



CHAPTER 18

Configuring AIP-SSM



Note

The number of concurrent CLI sessions is limited based on the platform. IDS-4215 and NM-CIDS are limited to three concurrent CLI sessions. All other platforms allow ten concurrent sessions.

This chapter contains procedures that are specific to configuring AIP-SSM. It contains the following sections:

- [Configuration Sequence, page 18-1](#)
- [Verifying AIP-SSM Initialization, page 18-2](#)
- [Creating Virtual Sensors, page 18-3](#)
- [Sending Traffic to AIP-SSM, page 18-9](#)
- [Adaptive Security Appliance, AIP-SSM, and Bypass Mode, page 18-12](#)
- [Reloading, Shutting Down, Resetting, and Recovering AIP-SSM, page 18-12](#)

Configuration Sequence

Perform the following tasks to configure AIP-SSM:

1. Log in to AIP-SSM.
2. Initialize AIP-SSM.
Run the **setup** command to initialize AIP-SSM.
3. Verify the AIP-SSM initialization.
4. If you have Cisco Adaptive Security Appliance Software 7.2.3 or later, configure multiple virtual sensors.



Note Virtualization is supported on ASA 7.2.3 only.

5. If you have Cisco Adaptive Security Appliance Software 7.2 or earlier, configure adaptive security appliance to send IPS traffic to AIP-SSM.
6. Perform other initial tasks, such as adding users, trusted hosts, and so forth.
7. Configure intrusion prevention.
8. Perform miscellaneous tasks to keep your AIP-SSM running smoothly.

9. Upgrade the IPS software with new signature updates and service packs.
10. Reimage AIP-SSM when needed.

For More Information

- For the procedure for logging in to AIP-SSM, see [Logging In to AIP-SSM, page 2-10](#).
- For the procedure for using the **setup** command to initialize AIP-SSM, see [Initializing AIP-SSM, page 3-24](#).
- For the procedure for verifying AIP-SSM initialization, see [Verifying AIP-SSM Initialization, page 18-2](#).
- For the procedure for creating virtual sensors, see [Creating Virtual Sensors, page 18-3](#).
- For the procedure for configuring ASA to send IPS traffic to AIM-SSM, see [Sending Traffic to AIP-SSM, page 18-9](#).
- For the procedures for setting up AIP-SSM, see [Chapter 4, “Initial Configuration Tasks.”](#)
- For the procedures for configuring intrusion prevention, see [Chapter 8, “Configuring Event Action Rules,” Chapter 7, “Defining Signatures,” and Chapter 13, “Configuring Attack Response Controller for Blocking and Rate Limiting.”](#)
- For the administrative procedures, see [Chapter 16, “Administrative Tasks for the Sensor.”](#)
- For more information on obtaining IPS software, see [Obtaining Cisco IPS Software, page 22-1](#).
- For the procedure for reimaging AIP-SSM, see [Installing the AIP-SSM System Image, page 21-51](#).

Verifying AIP-SSM Initialization

You can use the **show module slot details** command to verify that you have initialized AIP-SSM and to verify that you have the correct software version.

To verify initialization, follow these steps:

Step 1 Log in to the adaptive security appliance.

Step 2 Obtain the details about AIP-SSM:

```
asa# show module 1 details
ASA 5500 Series Security Services Module-10
Model:                ASA-SSM-10
Hardware version:    1.0
Serial Number:       JAB09370212
Firmware version:    1.0(10)0
Software version:    6.0(4)E1
MAC Address Range:   0012.d948.fe73 to 0012.d948.fe73
App. name:           IPS
App. Status:         Up
App. Status Desc:
App. version:        6.0(4)E1
Data plane Status:   Up
Status:              Up
Mgmt IP addr:        171.69.36.171
Mgmt web ports:      443
Mgmt TLS enabled:    true
asa#
```

Step 3 Confirm the information.

For More Information

For information on changing the AIP-SSM configuration, see [Configuration Sequence, page 18-1](#).

Creating Virtual Sensors



Caution

Cisco Adaptive Security Appliance Software 7.2.3 or later supports virtualization.

