



CHAPTER 5

Installing AIM-IPS



Note

All IPS platforms allow ten concurrent log in sessions.

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

- [Specifications, page 5-1](#)
- [Before Installing AIM-IPS, page 5-2](#)
- [Software and Hardware Requirements, page 5-2](#)
- [Interoperability With Other IPS Modules, page 5-3](#)
- [Restrictions, page 5-3](#)
- [Hardware Interfaces, page 5-4](#)
- [Installation and Removal Instructions, page 5-5](#)
- [Verifying Installation, page 5-6](#)

Specifications

Table 5-1 lists the specifications for 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 AIM-IPS

Follow these recommendations before installing 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 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 AIM-IPS and the Router](#).

Software and Hardware Requirements

The router and 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

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, NME-IPS disables all other modules. 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.



Caution

You cannot upgrade an NM-CIDS to NME-IPS. For more information on NM-CIDS, refer to [Introducing NM-CIDS](#) and [Installing NM-CIDS](#).

Restrictions

The following restrictions apply to AIM-IPS:

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

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 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.



Caution

When you reload the router, AIM-IPS also reloads. To ensure that there is no loss of data on AIM-IPS, make sure you shut down the module using the **shutdown** command before you use the **reload** command to reboot the router.

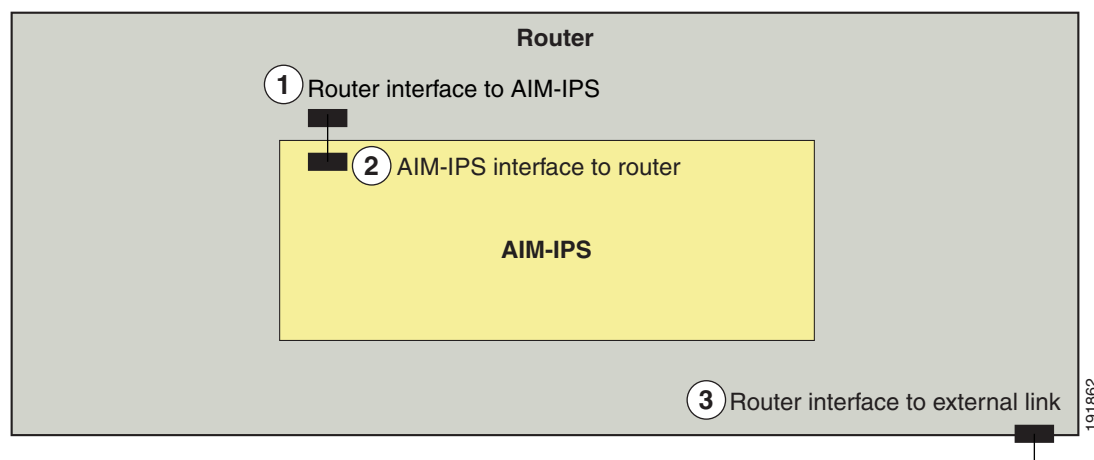
For More Information

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 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 AIM-IPS (IDS-Sensor 0/1) Uses the Cisco OS CLI to configure the IP address of the router interface that connects to AIM-IPS. This router IP address is used as the default router IP address when you configure Cisco IPS on AIM-IPS.
2	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 AIM-IPS. 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 AIM-IPS. This IP address belongs to the router itself and is used for routing traffic to the command and control interface of 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 6.1](#).
- For more information on IDM, refer to [Installing and Using Cisco Intrusion Prevention System Device Manager Version 6.1](#).
- For more information on IME, refer to [Installing and Using Cisco Intrusion Prevention System Manager Express 6.1](#).

Installation and Removal Instructions

For instructions on how to install and remove 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 AIM-IPS:

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

For More Information

- For the procedure for verifying that AIM-IPS is installed properly, see [Verifying Installation, page 5-6](#).
- For the procedure for using the **setup** command to initialize AIM-IPS, see [Initializing the Sensor, page 9-1](#).
- For more information about obtaining the most recent Cisco IPS software, see [Obtaining Cisco IPS Software, page 11-1](#).
- For the procedure to configure AIM-IPS to receive IPS traffic, refer to [Setting Up Interfaces on 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 documents:
 - [Installing and Using Cisco Intrusion Prevention System Device Manager 6.1](#)
 - [Installing and Using Cisco Intrusion Prevention System Manager Express 6.1](#)
 - [Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 6.1](#)

Verifying Installation

Use the **show inventory** command in privileged EXEC mode to verify the installation of 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 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 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#
```