          M-2008_APR_24_19_16   (Release)   2008-04-24T19:49:05-0500   Running
AnalysisEngine   M-2008_APR_24_19_16   (Release)   2008-04-24T19:49:05-0500   Not Running
CLI              M-2008_APR_24_19_16   (Release)   2008-04-24T19:49:05-0500

Upgrade History:

  IPS-K9-7.0-1-E3 01:16:00 UTC Fri Apr 25 2008

Recovery Partition Version 1.1 - 7.0(1)E3

Host Certificate Valid from: 29-Jun-2008 to 30-Jun-2010

sensor#
```

Step 3 If Analysis Engine is not running, look for any errors connected to it.

```
sensor# show events error fatal past 13:00:00 | include AnalysisEngine
evError: eventId=1077219258696330005 severity=warning

originator:
hostId: sensor
appName: sensorApp
appInstanceId: 1045
time: 2004/02/19 19:34:20 2004/02/19 19:34:20 UTC
errorMessage: name=errUnclassified Generating new Analysis Engine configuration file.
```

Note The date and time of the last restart is listed. In this example, the last restart was on 2-19-2004 at 7:34.

Step 4 Make sure you have the latest software updates.

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.0(1)E3

Host:
    Realm Keys          key1.0
Signature Definition:
    Signature Update    S329.0                  2008-04-16
    Virus Update        V1.2                    2005-11-24
OS Version:             2.4.30-IDS-smp-bigphys
Platform:               ASA-SSM-20
Serial Number:          JAB0948035P
License expired:        11-Apr-2008 UTC
Sensor up-time is 7 days.
Using 1018015744 out of 2093600768 bytes of available memory (48% usage)
system is using 17.7M out of 29.0M bytes of available disk space (61% usage)
application-data is using 39.7M out of 166.6M bytes of available disk space (25% usage)
boot is using 40.5M out of 68.5M bytes of available disk space (62% usage)


MainApp          M-2008_APR_24_19_16   (Release)   2008-04-24T19:49:05-0500   Running
AnalysisEngine   M-2008_APR_24_19_16   (Release)   2008-04-24T19:49:05-0500   Not Running
CLI              M-2008_APR_24_19_16   (Release)   2008-04-24T19:49:05-0500

Upgrade History:
```

```
  IPS-K9-7.0-1-E3 01:16:00 UTC Fri Apr 25 2008

Recovery Partition Version 1.1 - 7.0(1)E3

Host Certificate Valid from: 29-Jun-2008 to 30-Jun-2010

sensor#
```

If you do not have the latest software updates, download them from Cisco.com.

Step 5 Read the Readme that accompanies the software upgrade for any known DDTS for SensorApp or Analysis Engine.

For More Information

- For more information on IPS system architecture, refer to System Architecture.
- For the procedure for obtaining the latest Cisco IPS software, see Obtaining Cisco IPS Software, page 11-1.

Physical Connectivity, SPAN, or VACL Port Issue

If the sensor is not connected properly, you do not receive any alerts. To make sure the sensor is connected properly, follow these steps:

Step 1 Log in to the CLI.

Step 2 Make sure the interfaces are up and that the packet count is increasing.

```
sensor# show interfaces
Interface Statistics
   Total Packets Received = 0
   Total Bytes Received = 0
   Missed Packet Percentage = 0
   Current Bypass Mode = Auto_off
MAC statistics from interface GigabitEthernet0/1
   Media Type = backplane
   Missed Packet Percentage = 0
   Inline Mode = Unpaired
   Pair Status = N/A
   Link Status = Up
   Link Speed = Auto_1000
   Link Duplex = Auto_Full
   Total Packets Received = 0
   Total Bytes Received = 0
   Total Multicast Packets Received = 0
   Total Broadcast Packets Received = 0
   Total Jumbo Packets Received = 0
   Total Undersize Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 0
   Total Bytes Transmitted = 0
   Total Multicast Packets Transmitted = 0
   Total Broadcast Packets Transmitted = 0
   Total Jumbo Packets Transmitted = 0
   Total Undersize Packets Transmitted = 0
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
MAC statistics from interface GigabitEthernet0/0
```

```
   Media Type = TX
   Link Status = Up
   Link Speed = Auto_100
   Link Duplex = Auto_Full
   Total Packets Received = 1830137
   Total Bytes Received = 131624465
   Total Multicast Packets Received = 20
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 220052
   Total Bytes Transmitted = 103796666
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
sensor#
```

Step 3 If the Link Status is down, make sure the sensing port is connected properly.

a. Make sure the sensing port is connected properly on the appliance.

b. Make sure the sensing port is connected to the correct SPAN or VACL capture port on the IDSM2.

Step 4 Verify the interface configuration.

a. Make sure you have the interfaces configured properly.

b. Verify the SPAN and VACL capture port configuration on the Cisco switch. Refer to your switch documentation for the procedure.

Step 5 Verify again that the interfaces are up and that the packet count is increasing.

```
sensor# show interfaces
```

For More Information

- For the procedure for properly installing the sensing interface on your sensor, refer to the chapter on your appliance in this document.
- For the procedure for connecting SPAN and VACL capture ports on the IDSM2, refer to Configuring the IDSM2.
- For the procedures for configuring interfaces on your sensor, refer to Configuring Interfaces.

Unable to See Alerts

If you are not seeing alerts, try the following:

- Make sure the signature is enabled
- Make sure the signature is not retired
- Make sure that you have Produce Alert configured as an action

Note If you choose Produce Alert, but come back later and add another event action and do not add Produce Alert to the new configuration, alerts are not sent to the Event Store. Every time you configure a signature, the new configuration overwrites the old one, so make sure you have configured all the event actions you want for each signature.

- Make sure the sensor is seeing packets

- Make sure that alerts are being generated
- Make sure the sensing interface is in a virtual sensor

To make sure you can see alerts, follow these steps:

Step 1 Log in to the CLI.

Step 2 Make sure the signature is enabled.

```
sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)# signatures 1300 0
sensor(config-sig-sig)# status
sensor(config-sig-sig-sta)# show settings
   status
   ----------------------------------------------
      enabled: true <defaulted>
      retired: false <defaulted>
   ----------------------------------------------
sensor(config-sig-sig-sta)#
```

Step 3 Make sure you have Produce Alert configured.

```
sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)# signatures 1300 0
sensor(config-sig-sig)# engine ?
normalizer     Signature engine
sensor(config-sig-sig)# engine normalizer
sensor(config-sig-sig-nor)# event-action produce-alert
sensor(config-sig-sig-nor)# show settings
   normalizer
   ----------------------------------------------
      event-action: produce-alert default: produce-alert|deny-connection-inline
      edit-default-sigs-only
      ---------------------------------------------
sensor#
```

Step 4 Make sure the sensor is seeing packets.

```
sensor# show interfaces FastEthernet0/1
MAC statistics from interface FastEthernet0/1
   Media Type = backplane
   Missed Packet Percentage = 0
   Inline Mode = Unpaired
   Pair Status = N/A
   Link Status = Up
   Link Speed = Auto_100
   Link Duplex = Auto_Full
   Total Packets Received = 267581
   Total Bytes Received = 24886471
   Total Multicast Packets Received = 0
   Total Broadcast Packets Received = 0
   Total Jumbo Packets Received = 0
   Total Undersize Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 57301
   Total Bytes Transmitted = 3441000
   Total Multicast Packets Transmitted = 0
   Total Broadcast Packets Transmitted = 0
   Total Jumbo Packets Transmitted = 0
   Total Undersize Packets Transmitted = 0
```

```
   Total Transmit Errors = 1
   Total Transmit FIFO Overruns = 0
sensor#
```

Step 5 Check for alerts.

```
sensor# show statistics virtual-sensor
SigEvent Preliminary Stage Statistics
    Number of Alerts received = 0
    Number of Alerts Consumed by AlertInterval = 0
    Number of Alerts Consumed by Event Count = 0
    Number of FireOnce First Alerts = 0
    Number of FireOnce Intermediate Alerts = 0
    Number of Summary First Alerts  = 0
    Number of Summary Intermediate Alerts  = 0
    Number of Regular Summary Final Alerts  = 0
    Number of Global Summary Final Alerts  = 0
    Number of Alerts Output for further processing = 0alertDetails: Traffic Source: int0 ;
```

Sensor Not Seeing Packets

If the sensor is not seeing any packets on the network, you could have the interfaces set up incorrectly. If the sensor is not seeing packets, follow these steps:

Step 1 Log in to the CLI.

Step 2 Make sure the interfaces are up and receiving packets.

```
sensor# show interfaces GigabitEthernet0/1
MAC statistics from interface GigabitEthernet0/1
   Media Type = backplane
   Missed Packet Percentage = 0
   Inline Mode = Unpaired
   Pair Status = N/A
   Link Status = Down
   Link Speed = Auto_1000
   Link Duplex = Auto_Full
   Total Packets Received = 0
   Total Bytes Received = 0
   Total Multicast Packets Received = 0
   Total Broadcast Packets Received = 0
   Total Jumbo Packets Received = 0
   Total Undersize Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 0
   Total Bytes Transmitted = 0
   Total Multicast Packets Transmitted = 0
   Total Broadcast Packets Transmitted = 0
   Total Jumbo Packets Transmitted = 0
   Total Undersize Packets Transmitted = 0
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
sensor#
```

Step 3 If the interfaces are not up, do the following:

- Check the cabling.
- Enable the interface.

```
sensor# configure terminal
sensor(config)# service interface
sensor(config-int)# physical-interfaces GigabitEthernet0/1
sensor(config-int-phy)# admin-state enabled
sensor(config-int-phy)# show settings
   <protected entry>
   name: GigabitEthernet0/1
   ----------------------------------------------
      media-type: tx <protected>
      description: <defaulted>
      admin-state: enabled default: disabled
      duplex: auto <defaulted>
      speed: auto <defaulted>
      alt-tcp-reset-interface
      ---------------------------------------------
         none
         ---------------------------------------------
         ---------------------------------------------
      ---------------------------------------------
   ----------------------------------------------
sensor(config-int-phy)#
```

Step 4 Check to see that the interface is up and receiving packets.

```
sensor# show interfaces
MAC statistics from interface GigabitEthernet0/1
   Media Type = TX
   Missed Packet Percentage = 0
   Inline Mode = Unpaired
   Pair Status = N/A
   Link Status = Up
   Link Speed = Auto_100
   Link Duplex = Auto_Full
   Total Packets Received = 3
   Total Bytes Received = 900
   Total Multicast Packets Received = 3
   Total Broadcast Packets Received = 0
   Total Jumbo Packets Received = 0
   Total Undersize Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 0
   Total Bytes Transmitted = 0
   Total Multicast Packets Transmitted = 0
   Total Broadcast Packets Transmitted = 0
   Total Jumbo Packets Transmitted = 0
   Total Undersize Packets Transmitted = 0
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0 ...
```

For More Information

For the procedure for installing the sensor properly, refer to your sensor chapter in this document.

Cleaning Up a Corrupted SensorApp Configuration

If the SensorApp configuration has become corrupted and SensorApp cannot run, you must delete it entirely and restart SensorApp. To delete the SensorApp configuration, follow these steps:

Step 1 Log in to the service account.

Step 2 Su to root.

Step 3 Stop the IPS applications.

```
/etc/init.d/cids stop
```

Step 4 Replace the virtual sensor file.

```
cp /usr/cids/idsRoot/etc/defVirtualSensorConfig.xml
/usr/cids/idsRoot/etc/VS-Config/virtualSensor.xml
```

Step 5 Remove the cache files.

```
rm /usr/cids/idsRoot/var/virtualSensor/*.pmz
```

Step 6 Exit the service account.

Step 7 Log in to the sensor CLI.

Step 8 Start the IPS services.

```
sensor# cids start
```

Step 9 Log in to an account with administrator privileges.

Step 10 Reboot the sensor.

```
sensor# reset
Warning: Executing this command will stop all applications and reboot the node.
Continue with reset? [yes]:yes
Request Succeeded.
sensor#
```

For More Information

For more information on IPS system architecture, refer to System Architecture.

Blocking

This section provides troubleshooting help for blocking and the ARC service. It contains the following topics.

- Blocking Not Occurring for a Signature, page A-44
- Verifying the Master Blocking Sensor Configuration, page A-45

Troubleshooting Blocking

Note ARC was formerly known as Network Access Controller. Although the name has been changed since IPS 5.1, it still appears in IDM, IME, and the CLI as Network Access Controller, **nac**, and **network-access**.

After you have configured ARC, you can verify if it is running properly by using the **show version** command. To verify that ARC is connecting to the network devices, use the **show statistics network-access** command.

To troubleshoot ARC, follow these steps:

1. Verify that ARC is running.
2. Verify that ARC is connecting to the network devices.
3. Verify that the Event Action is set to Block Host for specific signatures.
4. Verify that the master blocking sensor is properly configured.

For More Information

- For the procedure to verify that ARC is running, see Verifying ARC is Running, page A-38.
- For the procedure to verify that ARC is connecting, see Verifying ARC Connections are Active, page A-39.
- For the procedure to verify that the Event Action is set to Block Host, see Blocking Not Occurring for a Signature, page A-44.
- For the procedure to verify that the master blocking sensor is properly configured, see Verifying the Master Blocking Sensor Configuration, page A-45.
- For a discussion of ARC architecture, refer to Attack Response Controller.

Verifying ARC is Running

To verify that ARC is running, use the **show version** command. If MainApp is not running, ARC cannot run. ARC is part of MainApp. To verify that ARC is running, following these steps:

Step 1 Log in to the CLI.

Step 2 Verify that MainApp is running.

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.0(1)E3

Host:
    Realm Keys          key1.0
Signature Definition:
    Signature Update    S388.0                  2009-03-25
    Virus Update        V1.4                    2007-03-02
OS Version:             2.4.30-IDS-smp-bigphys
```

```
Platform:               IPS4270-20-K9
Serial Number:          USE716N39B
Licensed, expires:      01-May-2009 UTC
Sensor up-time is 3 days.
Using 1888964608 out of 4029321216 bytes of available memory (46% usage)
system is using 16.5M out of 38.5M bytes of available disk space (43% usage)
application-data is using 44.4M out of 166.8M bytes of available disk space (28%
 usage)
boot is using 40.6M out of 69.5M bytes of available disk space (62% usage)
application-log is using 494.0M out of 513.0M bytes of available disk space (96%
 usage)


MainApp            B-BEAU_2009_APR_18_08_00_7_0_1   (Release)   2009-04-18T08:05
:25-0500   Running
AnalysisEngine     B-BEAU_2009_APR_18_08_00_7_0_1   (Release)   2009-04-18T08:05
:25-0500   Running
CollaborationApp   B-BEAU_2009_APR_18_08_00_7_0_1   (Release)   2009-04-18T08:05
:25-0500   Running
CLI                B-BEAU_2009_APR_18_08_00_7_0_1   (Release)   2009-04-18T08:05
:25-0500

Upgrade History:

  IPS-K9-7.0-1-E3   08:00:00 UTC Sat Apr 18 2009

Recovery Partition Version 1.1 - 7.0(1)E3

Host Certificate Valid from: 16-Apr-2009 to 17-Apr-2011

sensor#
```

Step 3 If MainApp displays `Not Running`, ARC has failed. Contact the TAC.

For More Information

For more information on IPS system architecture, refer to System Architecture.

Verifying ARC Connections are Active

If the State is not `Active` in the ARC statistics, there is a problem. To verify that the State is Active in the statistics, follow these steps:

Step 1 Log in to the CLI.

Step 2 Verify that ARC is connecting.

Check the State section of the output to verify that all devices are connecting.

```
sensor# show statistics network-access
Current Configuration
   LogAllBlockEventsAndSensors = true
   EnableNvramWrite = false
   EnableAclLogging = false
   AllowSensorBlock = false
   BlockMaxEntries = 250
   MaxDeviceInterfaces = 250
   NetDevice
      Type = Cisco
```

```
      IP = 10.89.147.54
      NATAddr = 0.0.0.0
      Communications = telnet
      BlockInterface
         InterfaceName = fa0/0
         InterfaceDirection = in
State
   BlockEnable = true
   NetDevice
      IP = 10.89.147.54
      AclSupport = uses Named ACLs
      Version = 12.2
      State = Active
sensor#
```

Step 3 If ARC is not connecting, look for recurring errors.

sensor# **show events error** *hh:mm:ss month day year* **| include : nac**

Example

sensor# **show events error 00:00:00 Apr 01 2007 | include : nac**

Step 4 Make sure you have the latest software updates.

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.0(1)E3

Host:
    Realm Keys          key1.0
Signature Definition:
    Signature Update    S388.0                  2009-03-25
    Virus Update        V1.4                    2007-03-02
OS Version:             2.4.30-IDS-smp-bigphys
Platform:               IPS4270-20-K9
Serial Number:          USE716N39B
Licensed, expires:      01-May-2009 UTC
Sensor up-time is 3 days.
Using 1888964608 out of 4029321216 bytes of available memory (46% usage)
system is using 16.5M out of 38.5M bytes of available disk space (43% usage)
application-data is using 44.4M out of 166.8M bytes of available disk space (28%
 usage)
boot is using 40.6M out of 69.5M bytes of available disk space (62% usage)
application-log is using 494.0M out of 513.0M bytes of available disk space (96%
 usage)


MainApp            B-BEAU_2009_APR_18_08_00_7_0_1   (Release)   2009-04-18T08:05
:25-0500   Running
AnalysisEngine     B-BEAU_2009_APR_18_08_00_7_0_1   (Release)   2009-04-18T08:05
:25-0500   Running
CollaborationApp   B-BEAU_2009_APR_18_08_00_7_0_1   (Release)   2009-04-18T08:05
:25-0500   Running
CLI                B-BEAU_2009_APR_18_08_00_7_0_1   (Release)   2009-04-18T08:05
:25-0500

Upgrade History:

  IPS-K9-7.0-1-E3   08:00:00 UTC Sat Apr 18 2009

Recovery Partition Version 1.1 - 7.0(1)E3

Host Certificate Valid from: 16-Apr-2009 to 17-Apr-2011
```

```
sensor#
```

Note If you do not have the latest software updates, download them from Cisco.com.

Step 5 Read the Readme that accompanies the software upgrade for any known DDTS for ARC.

Step 6 Make sure the configuration settings for each device are correct (the username, password, and IP address).

Step 7 Make sure the interface and directions for each network device are correct.

Step 8 If the network device is using SSH-DES or SSH-3DES, make sure that you have enabled SSH connections to the device.

Step 9 Verify that each interface and direction on each controlled device is correct.

For More Information

- For the procedure for obtaining the latest Cisco IPS software, see Obtaining Cisco IPS Software, page 11-1.
- For more information about configuring devices, see Device Access Issues, page A-41.
- For the procedure for verifying the interfaces and directions for each network device, see Verifying the Interfaces and Directions on the Network Device, page A-43.
- For the procedure for enabling SSH, see Enabling SSH Connections to the Network Device, page A-43.

Device Access Issues

ARC may not be able to access the devices it is managing. Make sure the you have the correct IP address and username and password for the managed devices and the correct interface and direction configured.

Note SSH devices must support SSH 1.5. The sensor does not support SSH 2.0.

To troubleshoot device access issues, follow these steps:

Step 1 Log in to the CLI.

Step 2 Verify the IP address for the managed devices.

```
sensor# configure terminal
sensor (config)# service network-access
sensor(config-net)# show settings
   general
   -----------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false <defaulted>
      enable-acl-logging: false <defaulted>
      allow-sensor-block: false <defaulted>
      block-enable: true <defaulted>
      block-max-entries: 250 <defaulted>
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
```

```
      ----------------------------------------------
      ----------------------------------------------
      never-block-hosts (min: 0, max: 250, current: 0)
      ----------------------------------------------
      ----------------------------------------------
      never-block-networks (min: 0, max: 250, current: 0)
      ----------------------------------------------
      ----------------------------------------------
      block-hosts (min: 0, max: 250, current: 0)
      ----------------------------------------------
      ----------------------------------------------
      block-networks (min: 0, max: 250, current: 0)
      ----------------------------------------------
      ----------------------------------------------
   ----------------------------------------------
   user-profiles (min: 0, max: 250, current: 1)
   ----------------------------------------------
      profile-name: r7200
      ----------------------------------------------
         enable-password: <hidden>
         password: <hidden>
         username: netrangr default:
      ----------------------------------------------
   ----------------------------------------------
   cat6k-devices (min: 0, max: 250, current: 0)
   ----------------------------------------------
   ----------------------------------------------
   router-devices (min: 0, max: 250, current: 1)
   ----------------------------------------------
      ip-address: 10.89.147.54
      ----------------------------------------------
         communication: telnet default: ssh-3des
         nat-address: 0.0.0.0 <defaulted>
         profile-name: r7200
         block-interfaces (min: 0, max: 100, current: 1)
         ----------------------------------------------
            interface-name: fa0/0
            direction: in
            ----------------------------------------------
               pre-acl-name: <defaulted>
               post-acl-name: <defaulted>
            ----------------------------------------------
         ----------------------------------------------
      ----------------------------------------------
   ----------------------------------------------
   firewall-devices (min: 0, max: 250, current: 0)
   ----------------------------------------------
   ----------------------------------------------
sensor(config-net)#
```

Step 3 Manually connect to the device to make sure you have used the correct username, password, and enable password, and to ensure that the device is reachable from the sensor.