This section describes how to create virtual sensors on AIP-SSM, and contains the following topics:

- [Overview, page 18-3](#)
- [Virtual Sensor Configuration Sequence, page 18-3](#)
- [Creating Virtual Sensors on AIP-SSM, page 18-4](#)
- [Assigning Virtual Sensors to Adaptive Security Appliance Contexts, page 18-6](#)

Overview

AIP-SSM has one interface, GigabitEthernet0/1. When you create multiple virtual sensors, you must assign this interface to only one virtual sensor. For the other virtual sensors you do not need to designate an interface.

After you create virtual sensors, you must map them to a security context on the adaptive security appliance using the **allocate-ips** command. You can map many security contexts to many virtual sensors.



Note

The **allocate-ips** command does not apply to single mode. In this mode, the security appliance accepts any virtual sensor named in a **policy-map** command.

The **allocate-ips** command adds a new entry to the security context database. A warning is issued if the specified virtual sensor does not exist; however, the configuration is allowed. The configuration is checked again when the service-policy command is processed. If the virtual sensor is not valid, and the **fail-open** policy is enforced.

For More Information

For more information on adaptive security appliance security context modes, refer to [Cisco Security Appliance Command Line Configuration Guide](#).

Virtual Sensor Configuration Sequence

Follow this sequence to create virtual sensors on AIP-SSM and to assign them to adaptive security device contexts:

1. Configure up to four virtual sensors on AIP-SSM.
2. Assign the AIP-SSM interface, GigabitEthernet0/1, to one of the virtual sensors.

3. Assign virtual sensors to different contexts on the adaptive security device.
4. Use MPF to direct traffic to the targeted virtual sensor.

Creating Virtual Sensors on AIP-SSM

Use the **virtual-sensor** *name* command in service analysis engine submode to create virtual sensors on AIP-SSM.



Note

You can create four virtual sensors.

You assign policies (anomaly detection, event action rules, and signature definition) to the virtual sensor. You can use the default policies, `ad0`, `rules0`, or `sig0`, or you can create new policies.

Then you assign the interface GigabitEthernet0/1 to one virtual sensor.

The following options apply:

- **anomaly-detection**—Anomaly detection parameters
 - **anomaly-detection-name** *name*—Name of the anomaly detection policy
 - **operational-mode**—Anomaly detection mode (**inactive**, **learn**, **detect**)
- **description**—Description of the virtual sensor
- **event-action-rules**—Name of the event action rules policy
- **signature-definition**—Name of the signature definition policy
- **physical-interfaces**—Name of the physical interface
- **no**—Removes an entry or selection

To create a virtual sensor on AIP-SSM, follow these steps:

Step 1 Log in to the CLI using an account with Administrator privileges.

Step 2 Enter service analysis mode:

```
sensor# configure terminal
sensor(config)# service analysis-engine
sensor(config-ana)#
```

Step 3 Add a virtual sensor.

```
sensor(config-ana)# virtual-sensor vs1
sensor(config-ana-vir)#
```

Step 4 Add a description for this virtual sensor:

```
sensor(config-ana-vir)# description virtual sensor 1
```

Step 5 Assign an anomaly detection policy and operational mode to this virtual sensor:

```
sensor(config-ana-vir)# anomaly-detection
sensor(config-ana-vir-ano)# anomaly-detection-name ad1
sensor(config-ana-vir-ano)# operational-mode learn
```

Step 6 Assign an event action rules policy to this virtual sensor:

```
sensor(config-ana-vir-ano)# exit
sensor(config-ana-vir)# event-action-rules rules1
```

Step 7 Assign a signature definition policy to this virtual sensor:

```
sensor(config-ana-vir)# signature-definition sig1
```

Step 8 Assign the interface to one virtual sensor:

```
sensor(config-ana-vir)# physical-interface GigabitEthernet0/1
```

