Configuring the AIP SSC-5

AIP SSC-5 Configuration Sequence

You configure both the adaptive security appliance and IPS software on the AIP SSC-5. Perform the following tasks to configure the AIP SSC-5:

1. Log (session) in to the AIP SSC-5.
2. Initialize the AIP SSC-5.

   \textbf{Note} \hfill You do not have to run the \texttt{setup} command to initialize the AIP SSC-5. You can initialize it using ASDM.

3. Verify the AIP SSC-5 initialization.
4. Configure the adaptive security appliance to send IPS traffic to the AIP SSC-5.
5. Perform other initial tasks, such as adding users, trusted hosts, and so forth.
6. Configure intrusion prevention.
7. Perform miscellaneous tasks to keep your AIP SSC-5 running smoothly.
8. Upgrade the IPS software with new signature updates and service packs.
9. Reimage the AIP SSC-5 when needed.

For More Information

- For the procedure for logging in to the AIP SSC-5, see Logging In to the AIP SSM and the AIP SSC-5, page 2-6
- For the procedure for verifying the AIP SSC-5 initialization, see Verifying the AIP SSC-5 Initialization, page 18-2.
- For the procedure for configuring ASA to send traffic to the AIP SSC-5, see Sending Traffic to the AIP SSC-5, page 18-5.
- For the procedures for setting up the sensor, see Chapter 4, “Setting Up the Sensor.”
- For the procedures for keeping your AIP SSC-5 running smoothly, see Chapter 16, “Administrative Tasks for the Sensor.”
- For more information on how to obtain Cisco IPS software, see Chapter 22, “Obtaining Software.”
- For the procedure for reimaging the AIP SSC-5, see Installing the AIP SSM and the AIP SSC-5 System Image, page 23-25.

## Verifying the AIP SSC-5 Initialization

You can use the `show module slot details` command to verify that you have initialized the AIP SSC-5 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 the AIP SSC-5.

```
asa# show module 1 details
Getting details from the Service Module, please wait...
ASA 5500 Series Security Services Card-5
Hardware version: 0.1
Serial Number: JAB11370240
Firmware version: 1.0(14)3
Software version: 6.2(1)E3
MAC Address Range: 001d.45c2.e832 to 001d.45c2.e832
App. Name: IPS
App. Status: Up
App. Status Desc: Not Applicable
Data plane Status: Up
Status: Up
Mgmt IP Addr: 209.165.201.29
Mgmt Network Mask: 255.255.224.0
```
Configuring the AIP SSC-5 Management Interface

This section describes the AIP SSC-5 default network settings, how to change them, and provides examples. It contains the following topics:

- Understanding the AIP SSC-5 Management Interface, page 18-3
- Changing the AIP SSC-5 Network Settings, page 18-4
- The AIP SSC-5 Management Interface Example, page 18-5

Understanding the AIP SSC-5 Management Interface

An AIP SSC-5 does not have any external interfaces. You configure a VLAN as a management VLAN to allow access to an internal management IP address over the backplane. By default, VLAN 1 is enabled for the AIP SSC-5 management address. You can only assign one VLAN as the AIP SSC-5 management VLAN.

Table 18-1 lists the default network settings for the AIP SSC-5.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management VLAN</td>
<td>VLAN 1</td>
</tr>
<tr>
<td>Management IP address</td>
<td>192.168.1.2/24</td>
</tr>
<tr>
<td>Management hosts</td>
<td>192.168.1.0/24</td>
</tr>
<tr>
<td>Gateway</td>
<td>192.168.1.1</td>
</tr>
</tbody>
</table>

Note

The default management IP address on the adaptive security appliance is 192.168.1.1/24.

Note

The management IP address, hosts, and gateway settings are written to the AIP SSC-5 configuration, not the adaptive security appliance configuration. You can view these settings from the ASA 5505 using the show module details command. You can also run the setup command from the AIP SSC-5 CLI to configure this setting.

Mgmt Gateway: 209.165.201.30
Mgmt Access List: 209.165.201.31/32
209.165.202.158/32
209.165.200.254/24
Mgmt Vlan: 20
asa#

Step 3
Confirm the information.
For More Information

- For the procedure for running the `setup` command, see Basic Sensor Setup, page 3-4.
- For the procedure for changing the network settings, see Changing the AIP SSC-5 Network Settings, page 18-4.