- **a.** Log in to the service account.
- **b.** Telnet or SSH to the network device to verify the configuration.
- **c.** Make sure you can reach the device.
- **d.** Verify the username and password.

Step 4 Verify that each interface and direction on each network device is correct.

For More Information

For the procedure for verifying the interfaces and directions for each network device, see Verifying the Interfaces and Directions on the Network Device, page A-43.

Verifying the Interfaces and Directions on the Network Device

To verify that each interface and direction on each controlled device is correct, you can send a manual block to a bogus host and then check to see if deny entries exist for the blocked addresses in the ACL of the router.

Note To perform a manual block using IDM, choose **Monitoring > Sensor Monitoring > Time-Based Actions > Host Blocks**. To perform a manual block using IME, choose **Configuration > *sensor_name* > Sensor Monitoring > Time-Based Actions > Host Blocks**.

To initiate a manual block to a bogus host, follow these steps:

Step 1 Enter ARC general submode.

```
sensor# configure terminal
sensor(config)# service network-access
sensor(config-net)# general
```

Step 2 Start the manual block of the bogus host IP address.

```
sensor(config-net-gen)# block-hosts 10.16.0.0
```

Step 3 Exit general submode.

```
sensor(config-net-gen)# exit
sensor(config-net)# exit
Apply Changes:? [yes]:
```

Step 4 Press **Enter** to apply the changes or type **no** to discard them.

Step 5 Telnet to the router and verify that a deny entry for the blocked address exists in the router ACL. Refer to the router documentation for the procedure.

Step 6 Remove the manual block by repeating Steps 1 through 4 except in Step 2 place **no** in front of the command.

```
sensor(config-net-gen)# no block-hosts 10.16.0.0
```

Enabling SSH Connections to the Network Device

If you are using SSH-DES or SSH-3DES as the communication protocol for the network device, you must make sure you have enabled it on the device.

To enable SSH connections to the network device, follow these steps:

Step 1 Log in to the CLI.

Step 2 Enter configuration mode:

```
sensor# configure terminal
```

Step 3 Enable SSH:

```
sensor(config)# ssh host blocking_device_ip_address
```

Step 4 Type **yes** when prompted to accept the device.

Blocking Not Occurring for a Signature

If blocking is not occurring for a specific signature, check that the event action is set to block the host. To make sure blocking is occurring for a specific signature, follow these steps:

Step 1 Log in to the CLI.

Step 2 Enter signature definition submode.

```
sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)#
```

Step 3 Make sure the event action is set to block the host.

Note If you want to receive alerts, you must always add **produce-alert** any time you configure the event actions.

```
sensor(config-sig)# signatures 1300 0
sensor(config-sig-sig)# engine normalizer
sensor(config-sig-sig-nor)# event-action produce-alert|request-block-host
sensor(config-sig-sig-nor)# show settings
   normalizer
   -----------------------------------------------
      event-action: produce-alert|request-block-host default: produce-alert|deny
-connection-inline
      edit-default-sigs-only
      ----------------------------------------------
         default-signatures-only
         ----------------------------------------------
            specify-service-ports
            ----------------------------------------------
               no
               ----------------------------------------------
               ----------------------------------------------
            ----------------------------------------------
            specify-tcp-max-mss
            ----------------------------------------------
               no
               ----------------------------------------------
               ----------------------------------------------
            ----------------------------------------------
            specify-tcp-min-mss
            ----------------------------------------------
               no
               ----------------------------------------------
               ----------------------------------------------
--MORE--
```

Step 4 Exit signature definition submode.

```
sensor(config-sig-sig-nor)# exit
```

```
sensor(config-sig-sig)# exit
sensor(config-sig)# exit
Apply Changes:?[yes]:
```

Step 5 Press **Enter** to apply the changes or type **no** to discard them.

Verifying the Master Blocking Sensor Configuration

To verify that a master blocking sensor is set up properly or to troubleshoot a master blocking sensor that is not set up properly, you can use the **show statistics network-access** command. Make sure that the forwarding sensor is set up as TLS trusted host if the remote master blocking sensor is using TLS for web access.

To verify a master blocking sensor configuration, follow these steps:

Step 1 Log in to the CLI.

Step 2 View the ARC statistics and verify that the master blocking sensor entries are in the statistics.

```
sensor# show statistics network-access
Current Configuration
   AllowSensorShun = false
   ShunMaxEntries = 250
   MasterBlockingSensor
      SensorIp = 10.89.149.46
      SensorPort = 443
      UseTls = 1
State
   ShunEnable = true
   ShunnedAddr
      Host
         IP = 122.122.122.44
         ShunMinutes = 60
         MinutesRemaining = 59
```

Step 3 If the master blocking sensor does not show up in the statistics, you need to add it.

Step 4 Initiate a manual block to a bogus host IP address to make sure the master blocking sensor is initiating blocks.

```
sensor# configure terminal
sensor(config)# service network-access
sensor(config-net)# general
sensor(config-net-gen)# block-hosts 10.16.0.0
```

Step 5 Exit network access general submode.

```
sensor(config-net-gen)# exit
sensor(config-net)# exit
Apply Changes:? [yes]:
```

Step 6 Press **Enter** to apply the changes or type **no** to discard them.

Step 7 Verify that the block shows up in the ARC statistics.

```
sensor# show statistics network-access
Current Configuration
   AllowSensorShun = false
   ShunMaxEntries = 100
State
   ShunEnable = true
```

```
   ShunnedAddr
      Host
         IP = 10.16.0.0
         ShunMinutes =
```

Step 8 Log in to the CLI of the master blocking sensor host, and using the **show statistics network-access** command, verify that the block also shows up in the master blocking sensor ARC statistics.

```
sensor# show statistics network-access
Current Configuration
   AllowSensorShun = false
   ShunMaxEntries = 250
   MasterBlockingSensor
      SensorIp = 10.89.149.46
      SensorPort = 443
      UseTls = 1
State
   ShunEnable = true
   ShunnedAddr
      Host
         IP = 10.16.0.0
         ShunMinutes = 60
         MinutesRemaining = 59
```

Step 9 If the remote master blocking sensor is using TLS for web access, make sure the forwarding sensor is configured as a TLS host.

```
sensor# configure terminal
sensor(config)# tls trust ip master_blocking_sensor_ip_address
```

For More Information

For the procedure to configure the sensor to be a master blocking sensor, refer to Configuring the Sensor to be a Master Blocking Sensor.

Logging

This section describes debug logging, and contains the following topics:

Understanding Debug Logging

TAC may suggest that you turn on debug logging for troubleshooting purposes. Logger controls what log messages are generated by each application by controlling the logging severity for different logging zones. By default, debug logging is not turned on.

If you enable individual zone control, each zone uses the level of logging that it is configured for. Otherwise, the same logging level is used for all zones.

Enabling Debug Logging

Caution Enabling debug logging seriously affects performance and should only be done when instructed by TAC.

To enable debug logging, follow these steps:

Step 1 Log in to the service account.

Step 2 Edit the log.conf file to increase the size of the log to accommodate the additional log statements.

```
vi /usr/cids/idsRoot/etc/log.conf
```

Step 3 Change `fileMaxSizeInK=500` to `fileMaxSizeInK=5000`.

Step 4 Locate the zone and CID section of the file and set the severity to debug.

```
severity=debug
```

Step 5 Save the file, exit the vi editor, and exit the service account.

Step 6 Log in to the CLI as administrator.

Step 7 Enter master control submode.

```
sensor# configure terminal
sensor(config)# service logger
sensor(config-log)# master-control
```

Step 8 To enable debug logging for all zones.

```
sensor(config-log-mas)# enable-debug true
sensor(config-log-mas)# show settings
   master-control
   -----------------------------------------------
      enable-debug: true default: false
      individual-zone-control: false <defaulted>
   -----------------------------------------------
sensor(config-log-mas)#
```

Step 9 To turn on individual zone control.

```
sensor(config-log-mas)# individual-zone-control true
sensor(config-log-mas)# show settings
   master-control
   -----------------------------------------------
      enable-debug: true default: false
      individual-zone-control: true default: false
   -----------------------------------------------
sensor(config-log-mas)#
```

Step 10 Exit master zone control.

```
sensor(config-log-mas)# exit
```

Step 11 View the zone names.

```
sensor(config-log)# show settings
   master-control
   -----------------------------------------------
      enable-debug: false <defaulted>
      individual-zone-control: true default: false
   -----------------------------------------------
   zone-control (min: 0, max: 999999999, current: 14)
```

```
   ----------------------------------------------
      <protected entry>
      zone-name: AuthenticationApp
      severity: warning <defaulted>
      <protected entry>
      zone-name: Cid
      severity: debug <defaulted>
      <protected entry>
      zone-name: Cli
      severity: warning <defaulted>
      <protected entry>
      zone-name: IdapiCtlTrans
      severity: warning <defaulted>
      <protected entry>
      zone-name: IdsEventStore
      severity: warning <defaulted>
      <protected entry>
      zone-name: MpInstaller
      severity: warning <defaulted>
      <protected entry>
      zone-name: cmgr
      severity: warning <defaulted>
      <protected entry>
      zone-name: cplane
      severity: warning <defaulted>
      <protected entry>
      zone-name: csi
      severity: warning <defaulted>
      <protected entry>
      zone-name: ctlTransSource
      severity: warning <defaulted>
      <protected entry>
      zone-name: intfc
      severity: warning <defaulted>
      <protected entry>
      zone-name: nac
      severity: warning <defaulted>
      <protected entry>
      zone-name: sensorApp
      severity: warning <defaulted>
      <protected entry>
      zone-name: tls
      severity: warning <defaulted>
   ----------------------------------------------
sensor(config-log)#
```

Step 12 Change the severity level (debug, timing, warning, or error) for a particular zone.

```
sensor(config-log)# zone-control IdsEventStore severity error
sensor(config-log)# show settings
   master-control
   ----------------------------------------------
      enable-debug: true default: false
      individual-zone-control: true default: false
   ----------------------------------------------
   zone-control (min: 0, max: 999999999, current: 14)
   ----------------------------------------------
      <protected entry>
      zone-name: AuthenticationApp
      severity: warning <defaulted>
      <protected entry>
      zone-name: Cid
      severity: debug <defaulted>
      <protected entry>
```

```
      zone-name: Cli
      severity: warning <defaulted>
      <protected entry>
      zone-name: IdapiCtlTrans
      severity: warning <defaulted>
      <protected entry>
      zone-name: IdsEventStore
      severity: error default: warning
      <protected entry>
      zone-name: MpInstaller
      severity: warning <defaulted>
      <protected entry>
      zone-name: cmgr
      severity: warning <defaulted>
      <protected entry>
      zone-name: cplane
      severity: warning <defaulted>
      <protected entry>
      zone-name: csi
      severity: warning <defaulted>
      <protected entry>
      zone-name: ctlTransSource
      severity: warning <defaulted>
      <protected entry>
      zone-name: intfc
      severity: warning <defaulted>
      <protected entry>
      zone-name: nac
      severity: warning <defaulted>
      <protected entry>
      zone-name: sensorApp
      severity: warning <defaulted>
      <protected entry>
      zone-name: tls
      severity: warning <defaulted>
   ----------------------------------------------
sensor(config-log)#
```

Step 13 Turn on debugging for a particular zone.

```
sensor(config-log)# zone-control nac severity debug
sensor(config-log)# show settings
   master-control
   ----------------------------------------------
      enable-debug: true default: false
      individual-zone-control: true default: false
   ----------------------------------------------
   zone-control (min: 0, max: 999999999, current: 14)
   ----------------------------------------------
      <protected entry>
      zone-name: AuthenticationApp
      severity: warning <defaulted>
      <protected entry>
      zone-name: Cid
      severity: debug <defaulted>
      <protected entry>
      zone-name: Cli
      severity: warning <defaulted>
      <protected entry>
      zone-name: IdapiCtlTrans
      severity: warning <defaulted>
      <protected entry>
      zone-name: IdsEventStore
      severity: error default: warning
```

```
      <protected entry>
      zone-name: MpInstaller
      severity: warning <defaulted>
      <protected entry>
      zone-name: cmgr
      severity: warning <defaulted>
      <protected entry>
      zone-name: cplane
      severity: warning <defaulted>
      <protected entry>
      zone-name: csi
      severity: warning <defaulted>
      <protected entry>
      zone-name: ctlTransSource
      severity: warning <defaulted>
      <protected entry>
      zone-name: intfc
      severity: warning <defaulted>
      <protected entry>
      zone-name: nac
      severity: debug default: warning
      <protected entry>
      zone-name: sensorApp
      severity: warning <defaulted>
      <protected entry>
      zone-name: tls
      severity: warning <defaulted>
   ------------------------------------------------
sensor(config-log)#
```

Step 14 Exit the logger submode.

```
sensor(config-log)# exit
Apply Changes:?[yes]:
```

Step 15 Press **Enter** to apply changes or type **no** to discard them:

For More Information

For a list of what each zone name refers to, see Zone Names, page A-50.

Zone Names

Table A-2 lists the debug logger zone names:

Table A-2 Debug Logger Zone Names

Zone Name	Description
AD	Anomaly Detection zone
AuthenticationApp	Authentication zone
Cid	General logging zone
Cli	CLI zone
IdapiCtlTrans	All control transactions zone
IdsEventStore	Event Store zone
MpInstaller	IDSM2 master partition installer zone

Table A-2 Debug Logger Zone Names (continued)

Zone Name	Description
cmgr	Card Manager service zone[1]
cplane	Control Plane zone[2]
csi	CIDS Servlet Interface[3]
ctlTransSource	Outbound control transactions zone
intfc	Interface zone
nac	ARC zone
rep	Reputation zone
sched	Automatic update scheduler zone
sensorApp	Analysis Engine zone
tls	SSL and TLS zone

1. The Card Manager service is used on the AIP SSM to exchange control and state information between modules in the chassis.
2. The Control Plane is the transport communications layer used by Card Manager on the AIP SSM.
3. The CIDS servlet interface is the interface layer between the CIDS web server and the servlets.

For More Information

To learn more about the IPS Logger service, refer to Logger.

Directing cidLog Messages to SysLog

It might be useful to direct cidLog messages to syslog. To direct cidLog messages to syslog, follow these steps:

Step 1 Go to the idsRoot/etc/log.conf file.

Step 2 Make the following changes:

a. Set [logApp] `enabled=false`

Comment out the `enabled=true` because `enabled=false` is the default.

b. Set [drain/main] `type=syslog`

The following example shows the logging configuration file:

```
timemode=local
;timemode=utc

[logApp]
;enabled=true
;-------- FIFO parameters --------
fifoName=logAppFifo
fifoSizeInK=240
;-------- logApp zone and drain parameters --------
zoneAndDrainName=logApp
fileName=main.log
fileMaxSizeInK=500

[zone/Cid]
```

```
severity=warning
drain=main

[zone/IdsEventStore]
severity=debug
drain=main

[drain/main]
type=syslog
```

The syslog output is sent to the syslog facility local6 with the following correspondence to syslog message priorities:

```
LOG_DEBUG,        //   debug
LOG_INFO,             //    timing
LOG_WARNING,   //    warning
LOG_ERR,             //    error
LOG_CRIT             //     fatal
```

Note Make sure that your /etc/syslog.conf has that facility enabled at the proper priority.

Caution The syslog is much slower than logApp (about 50 messages per second as opposed to 1000 or so). We recommend that you enable debug severity on one zone at a time.

TCP Reset Not Occurring for a Signature

Note TCP Resets are not supported over MPLS links or the following tunnels: GRE, IPv4 in IPv4, IPv6 in IPv4, or IPv4 in IPv6.

If you do not have the event action set to reset, the TCP reset does not occur for a specific signature. To troubleshoot a reset not occurring for a specific signature, follow these steps:

Step 1 Log in to the CLI.

Step 2 Make sure the event action is set to TCP reset.

```
sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)# signatures 1000 0
sensor(config-sig-sig)# engine atomic-ip
sensor(config-sig-sig-ato)# event-action reset-tcp-connection|produc-alert
sensor(config-sig-sig-ato)# show settings
   atomic-ip
   ----------------------------------------------
      event-action: produce-alert|reset-tcp-connection default: produce-alert
      fragment-status: any <defaulted>
      specify-l4-protocol
      ----------------------------------------------
         no
         ----------------------------------------------
         ----------------------------------------------
      ----------------------------------------------
```

```
      specify-ip-payload-length
      ---------------------------------------------
         no
         ---------------------------------------------
         ---------------------------------------------
      ---------------------------------------------
      specify-ip-header-length
      ---------------------------------------------
         no
         ---------------------------------------------
         ---------------------------------------------
      ---------------------------------------------
      specify-ip-tos
      ---------------------------------------------
--MORE--
```

Step 3 Exit signature definition submode.

```
sensor(config-sig-sig-ato)# exit
sensor(config-sig-sig)# exit
sensor(config-sig)# exit
Apply Changes:?[yes]:
```

Step 4 Press **Enter** to apply the changes or type **no** to discard them.

Step 5 Make sure the correct alarms are being generated.

```
sensor# show events alert
evAlert: eventId=1047575239898467370 severity=medium
originator:
hostId: sj_4250_40
appName: sensorApp
appInstanceId: 1004
signature: sigId=20000 sigName=STRING.TCP subSigId=0 version=Unknown
addr: locality=OUT 172.16.171.19
port: 32771
victim:
addr: locality=OUT 172.16.171.13 port: 23
actions:
tcpResetSent: true
```

Step 6 Make sure the switch is allowing incoming TCP reset packet from the sensor. Refer to your switch documentation for more information.

Step 7 Make sure the resets are being sent.

```
root# ./tcpdump -i eth0 src host 172.16.171.19
tcpdump: WARNING: eth0: no IPv4 address assigned
tcpdump: listening on eth0
13:58:03.823929 172.16.171.19.32770 > 172.16.171.13.telnet: R 79:79(0) ack 62 win 0
13:58:03.823930 172.16.171.19.32770 > 172.16.171.13.telnet: R 80:80(0) ack 62 win 0
13:58:03.823930 172.16.171.19.32770 > 172.16.171.13.telnet: R 80:80(0) ack 62 win 0
13:58:03.823930 172.16.171.19.32770 > 172.16.171.13.telnet: R 80:80(0) ack 62 win 0
```

Software Upgrades

This section helps in troubleshooting software upgrades. It contains the following topics:

- Issues With Automatic Update, page A-55
- Updating a Sensor with the Update Stored on the Sensor, page A-56

Upgrading and Analysis Engine

If you try to upgrade an IPS sensor, you may receive an error that Analysis Engine is not running:

```
sensor# upgrade scp://user@10.1.1.1/upgrades/IPS-K9-7.0-1-E3.pkg
Password: ********
Warning: Executing this command will apply a major version upgrade to the application
partition. The system may be rebooted to complete the upgrade.
Continue with upgrade?: yes
Error: AnalysisEngine is not running. Please reset box and attempt upgrade again.
```

If you receive this error, you must get Analysis Engine running before trying to upgrade again. This error is often caused by a defect in the currently running version. Try rebooting the sensor, and after reboot, run the **setup** command and remove the interfaces from the virtual sensor vs0. When it is not monitoring traffic, Analysis Engine usually stays up and running. You can upgrade at this time. After the upgrade, add the interfaces back to the virtual sensor vs0 using the **setup** command.

Or you can use the system image file to reimage the sensor directly to the version you want. You can reimage a sensor because the reimage process does not check to see if Analysis Engine is running.

Caution Reimaging using the system image file restores all configuration defaults.

For More Information

- For more information on running the **setup** command, see Chapter 10, "Initializing the Sensor."
- For more information on reimaging your sensor, see Chapter 12, "Upgrading, Downgrading, and Installing System Images."

Which Updates to Apply and Their Prerequisites

You must have the correct service pack and minor and major version of the software. If you are having trouble with applying new software, make sure that you are applying the proper updates with the proper prerequisites:

- Signature updates require the minimum version and engine version listed in the filename.
- Engine updates require the major or minor version in the engine update filename. Service packs require the correct minor version.
- Minor versions require the correct major version.
- Major versions require the previous major version.

For More Information

To understand how to interpret the IPS software filenames, see IPS Software Versioning, page 11-2.

Issues With Automatic Update

The following list provides suggestions for troubleshooting automatic updates:

- The Cisco.com IP address has been changed in the Auto Update configuration, which may cause connection problems.

Caution In IPS 7.0(8)E4 the default value of the Cisco server IP address has been changed from 198.133.219.25 to 72.163.4.161 in the Auto Update URL configuration. If you have automatic update configured on your sensor, you may need to update firewall rules to allow the sensor to connect to this new IP address.