Step 9 Verify the virtual sensor settings:

```
sensor(config-ana-vir)# show settings
name: vs1
-----
description: virtual sensor 1 default:
signature-definition: sig1 default: sig0
event-action-rules: rules1 default: rules0
anomaly-detection
-----
anomaly-detection-name: ad1 default: ad0
operational-mode: learn default: detect
-----
physical-interface (min: 0, max: 999999999, current: 2)
-----
name: GigabitEthernet0/1
subinterface-number: 0 <defaulted>
-----
logical-interface (min: 0, max: 999999999, current: 0)
-----
-----
sensor(config-ana-vir)#
```

Step 10 Exit analysis engine mode:

```
sensor(config-ana-vir)# exit
sensor(config-ana)# exit
Apply Changes:[yes]:
sensor(config)#
```

Step 11 Press **Enter** to apply the changes or enter **no** to discard them.

For More Information

- For more information on creating and configuring anomaly detection policies, see [Working With Anomaly Detection Policies, page 9-8](#).
- For more information on creating and configuring event action rules policies, see [Working With Event Action Rules Policies, page 8-6](#).
- For more information on creating and configuring signature definition policies, see [Working With Signature Definition Policies, page 7-1](#).

Assigning Virtual Sensors to Adaptive Security Appliance Contexts

After you create virtual sensors on AIP-SSM, you must assign them to a security context on the adaptive security appliance.

The following options apply:

- **[no] allocate-ips** *sensor_name* [*mapped_name*] [**default**]
—Allocates a virtual sensor to a security context. Supported mode are multiple mode, system context, and context submode.



Note You cannot allocate the same AIP-SSM twice in a context.

- *sensor_name*—Name of AIP-SSM configured on the AIP-SSM. You receive a warning message if the name is not valid.
- *mapped_name*—Name by which the security context knows AIP-SSM.



Note The mapped name is used to hide the real name of AIP-SSM from the context, usually done for reasons of security or convenience to make the context configuration more generic. If no mapped name is used, the real AIP-SSM name is used. You cannot reuse a mapped name for two different AIP-SSMs in a context.

- **no**—De-allocates the sensor, looks through the policy map configurations, and deletes any IPS subcommand that refers to it.
- **default**—Specifies this AIP-SSM as the default. All legacy IPS configurations that do not specify a virtual sensor are mapped to this AIP-SSM.



Caution

You can only configure one default AIP-SSM per context. You must turn off the default flag of an existing default AIP-SSM before you can designate another AIP-SSM as the default.

- **clear configure allocate-ips**—Removes the configuration.
- **allocate-ips?**—Displays the list of configured AIP-SSMs.
- **show ips** [**detail**]
—Displays all available virtual sensors. Supported modes are EXEC mode, single or multiple, system or user modes.
 - **detail**—Adds the virtual sensor ID number.



Note In single mode, the command shows the names of all available virtual sensors. In multiple mode user context, the command shows the mapped names of all virtual sensors that have been allocated to this context. In multiple mode system context, the command shows the names of all virtual sensors and with the detail keyword, the sensor ID number, allocated context, and mapped name are displayed.

- **show context** [**detail**]
—Updated to display information about virtual sensors. In user context mode, a new line is added to show the mapped names of all virtual sensors that have been allocated to this context. In system, two new lines are added to show the real and mapped names of virtual sensors allocated to this context.

The following procedure demonstrates how to add three security contexts in multiple mode and how to assign virtual sensors to these security contexts.

**Note**

You can assign multiple virtual sensors to a context. Multiple contexts can share one virtual sensor, and when sharing, the contexts can have different mapped names (aliases) for the same virtual sensor.

To assign AIP-SSM virtual sensors to adaptive security appliance contexts in multiple mode, follow these steps:

Step 1 Log in to the adaptive security appliance.