Changing the AIP SSC-5 Network Settings

To change the default settings on the AIP SSC-5, follow these steps:

**Step 1** Log in to the adaptive security appliance.

**Step 2** Enter configuration mode.

```
asa# configure terminal
```

**Step 3** Verify the current management VLAN. By default, this is VLAN 1.

```
asa (config)# interface vlan number
asa (config)# interface vlan 1
```

**Step 4** Disable the AIP SSC-5 management.

```
asa (config-if)# no allow-ssc-mgmt
```

**Step 5** Specify the new AIP SSC-5 management interface.

```
asa(config)# interface vlan number
asa(config)# interface vlan 20
```

**Step 6** Set the management IP address for the AIP SSC-5.

```
asa (config-if)# allow-ssc-mgmt
```

Make sure the address is on the same subnet as the adaptive security appliance VLAN interface.

**Step 7** Configure the AIP SSC-5 management interface.

```
asa# hw-module module 1 ip ip_address netmask gateway
asa# hw-module module 1 ip 209.165.200.255 255.255.255.224 209.165.200.245
```

If the management station is on a directly connected adaptive security appliance network, set the gateway to be the adaptive security appliance interface address. If the management station is on a remote network, set the gateway to the address of an upstream router on the management VLAN.

**Step 8** Set the hosts allowed to access the management IP address.

```
asa# hw-module module 1 allow-ip ip_address netmask
asa# hw-module module 1 ip allow-ip 209.165.200.255 255.255.255.224
```

**Step 9** Verify the settings.

```
asa# show running-config
```

**Step 10** Exit and save the configuration.
For More Information
- For an example management interface example, see The AIP SSC-5 Management Interface Example, page 18-5.
- For a list of the default network settings, see Understanding the AIP SSC-5 Management Interface, page 18-3.

The AIP SSC-5 Management Interface Example

The following example configures VLAN 20 as the AIP SSC-5 management VLAN. This VLAN is restricted to management traffic only. Only the host at 10.1.1.30 can access the AIP SSC-5 management IP address. VLAN 20 is assigned to switch port Ethernet 0/0. When you connect to ASDM on ASA interface 10.1.1.1, ASDM then accesses the AIP SSC-5 on 10.1.1.2.

```bash
hostname(config)# interface vlan 1
hostname(config-if)# no allow-ssc-mgmt

hostname(config-if)# interface vlan 20
hostname(config-if)# nameif inside
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# security-level 100
hostname(config-if)# allow-ssc-mgmt
hostname(config-if)# no shutdown
hostname(config-if)# management-only

hostname(config-if)# hw-module module 1 ip 10.1.1.2 255.255.255.0 10.1.1.1
hostname(config)# hw-module module 1 allow-ip 10.1.1.30 255.255.255.255

hostname(config)# interface ethernet 0/0
hostname(config-if)# switchport access vlan 20
hostname(config-if)# no shutdown
```

For More Information
For the procedure to change network settings, see Changing the AIP SSC-5 Network Settings, page 18-4.

Sending Traffic to the AIP SSC-5

This section describes how to configure the AIP SSC-5 to receive IPS traffic from the adaptive security appliance (Inline or promiscuous mode). The AIP SSC-5 must be running Cisco Adaptive Security Appliance Software 8.2 or later. It contains the following topics:
- Adaptive Security Appliance and the AIP SSC-5, page 18-5
- IPS Traffic Commands, page 18-6
- Configuring the Adaptive Security Appliance to Send IPS Traffic to the AIP SSC-5, page 18-7

Adaptive Security Appliance and the AIP SSC-5

The adaptive security appliance diverts packets to the AIP SSC-5 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 SSC-5.

You can configure the AIP SSC-5 to inspect traffic in Inline or promiscuous mode and in fail-open or fail-over mode.
Perform these steps on the adaptive security appliance to identify traffic to be diverted to and inspected by the AIP SSC-5:

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.

### IPS Traffic Commands

**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 adaptive security appliance to a specified virtual sensor on the AIP SSC-5. 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.