- Run TCPDUMP
  - Create a service account. **Su** to root and run TCPDUMP on the command and control interface to capture packets between the sensor and the FTP server.
  - Use the **upgrade** command to manually upgrade the sensor.
  - Look at the TCPDUMP output for errors coming back from the FTP server.
- Make sure the sensor is in the correct directory.

  The directory must be specified correctly. This has caused issues with Windows FTP servers. Sometimes an extra "/" or even two "/" are needed in front of the directory name.

  To verify this, use the same FTP commands you see in the TCPDUMP output through your own FTP connection.
- You must use the Windows FTP server setup option to emulate UNIX file structure and not MS-DOS file structure.
- If you are using SCP, make sure you have added the SSH host key to the known hosts list.
- If you get an unauthorized error message while configuring an automatic update, make sure you have the correct ports open on any firewalls between the sensor and Cisco.com. For example, you need port 443 for the initial automatic update connection to www.cisco.com, and you need port 80 to download the chosen package from a Cisco file server. The IP address may change for the Cisco file server, but you can find it in the lastDownloadAttempt section in the output of the show statistics host command.

Try the manual **upgrade** command before attempting the automatic update. If it works with the **upgrade** command and does not work with the automatic update, try the following:

- Determine which IPS software version your sensor has.
- Make sure the passwords are configured for automatic update. Make sure they match the same passwords used for manual update.
- Make sure that the filenames in the FTP server are exactly what you see on Downloads on Cisco.com. This includes capitalization.

  Some Windows FTP servers allow access to the file with the incorrect capitalization but the sensor ultimately rejects the file because the name has changed.
- If necessary, run TCPDUMP on automatic update. You can compare the successful manual update with the unsuccessful automatic update and troubleshoot from there.

For More Information

- For the procedure for creating the service account, see Creating the Service Account, page A-5.
- For the procedure for reimaging your sensor, see Chapter 12, "Upgrading, Downgrading, and Installing System Images."
- For the procedure for adding hosts to the SSH known hosts list, refer to Adding Hosts to the SSH Known Hosts List.
- For the procedure for determining the software version, see Displaying Version Information, page A-77.

Updating a Sensor with the Update Stored on the Sensor

You can store the update package in the /var directory on the sensor and update the sensor from there if you need to. To update the sensor with an update stored on the sensor, follow these steps:

Step 1 Log in to the service account.

Step 2 Obtain the update package file from Cisco.com.

Step 3 FTP or SCP the update file to the sensor /usr/cids/idsRoot/var directory.

Step 4 Set the file permissions:.

```
chmod 644 ips_package_file_name
```

Step 5 Exit the service account.

Step 6 Log in to the sensor using an account with administrator privileges.

Step 7 Store the sensor host key.

```
sensor# configure terminal
sensor(config)# service ssh
sensor(config-ssh)# rsa1-keys sensor_ip_address
```

Step 8 Upgrade the sensor.

```
sensor(config)# upgrade scp://service@Sensor_ip_address/upgrade/ips_package_file_name
Enter password: *****
Re-enter password: *****
```

For More Information

For the procedure for obtaining Cisco IPS software, see Obtaining Cisco IPS Software, page 11-1.

Troubleshooting IDM

Note These procedures also apply to the IPS section of ASDM.

This section contains troubleshooting procedures for IDM. It contains the following topics:

- Cannot Launch IDM - Loading Java Applet Failed, page A-57
- Cannot Launch IDM-Analysis Engine Busy, page A-58

- IDM, Remote Manager, or Sensing Interfaces Cannot Access Sensor, page A-58
- Signatures Not Producing Alerts, page A-59

Cannot Launch IDM - Loading Java Applet Failed

Symptom The browser displays `Loading Cisco IDM. Please wait ...` At the bottom left corner of the window, `Loading Java Applet Failed` is displayed.

Possible Cause This condition can occur if multiple Java Plug-ins are installed on the machine on which you are launching IDM.

Recommended Action Clear the Java cache and remove temp files and clear history in the browser you are using. The result is that neither of these plug-ins will be used by default and each applet should use the correct plug-in.

To clear the cache, follow these steps:

Step 1 Close all browser windows.

Step 2 If you have Java Plug-in 1.3.*x* installed:

a. Click **Start** > **Settings** > **Control Panel** > **Java Plug-in 1.3.x**.
b. Click the **Advanced** tab.
c. Under Java Runtime Environment, select **JRE 1.3.x** from the drop-down menu.
d. Click the **Cache** tab.
e. Click **Clear**.

Step 3 If you have Java Plug-in 1.4.*x* installed:

a. Click **Start** > **Settings** > **Control Panel** > **Java Plug-in 1.4.x**.
b. Click the **Advanced** tab.
c. Under Java Runtime Environment, select **JRE 1.3.x** from the drop-down menu.
d. Click the **Cache** tab.
e. Click the **Browser** tab.
f. Deselect all browser check boxes.
g. Click **Clear Cache**.

Step 4 Delete the temp files and clear the history in the browser.

Cannot Launch IDM-Analysis Engine Busy

Error Message `Error connecting to sensor. Failed to load sensor-errNotAvailable-Analysis Engine is busy. Exiting IDM.`

Possible Cause This condition can occur if the Analysis Engine in the sensor is busy getting ready to perform a task and so does not respond to IDM.

Recommended Action Wait for a while and try again to connect.

IDM, Remote Manager, or Sensing Interfaces Cannot Access Sensor

If IDM, a remote manager, or sensing interfaces cannot access the sensor, but you can access the sensor CLI using SSH or Telnet (if enabled), follow these steps:

Step 1 Make sure the network configuration allows access to the web server port that is configured on the sensor:

```
sensor# setup


    --- System Configuration Dialog ---

At any point you may enter a question mark '?' for help.
User ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.


Current Configuration:


service host
network-settings
host-ip 10.89.130.108/23,10.89.130.1
host-name sensor
telnet-option enabled
access-list 0.0.0.0/0
ftp-timeout 300
no login-banner-text
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
summertime-option disabled
ntp-option disabled
exit
service web-server
port 443
exit
```

Step 2 If network devices, such as routers, switches, or firewalls, are between the sensor and the workstation, make sure these devices are configured to allow the workstation to access the sensor web server port.

All remote management communication is performed by the sensor web server.

For More Information

For the procedure for enabling and disabling Telnet on the sensor, and configuring the web server, refer to Changing Network Settings.

Signatures Not Producing Alerts

Caution You cannot add other actions each time you configure the event actions. You are actually replacing the list of event actions every time you configure it, so make sure you choose Produce Alert every time you configure event actions.

If you are not seeing any alerts when signatures are firing, make sure that you have configured Produce Alert as an event action. For example, if you choose Produce Alert, but later add another event action and do not add Produce Alert to the new configuration, alerts are not sent to the Event Store. To make sure you are getting alerts, check the statistics for the virtual sensor and Event Store.

For More Information

- For more information about event actions, refer to Event Actions.
- For the procedure for configuring event actions, refer to Assigning Actions to Signatures.
- For the procedure for obtaining statistics about virtual sensor and Event Store, refer to Displaying Statistics.

Troubleshooting IME

This section describes troubleshooting tools for IME, and contains the following sections:

Time Synchronization on IME and the Sensor

Symptom IME displays `No Data Available` on the Events dashboard. A historical query does not return any events; however, events are coming in to IME and they appear in the real-time event viewer.

Possible Cause The time is not synchronized between the sensor and the IME local server. The IME dashboards use a time relative to the IME local time. If these times are not synchronized, the query does not return any results. When you add a sensor to IME, it checks for the time synchronization and warns you to correct it if is in wrong. IME also displays a clock warning in Home > Devices > Device List to warn you about problems with synchronization.

Recommended Action Change the time settings on the sensor or IME local server. In most cases, the time change is required for the sensor because it is configured with the incorrect or default time.

For More Information

- For more information on time and the sensor, see Time Sources and the Sensor, page A-16.
- For the procedure for changing the time on the sensor, see Correcting Time on the Sensor, page A-18.

Not Supported Error Message

Symptom IME displays `Not Supported` in the device list table and in some gadgets, and no data is included.

Possible Cause Click **Details** to see an explanation for this message. IME needs IPS 6.1 or later to obtain certain information. IME still operates with event monitoring and reporting for IPS 5.0 and later and specific IOS IPS versions, but some functions, such as health information and integrated configuration, are not available.

Recommended Action Upgrade to IPS 6.1 or later.

Troubleshooting the IDSM2

This section pertains specifically to troubleshooting the IDSM2, and contains the following topics:

Diagnosing IDSM2 Problems

Use the following list to diagnose IDSM2 problems:

- The ribbon cable between the IDSM2 and the motherboard is loose.

  During physical handling of the module, the connector can come loose from the base card, and cause the daughter card and the base card to lose contact with each other. A loose ribbon cable connector causes an on-line diagnostic error on ports 7 and 8. The module cannot operate when this condition exists. For more information, refer to Partner Field Notice 29877.

- Some IDSM2s were shipped with faulty DIMMs. For the procedure for checking the IDSM2 for faulty memory, refer to Partner Field Notice 29837.
- The hard-disk drive fails to read or write. When the hard-disk drive has been in constant use for extended periods of time (for more than 2 weeks), multiple symptoms, such as the following, can occur:
  - An inability to log in
  - I/O errors to the console when doing read/write operations (the **ls** command)
  - Commands do not execute properly (cannot find the path to the executable)

  The switch reports that the module is ok, but if you log in to the Service account and try to execute commands, you see that the problem exists. The 4.1(4) service pack alleviates this problem, but if you reimage the IDSM2 with the 4.1(4) application partition image, you must apply the 4.1(4b) patch. For more information, refer to CSCef12198.
- SensorApp either crashes or takes 99% of the CPU when IP logging is enabled for stream-based signatures (1300 series). For the workaround, refer to CSCed32093.
- The IDSM2 appears to lock up and remote access is prohibited (SSH, Telnet, IDM, Event Server, Control Transaction Server, and IP log Server). This defect is related to using SWAP. The IDSM2 responds to pings. Apply the 4.1(4) service pack to resolve this issue. For more information, refer to CSCed54146.
- Shortly after you upgrade the IDSM2 or you tune a signature with VMS, the IDSM2 becomes unresponsive and often produces a SensorApp core file. Apply the 4.1(4b) patch to fix this issue.
- Confirm that the IDSM2 has the supported configurations.

If you have confirmed that the IDSM2 does not suffer from any of the problems listed above and yet it appears unresponsive, for example, you cannot log in through SSH or Telnet, nor can you session to the switch, determine if the IDSM2 responds to pings and if you can log in through the service account. If you can log in, obtain a cidDump and any core files and contact TAC.

For More Information

- The IDSM2 has the same software architecture as the 4200 series sensors. You can use the same troubleshooting tools as outlined in Troubleshooting the Appliance, page A-23.
- For information about the Bug Toolkit and how to access it, see Bug Toolkit, page A-1.
- For a table listing the supported IDSM2 configurations, see Minimum Supported IDSM2 Configurations, page A-61.

Minimum Supported IDSM2 Configurations

Note The following matrix is not intended to recommend any particular version, but rather lists the earliest supported versions.

Table A-3 lists the minimum supported configurations for the IDSM2.

Table A-3 Minimum Catalyst 6500 Software Version for IDSM2 Feature Support

Catalyst/IDSM2 Feature	Catalyst Software				Cisco IOS Software			
	Sup1	Sup2	Sup32	Sup720	Sup1	Sup2	Sup32	Sup720
SPAN	7.5(1)	7.5(1)	8.4(1)	8.1(1)	12.1(19)E1	12.1(19)E1 12.2(18)SXF1	12.2(18)SXF1	12.2(14)SX1
VACL capture[1]	7.5(1)	7.5(1)	8.4(1)	8.1(1)	12.1(19)E1	12.1(19)E1 12.2(18)SXF1	12.2(18)SXF1	12.2(14)SX1
ECLB with VACL capture[2]	8.5(1)	8.5(1)	8.5(1)	8.5(1)	N/A	12.2(18)SXF4	12.2(18)SXF1	12.2(18)SXE1
Inline interface pairs	8.4(1)	8.4(1)	8.4(1)	8.4(1)	N/A	12.2(18)SXF4	12.2(18)SXF4	12.2(18)SXE1
ECLB with inline interface pairs	8.5(1)	8.5(1)	8.5(1)	8.5(1)	N/A	12.2(18)SXF4	12.2(18)SXF4	12.2(18)SXF4
Inline VLAN pairs	8.4(1)	8.4(1)	8.4(1)	8.4(1)	N/A	12.2(18)SXF4	12.2(18)SXF4	12.2(18)SXF4
ECLB with inline VLAN pairs	8.5(1)	8.5(1)	8.5(1)	8.5(1)	N/A	12.2(18)SXF4	12.2(18)SXF4	12.2(18)SXF4

1. Requires PFC2/3 or MSFC2/3.
2. Requires PFC2/3 or MSFC2/3.

Switch Commands for Troubleshooting

The following switch commands help you troubleshoot the IDSM2:

- **show module** (Catalyst software and Cisco IOS software)
- **show version** (Catalyst software and Cisco IOS software)
- **show port** (Catalyst software)
- **show trunk** (Catalyst software)
- **show span** (Catalyst software)
- **show security acl** (Catalyst software)
- **show intrusion-detection module** (Cisco IOS software)
- **show monitor** (Cisco IOS software)
- **show vlan access-map** (Cisco IOS software)
- **show vlan filter** (Cisco IOS software)

Status LED Off

Note It is normal for the status to read `other` when the IDSM2 is first installed. After the IDSM2 completes the diagnostics routines and comes online, the status reads `ok`. Allow up to 5 minutes for the IDSM2 to come online.

If the status indicator is off on the IDSM2, you need to turn power on to the IDSM2. To determine the status of the IDSM2, follow these steps:

Step 1 Log in to the console.

Step 2 Verify that the IDSM2 is online.

- Catalyst Software

```
console> enable

Enter password:
console> (enable) show module
Mod Slot Ports Module-Type               Model               Sub Status
--- ---- ----- ------------------------- ------------------- --- --------
1   1    2     1000BaseX Supervisor      WS-X6K-SUP1A-2GE    yes ok
15  1    1     Multilayer Switch Feature WS-F6K-MSFC         no  ok
2   2    48    10/100BaseTX Ethernet     WS-X6248-RJ-45      no  ok
3   3    48    10/100/1000BaseT Ethernet WS-X6548-GE-TX      no  ok
4   4    16    1000BaseX Ethernet        WS-X6516A-GBIC      no  ok
6   6    8     Intrusion Detection Mod   WS-SVC-IDSM2        yes ok

Mod Module-Name          Serial-Num
--- -------------------- -----------
1                        SAD041308AN
15                       SAD04120BRB
2                        SAD03475400
3                        SAD073906RC
4                        SAL0751QYN0
6                        SAD062004LV

Mod MAC-Address(es)                         Hw     Fw          Sw
--- -------------------------------------- ------ ---------- ----------------
1   00-d0-c0-cc-0e-d2 to 00-d0-c0-cc-0e-d3 3.1    5.3.1      8.4(1)
    00-d0-c0-cc-0e-d0 to 00-d0-c0-cc-0e-d1
    00-30-71-34-10-00 to 00-30-71-34-13-ff
15  00-30-7b-91-77-b0 to 00-30-7b-91-77-ef 1.4    12.1(23)E2 12.1(23)E2
2   00-30-96-2b-c7-2c to 00-30-96-2b-c7-5b 1.1    4.2(0.24)V 8.4(1)
3   00-0d-29-f6-01-98 to 00-0d-29-f6-01-c7 5.0    7.2(1)     8.4(1)
4   00-0e-83-af-15-48 to 00-0e-83-af-15-57 1.0    7.2(1)     8.4(1)
6   00-e0-b0-ff-3b-80 to 00-e0-b0-ff-3b-87 0.102  7.2(0.67)  5.0(0.30)

Mod Sub-Type                Sub-Model           Sub-Serial  Sub-Hw Sub-Sw
--- ----------------------- ------------------- ----------- ------ ------
1   L3 Switching Engine     WS-F6K-PFC          SAD041303G6 1.1
6   IDS 2 accelerator board WS-SVC-IDSUPG       .           2.0
console> (enable)
```

- Cisco IOS Software

```
router# show module
Mod Ports Card Type                                Model              Serial No.
--- ----- ------------------------------------- ------------------ -----------
  1   48  48 port 10/100 mb RJ-45 ethernet       WS-X6248-RJ-45     SAD0401012S
  2   48  48 port 10/100 mb RJ45                 WS-X6348-RJ-45     SAL04483QBL
  3   48  SFM-capable 48 port 10/100/1000mb RJ45 WS-X6548-GE-TX     SAD073906GH
  5    8  Intrusion Detection System             WS-SVC-IDSM2      SAD0751059U
  6   16  SFM-capable 16 port 1000mb GBIC        WS-X6516A-GBIC     SAL0740MMYJ
  7    2  Supervisor Engine 720 (Active)         WS-SUP720-3BXL     SAD08320L2T
  9    1  1 port 10-Gigabit Ethernet Module      WS-X6502-10GE      SAD071903BT
 11    8  Intrusion Detection System             WS-SVC-IDSM2       SAD05380608
 13    8  Intrusion Detection System             WS-SVC-IDSM2      SAD072405D8

Mod MAC addresses                       Hw    Fw           Sw           Status
```

```
--- ---------------------------------- ------ ------------ ------------ -------
  1  00d0.d328.e2ac to 00d0.d328.e2db   1.1   4.2(0.24)VAI 8.5(0.46)ROC Ok
  2  0003.6c14.e1d0 to 0003.6c14.e1ff   1.4   5.4(2)       8.5(0.46)ROC Ok
  3  000d.29f6.7a80 to 000d.29f6.7aaf   5.0   7.2(1)       8.5(0.46)ROC Ok
  5  0003.fead.651a to 0003.fead.6521   4.0   7.2(1)       5.0(1.1)     Ok
  6  000d.ed23.1658 to 000d.ed23.1667   1.0   7.2(1)       8.5(0.46)ROC Ok
  7  0011.21a1.1398 to 0011.21a1.139b   4.0   8.1(3)       12.2(PIKESPE Ok
  9  000d.29c1.41bc to 000d.29c1.41bc   1.3   Unknown      Unknown      PwrDown
 11  00e0.b0ff.3340 to 00e0.b0ff.3347   0.102 7.2(0.67)    5.0(1.1)     Ok
 13  0003.feab.c850 to 0003.feab.c857   4.0   7.2(1)       5.0(1)       Ok

Mod Sub-Module                  Model               Serial        Hw     Status
--- --------------------------- ------------------ ------------ ------- -------
  5 IDS 2 accelerator board     WS-SVC-IDSUPG      07E91E508A    2.0    Ok
  7 Policy Feature Card 3       WS-F6K-PFC3BXL     SAD083305A1   1.3    Ok
  7 MSFC3 Daughterboard         WS-SUP720          SAD083206JX   2.1    Ok
 11 IDS 2 accelerator board     WS-SVC-IDSUPG      .             2.0    Ok
 13 IDS 2 accelerator board     WS-SVC-IDSUPG      0347331976    2.0    Ok

Mod Online Diag Status
--- -------------------
  1 Pass
  2 Pass
  3 Pass
  5 Pass
  6 Pass
  7 Pass
  9 Unknown
 11 Pass
 13 Pass
router#
```

Step 3 If the status does not read `ok`, turn the module on.

```
router# set module power up module_number
```

Status LED On But the IDSM2 Does Not Come Online

If the status indicator is on, but the IDSM2 does not come online, try the following troubleshooting tips:

- Reset the IDSM2.
- Make sure the IDSM2 is installed properly in the switch.
- If the hard-disk drive status has failed, reimage the application partition.

To enable the IDSM2, follow these steps:

Step 1 Log in to the console.

Step 2 Make sure the IDSM2 is enabled.

```
router# show module
```

Step 3 If the status does not read `ok`, enable the IDSM2.

```
router# set module enable module_number
```

Step 4 If the IDSM2 still does not come online, reset it.

```
router# reset module_number
```

Wait for about 5 minutes for the IDSM2 to come online.

Step 5 If the IDSM2 still does not come online, make sure the hardware and operating system are ok.

```
router# show test module_number
```

Step 6 If the `port` status reads `fail`, make sure the IDSM2 is firmly connected in the switch.

Step 7 If the `hdd` status reads `fail`, you must reimage the application partition.

For More Information

For the procedure for reimaging the application partition, see Recovering the Application Partition, page 12-11.

Cannot Communicate With the IDSM2 Command and Control Port

If you cannot communicate with the IDSM2 command and control port, the command and control port may not be in the correct VLAN. To communicate with the command and control port of the IDSM2, follow these steps:

Step 1 Log in to the console.

Step 2 Make sure you can ping the command port from any other system.

Step 3 Make sure the IP address, mask, and gateway settings are correct.

```
router# show configuration
```

Step 4 Make sure the command and control port is in the correct VLAN.