Step 2 Display the list of available virtual sensors:

```
asa# show ips detail
Sensor Name      Sensor ID
-----
vs0              1
vs1              2
asa#
```

Step 3 Enter configuration mode:

```
asa# configure terminal
asa(config)#
```

Step 4 Enter multiple mode:

```
asa(config)# mode multiple
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm] yes
asa(config)#
```

Step 5 Add three context modes to multiple mode:

```
asa(config)# admin-context admin
Creating context 'admin'... Done. (13)
asa(config)# context admin
asa(config-ctx)# allocate-interface GigabitEthernet0/0.101
asa(config-ctx)# allocate-interface GigabitEthernet0/1.102
asa(config-ctx)# allocate-interface Management0/0
asa(config-ctx)# config-url disk0:/admin.cfg
Cryptoschecksum (changed): 0c34dc67 f413ad74 e297464a db211681
INFO: Context admin was created with URL disk0:/admin.cfg
INFO: Admin context will take some time to come up ... please wait.
asa(config-ctx)#
asa(config-ctx)# context c2
Creating context 'c2'... Done. (14)
asa(config-ctx)# allocate-interface GigabitEthernet0/0.103
asa(config-ctx)# allocate-interface GigabitEthernet0/1.104
asa(config-ctx)# config-url disk0:/c2.cfg

WARNING: Could not fetch the URL disk0:/c2.cfg
INFO: Creating context with default config
asa(config-ctx)#
asa(config-ctx)# context c3
Creating context 'c3'... Done. (15)
asa(config-ctx)# all
asa(config-ctx)# allocate-in
asa(config-ctx)# allocate-interface g0/2
asa(config-ctx)# allocate-interface g0/3
```

```
asa(config-ctx)# config-url disk0:/c3.cfg

WARNING: Could not fetch the URL disk0:/c3.cfg
INFO: Creating context with default config
asa(config-ctx)#
```

Step 6 Assign virtual sensors to the security contexts:

```
asa(config)# context admin
asa(config-ctx)# allocate-ips vs0 adminvs0
asa(config-ctx)# exit
asa(config)# context c2
asa(config-ctx)# allocate-ips vs1 c2vs1
asa(config)# context c3
asa(config-ctx)# allocate-ips vs0 c3vs0
asa(config-ctx)# allocate-ips vs1 c3vs1
asa(config-ctx)#
```

Step 7 Configure MPF for each context:

Note The following example shows context 3 (c3).

```
asa(config)# changeto context c3
asa/c3(config)# class-map any
asa/c3(config-cmap)# match access-list any
asa/c3(config-cmap)# exit
asa/c3(config)# policy-map ips_out
asa/c3(config-pmap)# class any
asa/c3(config-pmap-c)# ips promiscuous fail-close sensor c3vs1
asa/c3(config-pmap-c)# policy-map ips_in
asa/c3(config-pmap)# class any
asa/c3(config-pmap-c)# ips inline fail-open sensor c3vs0
asa/c3(config-pmap-c)# service-policy ips_out interface outside
asa/c3(config)# service-policy ips_in interface inside
asa/c3(config)#
```

Step 8 Confirm the configuration:

```
asa/c3(config)# exit
asa(config)# show ips detail
Sensor Name      Sensor ID      Allocated To      Mapped Name
-----
vs0              1              admin              adminvs0
                  c3              c3vs0
vs1              2              c2                 c2vs1
                  c3                 c3vs1
asa(config)#
```

Sending Traffic to AIP-SSM

**Note**

This section applies to Cisco Adaptive Security Appliance Software 7.2 or earlier.

This section describes how to configure AIP-SSM to receive IPS traffic from the adaptive security appliance (inline or promiscuous mode), and contains the following sections:

- [Overview, page 18-9](#)
- [Configuring the Adaptive Security Appliance to Send IPS Traffic to AIP-SSM, page 18-9](#)

Overview

The adaptive security appliance diverts packets to 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 AIP-SSM.

You can configure AIP-SSM to inspect traffic in inline or promiscuous mode and in fail-open or fail-over mode.

On the adaptive security appliance, to identify traffic to be diverted to and inspected by AIP-SSM:

1. Create or use an existing ACL.
2. Use the **class-map** command to define the IPS traffic class.
3. Use the **policy-map** command to create an IPS policy map by associating the traffic class with one or more actions.
4. Use the **service-policy** command to create an IPS security policy by associating the policy map with one or more interfaces.

You can use the adaptive security appliance CLI or ASDM to configure IPS traffic inspection.