**Note**

The AIP SSC-5 does not support virtualization.

- **inline**—Places the AIP SSC-5 directly in the traffic flow.

No traffic can continue through the adaptive security appliance without first passing through and being inspected by the AIP SSC-5. This mode is the most secure because every packet is analyzed before being permitted through. Also, the AIP SSC-5 can implement a blocking policy on a packet-by-packet basis. This mode, however, can affect throughput.
Sending Traffic to the AIP SSC-5

- **promiscuous**—Sends a duplicate stream of traffic to the AIP SSC-5. This mode is less secure, but has little impact on traffic throughput. Unlike when in inline mode, the AIP SSC-5 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 the AIP SSC-5 is unavailable.

- **fail-open**—Sets the adaptive security appliance to permit all traffic through, uninspected, if the AIP SSC-5 is unavailable.

**Note**
The adaptive security appliance fail-open/fail-close behavior depends on low-level heartbeats, which are turned off when the AIP SSC-5 is shut down or reset. If the AIP SSC-5 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.

**For More Information**
For more information about the AIP SSC-5, the adaptive security appliance, and bypass mode, see *The Adaptive Security Appliance, the AIP SSC-5, and Bypass Mode*, page 18-9.

Configuring the Adaptive Security Appliance to Send IPS Traffic to the AIP SSC-5

To send traffic from the adaptive security appliance to the AIP SSC-5 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 an IPS class map to identify the traffic you want to send to the AIP SSC-5.

```
asa(config)# class-map class_map_name
```
Example

```
asa(config)# class-map ips_class
```

**Note** You can create multiple traffic class maps to send multiple traffic classes to the AIP SSC-5.

**Step 5** Specify the traffic in the class map.

```
asa(config-cmap)# match parameter
```

Example

```
asa(config-cmap)# match (access-list | any)
```

**Step 6** Add an IPS policy map that sets the actions to take with the class map traffic.

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

Example

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

**Step 7** Identify the class map you created in Step 4.

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

Example

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

**Step 8** Assign traffic to the AIP SSC-5.

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

Example

```
asa(config-pmap-c)# ips promiscuous fail-close
```

**Step 9** (Optional) If you created multiple traffic class maps for IPS traffic, you can specify another class.

```
asa(config-pmap)# class class_map_name_2
```

Example

```
asa(config-pmap)# class ips_class_2
```

**Step 10** (Optional) Specify the second class of traffic to send to the AIP SSC-5.

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

Example

```
asa(config-pmap-c)# ips promiscuous fail-close
```

**Step 11** Activate the IPS service policy map on one or more interfaces.

```
asa(config)# service-policy policymap_name (global | interface interface_name)
```

Example

```
asa(config)# service-policy tcp_bypass_policy outside
```
Step 12 Verify the settings.
   ```
esa# show running-config
   ```

Step 13 Exit and save the configuration.

---

For More Information

For more information on bypass mode, see The Adaptive Security Appliance, the AIP SSC-5, and Bypass Mode, page 18-9.

The Adaptive Security Appliance, the AIP SSC-5, and Bypass Mode

The following conditions apply to bypass mode configuration, the adaptive security appliance, and the AIP SSC-5:

**The SensorApp Fails OR a Configuration Update is Taking Place**

The following occurs when bypass is set to Auto or Off on the AIP SSC-5:

- **Bypass Auto**—Traffic passes without inspection.
- **Bypass Off**—If the adaptive security appliance is configured for failover, then the adaptive security appliance fails over.
  - If the adaptive security appliance is not configured for failover or failover is not possible:
    - If set to fail-open, the adaptive security appliance passes traffic without sending it to the AIP SSC-5.
    - If set to fail-close, the adaptive security appliance stops passing traffic until the AIP SSC-5 is restarted or completes reconfiguration.

**Note**

When bypass is set to On, traffic passes without inspection regardless of the state of the SensorApp.

**The AIP SSC-5 Is Rebooted or Not Responding**

The following occurs according to how the adaptive security appliance is configured for failover:

- If the adaptive security appliance is configured for failover, then the adaptive security appliance fails over.
- If the adaptive security appliance is not configured for failover or failover is not possible:
  - If set to fail-open, the adaptive security appliance passes traffic without sending it to the AIP SSC-5.
  - If set to fail-close, the adaptive security appliance stops passing traffic until the AIP SSC-5 is restarted.