- Catalyst software

```
console> (enable) show port 6/8
* = Configured MAC Address

# = 802.1X Authenticated Port Name.

Port  Name                 Status     Vlan       Duplex Speed       Type
----- -------------------- ---------- ---------- ------ ----------- ------------
 6/8                       connected  trunk        full        1000 IDS


Port  Status      ErrDisable Reason    Port ErrDisableTimeout  Action on Timeout
----  ----------  -------------------  ----------------------  -----------------
 6/8  connected                      -  Enable                  No Change

Port  Align-Err  FCS-Err    Xmit-Err   Rcv-Err    UnderSize
----- ---------- ---------- ---------- ---------- ---------
 6/8           0          0          0          0         0

Port  Single-Col Multi-Coll Late-Coll  Excess-Col Carri-Sen Runts     Giants
----- ---------- ---------- ---------- ---------- --------- --------- ---------
 6/8           0          0          0          0         0         0         -

Port  Last-Time-Cleared
----- --------------------------
 6/8  Wed Mar 2 2005, 15:29:49
```

```
Idle Detection
--------------
   --
console> (enable)
```

- Cisco IOS Software

```
router# show intrusion-detection module 5 management-port state
Intrusion-detection module 5 management-port:

Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Vlans allowed on trunk:1
Vlans allowed and active in management domain: 1
Vlans in spanning tree forwarding state and not pruned:
   1
Access Vlan = 1


router#
```

Step 5 If the command and control port is not in the correct VLAN, put it in the correct VLAN.

For More Information

For the procedure for configuring the switch for command and control access to the IDSM2, refer to Configuring the Catalyst 6500 Series Switch for Command and Control Access to the IDSM2.

Using the TCP Reset Interface

The IDSM2 has a TCP reset interface—port 1. The IDSM2 has a specific TCP reset interface because it cannot send TCP resets on its sensing ports.

If you have reset problems with the IDSM2, and the switch is running Catalyst software, try the following:

- If the sensing ports are access ports (a single VLAN), you need to configure the reset port to be in the same VLAN.
- If the sensing ports are dot1q trunk ports (multi-VLAN), the sensing ports and reset port all must have the same native VLAN, and the reset port must trunk all the VLANs being trunked by both the sensing ports.

Note In Cisco IOS when the IDSM2 is in promiscuous mode, the IDSM2 ports are always dot1q trunk ports (even when monitoring only 1 VLAN), and the TCP reset port is automatically set to a trunk port and is not configurable.

For More Information

For more information about the IDSM2 and TCP reset, refer to Configuring the IDSM2.

Connecting a Serial Cable to the IDSM2

You can connect a serial cable directly to the serial console port on the IDSM2. This lets you bypass the switch and module network interfaces. To connect a serial cable to the IDSM2, follow these steps:

Step 1 Locate the two RJ-45 ports on the IDSM2. You can find them approximately in the center of the mother board. If you are facing the module faceplate, the RJ-45 port on the right is the serial console port.

Step 2 Connect a straight-through cable to the right port on the IDSM2, and then connect the other end of the cable to a terminal server port.

Step 3 Configure the terminal server port to be 19200 baud, 8 bits, no parity. You can now log directly in to the IDSM2.

Note Connecting a serial cable to the IDSM2 works only if there is no module located above the IDSM2 in the switch chassis, because the cable has to come out through the front of the chassis.

Troubleshooting the AIP SSM

The following section contains information for troubleshooting the AIP SSM, and contains the following topics:

Health and Status Information

To see the general health of the AIP SSM, use the **show module 1 details** command:

```
asa# show module 1 details
Getting details from the Service Module, please wait...
ASA 5500 Series Security Services Module-20
Model:              ASA-SSM-20
Hardware version:   0.2
Serial Number:      P2B000005D0
Firmware version:   1.0(10)0
Software version:   5.1(0.1)S153.0
Status:             Up
Mgmt IP addr:       10.89.149.219
Mgmt web ports:     443
Mgmt TLS enabled:   true
asa#
```

The output shows that the AIP SSM is up. If the status reads `Down`, you can reset the AIP module using the **hw-module module 1 reset** command:

```
asa# hw-module module 1 reset
The module in slot 1 should be shut down before
resetting it or loss of configuration may occur.
Reset module in slot 1? [confirm]
Reset issued for module in slot 1
asa(config)# show module

Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  0 ASA 5520 Adaptive Security Appliance         ASA5520            P2A00000014
  1 ASA 5500 Series Security Services Module-10  ASA-SSM-10         P2A0000067U

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  0 000b.fcf8.7bdc to 000b.fcf8.7be0  0.2          1.0(10)0     7.0(1)
  1 000b.fcf8.0176 to 000b.fcf8.0176  0.2          1.0(10)0     5.1(0.1)S153.0

Mod Status
--- ------------------
  0 Up Sys
  1 Shutting Down
**************************************************
asa(config)# show module

Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  0 ASA 5520 Adaptive Security Appliance         ASA5520            P2A00000014
  1 ASA 5500 Series Security Services Module-10  ASA-SSM-10         P2A0000067U

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  0 000b.fcf8.7bdc to 000b.fcf8.7be0  0.2          1.0(10)0     7.0(1)
  1 000b.fcf8.0176 to 000b.fcf8.0176  0.2          1.0(10)0     5.1(0.1)S153.0

Mod Status
--- ------------------
  0 Up Sys
  1 Up
asa(config)#
```

If you have problems with recovering the AIP SSM, use the **debug module-boot** command to see the output as the AIP module boots. Make sure you have the correct IP address for the TFTP server and you have the correct file on the TFTP server. Then use the **hw-module module 1 recover** command again to recover the module:

```
asa(config)# hw-module module 1 recover configure
Image URL [tftp://0.0.0.0/]: tftp://10.89.146.1/IPS-SSM-K9-sys-1.1-a-5.1-0.1.i$
Port IP Address [0.0.0.0]: 10.89.150.227
VLAN ID [0]:
Gateway IP Address [0.0.0.0]: 10.89.149.254
asa(config)# debug module-boot
debug module-boot  enabled at level 1
asa(config)# hw-module module 1 recover boot
The module in slot 1 will be recovered.  This may erase all configuration and all data on
that device and attempt to download a new image for it.
Recover module in slot 1? [confirm]
Recover issued for module in slot 1
asa(config)# Slot-1 140> Cisco Systems ROMMON Version (1.0(10)0) #0: Fri Mar 25 23:02:10
PST 2005
```

```
Slot-1 141> Platform ASA-SSM-10
Slot-1 142> GigabitEthernet0/0
Slot-1 143> Link is UP
Slot-1 144> MAC Address: 000b.fcf8.0176
Slot-1 145> ROMMON Variable Settings:
Slot-1 146>   ADDRESS=10.89.150.227
Slot-1 147>   SERVER=10.89.146.1
Slot-1 148>   GATEWAY=10.89.149.254
Slot-1 149>   PORT=GigabitEthernet0/0
Slot-1 150>   VLAN=untagged
Slot-1 151>   IMAGE=IPS-SSM-K9-sys-1.1-a-5.1-0.1.img
Slot-1 152>   CONFIG=
Slot-1 153>   LINKTIMEOUT=20
Slot-1 154>   PKTTIMEOUT=4
Slot-1 155>   RETRY=20
Slot-1 156> tftp IPS-SSM-K9-sys-1.1-a-5.1-0.1.img@10.89.146.1 via 10.89.149.254
Slot-1 157> TFTP failure: Packet verify failed after 20 retries
Slot-1 158> Rebooting due to Autoboot error ...
Slot-1 159> Rebooting....
Slot-1 160> Cisco Systems ROMMON Version (1.0(10)0) #0: Fri Mar 25 23:02:10 PST 2005
Slot-1 161> Platform ASA-SSM-10
Slot-1 162> GigabitEthernet0/0
Slot-1 163> Link is UP
Slot-1 164> MAC Address: 000b.fcf8.0176
Slot-1 165> ROMMON Variable Settings:
Slot-1 166>   ADDRESS=10.89.150.227
Slot-1 167>   SERVER=10.89.146.1
Slot-1 168>   GATEWAY=10.89.149.254
Slot-1 169>   PORT=GigabitEthernet0/0
Slot-1 170>   VLAN=untagged
Slot-1 171>   IMAGE=IPS-SSM-K9-sys-1.1-a-5.1-0.1.img
Slot-1 172>   CONFIG=
Slot-1 173>   LINKTIMEOUT=20
Slot-1 174>   PKTTIMEOUT=4
Slot-1 175>   RETRY=20
Slot-1 176> tftp IPS-SSM-K9-sys-1.1-a-5.1-0.1.img@10.89.146.1 via 10.89.149.254
```

For More Information

The AIP SSM has the same software architecture as the 4200 series sensors. You can use the same troubleshooting tools as outlined in Troubleshooting the Appliance, page A-23.

Failover Scenarios

The following failover scenarios apply to the ASA in the event of configuration changes, signature/signature engine updates, service packs, and SensorApp crashes on the AIP SSM.

Single ASA in Fail-Open Mode

- If the ASA is configured in fail-open mode for the AIP SSM, and the AIP SSM experiences a configuration change or signature/signature engine update, traffic is passed through the ASA without being inspected.
- If the ASA is configured in fail-open mode for the AIP SSM, and the AIP SSM experiences a SensorApp crash or a service pack upgrade, traffic is passed through the ASA without being inspected.

Single ASA in Fail-Close Mode

- If the ASA is configured in fail-close mode for the AIP SSM, and the AIP SSM experiences a configuration change or a signature/signature engine update, traffic is stopped from passing through the ASA.
- If the ASA is configured in fail-close mode for the AIP SSM, and the AIP SSM experiences a SensorApp crash or a service pack upgrade, traffic is stopped from passing through the ASA.

Two ASAs in Fail-Open Mode

- If the ASAs are configured in fail-open mode and if the AIP SSM on the active ASA experiences a configuration change or a signature/signature engine update, traffic is still passed through the active ASA without being inspected. Failover is not triggered.
- If the ASAs are configured in fail-open mode, and if the AIP SSM on the active ASA experiences a SensorApp crash or a service pack upgrade, failover is triggered and traffic passes through the AIP SSM that was previously the standby module.

Two ASAs in Fail-Close Mode

- If the ASAs are configured in fail-close mode, and if the AIP SSM on the active ASA experiences a configuration change or a signature/signature engine update, traffic is stopped from passing through the active ASA. No failover is triggered.
- If the ASAs are configured in fail-close mode, and if the AIP SSM on the active ASA experiences a SensorApp crash or a service pack upgrade, failover is triggered and traffic passes through the module that was previously the standby for the AIP SSM.

Configuration Examples

Use the following configuration for the primary ASA:

```
interface GigabitEthernet0/7
 description LAN Failover Interface

failover
failover lan unit primary
failover lan interface folink GigabitEthernet0/7
failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
```

Use the following configuration for the secondary ASA:

```
interface GigabitEthernet0/7
 description LAN Failover Interface

failover
failover lan unit secondary
failover lan interface folink GigabitEthernet0/7
failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
```

The AIP SSM and the Data Plane

Symptom The AIP SSM data plane is kept in the Up state while applying signature updates. You can check the AIP SSM data plane status by using the **show module** command during signature updates.

Possible Cause Bypass mode is set to off. The issue is seen when updating signatures, and when you use either CSM or IDM to apply signature updates. This issue is not seen when upgrading IPS system software.

The AIM SSP and the Normalizer Engine

The majority of the features in the Normalizer engine are not used on the AIP SSM, because the ASA itself handles the normalization. Packets on the ASA IPS modules go through a special path in the Normalizer that only reassembles fragments and puts packets in the right order for the TCP stream. The Normalizer does not do any of the normalization that is done on an inline IPS appliance, because that causes problems in the way the ASA handles the packets.

The following Normalizer engine signatures are not supported:

- 1300.0
- 1304.0
- 1305.0
- 1307.0
- 1308.0
- 1309.0
- 1311.0
- 1315.0
- 1316.0
- 1317.0
- 1330.0
- 1330.1
- 1330.2
- 1330.9
- 1330.10
- 1330.12
- 1330.14
- 1330.15
- 1330.16
- 1330.17
- 1330.18

For More Information

For detailed information about the Normalizer engine, refer to Normalizer Engine.

TCP Reset Differences Between IPS Appliances and the AIP SSM

The IPS appliance sends TCP reset packets to both the attacker and victim when is selected. The IPS appliance sends a TCP reset packet only to the victim under the following circumstances:

- When a or is selected
- When TCP-based signatures and have NOT been selected

In the case of the AIP SSM, the TCP reset request is sent to the ASA, and then the ASA sends the TCP reset packets. The ASA sends TCP reset packets to both the attacker and victim when the is selected. When or is selected, the ASA sends the TCP reset packet to either the attacker or victim depending on the configuration of the signature. Signatures configured to swap the attacker and victim when reporting the alert can cause the ASA to send the TCP reset packet to the attacker.

For More Information

For detailed information about event actions, refer to Event Actions.

Troubleshooting the AIM IPS and the NME IPS

This section contains information for troubleshooting the IPS network modules, the AIM IPS and the NME IPS. It contains the following section:

- Interoperability With Other IPS Network Modules, page A-72

Interoperability With Other IPS Network Modules

Caution You cannot upgrade an NM CIDS to an NME IPS.

The Cisco access routers only support one IDS/IPS module per router. If you have more than one IDS/IPS module installed, the most capable card is enabled. The most capable hierarchy is:

1. NME IPS
2. AIM IPS
3. NM CIDS

This means, for example, that if all modules are installed, the NME IPS disables all other modules. The AIM IPS disables all NM CIDS. If there are multiple modules with the same level of capability, the first one discovered is enabled and all others are disabled.

You cannot bring up, enable, or configure a disabled module. To bring up a less capable module, you must remove the more capable module from the router and reboot. Disabled modules are reported in the **show diag** command output. The state of the module is reported as present but disabled.

If the most capable module slot and port do not match the **interface ids slot/port** configuration command, the most capable module is disabled with the following warning:

```
The module in slot x will be disabled and configuration ignored.
```

The correct slot/port number are displayed so that you can change the configuration.

For More Information

For more information on the NM CIDS, refer to Introducing the NM CIDS and Installing the NM CIDS.

Gathering Information

You can use the following CLI commands and scripts to gather information and diagnose the state of the sensor when problems occur. You can use the **show tech-support** command to gather all the information of the sensor, or you can use the other individual commands listed in this section for specific information. This section describes how to use CLI commands to obtain information about your sensor, contains the following topics:

Health and Network Security Information

Use the **show health** command in privileged EXEC mode to display the overall health status information of the sensor. The health status categories are rated by red and green with red being critical.

Caution When the sensor is first starting, it is normal for certain health metric statuses to be red until the sensor is fully up and running.

To display the overall health status of the sensor, follow these steps:

Step 1 Log in to the CLI.

Step 2 Show the health and security status of the sensor.

```
sensor# show health
Overall Health Status                                  Red
Health Status for Failed Applications                  Green
Health Status for Signature Updates                    Green
Health Status for License Key Expiration               Red
Health Status for Running in Bypass Mode               Green
Health Status for Interfaces Being Down                Red
Health Status for the Inspection Load                  Green
Health Status for the Time Since Last Event Retrieval  Green
Health Status for the Number of Missed Packets         Green
Health Status for the Memory Usage                     Not Enabled
```

```
Security Status for Virtual Sensor vs0   Green
sensor#
```

Tech Support Information

The **show tech-support** command is useful for capturing all sensor status and configuration information. This section describes the **show tech-support** command, and contains the following topics:

- Understanding the show tech-support Command, page A-74
- Displaying Tech Support Information, page A-74
- Tech Support Command Output, page A-75

Understanding the show tech-support Command

Note Always run the **show tech-support** command before contacting TAC.

The **show tech-support** command captures all status and configuration information on the sensor and includes the current configuration, version information, and cidDump information. The output can be large, over 1 MB. You can transfer the output to a remote system.

For More Information

For the procedure for copying the output to a remote system, see Displaying Tech Support Information, page A-74.

Displaying Tech Support Information

Use the **show tech-support** [**page**] [**destination-url** *destination_url*] command to display system information on the screen or have it sent to a specific URL. You can use the information as a troubleshooting tool with TAC.

The following parameters are optional:

- **page**—Displays the output, one page of information at a time.

  Press **Enter** to display the next line of output or use the spacebar to display the next page of information.
- **destination-url**—Indicates the information should be formatted as HTML and sent to the destination that follows this command. If you use this keyword, the output is not displayed on the screen.
- *destination_url*—Indicates the information should be formatted as HTML. The URL specifies where the information should be sent. If you do not use this keyword, the information is displayed on the screen.

To display tech support information, follow these steps:

Step 1 Log in to the CLI using an account with administrator privileges.

Step 2 View the output on the screen.

```
sensor# show tech-support page
```

The system information appears on the screen, one page at a time. Press the spacebar to view the next page or press **Ctrl-C** to return to the prompt.

Step 3 Send the output (in HTML format) to a file, follow these steps.

a. Enter the following command, followed by a valid destination.

```
sensor# show tech-support destination-url destination_url
```

You can specify the following destination types:

- **ftp:**—Destination URL for FTP network server. The syntax for this prefix is `ftp:[[//username@location]/relativeDirectory]/filename` or `ftp:[[//username@location]//absoluteDirectory]/filename`.
- **scp:**—Destination URL for the SCP network server. The syntax for this prefix is `scp:[[//username@]location]/relativeDirectory]/filename` or `scp:[[//username@]location]//absoluteDirectory]/filename`.

For example, to send the tech support output to the file `/absolute/reports/sensor1Report.html`:

```
sensor# show tech support dest
ftp://csidsuser@10.2.1.2//absolute/reports/sensor1Report.html
```

The `password:` prompt appears.

b. Enter the password for this user account. The `Generating report:` message is displayed.

Tech Support Command Output

The following is an example of the **show tech-support** command output:

Note This output example shows the first part of the command and lists the information for the Interfaces, ARC, and cidDump services.

```
sensor# show tech-support page
System Status Report
This Report was generated on Wed Apr  8 21:42:39 2009.
Output from show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.0(1)E3

Host:
    Realm Keys          key1.0
Signature Definition:
    Signature Update    S383.0                  2009-02-20
    Virus Update        V1.4                    2007-03-02
OS Version:             2.4.30-IDS-smp-bigphys
Platform:               IPS 4240-K9
Serial Number:          JMX1013K020
```

```
No license present
Sensor up-time is 1 day.
Using 1421914112 out of 1984552960 bytes of available memory (71% usage)
system is using 16.5M out of 38.5M bytes of available disk space (43% usage)
application-data is using 43.5M out of 166.8M bytes of available disk space (27%
 usage)
boot is using 40.5M out of 68.6M bytes of available disk space (62% usage)
application-log is using 123.5M out of 513.0M bytes of available disk space (24%
 usage)


MainApp            B-BEAU_2009_APR_07_08_00_7_0_0_118   (Release)   2009-04-07T0
8:05:05-0500   Running
AnalysisEngine     B-BEAU_2009_APR_07_08_00_7_0_0_118   (Release)   2009-04-07T0
8:05:05-0500   Running
CollaborationApp   B-BEAU_2009_APR_07_08_00_7_0_0_118   (Release)   2009-04-07T0
8:05:05-0500   Running
CLI                B-BEAU_2009_APR_07_08_00_7_0_0_118   (Release)   2009-04-07T0
8:05:05-0500

Upgrade History:

  IPS-K9-7.0-E3   21:41:28 UTC Mon Feb 22 2010

Recovery Partition Version 1.1 - 7.0(1)E3

Host Certificate Valid from: 08-Apr-2009 to 09-Apr-2011


Output from show interfaces
Interface Statistics
   Total Packets Received = 0
   Total Bytes Received = 0
   Missed Packet Percentage = 0
   Current Bypass Mode = Auto_off
MAC statistics from interface GigabitEthernet0/0
   Interface function = Sensing interface
   Description =
   Media Type = TX
   Default Vlan = 0
   Inline Mode = Unpaired
   Pair Status = N/A
   Hardware Bypass Capable = No
   Hardware Bypass Paired = N/A
   Link Status = Down
   Admin Enabled Status = Disabled
   Link Speed = N/A
   Link Duplex = N/A
   Missed Packet Percentage = 0
   Total Packets Received = 0
   Total Bytes Received = 0
   Total Multicast Packets Received = 0
   Total Broadcast Packets Received = 0
   Total Jumbo Packets Received = 0
   Total Undersize Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 0
   Total Bytes Transmitted = 0
   Total Multicast Packets Transmitted = 0
   Total Broadcast Packets Transmitted = 0
   Total Jumbo Packets Transmitted = 0
   Total Undersize Packets Transmitted = 0
   Total Transmit Errors = 0
```

```
   Total Transmit FIFO Overruns = 0
MAC statistics from interface Management0/0
   Interface function = Command-control interface
--MORE--
```

Version Information

The **show version** command is useful for obtaining sensor information. This section describes the **show version** command, and contains the following topics:

- Understanding the show version Command, page A-77
- Displaying Version Information, page A-77

Understanding the show version Command

The **show version** command shows the basic sensor information and can indicate where a failure is occurring. It gives the following information:

- Which applications are running
- Versions of the applications
- Disk and memory usage
- Upgrade history of the applications

Note To get the same information from IDM, choose **Monitoring > Sensor Monitoring > Support Information > Diagnostics Report.** To get the same information from IME, choose **Configuration >** ***sensor_name*** **> Sensor Monitoring > Support Information > Diagnostics Report.**

Displaying Version Information

Use the **show version** command to display version information for all installed operating system packages, signature packages, and IPS processes running on the system. To view the configuration for the entire system, use the **more current-config** command.