Configuring the Adaptive Security Appliance to Send IPS Traffic to AIP-SSM

**Note**

For more information on these commands, refer to “Using Modular Policy Framework,” in [Cisco Security Appliance Command Line Configuration Guide](#).

The following options apply:

- **access-list** *word*—Configures an access control element; *word* is the access list identifier (up to 241 characters).
- **class-map** *class_map_name*—Defines the IPS traffic class.
- **match**—Identifies the traffic included in the traffic class.

A traffic class map contains a **match** command. When a packet is matched against a class map, the match result is either a match or a no match.

- **access-list**—Matches an access list.
- **any**—Matches any packet.

- **policy-map** *policy_map_name*—Creates an IPS policy map by associating the traffic class with one or more actions.
- **ips** {**inline** | **promiscuous**}[**fail-open** | **fail-close**] [**sensor** *sensor_name*]—Assigns traffic from the security appliance to a specified virtual sensor on AIP-SSM. If no virtual sensor is specified, traffic is assigned to the default virtual sensor. Supported modes are single or multi mode, user context, config mode, and policy map class submode.
 - **inline**—Places AIP-SSM directly in the traffic flow.

No traffic can continue through the adaptive security appliance without first passing through and being inspected by AIP-SSM. This mode is the most secure because every packet is analyzed before being permitted through. Also, AIP-SSM can implement a blocking policy on a packet-by-packet basis. This mode, however, can affect throughput.
 - **promiscuous**—Sends a duplicate stream of traffic to AIP-SSM.

This mode is less secure, but has little impact on traffic throughput. Unlike when in inline mode, AIP-SSM cannot block traffic by instructing the adaptive security appliance to block the traffic or by resetting a connection on the adaptive security appliance.
 - **fail-close**—Sets the adaptive security appliance to block all traffic if AIP-SSM is unavailable.
 - **fail-open**—Sets the adaptive security appliance to permit all traffic through, uninspected, if AIP-SSM is unavailable.



Note The adaptive security appliance fail-open/fail-close behavior depends on low-level heartbeats, which are turned off when AIP-SSM is shut down or reset. If AIP-SSM fails, the adaptive security appliance cannot detect this failure because the heartbeats are still received. For inline inspection of traffic, use IPS bypass mode to drop or permit traffic through.

- **sensor** *sensor_name*—Name of the allocated virtual sensor. If the sensor name was mapped, the mapped name is used. Otherwise, the real sensor name is used.
- **service-policy** *service_policy_name* {**global** | **interface** *interface_name*}—Creates an IPS security policy by associating the policy map with one or more interfaces.
 - **global**—Applies the policy map to all interfaces.

Only one global policy is allowed. You can override the global policy on an interface by applying a service policy to that interface. You can only apply one policy map to each interface.
 - **interface**—Applies the policy to one interface.

You can assign a different policy for each interface.

To allocate virtual sensors and send traffic from the adaptive security appliance to AIP-SSM for the IPS to inspect, follow these steps:

-
- Step 1** Log in to the adaptive security appliance.
- Step 2** Enter configuration mode:
- ```
asa# configure terminal
```
- Step 3** Create an IPS access list:
- ```
asa(config)# access-list IPS permit ip any any
```

Step 4 Define the IPS traffic class:

```
asa(config)# class-map class_map_name
asa(config-cmap)# match [access-list | any]
```

Step 5 Define the IPS policy map:

```
asa(config-cmap)# policy-map policy_map_name
```

Step 6 Identify the class map from Step 5 to which you want to assign an action:

```
asa(config-pmap)# class class_map_name
```

Step 7 Assign traffic to AIP-SSM:

```
asa(config-pmap-c)# ips {inline | promiscuous} [fail-close | fail-open]
```

Step 8 Define the IPS service policy:

```
asa(config-pmap-c)# service-policy policymap_name {global | interface interface_name}
```

Step 9 Verify the settings:

```
asa(config-pmap-c)# show running-config
!
class-map my_ips_class
match access-list IPS
class-map all_traffic
  match access-list all_traffic
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map my-ids-policy
  class my-ips-class
    ips promiscuous fail-close
!
service-policy my-ids-policy global
```