To display the version and configuration, follow these steps:

Step 1 Log in to the CLI.

Step 2 View version information.

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.0(1)E3

Host:
    Realm Keys          key1.0
Signature Definition:
    Signature Update    S383.0                  2009-02-20
    Virus Update        V1.4                    2007-03-02
OS Version:             2.4.30-IDS-smp-bigphys
Platform:               IPS 4240-K9
Serial Number:          JMX1013K020
```

```
No license present
Sensor up-time is 23:01.
Using 1421856768 out of 1984552960 bytes of available memory (71% usage)
system is using 16.5M out of 38.5M bytes of available disk space (43% usage)
application-data is using 43.5M out of 166.8M bytes of available disk space (27%
 usage)
boot is using 40.5M out of 68.6M bytes of available disk space (62% usage)
application-log is using 123.5M out of 513.0M bytes of available disk space (24%
 usage)


MainApp            B-BEAU_2009_APR_07_08_00_7_0_0_118   (Release)   2009-04-07T0
8:05:05-0500   Running
AnalysisEngine     B-BEAU_2009_APR_07_08_00_7_0_0_118   (Release)   2009-04-07T0
8:05:05-0500   Running
CollaborationApp   B-BEAU_2009_APR_07_08_00_7_0_0_118   (Release)   2009-04-07T0
8:05:05-0500   Running
CLI                B-BEAU_2009_APR_07_08_00_7_0_0_118   (Release)   2009-04-07T0
8:05:05-0500

Upgrade History:

  IPS-K9-7.0-1-E3   21:41:28 UTC Mon Feb 22 2010

Recovery Partition Version 1.1 - 7.0(1)E3

Host Certificate Valid from: 08-Apr-2009 to 09-Apr-2011
sensor#
```

Note If the `--MORE--` prompt is displayed, press the spacebar to see more information or **Ctrl-C** to cancel the output and get back to the CLI prompt.

Step 3 View configuration information.

Note You can use the **more current-config** or **show configuration** commands.

```
sensor# more current-config
! ------------------------------
! Current configuration last modified Fri Apr 10 13:29:06 2009
! ------------------------------
! Version 7.0(1)
! Host:
!     Realm Keys          key1.0
! Signature Definition:
!     Signature Update    S383.0   2009-02-20
!     Virus Update        V1.4     2007-03-02
! ------------------------------
service interface
exit
! ------------------------------
service authentication
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
service host
network-settings
host-ip 10.89.147.24/25,10.89.147.126
telnet-option enabled
```

```
access-list 0.0.0.0/0
exit
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
exit
! ------------------------------
service notification
exit
! ------------------------------
service signature-definition sig0
exit
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
service trusted-certificates
exit
! ------------------------------
service web-server
exit
! ------------------------------
service anomaly-detection ad0
exit
! ------------------------------
service external-product-interface
exit
! ------------------------------
service health-monitor
exit
! ------------------------------
service global-correlation
exit
! ------------------------------
service analysis-engine
exit
sensor#
```

Statistics Information

The **show statistics** command is useful for examining the state of the sensor services. This section describes the **show statistics** command, and contains the following topics:

- Understanding the show statistics Command, page A-79
- Displaying Statistics, page A-80

Understanding the show statistics Command

The **show statistics** command provides a snapshot of the state of the sensor services. The following services provide statistics:

- Analysis Engine
- Authentication

- Denied Attackers
- Event Server
- Event Store
- Host
- Logger
- Attack Response (formerly known as Network Access)
- Notification
- SDEE Server
- Transaction Server
- Transaction Source
- Virtual Sensor
- Web Server

Note To get the same information from IDM, choose **Monitoring > Sensor Monitoring > Support Information > Statistics.** To get the same information from IME, choose **Configuration >** ***sensor_name*** **> Sensor Monitoring > Support Information >Statistics**.

Displaying Statistics

Use the **show statistics [analysis-engine | anomaly-detection | authentication | denied-attackers | event-server | event-store | external-product-interface | global-correlation | host | logger | network-access | notification | os-identification | sdee-server | transaction-server | virtual-sensor | web-server**] [**clear**] command to display statistics for each sensor application.

Use the **show statistics** {**anomaly-detection | denied-attackers | os-identification | virtual-sensor**} [***name*** **| clear**] to display statistics for these components for all virtual sensors. If you provide the virtual sensor name, the statistics for that virtual sensor only are displayed.

Note The **clear** option is not available for the analysis engine, anomaly detection, host, network access, or OS identification applications.

To display statistics for the sensor, follow these steps:

Step 1 Log in to the CLI.

Step 2 Display the statistics for Analysis Engine.

```
sensor# show statistics analysis-engine
Analysis Engine Statistics
   Number of seconds since service started = 1421127
   Measure of the level of current resource utilization = 0
   Measure of the level of maximum resource utilization = 0
   The rate of TCP connections tracked per second = 0
   The rate of packets per second = 0
   The rate of bytes per second = 0
   Receiver Statistics
      Total number of packets processed since reset = 0
      Total number of IP packets processed since reset = 0
   Transmitter Statistics
```

```
      Total number of packets transmitted = 0
      Total number of packets denied = 0
      Total number of packets reset = 0
   Fragment Reassembly Unit Statistics
      Number of fragments currently in FRU = 0
      Number of datagrams currently in FRU = 0
   TCP Stream Reassembly Unit Statistics
      TCP streams currently in the embryonic state = 0
      TCP streams currently in the established state = 0
      TCP streams currently in the closing state = 0
      TCP streams currently in the system = 0
      TCP Packets currently queued for reassembly = 0
   The Signature Database Statistics.
      Total nodes active = 0
      TCP nodes keyed on both IP addresses and both ports = 0
      UDP nodes keyed on both IP addresses and both ports = 0
      IP nodes keyed on both IP addresses = 0
   Statistics for Signature Events
      Number of SigEvents since reset = 0
   Statistics for Actions executed on a SigEvent
      Number of Alerts written to the IdsEventStore = 0
sensor#
```

Step 3 Display the statistics for anomaly detection.

```
sensor# show statistics anomaly-detection
Statistics for Virtual Sensor vs0
   No attack
   Detection - ON
   Learning - ON
   Next KB rotation at 10:00:01 UTC Sat Jan 18 2008
   Internal Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
   External Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
   Illegal Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
Statistics for Virtual Sensor vs1
   No attack
   Detection - ON
   Learning - ON
   Next KB rotation at 10:00:00 UTC Sat Jan 18 2008
   Internal Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
   External Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
   Illegal Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
sensor#
```

Step 4 Display the statistics for authentication.

```
sensor# show statistics authentication
General
   totalAuthenticationAttempts = 128
   failedAuthenticationAttempts = 0
sensor#
```

Step 5 Display the statistics for the denied attackers in the system.

```
sensor# show statistics denied-attackers
Denied Attackers and hit count for each.
Denied Attackers and hit count for each.
Statistics for Virtual Sensor vs0
   Denied Attackers with percent denied and hit count for each.


   Denied Attackers with percent denied and hit count for each.


Statistics for Virtual Sensor vs1
   Denied Attackers with percent denied and hit count for each.


   Denied Attackers with percent denied and hit count for each.


sensor#
```

Step 6 Display the statistics for Event Server.

```
sensor# show statistics event-server
General
   openSubscriptions = 0
   blockedSubscriptions = 0
Subscriptions
sensor#
```

Step 7 Display the statistics for Event Store.

```
sensor# show statistics event-store
Event store statistics
   General information about the event store
      The current number of open subscriptions = 2
      The number of events lost by subscriptions and queries = 0
      The number of queries issued = 0
      The number of times the event store circular buffer has wrapped = 0
   Number of events of each type currently stored
      Debug events = 0
      Status events = 9904
      Log transaction events = 0
      Shun request events = 61
      Error events, warning = 67
      Error events, error = 83
      Error events, fatal = 0
      Alert events, informational = 60
      Alert events, low = 1
      Alert events, medium = 60
      Alert events, high = 0
sensor#
```

Step 8 Display the statistics for global correlation:

```
sensor# show statistics global-correlation
Network Participation:
```

```
   Counters:
      Total Connection Attempts = 0
      Total Connection Failures = 0
      Connection Failures Since Last Success = 0
   Connection History:
Updates:
   Status Of Last Update Attempt = Disabled
   Time Since Last Successful Update = never
   Counters:
      Update Failures Since Last Success = 0
      Total Update Attempts = 0
      Total Update Failures = 0
   Update Interval In Seconds = 300
   Update Server = update-manifests.ironport.com
   Update Server Address = Unknown
   Current Versions:
Warnings:
   Unlicensed = Global correlation inspection and reputation filtering have been
 disabled because the sensor is unlicensed.
   Action Required = Obtain a new license from http://www.cisco.com/go/license.
sensor#
```

Step 9 Display the statistics for the host.

```
sensor# show statistics host
General Statistics
   Last Change To Host Config (UTC) = 16:11:05 Thu Feb 10 2008
   Command Control Port Device = FastEthernet0/0
Network Statistics
   fe0_0     Link encap:Ethernet HWaddr 00:0B:46:53:06:AA
             inet addr:10.89.149.185 Bcast:10.89.149.255 Mask:255.255.255.128
             UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
             RX packets:1001522 errors:0 dropped:0 overruns:0 frame:0
             TX packets:469569 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:57547021 (54.8 Mib) TX bytes:63832557 (60.8 MiB)
             Interrupt:9 Base address:0xf400 Memory:c0000000-c0000038
NTP Statistics
   status = Not applicable
Memory Usage
   usedBytes = 500592640
   freeBytes = 8855552
   totalBytes = 509448192
Swap Usage
   Used Bytes = 77824
   Free Bytes = 600649728

   Total Bytes = 600727552
CPU Statistics
   Usage over last 5 seconds = 0
   Usage over last minute = 1
   Usage over last 5 minutes = 1
Memory Statistics
   Memory usage (bytes) = 500498432
   Memory free (bytes) = 894976032
Auto Update Statistics
   lastDirectoryReadAttempt = 15:26:33 CDT Tue Jun 17 2008
    =   Read directory: http://tester@198.133.219.243//cisco/ciscosecure/ips/6.x/sigup/
    =   Success
   lastDownloadAttempt = 15:26:33 CDT Tue Jun 17 2008
    =   Download: http://bmarquardt@198.133.219.243//cisco/ciscosecure/ips/6.x/sigup/IPS-
sig-S338-req-E1.pkg
    =   Error: httpResponse status returned:  Unauthorized
   lastInstallAttempt = N/A
```

```
   nextAttempt = 16:26:30 CDT Tue Jun 17 2008

sensor#
```

Step 10 Display the statistics for the logging application.

```
sensor# show statistics logger
The number of Log interprocessor FIFO overruns = 0
The number of syslog messages received = 11
The number of <evError> events written to the event store by severity
   Fatal Severity = 0
   Error Severity = 64
   Warning Severity = 35
   TOTAL = 99
The number of log messages written to the message log by severity
   Fatal Severity = 0
   Error Severity = 64
   Warning Severity = 24
   Timing Severity = 311
   Debug Severity = 31522
   Unknown Severity = 7
   TOTAL = 31928
sensor#
```

Step 11 Display the statistics for ARC.

```
sensor# show statistics network-access
Current Configuration
   LogAllBlockEventsAndSensors = true
   EnableNvramWrite = false
   EnableAclLogging = false
   AllowSensorBlock = false
   BlockMaxEntries = 11
   MaxDeviceInterfaces = 250
   NetDevice
      Type = PIX
      IP = 10.89.150.171
      NATAddr = 0.0.0.0
      Communications = ssh-3des
   NetDevice
      Type = PIX
      IP = 10.89.150.219
      NATAddr = 0.0.0.0
      Communications = ssh-des
   NetDevice
      Type = PIX
      IP = 10.89.150.250
      NATAddr = 0.0.0.0
      Communications = telnet
   NetDevice
      Type = Cisco
      IP = 10.89.150.158
      NATAddr = 0.0.0.0
      Communications = telnet
      BlockInterface
         InterfaceName = ethernet0/1
         InterfaceDirection = out
         InterfacePostBlock = Post_Acl_Test
      BlockInterface
         InterfaceName = ethernet0/1
         InterfaceDirection = in
         InterfacePreBlock = Pre_Acl_Test
         InterfacePostBlock = Post_Acl_Test
   NetDevice
```

```
      Type = CAT6000_VACL
      IP = 10.89.150.138
      NATAddr = 0.0.0.0
      Communications = telnet
      BlockInterface
         InterfaceName = 502
         InterfacePreBlock = Pre_Acl_Test
      BlockInterface
         InterfaceName = 507
         InterfacePostBlock = Post_Acl_Test
State
   BlockEnable = true
   NetDevice
      IP = 10.89.150.171
      AclSupport = Does not use ACLs
      Version = 6.3
      State = Active
      Firewall-type = PIX
   NetDevice
      IP = 10.89.150.219
      AclSupport = Does not use ACLs
      Version = 7.0
      State = Active
      Firewall-type = ASA
   NetDevice
      IP = 10.89.150.250
      AclSupport = Does not use ACLs
      Version = 2.2
      State = Active
      Firewall-type = FWSM
   NetDevice
      IP = 10.89.150.158
      AclSupport = uses Named ACLs
      Version = 12.2
      State = Active
   NetDevice
      IP = 10.89.150.138
      AclSupport = Uses VACLs
      Version = 8.4
      State = Active
   BlockedAddr
      Host
         IP = 22.33.4.5
         Vlan =
         ActualIp =
         BlockMinutes =
      Host
         IP = 21.21.12.12
         Vlan =
         ActualIp =
         BlockMinutes =
      Host
         IP = 122.122.33.4
         Vlan =
         ActualIp =
         BlockMinutes = 60
         MinutesRemaining = 24
      Network
         IP = 111.22.0.0
         Mask = 255.255.0.0
         BlockMinutes =
sensor#
```

Step 12 Display the statistics for the notification application.

```
sensor# show statistics notification
General
   Number of SNMP set requests = 0
   Number of SNMP get requests = 0
   Number of error traps sent = 0
   Number of alert traps sent = 0
sensor#
```

Step 13 Display the statistics for OS identification:

```
sensor# show statistics os-identification
Statistics for Virtual Sensor vs0
   OS Identification
      Configured
      Imported
      Learned
sensor#
```

Step 14 Display the statistics for the SDEE server.

```
sensor# show statistics sdee-server
General
   Open Subscriptions = 0
   Blocked Subscriptions = 0
   Maximum Available Subscriptions = 5
   Maximum Events Per Retrieval = 500
Subscriptions
sensor#
```

Step 15 Display the statistics for the transaction server.

```
sensor# show statistics transaction-server
General
   totalControlTransactions = 35
   failedControlTransactions = 0
sensor#
```

Step 16 Display the statistics for a virtual sensor.

```
sensor# show statistics virtual-sensor vs0
   Statistics for Virtual Sensor vs0
      Name of current Signature-Definition instance = sig0
      Name of current Event-Action-Rules instance = rules0
      List of interfaces monitored by this virtual sensor =
      General Statistics for this Virtual Sensor
         Number of seconds since a reset of the statistics = 1421711
         Measure of the level of resource utilization = 0
         Total packets processed since reset = 0
         Total IP packets processed since reset = 0
         Total packets that were not IP processed since reset = 0
         Total TCP packets processed since reset = 0
         Total UDP packets processed since reset = 0
         Total ICMP packets processed since reset = 0
         Total packets that were not TCP, UDP, or ICMP processed since reset =
         Total ARP packets processed since reset = 0
         Total ISL encapsulated packets processed since reset = 0
         Total 802.1q encapsulated packets processed since reset = 0
         Total packets with bad IP checksums processed since reset = 0
         Total packets with bad layer 4 checksums processed since reset = 0
         Total number of bytes processed since reset = 0
         The rate of packets per second since reset = 0
         The rate of bytes per second since reset = 0
         The average bytes per packet since reset = 0
```

```
Denied Address Information
   Number of Active Denied Attackers = 0
   Number of Denied Attackers Inserted = 0
   Number of Denied Attacker Victim Pairs Inserted = 0
   Number of Denied Attacker Service Pairs Inserted = 0
   Number of Denied Attackers Total Hits = 0
   Number of times max-denied-attackers limited creation of new entry = 0
   Number of exec Clear commands during uptime = 0
Denied Attackers and hit count for each.
Denied Attackers with percent denied and hit count for each.


The Signature Database Statistics.
   The Number of each type of node active in the system (can not be reset
      Total nodes active = 0
      TCP nodes keyed on both IP addresses and both ports = 0
      UDP nodes keyed on both IP addresses and both ports = 0
      IP nodes keyed on both IP addresses = 0
   The number of each type of node inserted since reset
      Total nodes inserted = 0
      TCP nodes keyed on both IP addresses and both ports = 0
      UDP nodes keyed on both IP addresses and both ports = 0
      IP nodes keyed on both IP addresses = 0
   The rate of nodes per second for each time since reset
      Nodes per second = 0
      TCP nodes keyed on both IP addresses and both ports per second = 0
      UDP nodes keyed on both IP addresses and both ports per second = 0
      IP nodes keyed on both IP addresses per second = 0
   The number of root nodes forced to expire because of memory constraint
      TCP nodes keyed on both IP addresses and both ports = 0
   Packets dropped because they would exceed Database insertion rate limit s = 0
Fragment Reassembly Unit Statistics for this Virtual Sensor
   Number of fragments currently in FRU = 0
   Number of datagrams currently in FRU = 0
   Number of fragments received since reset = 0
   Number of fragments forwarded since reset = 0
   Number of fragments dropped since last reset = 0
   Number of fragments modified since last reset = 0
   Number of complete datagrams reassembled since last reset = 0
   Fragments hitting too many fragments condition since last reset = 0
   Number of overlapping fragments since last reset = 0
   Number of Datagrams too big since last reset = 0
   Number of overwriting fragments since last reset = 0
   Number of Initial fragment missing since last reset = 0
   Fragments hitting the max partial dgrams limit since last reset = 0
   Fragments too small since last reset = 0
   Too many fragments per dgram limit since last reset = 0
   Number of datagram reassembly timeout since last reset = 0
   Too many fragments claiming to be the last since last reset = 0
   Fragments with bad fragment flags since last reset = 0
TCP Normalizer stage statistics
   Packets Input = 0
   Packets Modified = 0
   Dropped packets from queue = 0
   Dropped packets due to deny-connection = 0
   Current Streams = 0
   Current Streams Closed = 0
   Current Streams Closing = 0
   Current Streams Embryonic = 0
   Current Streams Established = 0
   Current Streams Denied = 0
Statistics for the TCP Stream Reassembly Unit
   Current Statistics for the TCP Stream Reassembly Unit
      TCP streams currently in the embryonic state = 0
```

```
      TCP streams currently in the established state = 0
      TCP streams currently in the closing state = 0
      TCP streams currently in the system = 0
      TCP Packets currently queued for reassembly = 0
   Cumulative Statistics for the TCP Stream Reassembly Unit since reset
      TCP streams that have been tracked since last reset = 0
      TCP streams that had a gap in the sequence jumped = 0
      TCP streams that was abandoned due to a gap in the sequence = 0
      TCP packets that arrived out of sequence order for their stream = 0
      TCP packets that arrived out of state order for their stream = 0
      The rate of TCP connections tracked per second since reset = 0
SigEvent Preliminary Stage Statistics
   Number of Alerts received = 0
   Number of Alerts Consumed by AlertInterval = 0
   Number of Alerts Consumed by Event Count = 0
   Number of FireOnce First Alerts = 0
   Number of FireOnce Intermediate Alerts = 0
   Number of Summary First Alerts = 0
   Number of Summary Intermediate Alerts = 0
   Number of Regular Summary Final Alerts = 0
   Number of Global Summary Final Alerts = 0
   Number of Active SigEventDataNodes = 0
   Number of Alerts Output for further processing = 0
SigEvent Action Override Stage Statistics
   Number of Alerts received to Action Override Processor = 0
   Number of Alerts where an override was applied = 0
   Actions Added
      deny-attacker-inline = 0
      deny-attacker-victim-pair-inline = 0
      deny-attacker-service-pair-inline = 0
      deny-connection-inline = 0
      deny-packet-inline = 0
      modify-packet-inline = 0
      log-attacker-packets = 0
      log-pair-packets = 0
      log-victim-packets = 0
      produce-alert = 0
      produce-verbose-alert = 0
      request-block-connection = 0
      request-block-host = 0
      request-snmp-trap = 0
      reset-tcp-connection = 0
      request-rate-limit = 0
SigEvent Action Filter Stage Statistics
   Number of Alerts received to Action Filter Processor = 0
   Number of Alerts where an action was filtered = 0
   Number of Filter Line matches = 0
   Number of Filter Line matches causing decreased DenyPercentage = 0
   Actions Filtered
      deny-attacker-inline = 0
      deny-attacker-victim-pair-inline = 0
      deny-attacker-service-pair-inline = 0
      deny-connection-inline = 0
      deny-packet-inline = 0
      modify-packet-inline = 0
      log-attacker-packets = 0
      log-pair-packets = 0
      log-victim-packets = 0
      produce-alert = 0
      produce-verbose-alert = 0
      request-block-connection = 0
      request-block-host = 0
      request-snmp-trap = 0
      reset-tcp-connection = 0
```

```
            request-rate-limit = 0
      SigEvent Action Handling Stage Statistics.
         Number of Alerts received to Action Handling Processor = 0
         Number of Alerts where produceAlert was forced = 0
         Number of Alerts where produceAlert was off = 0
         Actions Performed
            deny-attacker-inline = 0
            deny-attacker-victim-pair-inline = 0
            deny-attacker-service-pair-inline = 0
            deny-connection-inline = 0
            deny-packet-inline = 0
            modify-packet-inline = 0
            log-attacker-packets = 0
            log-pair-packets = 0
            log-victim-packets = 0
            produce-alert = 0
            produce-verbose-alert = 0
--MORE--
```

Step 17 Display the statistics for Web Server.

```
sensor# show statistics web-server
listener-443
   number of server session requests handled = 61
   number of server session requests rejected = 0
   total HTTP requests handled = 35
   maximum number of session objects allowed = 40
   number of idle allocated session objects = 10
   number of busy allocated session objects = 0
crypto library version = 6.0.3
sensor#
```

Step 18 Clear the statistics for an application, for example, the logging application.

```
sensor# show statistics logger clear
The number of Log interprocessor FIFO overruns = 0
The number of syslog messages received = 141
The number of <evError> events written to the event store by severity
   Fatal Severity = 0
   Error Severity = 14
   Warning Severity = 142
   TOTAL = 156
The number of log messages written to the message log by severity
   Fatal Severity = 0
   Error Severity = 14
   Warning Severity = 1
   Timing Severity = 0
   Debug Severity = 0
   Unknown Severity = 28
   TOTAL = 43
```

The statistics were retrieved and cleared.

Step 19 Verify that the statistics have been cleared.

```
sensor# show statistics logger
The number of Log interprocessor FIFO overruns = 0
The number of syslog messages received = 0
The number of <evError> events written to the event store by severity
   Fatal Severity = 0
   Error Severity = 0
   Warning Severity = 0
   TOTAL = 0
The number of log messages written to the message log by severity
   Fatal Severity = 0
```

```
   Error Severity = 0
   Warning Severity = 0
   Timing Severity = 0
   Debug Severity = 0
   Unknown Severity = 0
   TOTAL = 0
sensor#
```

The statistics all begin from 0.

Interfaces Information

The **show interfaces** command is useful for gathering information on the sensing and command and control interfaces. This section describes the **show interfaces** command, and contains the following topics:

- Understanding the show interfaces Command, page A-90
- Interfaces Command Output, page A-90

Understanding the show interfaces Command

You can learn the following information from the **show interfaces** command:

- Whether the interface is up or down
- Whether or not packets are being seen, and on which interfaces
- Whether or not packets are being dropped by SensorApp
- Whether or not there are errors being reported by the interfaces that can result in packet drops

The **show interfaces** command displays statistics for all system interfaces. Or you can use the individual commands to display statistics for the command and control interface (**show interfaces** *command_control_interface_name*), the sensing interface (**show interfaces** *interface_name*).

Interfaces Command Output

The following example shows the output from the **show interfaces** command:

```
sensor# show interfaces
Interface Statistics
   Total Packets Received = 0
   Total Bytes Received = 0
   Missed Packet Percentage = 0
   Current Bypass Mode = Auto_off
MAC statistics from interface GigabitEthernet0/1
   Media Type = backplane
   Missed Packet Percentage = 0
   Inline Mode = Unpaired
   Pair Status = N/A
   Link Status = Up
   Link Speed = Auto_1000
   Link Duplex = Auto_Full
   Total Packets Received = 0
   Total Bytes Received = 0
   Total Multicast Packets Received = 0
   Total Broadcast Packets Received = 0
```

```
   Total Jumbo Packets Received = 0
   Total Undersize Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 0
   Total Bytes Transmitted = 0
   Total Multicast Packets Transmitted = 0
   Total Broadcast Packets Transmitted = 0
   Total Jumbo Packets Transmitted = 0
   Total Undersize Packets Transmitted = 0
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
MAC statistics from interface GigabitEthernet0/0
   Media Type = TX
   Link Status = Up
   Link Speed = Auto_100
   Link Duplex = Auto_Full
   Total Packets Received = 2211296
   Total Bytes Received = 157577635
   Total Multicast Packets Received = 20
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 239723
   Total Bytes Transmitted = 107213390
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
sensor#
```

Events Information

You can use the **show events** command to view the alerts generated by SensorApp and errors generated by an application. This section describes the **show events** command, and contains the following topics:

Sensor Events

Events remain in the Event Store until they are overwritten by newer events. There are five types of events:

- evAlert—Intrusion detection alerts
- evError—Application errors
- evStatus—Status changes, such as an IP log being created
- evLogTransaction—Record of control transactions processed by each sensor application
- evShunRqst—Block requests

Understanding the show events Command

The **show events** command is useful for troubleshooting event capture issues in which you are not seeing events in Event Viewer or Security Monitor. You can use the **show events** command to determine which events are being generated on the sensor to make sure events are being generated and that the fault lies with the monitoring side.

You can clear all events from Event Store by using the **clear events** command.

Here are the parameters for the **show events** command:

```
sensor# show events
<cr>
alert          Display local system alerts.
error          Display error events.
hh:mm[:ss]     Display start time.
log            Display log events.
nac            Display NAC shun events.
past           Display events starting in the past specified time.
status         Display status events.
|              Output modifiers.
```

Displaying Events

Note The Event Store has a fixed size of 30 MB for all platforms.

Use the **show events** [{**alert** [informational] [low] [medium] [high] [**include-traits** ***traits***] [**exclude-traits** ***traits***] [**min-threat-rating** *min-rr*] [**max-threat-rating** *max-rr*] | **error** [warning] [error] [fatal] | **NAC** | **status**}] [*hh:mm:ss* [*month day* [*year*]] | **past** *hh:mm:ss*] command to display events from Event Store.

Events are displayed beginning at the start time. If you do not specify a start time, events are displayed beginning at the current time. If you do not specify an event type, all events are displayed.

Note Events are displayed as a live feed. To cancel the request, press **Ctrl-C.**

The following options apply:

- **alert**—Displays alerts. Provides notification of some suspicious activity that may indicate an attack is in process or has been attempted. Alert events are generated by Analysis Engine whenever a signature is triggered by network activity. If no level is selected (informational, low, medium, or high), all alert events are displayed.
- **include-traits**—Displays alerts that have the specified traits.
- **exclude-traits**—Does not display alerts that have the specified traits.
- **traits**—Trait bit position in decimal (0 to 15).
- **min-threat-rating**—Displays events with a threat rating above or equal to this value. The default is 0. The valid range is 0 to 100.
- **max-threat-rating**—Displays events with a threat rating below or equal to this value. The default is 100. The valid range is 0 to 100.
- **error**—Displays error events. Error events are generated by services when error conditions are encountered. If no level is selected (warning, error, or fatal), all error events are displayed.

- **NAC**—Displays ARC (block) requests.

  Note ARC is formerly known as NAC. This name change has not been completely implemented throughout IDM, IME, and the CLI for Cisco IPS 7.0.

- **status**—Displays status events.
- **past**—Displays events starting in the past for the specified hours, minutes, and seconds.
- *hh:mm:ss*—Hours, minutes, and seconds in the past to begin the display.

Note The **show events** command continues to display events until a specified event is available. To exit, press **Ctrl-C**.

To display events from Event Store, follow these steps:

Step 1 Log in to the CLI.

Step 2 Display all events starting now.

```
sensor# show events
evError: eventId=1041472274774840147 severity=warning vendor=Cisco
  originator:
    hostId: sensor2
    appName: cidwebserver
    appInstanceId: 12075
  time: 2008/01/07 04:41:45 2008/01/07 04:41:45 UTC
  errorMessage: name=errWarning received fatal alert: certificate_unknown

evError: eventId=1041472274774840148 severity=error vendor=Cisco
  originator:
    hostId: sensor2
    appName: cidwebserver
    appInstanceId: 351
  time: 2008/01/07 04:41:45 2008/01/07 04:41:45 UTC
  errorMessage: name=errTransport WebSession::sessionTask(6) TLS connection exception:
handshake incomplete.
```

The feed continues showing all events until you press **Ctrl-C**.

Step 3 Display the block requests beginning at 10:00 a.m. on February 9, 2008.

```
sensor# show events NAC 10:00:00 Feb 9 2008
evShunRqst: eventId=1106837332219222281 vendor=Cisco
  originator:
    deviceName: Sensor1
    appName: NetworkAccessControllerApp
    appInstance: 654
  time: 2008/02/09 10:33:31 2008/08/09 13:13:31
  shunInfo:
    host: connectionShun=false
      srcAddr: 11.0.0.1
      destAddr:
      srcPort:
      destPort:
      protocol: numericType=0 other
    timeoutMinutes: 40
  evAlertRef: hostId=esendHost 123456789012345678
sensor#
```

Step 4 Display errors with the warning level starting at 10:00 a.m. on February 9, 2008.

```
sensor# show events error warning 10:00:00 Feb 9 2008
evError: eventId=1041472274774840197 severity=warning vendor=Cisco
  originator:
    hostId: sensor
    appName: cidwebserver
    appInstanceId: 12160
  time: 2008/01/07 04:49:25 2008/01/07 04:49:25 UTC
  errorMessage: name=errWarning received fatal alert: certificate_unknown
```

Step 5 Display alerts from the past 45 seconds.

```
sensor# show events alert past 00:00:45

evIdsAlert: eventId=1109695939102805307 severity=medium vendor=Cisco
  originator:
    hostId: sensor
    appName: sensorApp
    appInstanceId: 367
  time: 2008/03/02 14:15:59 2008/03/02 14:15:59 UTC
  signature: description=Nachi Worm ICMP Echo Request id=2156 version=S54
    subsigId: 0
    sigDetails: Nachi ICMP
  interfaceGroup:
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 10.89.228.202
    target:
      addr: locality=OUT 10.89.150.185
  riskRatingValue: 70
  interface: fe0_1
  protocol: icmp


evIdsAlert: eventId=1109695939102805308 severity=medium vendor=Cisco
  originator:
--MORE--
```

Step 6 Display events that began 30 seconds in the past.

```
sensor# show events past 00:00:30
evStatus: eventId=1041526834774829055 vendor=Cisco
  originator:
    hostId: sensor
    appName: mainApp
    appInstanceId: 2215
  time: 2008/01/08 02:41:00 2008/01/08 02:41:00 UTC
  controlTransaction: command=getVersion successful=true
    description: Control transaction response.
    requestor:
      user: cids
      application:
        hostId: 64.101.182.101
        appName: -cidcli
        appInstanceId: 2316


evStatus: eventId=1041526834774829056 vendor=Cisco
  originator:
    hostId: sensor
    appName: login(pam_unix)
    appInstanceId: 2315
  time: 2008/01/08 02:41:00 2008/01/08 02:41:00 UTC
```

```
  syslogMessage:
    description: session opened for user cisco by cisco(uid=0)
```

Clearing Events

Use the **clear events** command to clear Event Store. To clear events from Event Store, follow these steps:

Step 1 Log in to the CLI using an account with administrator privileges.

Step 2 Clear Event Store.

```
sensor# clear events
Warning: Executing this command will remove all events currently stored in the event
store.
Continue with clear? []:
```

Step 3 Enter **yes** to clear the events.

cidDump Script

If you do not have access to IDM, IME, or the CLI, you can run the underlying script cidDump from the Service account by logging in as root and running /usr/cids/idsRoot/bin/cidDump. The path of the cidDump file is /usr/cids/idsRoot/htdocs/private/cidDump.html.

cidDump is a script that captures a large amount of information including the IPS processes list, log files, OS information, directory listings, package information, and configuration files.

To run the cidDump script, follow these steps:

Step 1 Log in to the sensor Service account.

Step 2 **Su** to **root** using the Service account password.

Step 3 Enter the following command.

```
/usr/cids/idsRoot/bin/cidDump
```

Step 4 Enter the following command to compress the resulting /usr/cids/idsRoot/log/cidDump.html file.