Step 10 Exit and save the configuration:

```
asa(config-pmap-c)# exit
asa(config-pmap)# exit
asa(config)# exit
asa#
```

The following example diverts all IP traffic to AIP-SSM in inline mode, and blocks all IP traffic should AIP-SSM fail for any reason:

```
hostname(config)# access-list IPS permit ip any any
hostname(config)# class-map my-ips-class
hostname(config-cmap)# match access-list IPS
hostname(config-cmap)# policy-map my-ids-policy
hostname(config-pmap)# class my-ips-class
hostname(config-pmap-c)# ips inline fail-close
hostname(config-pmap-c)# service-policy my-ids-policy global
```

For More Information

For more information on bypass mode, see [Adaptive Security Appliance, AIP-SSM, and Bypass Mode, page 18-12](#).

Adaptive Security Appliance, AIP-SSM, and Bypass Mode

The following conditions apply to bypass mode and AIP-SSM:

- Bypass Auto or Off
The adaptive security appliance permits or blocks traffic from going through according to the configured fail-open or fail-close rules when AIP-SSM is shut down or reset.
- Bypass Auto
If SensorApp stops in AIP-SSM, the adaptive security appliance permits all traffic through regardless of the configured fail-open or fail-close rules, because the AIP-SSM NIC driver is still functioning and passing heartbeat packets.
- Bypass Off
If SensorApp stops in AIP-SSM, the adaptive security appliance stops all traffic from going through regardless of the configured fail-open or fail-close rules.

For More Information

For more information on IPS software bypass mode, see [Configuring Bypass Mode, page 5-34](#).

Reloading, Shutting Down, Resetting, and Recovering AIP-SSM



Note

You can enter the **hw-module** commands from privileged EXEC mode or from global configuration mode. You can enter the commands in single routed mode and single transparent mode. For adaptive security devices operating in multi-mode (routed or transparent multi-mode) you can only execute the **hw-module** commands from the system context (not from Administrator or user contexts).

Use the following commands to reload, shut down, reset, recover the password, and recover AIP-SSM directly from the adaptive security appliance:

- **hw-module module slot_number reload**
This command reloads the software on AIP-SSM without doing a hardware reset. It is effective only when AIP-SSM is in the Up state.
- **hw-module module slot_number shutdown**
This command shuts down the software on AIP-SSM. It is effective only when AIP-SSM is in Up state.
- **hw-module module slot_number reset**
This command performs a hardware reset of AIP-SSM. It is applicable when the card is in the Up/Down/Unresponsive/Recover states.
- **hw-module module slot_number password-reset**
This command restores the cisco CLI account password to the default **cisco**.

- **hw-module module *slot_number* recover [boot | stop | configure]**

The **recover** command displays a set of interactive options for setting or changing the recovery parameters. You can change the parameter or keep the existing setting by pressing Enter.

- **hw-module module *slot_number* recover boot**

This command initiates recovery of AIP-SSM. It is applicable only when AIP-SSM is in the Up state.

- **hw-module module *slot_number* recover stop**

This command stops recovery of AIP-SSM. It is applicable only when AIP-SSM is in the Recover state.

**Caution**

If AIP-SSM recovery needs to be stopped, you must issue the **hw-module module 1 recover stop** command within 30 to 45 seconds after starting AIP-SSM recovery. Waiting any longer can lead to unexpected consequences. For example, AIP-SSM may come up in the Unresponsive state.

- **hw-module module 1 recover configure**

Use this command to configure parameters for module recovery. The essential parameters are the IP address and recovery image TFTP URL location.

Example:

```
aip-ssm# hardware-module module 1 recover configure
Image URL [tftp://10.89.146.1/IPS-SSM-K9-sys-1.1-a-5.1-1.img]:
Port IP Address [10.89.149.226]:
VLAN ID [0]:
Gateway IP Address [10.89.149.254]:
```

For More Information

For the procedure for recovering AIP-SSM, see [Installing the AIP-SSM System Image, page 21-51](#).