```
gzip /usr/cids/idsRoot/log/cidDump.html
```

Step 5 Send the resulting HTML file to TAC or the IPS developers in case of a problem.

For More Information

For the procedure for putting a file on the Cisco FTP site, see Uploading and Accessing Files on the Cisco FTP Site, page A-96.

Uploading and Accessing Files on the Cisco FTP Site

You can upload large files, for example, cidDump.html, the **show tech-support** command output, and cores, to the ftp-sj server. To upload and access files on the Cisco FTP site, follow these steps:

Step 1 Log in to ftp-sj.cisco.com as anonymous.

Step 2 Change to the /incoming directory.

Step 3 Use the **put** command to upload the files. Make sure to use the binary transfer type.

Step 4 To access uploaded files, log in to an ECS-supported host.

Step 5 Change to the /auto/ftp/incoming directory.

GLOSSARY

Numerals

3DES Triple Data Encryption Standard. A stronger version of DES, which is the default encryption method for SSH version 1.5. Used when establishing an SSH session with the sensor. It can be used when the sensor is managing a device.

802.x A set of IEEE standards for the definition of LAN protocols.

A

AAA authentication, authorization, and accounting. Pronounced “triple a.” The primary and recommended method for access control in Cisco devices.

ACE Access Control Entry. An entry in the ACL that describes what action should be taken for a specified address or protocol. The sensor adds/removes ACE to block hosts.

ACK acknowledgement. Notification sent from one network device to another to acknowledge that some event occurred (for example, the receipt of a message).

ACL Access Control List. A list of ACEs that control the flow of data through a router. There are two ACLs per router interface for inbound data and outbound data. Only one ACL per direction can be active at a time. ACLs are identified by number or by name. ACLs can be standard, enhanced, or extended. You can configure the sensor to manage ACLs.

action The response of the sensor to an event. An action only happens if the event is not filtered. Examples include TCP reset, block host, block connection, IP logging, and capturing the alert trigger packet.

active ACL The ACL created and maintained by ARC and applied to the router block interfaces.

adaptive security appliance ASA. Combines firewall, VPN concentrator, and intrusion prevention software functionality into one software image. You can configure the adaptive security appliance in single mode or multi-mode.

AIC engine Application Inspection and Control engine. Provides deep analysis of web traffic. It provides granular control over HTTP sessions to prevent abuse of the HTTP protocol. It allows administrative control over applications that try to tunnel over specified ports, such as instant messaging, and tunneling applications, such as gotomypc. It can also inspect FTP traffic and control the commands being issued.

AIM IPS Advanced Integration Module. A type of IPS network module installed in Cisco routers.

AIP SSM Advanced Inspection and Prevention Security Services Module. The IPS plug-in module in the Cisco ASA 5500 series adaptive security appliance. AIP-SSM is an IPS services module that monitors and performs real-time analysis of network traffic by looking for anomalies and misuse based on an extensive, embedded signature library. When AIP-SSM detects unauthorized activity, it can terminate the specific connection, permanently block the attacking host, log the incident, and send an alert to the device manager. See also adaptive security appliance.

Alarm Channel The IPS software module that processes all signature events generated by the inspectors. Its primary function is to generate alerts for each event it receives.

alert Specifically, an IPS event type; it is written to the Event Store as an evidsAlert. In general, an alert is an IPS message that indicates a network exploit in progress or a potential security problem occurrence. Also known as an alarm.

Analysis Engine The IPS software module that handles sensor configuration. It maps the interfaces and also the signature and alarm channel policy to the configured interfaces. It performs packet analysis and alert detection. The Analysis Engine functionality is provided by the SensorApp process.

anomaly detection AD. The sensor component that creates a baseline of normal network traffic and then uses this baseline to detect worm-infected hosts.

API Application Programming Interface. The means by which an application program talks to communications software. Standardized APIs allow application programs to be developed independently of the underlying method of communication. Computer application programs run a set of standard software interrupts, calls, and data formats to initiate contact with other devices (for example, network services, mainframe communications programs, or other program-to-program communications). Typically, APIs make it easier for software developers to create links that an application needs to communicate with the operating system or with the network.

application Any program (process) designed to run in the Cisco IPS environment.

application image Full IPS image stored on a permanent storage device used for operating the sensor.

application instance A specific application running on a specific piece of hardware in the IPS environment. An application instance is addressable by its name and the IP address of its host computer.

application partition The bootable disk or compact-flash partition that contains the IPS software image.

ARC Attack Response Controller. Formerly known as Network Access Controller (NAC). A component of the IPS. A software module that provides block and unblock functionality where applicable.

architecture The overall structure of a computer or communication system. The architecture influences the capabilities and limitations of the system.

ARP Address Resolution Protocol. Internet protocol used to map an IP address to a MAC address. Defined in RFC 826.

ASDM Adaptive Security Device Manager. A web-based application that lets you configure and manage your adaptive security device.

ASN.1 Abstract Syntax Notation 1. Standard for data presentation.

aspect version Version information associated with a group of IDIOM default configuration settings. For example, Cisco Systems publishes the standard set of attack signatures as a collection of default settings with the S aspect. The S-aspect version number is displayed after the S in the signature update package file name. Other aspects include the Virus signature definitions in the V-aspect and IDIOM signing keys in the key-aspect.

atomic attack Represents exploits contained within a single packet. For example, the "ping of death" attack is a single, abnormally large ICMP packet.

Atomic engine There are two Atomic engines: Atomic IP inspects IP protocol packets and associated Layer-4 transport protocols, and Atomic ARP inspects Layer-2 ARP protocol.

attack An assault on system security that derives from an intelligent threat, that is, an intelligent act that is a deliberate attempt (especially in the sense of method or technique) to evade security services and violate the security policy of a system.

attack relevance rating ARR. A weight associated with the relevancy of the targeted OS. The attack relevance rating is a derived value (relevant, unknown, or not relevant), which is determined at alert time. The relevant OSes are configured per signature.

attack severity rating ASR. A weight associated with the severity of a successful exploit of the vulnerability. The attack severity rating is derived from the alert severity parameter (informational, low, medium, or high) of the signature. The attack severity rating is configured per signature and indicates how dangerous the event detected is.

authentication Process of verifying that a user has permission to use the system, usually by means of a password key or certificate.

AuthenticationApp A component of the IPS. Authorizes and authenticates users based on IP address, password, and digital certificates.

autostate In normal autostate mode, the Layer 3 interfaces remain up if at least one port in the VLAN remains up. If you have appliances, such as load balancers or firewall servers that are connected to the ports in the VLAN, you can configure these ports to be excluded from the autostate feature to make sure that the forwarding SVI does not go down if these ports become inactive.

AV Anti-Virus.

B

backplane The physical connection between an interface processor or card and the data buses and the power distribution buses inside a chassis.

base version A software release that must be installed before a follow-up release, such as a service pack or signature update, can be installed. Major and minor updates are base version releases.

benign trigger A situation in which a signature is fired correctly, but the source of the traffic is nonmalicious.

BIOS Basic Input/Output System. The program that starts the sensor and communicates between the devices in the sensor and the system.

blackhole Routing term for an area of the internetwork where packets enter, but do not emerge, due to adverse conditions or poor system configuration within a portion of the network.

block The ability of the sensor to direct a network device to deny entry to all packets from a specified network host or network.

block interface The interface on the network device that the sensor manages.

BO BackOrifice. The original Windows back door Trojan that ran over UDP only.

BO2K BackOrifice 2000. A Windows back door Trojan that runs over TCP and UDP.

bootloader A small set of system software that runs when the system first powers up. It loads the operating system (from the disk, network, external compact flash, or external USB flash), which loads and runs the IPS application. For the AIM IPS, it boots the module from the network and assists in software installation and upgrades, disaster recovery, and other operations when the module cannot access its software.

Botnets A collection of software robots, or bots, that run autonomously and automatically. The term is often associated with malicious software but it can also refer to the network of computers using distributed computing software. The term Botnet is used to refer to a collection of compromised computers (called Zombie computers) running software, usually installed through worms, Trojan horses, or back doors, under a common command-and-control infrastructure.

Bpdu Bridge Protocol Data Unit. Spanning-Tree Protocol hello packet that is sent out at configurable intervals to exchange information among bridges in the network.

bypass mode Mode that lets packets continue to flow through the sensor even if the sensor fails. Bypass mode is only applicable to inline-paired interfaces.

C

CA certification authority. Entity that issues digital certificates (especially X.509 certificates) and vouches for the binding between the data items in a certificate. Sensors use self-signed certificates.

CA certificate Certificate for one CA issued by another CA.

CEF Cisco Express Forwarding. CEF is advanced, Layer 3 IP switching technology. CEF optimizes network performance and scalability for networks with large and dynamic traffic patterns, such as the Internet, on networks characterized by intensive Web-based applications, or interactive sessions.

certificate Digital representation of user or device attributes, including a public key, that is signed with an authoritative private key.

cidDump A script that captures a large amount of information including the IPS processes list, log files, OS information, directory listings, package information, and configuration files.

CIDEE Cisco Intrusion Detection Event Exchange. Specifies the extensions to SDEE that are used by Cisco IPS systems. The CIDEE standard specifies all possible extensions that may be supported by Cisco IPS systems.

CIDS header The header that is attached to each packet in the IPS system. It contains packet classification, packet length, checksum results, timestamp, and the receive interface.

cipher key The secret binary data used to convert between clear text and cipher text. When the same cipher key is used for both encryption and decryption, it is called symmetric. When it is used for either encryption or decryption (but not both), it is called asymmetric.

Cisco IOS Cisco system software that provides common functionality, scalability, and security for all products under the CiscoFusion architecture. Cisco IOS allows centralized, integrated, and automated installation and management of internetworks while supporting a wide variety of protocols, media, services, and platforms.

CLI command-line interface. A shell provided with the sensor used for configuring and controlling the sensor applications.

CollaborationApp A component of the IPS. Shares information with other devices through a global correlation database to improve the combined efficacy of all the devices.

command and control interface The interface on the sensor that communicates with the IPS manager and other network devices. This interface has an assigned IP address.

community In SNMP, a logical group of managed devices and NMSs in the same administrative domain.

composite attack Spans multiple packets in a single session. Examples include most conversation attacks such as FTP, Telnet, and most Regex-based attacks.

connection block ARC blocks traffic from a given source IP address to a given destination IP address and destination port.

console A terminal or laptop computer used to monitor and control the sensor.

console port An RJ45 or DB9 serial port on the sensor that is used to connect to a console device.

control interface When ARC opens a Telnet or SSH session with a network device, it uses one of the routing interfaces of the device as the remote IP address. This is the control interface.

control transaction CT. An IPS message containing a command addressed to a specific application instance. Example control transactions include *start*, *stop*, *getConfig*.

Control Transaction Server A component of the IPS. Accepts control transactions from a remote client, initiates a local control transaction, and returns the response to the remote client.

Control Transaction Source A component of the IPS. Waits for control transactions directed to remote applications, forwards the control transactions to the remote node, and returns the response to the initiator.

cookie A piece of information sent by a web server to a web browser that the browser is expected to save and send back to the web server whenever the browser makes additional requests of the web server.

CSA MC Cisco Security Agent Management Center. CSA MC receives host posture information from the CSA agents it manages. It also maintains a watch list of IP addresses that it has determined should be quarantined from the network.

CSM Cisco Security Manager, the provisioning component of the Cisco Self-Defending Networks solution. CS-Manager is fully integrated with CS-MARS.

CS-MARS Cisco Security Monitoring, Analysis and Reporting System. The monitoring component of the Cisco Self-Defending Networks solution. CS-MARS is fully integrated with CS-Manager

CVE Common Vulnerabilities and Exposures. A list of standardized names for vulnerabilities and other information security exposures maintained at http://cve.mitre.org/.

D

darknets A virtual private network where users connect only to people they trust. In its most general meaning, a darknet can be any type of closed, private group of people communicating, but the name is most often used specifically for file-sharing networks. Darknet can be used to refer collectively to all covert communication networks.

Database Processor A processor in the IPS. Maintains the signature state and flow databases.

datagram Logical grouping of information sent as a network layer unit over a transmission medium without prior establishment of a virtual circuit. IP datagrams are the primary information units in the Internet. The terms cell, frame, message, packet, and segment also are used to describe logical information groupings at various layers of the OSI reference model and in various technology circles.

DCE data circuit-terminating equipment (ITU-T expansion). Devices and connections of a communications network that comprise the network end of the user-to-network interface. The DCE provides a physical connection to the network, forwards traffic, and provides a clocking signal used to synchronize data transmission between DCE and DTE devices. Modems and interface cards are examples of DCE.

DCOM Distributed Component Object Model. Protocol that enables software components to communicate directly over a network. Developed by Microsoft and previously called Network OLE, DCOM is designed for use across multiple network transports, including such Internet protocols as HTTP.

DDoS Distributed Denial of Service. An attack in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users.

Deny Filters Processor A processor in the IPS. Handles the deny attacker functions. It maintains a list of denied source IP addresses.

DES Data Encryption Standard. A strong encryption method where the strength lies in a 56-bit key rather than an algorithm.

destination address Address of a network device that is receiving data.

DIMM Dual In-line Memory Modules.

DMZ demilitarized zone. A separate network located in the neutral zone between a private (inside) network and a public (outside) network.

DNS Domain Name System. An Internet-wide hostname to IP address mapping. DNS enables you to convert human-readable names into the IP addresses needed for network packets.

DoS Denial of Service. An attack whose goal is just to disrupt the operation of a specific system or network.

DRAM dynamic random-access memory. RAM that stores information in capacitors that must be refreshed periodically. Delays can occur because DRAMs are inaccessible to the processor when refreshing their contents. However, DRAMs are less complex and have greater capacity than SRAMs.

DTE Data Terminal Equipment. Refers to the role of a device on an RS-232C connection. A DTE writes data to the transmit line and reads data from the receive line.

DTP Dynamic Trunking Protocol. A Cisco proprietary protocol in the VLAN group used for negotiating trunking on a link between two devices and for negotiating the type of trunking encapsulation (ISL or 802.1q) to be used.

E

ECLB Ether Channel Load Balancing. Lets a Catalyst switch split traffic flows over different physical paths.

egress Traffic leaving the network.

encryption Application of a specific algorithm to data to alter the appearance of the data making it incomprehensible to those who are not authorized to see the information.

engine A component of the sensor designed to support many signatures in a certain category. Each engine has parameters that can be used to create signatures or tune existing signatures.

enterprise network Large and diverse network connecting most major points in a company or other organization. Differs from a WAN in that it is privately owned and maintained.

escaped expression Used in regular expression. A character can be represented as its hexadecimal value, for example, \x61 equals ‘a,’ so \x61 is an escaped expression representing the character ‘a.’

ESD electrostatic discharge. Electrostatic discharge is the rapid movement of a charge from one object to another object, which produces several thousand volts of electrical charge that can cause severe damage to electronic components or entire circuit card assemblies.

event An IPS message that contains an alert, a block request, a status message, or an error message.

Event Store One of the components of the IPS. A fixed-size, indexed store (30 MB) used to store IPS events.

evIdsAlert The XML entity written to the Event Store that represents an alert.

F

fail closed Blocks traffic on the device after a hardware failure.

fail open Lets traffic pass through the device after a hardware failure.

false negative A signature is not fired when offending traffic is detected.

false positive Normal traffic or a benign action causes a signature to fire.

Fast Ethernet Any of a number of 100-Mbps Ethernet specifications. Fast Ethernet offers a speed increase 10 times that of the 10BaseT Ethernet specification while preserving such qualities as frame format, MAC mechanisms, and MTU. Such similarities allow the use of existing 10BaseT applications and network management tools on Fast Ethernet networks. Based on an extension to the IEEE 802.3 specification.

firewall Router or access server, or several routers or access servers, designated as a buffer between any connected public networks and a private network. A firewall router uses access lists and other methods to ensure the security of the private network.

Flood engine Detects ICMP and UDP floods directed at hosts and networks.

flooding Traffic passing technique used by switches and bridges in which traffic received on an interface is sent out all the interfaces of that device except the interface on which the information was received originally.

forwarding Process of sending a frame toward its ultimate destination by way of an internetworking device.

fragment Piece of a larger packet that has been broken down to smaller units.

fragmentation Process of breaking a packet into smaller units when transmitting over a network medium that cannot support the original size of the packet.

Fragment Reassembly Processor A processor in the IPS. Reassembles fragmented IP datagrams. It is also responsible for normalization of IP fragments when the sensor is in inline mode.

FTP File Transfer Protocol. Application protocol, part of the TCP/IP protocol stack, used for transferring files between network nodes. FTP is defined in RFC 959.

FTP server File Transfer Protocol server. A server that uses the FTP protocol for transferring files between network nodes.

full duplex Capability for simultaneous data transmission between a sending station and a receiving station.

FWSM Firewall Security Module. A module that can be installed in a Catalyst 6500 series switch. It uses the **shun** command to block. You can configure the FWSM in either single mode or multi-mode.

G

GBIC GigaBit Interface Converter. Often refers to a fiber optic transceiver that adapts optical cabling to fiber interfaces. Fiber-ready switches and NICs generally provide GBIC and/or SFP slots. For more information, refer to the *Catalyst Switch Cable, Connector, and AC Power Cord Guide.*

Gigabit Ethernet Standard for a high-speed Ethernet, approved by the IEEE (Institute of Electrical and Electronics Engineers) 802.3z standards committee in 1996.

global correlation The IPS sensor shares information with other devices through a global correlation database to improve the combined efficacy of all devices.

global correlation client The software component of CollaborationApp that obtains and installs updates to the local global correlation databases.

global correlation database The collective information obtained from and shared with collaborative devices such as IPS sensors.

GMT Greenwich Mean Time. Time zone at zero degrees longitude. Now called Coordinated Universal Time (UTC).

GRUB Grand Unified Bootloader. Boot loader is the first software program that runs when a computer starts. It is responsible for loading and transferring control to the operating system kernel software. The kernel, in turn, initializes the rest of the operating system.

H

H.225.0 An ITU standard that governs H.225.0 session establishment and packetization. H.225.0 actually describes several different protocols: RAS, use of Q.931, and use of RTP.

H.245 An ITU standard that governs H.245 endpoint control.

H.323 Allows dissimilar communication devices to communicate with each other by using a standardized communication protocol. H.323 defines a common set of CODECs, call setup and negotiating procedures, and basic data transport methods.

half duplex Capability for data transmission in only one direction at a time between a sending station and a receiving station. BSC is an example of a half-duplex protocol.

handshake Sequence of messages exchanged between two or more network devices to ensure transmission synchronization.

hardware bypass A specialized interface card that pairs physical interfaces so that when a software error is detected, a bypass mechanism is engaged that directly connects the physical interfaces and allows traffic to flow through the pair. Hardware bypass passes traffic at the network interface, does not pass it to the IPS system.

host block ARC blocks all traffic from a given IP address.

HTTP Hypertext Transfer Protocol. The stateless request/response media transfer protocol used in the IPS architecture for remote data exchange.

HTTPS An extension to the standard HTTP protocol that provides confidentiality by encrypting the traffic from the website. By default this protocol uses TCP port 443.

I

ICMP Internet Control Message Protocol. Network layer Internet protocol that reports errors and provides other information relevant to IP packet processing. Documented in RFC 792.

ICMP flood Denial of Service attack that sends a host more ICMP echo request (“ping”) packets than the protocol implementation can handle.

IDAPI Intrusion Detection Application Programming Interface. Provides a simple interface between IPS architecture applications. IDAPI reads and writes event data and provides a mechanism for control transactions.

IDCONF Intrusion Detection Configuration. A data format standard that defines operational messages that are used to configure intrusion detection and prevention systems.

IDENT Ident protocol, specified in RFC 1413, is an Internet protocol that helps identify the user of a particular TCP connection.

IDIOM Intrusion Detection Interchange and Operations Messages. A data format standard that defines the event messages that are reported by intrusion detection systems and the operational messages that are used to configure and control intrusion detection systems.

IDM IPS Device Manager. A web-based application that lets you configure and manage your sensor. The web server for IDM resides on the sensor. You can access it through Internet Explorer or Firefox web browsers.

IDMEF Intrusion Detection Message Exchange Format. The IETF Intrusion Detection Working Group draft standard.

IDSM2 Intrusion Detection System Module. A switching module that performs intrusion detection in the Catalyst 6500 series switch.

IDS MC Management Center for IDS Sensors. A web-based IDS manager that can manage configurations for up to 300 sensors.

IME IPS Manager Express. A network management application that provides system health monitoring, events monitoring, reporting, and configuration for up to ten sensors.

inline mode All packets entering or leaving the network must pass through the sensor.

inline interface A pair of physical interfaces configured so that the sensor forwards all traffic received on one interface out to the other interface in the pair.

InterfaceApp A component of the IPS. Handles bypass and physical settings and defines paired interfaces. Physical settings are speed, duplex, and administrative state.

intrusion detection system IDS. A security service that monitors and analyzes system events to find and provide real-time or near real-time warning of attempts to access system resources in an unauthorized manner.

IP address 32-bit address assigned to hosts using TCP/IP. An IP address belongs to one of five classes (A, B, C, D, or E) and is written as 4 octets separated by periods (dotted decimal format). Each address consists of a network number, an optional subnetwork number, and a host number. The network and subnetwork numbers together are used for routing, and the host number is used to address an individual host within the network or subnetwork. A subnet mask is used to extract network and subnetwork information from the IP address.

IPS Intrusion Prevention System. A system that alerts the user to the presence of an intrusion on the network through network traffic analysis techniques.

IPS data or message Describes the messages transferred over the command and control interface between IPS applications.

iplog A log of the binary packets to and from a designated address. Iplogs are created when the log Event Action is selected for a signature. Iplogs are stored in a libpcap format, which can be read by WireShark and TCPDUMP.

IP spoofing IP spoofing attack occurs when an attacker outside your network pretends to be a trusted user either by using an IP address that is within the range of IP addresses for your network or by using an authorized external IP address that you trust and to which you want to provide access to specified resources on your network. Should an attacker get access to your IPSec security parameters, that attacker can masquerade as the remote user authorized to connect to the corporate network.

IPv6 IP version 6. Replacement for the current version of IP (version 4). IPv6 includes support for flow ID in the packet header, which can be used to identify flows. Formerly called IPng (next generation).

ISL Inter-Switch Link. Cisco-proprietary protocol that maintains VLAN information as traffic flows between switches and routers.

J

Java Web Start Java Web Start provides a platform-independent, secure, and robust deployment technology. It enables developers to deploy full-featured applications to you by making the applications available on a standard web server. With any web browser, you can launch the applications and be confident you always have the most-recent version.

JNLP Java Network Launching Protocol. Defined in an XML file format specifying how Java Web Start applications are launched. JNLP consists of a set of rules defining how exactly the launching mechanism should be implemented.

K

KB Knowledge Base. The sets of thresholds learned by Anomaly Detection and used for worm virus detection.

Knowledge Base See KB.

L

LACP Link Aggregation Control Protocol. LACP aids in the automatic creation of EtherChannel links by exchanging LACP packets between LAN ports. This protocol is defined in IEEE 802.3ad.

LAN Local Area Network. Refers to the Layer 2 network domain local to a given host. Packets exchanged between two hosts on the same LAN do not require Layer 3 routing.

Layer 2 Processor A processor in the IPS. Processes layer 2-related events. It also identifies malformed packets and removes them from the processing path.

Logger A component of the IPS. Writes all the log messages of the application to the log file and the error messages of the application to the Event Store.

logging Gathers actions that have occurred in a log file. Logging of security information is performed on two levels: logging of events (such as IPS commands, errors, and alerts), and logging of individual IP session information.

LOKI Remote access, back door Trojan, ICMP tunneling software. When the computer is infected, the malicious code creates an ICMP tunnel that can be used to send small payload ICMP replies.

M

MainApp The main application in the IPS. The first application to start on the sensor after the operating system has booted. Reads the configuration and starts applications, handles starting and stopping of applications and node reboots, handles software upgrades.

maintenance partition The bootable disk partition on the IDSM2, from which an IPS image can be installed on the application partition. No IPS capability is available while the IDSM2 is booted into the maintenance partition.

maintenance partition image The bootable software image installed on the maintenance partition on an IDSM2. You can install the maintenance partition image only while booted into the application partition.

major update A base version that contains major new functionality or a major architectural change in the product.

Malware Malicious software that is installed on an unknowing host.

manufacturing image Full IPS system image used by manufacturing to image sensors.

master blocking sensor A remote sensor that controls one or more devices. Blocking forwarding sensors send blocking requests to the master blocking sensor and the master blocking sensor executes the blocking requests.

MD5 Message Digest 5. A one-way hashing algorithm that produces a 128-bit hash. Both MD5 and Secure Hash Algorithm (SHA) are variations on MD4 and strengthen the security of the MD4 hashing algorithm. Cisco uses hashes for authentication within the IPSec framework. Also used for message authentication in SNMP v.2. MD5 verifies the integrity of the communication, authenticates the origin, and checks for timeliness.

Meta engine Defines events that occur in a related manner within a sliding time interval. This engine processes events rather than packets.

MIB Management Information Base. Database of network management information that is used and maintained by a network management protocol, such as SNMP or CMIP. The value of a MIB object can be changed or retrieved using SNMP or CMIP commands, usually through a GUI network management system. MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

MIME Multipurpose Internet Mail Extension. Standard for transmitting nontext data (or data that cannot be represented in plain ASCII code) in Internet mail, such as binary, foreign language text (such as Russian or Chinese), audio, or video data. MIME is defined in RFC 2045.

minor update A minor version that contains minor enhancements to the product line. Minor updates are incremental to the major version, and are also base versions for service packs.

module A removable card in a switch, router, or security appliance chassis. The AIM IPS, AIP SSM, IDSM2, and NME IPS are IPS modules.

monitoring interface See sensing interface.

MPF Modular Policy Framework. A means of configuring security appliance features in a manner similar to Cisco IOS software Modular QoS CLI.

MSFC, MSFC2 Multilayer Switch Feature Card. An optional card on a Catalyst 6000 supervisor engine that performs L3 routing for the switch.

MSRPC Microsoft Remote Procedure Call. MSRPC is the Microsoft implementation of the DCE RPC mechanism. Microsoft added support for Unicode strings, implicit handles, inheritance of interfaces (which are extensively used in DCOM), and complex calculations in the variable-length string and structure paradigms already present in DCE/RPC.

MySDN My Self-Defending Network. A part of the signature definition section of IDM and IME. It provides detailed information about signatures.

N

NAC Network Access Controller. See ARC.

NAT Native Address Translation. A network device can present an IP address to the outside networks that is different from the actual IP address of a host.

NBD Next Business Day. The arrival of replacement hardware according to Cisco service contracts.

Neighborhood Discovery Protocol for IPv6. IPv6 nodes on the same link use Neighbor Discovery to discover each other's presence, to determine each other's link-layer addresses, to find routers, and to maintain reachability information about the paths to active neighbors.

network device A device that controls IP traffic on a network and can block an attacking host. An example of a network device is a Cisco router or PIX Firewall.

network participation Networks contributing learned information to the global correlation database.

network participation client The software component of CollaborationApp that sends data to the SensorBase Network.

never block address Hosts and networks you have identified that should never be blocked.

never shun address See never block address.

NIC Network Interface Card. Board that provides network communication capabilities to and from a computer system.

NME IPS Network Module Enhanced. An IPS module that you can install in any network module slot in the Cisco 2800 and 3800 series integrated services routers.

NMS network management system. System responsible for managing at least part of a network. An NMS is generally a reasonably powerful and well-equipped computer, such as an engineering workstation. NMSs communicate with agents to help keep track of network statistics and resources.

node A physical communicating element on the command and control network. For example, an appliance, an IDSM2, or a router.

Normalizer engine Configures how the IP and TCP normalizer functions and provides configuration for signature events related to the IP and TCP normalizer.

NOS network operating system. Generic term used to refer to distributed file systems. Examples include LAN Manager, NetWare, NFS, and VINES.

NotificationApp A component of the IPS. Sends SNMP traps when triggered by alert, status, and error events. NotificationApp uses the public domain SNMP agent. SNMP GETs provide information about the general health of the sensor.

NTP Network Timing Protocol. Protocol built on top of TCP that ensures accurate local time-keeping with reference to radio and atomic clocks located on the Internet. This protocol is capable of synchronizing distributed clocks within milliseconds over long time periods.

NTP server Network Timing Protocol server. A server that uses NTP. NTP is a protocol built on top of TCP that ensures accurate local time-keeping with reference to radio and atomic clocks located on the Internet. This protocol is capable of synchronizing distributed clocks within milliseconds over long time periods.

NVRAM Non-Volatile Read/Write Memory. RAM that retains its contents when a unit is powered off.

O

OIR online insertion and removal. Feature that permits you to add, replace, or remove cards without interrupting the system power, entering console commands, or causing other software or interfaces to shutdown.

OPS Outbreak Prevention Service.

P

P2P Peer-to-Peer. P2P networks use nodes that can simultaneously function as both client and server for the purpose of file sharing.

packet Logical grouping of information that includes a header containing control information and (usually) user data. Packets most often are used to refer to network layer units of data. The terms datagram, frame, message, and segment also are used to describe logical information groupings at various layers of the OSI reference model and in various technology circles.

PAgP Port Aggregation Control Protocol. PAgP aids in the automatic creation of EtherChannel links by exchanging PAgP packets between LAN ports. It is a Cisco-proprietary protocol.

passive fingerprinting Act of determining the OS or services available on a system from passive observation of network interactions.

Passive OS Fingerprinting The sensor determines host operating systems by inspecting characteristics of the packets exchanged on the network.

PASV Port Spoof An attempt to open connections through a firewall to a protected FTP server to a non-FTP port. This happens when the firewall incorrectly interprets an FTP 227 **passive** command by opening an unauthorized connection.

PAT Port Address Translation. A more restricted translation scheme than NAT in which a single IP address and different ports are used to represent the hosts of a network.

patch release Release that addresses defects identified in the update (minor, major, or service pack) binaries after a software release (service pack, minor, or major update) has been released.

PAWS Protection Against Wrapped Sequence. Protection against wrapped sequence numbers in high performance TCP networks. See RFC 1323.

PCI Peripheral Component Interface. The most common peripheral expansion bus used on Intel-based computers.

PDU protocol data unit. OSI term for packet. See also BPDU and packet.

PEP Cisco Product Evolution Program. PEP is the UDI information that consists of the PID, the VID, and the SN of your sensor. PEP provides hardware version and serial number visibility through electronic query, product labels, and shipping items.

PER packed encoding rules. Instead of using a generic style of encoding that encodes all types in a uniform way, PER specializes the encoding based on the date type to generate much more compact representations.

PFC Policy Feature Card. An optional card on a Catalyst 6000 supervisor engine that supports VACL packet filtering.

PID Product Identifier. The orderable product identifier that is one of the three parts of the UDI. The UDI is part of the PEP policy.

ping packet internet groper. Often used in IP networks to test the reachability of a network device. It works by sending ICMP echo request packets to the target host and listening for echo response replies.

PIX Firewall Private Internet Exchange Firewall. A Cisco network security device that can be programmed to block/enable addresses and ports between networks.

PKI Public Key Infrastructure. Authentication of HTTP clients using the clients X.509 certificates.

POST Power-On Self Test. Set of hardware diagnostics that runs on a hardware device when that device is powered up.

Post-ACL Designates an ACL from which ARC should read the ACL entries, and where it places entries after all deny entries for the addresses being blocked.

Pre-ACL Designates an ACL from which ARC should read the ACL entries, and where it places entries before any deny entries for the addresses being blocked.

promiscuous delta PD. A weight in the range of 0 to 30 configured per signature. This weight can be subtracted from the overall risk rating in promiscuous mode.

promiscuous mode A passive interface for monitoring packets of the network segment. The sensing interface does not have an IP address assigned to it and is therefore invisible to attackers.

Q

Q.931 ITU-T specification for signaling to establish, maintain, and clear ISDN network connections.

QoS quality of service. Measure of performance for a transmission system that reflects its transmission quality and service availability.

R

rack mounting Refers to mounting a sensor in an equipment rack.

RAM random-access memory. Volatile memory that can be read and written by a microprocessor.

RAS Registration, Admission, and Status Protocol. Protocol that is used between endpoints and the gatekeeper to perform management functions. RAS signalling function performs registration, admissions, bandwidth changes, status, and disengage procedures between the VoIP gateway and the gatekeeper.

RBCP Router Blade Control Protocol. RBCP is based on SCP, but modified specifically for the router application. It is designed to run over Ethernet interfaces and uses 802.2 SNAP encapsulation for messages.

reassembly The putting back together of an IP datagram at the destination after it has been fragmented either at the source or at an intermediate node.

recovery package An IPS package file that includes the full application image and installer used for recovery on sensors.

regex See regular expression.

regular expression A mechanism by which you can define how to search for a specified sequence of characters in a data stream or file. Regular expressions are a powerful and flexible notation almost like a mini-programming language that allow you to describe text. In the context of pattern matching, regular expressions allow a succinct description of any arbitrary pattern.

repackage release A release that addresses defects in the packaging or the installer.

reputation Similar to human social interaction, reputation is an opinion toward a device on the Internet. It enables the installed base of IPS sensors in the field to collaborate using the existing network infrastructure. A network device with reputation is most probably malicious or infected.

risk rating RR. A risk rating is a value between 0 and 100 that represents a numerical quantification of the risk associated with a particular event on the network. The risk of the attack accounts for the severity, fidelity, relevance, and asset value of the attack, but not any response or mitigation actions. This risk is higher when more damage could be inflicted on your network.

RMA Return Materials Authorization. The Cisco program for returning faulty hardware and obtaining a replacement.

ROMMON Read-Only-Memory Monitor. ROMMON lets you TFTP system images onto the sensor for recovery purposes.

round-trip time See RTT.

RPC remote-procedure call. Technological foundation of client/server computing. RPCs are procedure calls that are built or specified by clients and are executed on servers, with the results returned over the network to the clients.

RSM Router Switch Module. A router module that is installed in a Catalyst 5000 switch. It functions exactly like a standalone router.

RTP Real-Time Transport Protocol. Commonly used with IP networks. RTP is designed to provide end-to-end network transport functions for applications transmitting real-time data, such as audio, video, or simulation data, over multicast or unicast network services. RTP provides such services as payload type identification, sequence numbering, timestamping, and delivery monitoring to real-time applications.

RTT round-trip time. A measure of the time delay imposed by a network on a host from the sending of a packet until acknowledgement of the receipt.

RU rack unit. A rack is measured in rack units. An RU is equal to 44 mm or 1.75 inches.

S

SCP Switch Configuration Protocol. Cisco control protocol that runs directly over the Ethernet.

SCEP Simple Certificate Enrollment Protocol. The Cisco Systems PKI communication protocol that leverages existing technology by using PKCS#7 and PKCS#10. SCEP is the evolution of the enrollment protocol.

SDEE Security Device Event Exchange. A product-independent standard for communicating security device events. It adds extensibility features that are needed for communicating events generated by various types of security devices.

SDEE Server Accepts requests for events from remote clients.

Secure Shell Protocol Protocol that provides a secure remote connection to a router through a Transmission Control Protocol (TCP) application.

security context You can partition a single adaptive security appliance into multiple virtual devices, known as security contexts. Each context is an independent device, with its own security policy, interfaces, and administrators. Multiple contexts are similar to having multiple standalone devices. Many features are supported in multiple context mode, including routing tables, firewall features, IPS, and management.

Security Monitor Monitoring Center for Security. Provides event collection, viewing, and reporting capability for network devices. Used with the IDS MC.

sensing interface The interface on the sensor that monitors the desired network segment. The sensing interface is in promiscuous mode; it has no IP address and is not visible on the monitored segment.

sensor The sensor is the intrusion detection engine. It analyzes network traffic searching for signs of unauthorized activity.

SensorApp A component of the IPS. Performs packet capture and analysis. SensorApp analyzes network traffic for malicious content. Packets flow through a pipeline of processors fed by a producer designed to collect packets from the network interfaces on the sensor. SensorApp is the standalone executable that runs Analysis Engine.

Service engine Deals with specific protocols, such as DNS, FTP, H255, HTTP, IDENT, MS RPC, MS SQL, NTP, P2P, RPC, SMB, SNMP, SSH, and TNS.

service pack Used for the release of defect fixes and for the support of new signature engines. Service packs contain all of the defect fixes since the last base version (minor or major) and any new defects fixes.

session command Command used on routers and switches to provide either Telnet or console access to a module in the router or switch.

SFP Small Form-factor Pluggable. Often refers to a fiber optic transceiver that adapts optical cabling to fiber interfaces. See GBIC for more information.

shun command Enables a dynamic response to an attacking host by preventing new connections and disallowing packets from any existing connection. It is used by ARC when blocking with a PIX Firewall.

Signature Analysis Processor A processor in the IPS. Dispatches packets to the inspectors that are not stream-based and that are configured for interest in the packet in process.

signature A signature distills network information and compares it against a rule set that indicates typical intrusion activity.

signature engine A component of the sensor that supports many signatures in a certain category. An engine is composed of a parser and an inspector. Each engine has a set of legal parameters that have allowable ranges or sets of values.

signature engine update Executable file with its own versioning scheme that contains binary code to support new signature updates.

Signature Event Action Filter Subtracts actions based on the signature event signature ID, addresses, and risk rating. The input to the Signature Event Action Filter is the signature event with actions possibly added by the Signature Event Action Override.

Signature Event Action Handler Performs the requested actions. The output from Signature Event Action Handler is the actions being performed and possibly an evIdsAlert written to the Event Store.

Signature Event Action Override Adds actions based on the risk rating value. Signature Event Action Override applies to all signatures that fall into the range of the configured risk rating threshold. Each Signature Event Action Override is independent and has a separate configuration value for each action type.

Signature Event Action Processor Processes event actions. Event actions can be associated with an event risk rating threshold that must be surpassed for the actions to take place.

signature fidelity rating SFR. A weight associated with how well a signature might perform in the absence of specific knowledge of the target. The signature fidelity rating is configured per signature and indicates how accurately the signature detects the event or condition it describes.

signature update Executable file that contains a set of rules designed to recognize malicious network activities, such as worms, DDOS, viruses, and so forth. Signature updates are released independently, are dependent on a required signature engine version, and have their own versioning scheme.

Slave Dispatch Processor A processor in the IPS. Process found on dual CPU systems.

SMB Server Message Block. File-system protocol used in LAN manager and similar NOSs to package data and exchange information with other systems.

SMTP Simple Mail Transfer Protocol. Internet protocol providing e-mail services.

SN Serial Number. Part of the UDI. The SN is the serial number of your Cisco product.

SNAP Subnetwork Access Protocol. Internet protocol that operates between a network entity in the subnetwork and a network entity in the end system. SNAP specifies a standard method of encapsulating IP datagrams and ARP messages on IEEE networks. The SNAP entity in the end system makes use of the services of the subnetwork and performs three key functions: data transfer, connection management, and QoS selection.

sniffing interface See sensing interface.

SNMP Simple Network Management Protocol. Network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

SNMP2 SNMP Version 2. Version 2 of the network management protocol. SNMP2 supports centralized and distributed network management strategies, and includes improvements in the SMI, protocol operations, management architecture, and security.

software bypass Passes traffic through the IPS system without inspection.

source address Address of a network device that is sending data.

SPAN Switched Port Analyzer. Feature of the Catalyst 5000 switch that extends the monitoring abilities of existing network analyzers into a switched Ethernet environment. SPAN mirrors the traffic at one switched segment onto a predefined SPAN port. A network analyzer attached to the SPAN port can monitor traffic from any other Catalyst switched port.

spanning tree Loop-free subset of a network topology.

SQL Structured Query Language. International standard language for defining and accessing relational databases.

SRAM Type of RAM that retains its contents for as long as power is supplied. SRAM does not require constant refreshing, like DRAM.

SSH Secure Shell. A utility that uses strong authentication and secure communications to log in to another computer over a network.

SSL Secure Socket Layer. Encryption technology for the Internet used to provide secure transactions, such as the transmission of credit card numbers for e-commerce.

Stacheldraht A DDoS tool that relies on the ICMP protocol.

State engine Stateful searches of HTTP strings.

Statistics Processor A processor in the IPS. Keeps track of system statistics such as packet counts and packet arrival rates.

Stream Reassembly Processor A processor in the IPS. Reorders TCP streams to ensure the arrival order of the packets at the various stream-based inspectors. It is also responsible for normalization of the TCP stream. The normalizer engine lets you enable or disable alert and deny actions.

String engine A signature engine that provides regular expression-based pattern inspection and alert functionality for multiple transport protocols, including TCP, UDP, and ICMP.

subsignature A more granular representation of a general signature. It typically further defines a broad scope signature.

surface mounting Refers to attaching rubber feet to the bottom of a sensor when it is installed on a flat surface. The rubber feet allow proper airflow around the sensor and they also absorb vibration so that the hard-disk drive is less impacted.

switch Network device that filters, forwards, and floods frames based on the destination address of each frame. The switch operates at the data link layer of the OSI model.

SYN flood Denial of Service attack that sends a host more TCP SYN packets (request to synchronize sequence numbers, used when opening a connection) than the protocol implementation can handle.

system image The full IPS application and recovery image used for reimaging an entire sensor.

T

TAC A Cisco Technical Assistance Center. There are four TACs worldwide.

TACACS+ Terminal Access Controller Access Control System Plus. Proprietary Cisco enhancement to Terminal Access Controller Access Control System (TACACS). Provides additional support for authentication, authorization, and accounting.

target value rating TVR. A weight associated with the perceived value of the target. Target value rating is a user-configurable value (zero, low, medium, high, or mission critical) that identifies the importance of a network asset (through its IP address).

TCP Transmission Control Protocol. Connection-oriented transport layer protocol that provides reliable full-duplex data transmission. TCP is part of the TCP/IP protocol stack.

TCPDUMP The TCPDUMP utility is a free network protocol analyzer for UNIX and Windows. It lets you examine data from a live network or from a capture file on disk. You can use different options for viewing summary and detail information for each packet. For more information, see http://www.tcpdump.org/.

TCP reset interface The interface on the IDSM2 that can send TCP resets. On most sensors the TCP resets are sent out on the same sensing interface on which the packets are monitored, but on the IDSM2 the sensing interfaces cannot be used for sending TCP resets. On the IDSM2 the TCP reset interface is designated as port 1 with Catalyst software, and is not visible to the user in Cisco IOS software. The TCP reset action is only appropriate as an action selection on those signatures that are associated with a TCP-based service.

Telnet Standard terminal emulation protocol in the TCP/IP protocol stack. Telnet is used for remote terminal connection, enabling users to log in to remote systems and use resources as if they were connected to a local system. Telnet is defined in RFC 854.

terminal server A router with multiple, low speed, asynchronous ports that are connected to other serial devices. Terminal servers can be used to remotely manage network equipment, including sensors.

TFN Tribe Flood Network. A common type of DoS attack that can take advantage of forged or rapidly changing source IP addresses to allow attackers to thwart efforts to locate or filter the attacks.

TFN2K Tribe Flood Network 2000. A common type of DoS attack that can take advantage of forged or rapidly changing source IP addresses to allow attackers to thwart efforts to locate or filter the attacks.

TFTP Trivial File Transfer Protocol. Simplified version of FTP that lets files be transferred from one computer to another over a network, usually without the use of client authentication (for example, username and password).

threat rating TR. A threat rating is a value between 0 and 100 that represents a numerical decrease of the risk rating of an attack based on the response action that depicts the threat of an alert on the monitored network.

three-way handshake Process whereby two protocol entities synchronize during connection establishment.

threshold A value, either upper- or lower-bound that defines the maximum/minimum allowable condition before an alarm is sent.

Time Processor A processor in the IPS. Processes events stored in a time-slice calendar. Its primary task is to make stale database entries expire and to calculate time-dependent statistics.

TLS Transport Layer Security. The protocol used over stream transports to negotiate the identity of peers and establish encrypted communications.

TNS Transparent Network Substrate. Provides database applications with a single common interface to all industry-standard network protocols. With TNS, database applications can connect to other database applications across networks with different protocols.

topology Physical arrangement of network nodes and media within an enterprise networking structure.

TPKT Transport Packet. RFC 1006-defined method of demarking messages in a packet. The protocol uses ISO transport services on top of TCP.

traceroute Program available on many systems that traces the path a packet takes to a destination. It is used mostly to debug routing problems between hosts. A traceroute protocol is also defined in RFC 1393.

traffic analysis Inference of information from observable characteristics of data flow(s), even when the data is encrypted or otherwise not directly available. Such characteristics include the identities and locations of the source(s) and destination(s), and the presence, amount, frequency, and duration of occurrence.

Traffic ICMP engine Analyzes traffic from nonstandard protocols, such as TFN2K, LOKI, and DDOS.

trap Message sent by an SNMP agent to an NMS, a console, or a terminal to indicate the occurrence of a significant event, such as a specifically defined condition or a threshold that was reached.

Trojan engine Analyzes traffic from nonstandard protocols, such as BO2K and TFN2K.

trunk Physical and logical connection between two switches across which network traffic travels. A backbone is composed of a number of trunks.

trusted certificate Certificate upon which a certificate user relies as being valid without the need for validation testing; especially a public-key certificate that is used to provide the first public key in a certification path.

trusted key Public key upon which a user relies; especially a public key that can be used as the first public key in a certification path.

tune Adjusting signature parameters to modify an existing signature.

U

UDI Unique Device Identifier. Provides a unique identity for every Cisco product. The UDI is composed of the PID, VID, and SN. The UDI is stored in the Cisco IPS ID PROM.

UDLD UniDirectional Link Detection. Cisco proprietary protocol that allows devices connected through fiber-optic or copper Ethernet cables connected to LAN ports to monitor the physical configuration of the cables and detect when a unidirectional link exists. When a unidirectional link is detected, UDLD shuts down the affected LAN port and sends an alert, since unidirectional links can cause a variety of problems, such as, spanning tree topology loops.

UDP User Datagram Protocol. Connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols. UDP is defined in RFC 768.

unblock To direct a router to remove a previously applied block.

UniDirectional Link Detection See UDLD.

unvirtualized sensing interface An unvirtualized sensing interface has not been divided into subinterfaces and the entire interfaces can be associated with at most one virtual sensor.

UPS Uninterruptable Power Source.

UTC Coordinated Universal Time. Time zone at zero degrees longitude. Formerly called Greenwich Mean Time (GMT) and Zulu time.

V

VACL VLAN ACL. An ACL that filters all packets (both within a VLAN and between VLANs) that pass through a switch. Also known as security ACLs.

VID Version identifier. Part of the UDI.

VIP Versatile Interface Processor. Interface card used in Cisco 7000 and Cisco 7500 series routers. The VIP provides multilayer switching and runs Cisco IOS. The most recent version of the VIP is VIP2.

virtual sensor A logical grouping of sensing interfaces and the configuration policy for the signature engines and alarm filters to apply to them. In other words, multiple virtual sensors running on the same appliance, each configured with different signature behavior and traffic feeds.

virtualized sensing interface A virtualized interface has been divided into subinterfaces each of which consists of a group of VLANs. You can associate a virtual sensor with one or more subinterfaces so that different intrusion prevention policies can be assigned to those subinterfaces. You can virtualize both physical and inline interfaces.

virus Hidden, self-replicating section of computer software, usually malicious logic, that propagates by infecting—that is, inserting a copy of itself into and becoming part of—another program. A virus cannot run by itself; it requires that its host program be run to make the virus active.

virus update A signature update specifically addressing viruses.

VLAN Virtual Local Area Network. Group of devices on one or more LANs that are configured (using management software) so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

VTP VLAN Trunking Protocol. Cisco Layer 2 messaging protocol that manages the addition, deletion, and renaming of VLANs on a network-wide basis.

VMS CiscoWorks VPN/Security Management Solution. A suite of network security applications that combines web-based tools for configuring, monitoring, and troubleshooting enterprise VPN, firewalls, network intrusion detection systems and host-based intrusion prevention systems.

VoIP Voice over IP. The capability to carry normal telephony-style voice over an IP-based internet with POTS-like functionality, reliability, and voice quality. VoIP enables a router to carry voice traffic (for example, telephone calls and faxes) over an IP network. In VoIP, the DSP segments the voice signal into frames, which then are coupled in groups of two and stored in voice packets. These voice packets are transported using IP in compliance with ITU-T specification H.323.

VPN Virtual Private Network(ing). Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses “tunneling” to encrypt all information at the IP level.

VTP VLAN Trunking Protocol. A Cisco Layer 2 messaging protocol that manages the addition, deletion, and renaming of VLANs on a network-wide basis.

vulnerability One or more attributes of a computer or a network that permit a subject to initiate patterns of misuse on that computer or network.

W

WAN wide-area network. Data communications network that serves users across a broad geographic area and often uses transmission devices provided by common carriers. Frame Relay, SMDS, and X.25 are examples of WANs.

watch list rating WLR. A weight associated with the CSA MC watch list in the range of 0 to 100 (CSA MC only uses the range 0 to 35).

Web Server A component of the IPS. Waits for remote HTTP client requests and calls the appropriate servlet application.

WHOIS A TCP-based query/response protocol used for querying an official database to determine the owner of a domain name or an IP address.

Wireshark Wireshark is a free network protocol analyzer for UNIX and Windows. It lets you examine data from a live network or from a capture file on disk. You can interactively browse the capture data, viewing summary and detail information for each packet. Wireshark has several powerful features, including a rich display filter language and the ability to view the reconstructed stream of a TCP session. For more information, see http://www.wireshark.org.

worm A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and can consume computer resources destructively.

X

X.509 Standard that defines information contained in a certificate.

XML eXtensible Markup Language. Textual file format used for data interchange between heterogeneous hosts.

Z

zone A set of destination IP addresses sorted into an internal, illegal, or external zone used by Anomaly Detection.

INDEX

Numerics

A

B

C

D

E

L

M

N

O

P

R

S

T

U

V