For More Information

For more information on bypass mode, see Inline Bypass Mode, page 5-35.
Reloading, Shutting Down, Resetting, and Recovering the AIP SSC-5

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 the AIP SSC-5 directly from the adaptive security appliance:

- **hw-module module slot_number reload**
  This command reloads the software on the AIP SSC-5 without doing a hardware reset. It is effective only when the AIP SSC-5 is in the Up state.

- **hw-module module slot_number shutdown**
  This command shuts down the software on the AIP SSC-5. It is effective only when the AIP SSC-5 is in Up state.

- **hw-module module slot_number reset**
  This command performs a hardware reset of the AIP SSC-5. It is applicable when the AIP SSC-5 is in the Up/Down/Unresponsive/Recover states.

- **hw-module module slot_number password-reset**
  This command restores the cisco CLI account password on the AIP SSC-5 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. To change the parameter or keep the existing setting, press Enter.

**Caution**

The AIP SSC-5 can take up to 20 minutes to come online when it reboots after the installation of a new system image. You must let the process complete before you can make configuration changes to the AIP SSC-5. If you try to modify and save configuration changes before the process is complete, you receive an error message.

- **hw-module module slot_number recover boot**
  This command initiates recovery of the AIP SSC-5. It is applicable only when the AIP SSC-5 is in the Up state.

- **hw-module module slot_number recover stop**
  This command stops recovery of the AIP SSC-5. It is applicable only when the AIP SSC-5 is in the Recover state.

**Caution**

If the AIP SSC-5 recovery needs to be stopped, you must issue the hw-module module 1 recover stop command within 30 to 45 seconds after starting the AIP SSC-5 recovery. Waiting any longer can lead to unexpected consequences. For example, the AIP SSC-5 may come up in the Unresponsive state.
- **hw-module module 1 recover configure**

  Use this command to configure parameters for the AIP SSC-5 recovery. The essential parameters are the IP address and recovery image TFTP URL location.

  Example

  aip-ssc# hardware-module module 1 recover configure
  Image URL [tftp://10.89.146.1/IPS-SSC-K9-sys-1.1-a-6.2-1-E3.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 the AIP SSC-5, see Installing the AIP SSM and the AIP SSC-5 System Image, page 23-25.

### New and Modified Commands

**Note**


This section describes the new and modified Cisco ASA commands that support the AIP SSC-5 and are used to configure the AIP SSC-5. It contains the following topics:

- hw-module module allow-ip, page 18-11
- hw-module module ip, page 18-12

#### hw-module module allow-ip

To configure host parameters on the AIP SSC-5, use the **hw-module module allow-ip** command in privileged EXEC mode.

```
hw-module module slot_number allow-ip ip_address netmask
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>allow-ip ip_address</td>
<td>Specifies the allowed host IP address on the AIP SSC-5.</td>
</tr>
<tr>
<td>netmask</td>
<td>Specifies the allowed host network mask on the AIP SSC-5.</td>
</tr>
<tr>
<td>slot_num</td>
<td>Specifies the slot number, which is always 1.</td>
</tr>
</tbody>
</table>

**Defaults**

No default behavior or values.
Command Modes

The following table shows the modes in which you can enter the command:

<table>
<thead>
<tr>
<th>Command Mode</th>
<th>Firewall Mode</th>
<th>Security Context</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Routed</td>
<td>Transparent</td>
</tr>
<tr>
<td>Privileged EXEC</td>
<td>•</td>
<td>•</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.2(1)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

This command is only valid when the AIP SSC-5 status is Up. Default values that are currently in effect are provided. To obtain these values, use the `show module details` command. These settings are saved as part of the AIP SSC-5 configuration.

Examples

The following example shows how to configure host parameters on the AIP SSC-5:

```
hostname# hw-module module 1 allow-ip 209.165.201.29 255.255.255.0
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hw-module module ip</td>
<td>Allows you to configure the AIP SSC-5 management parameters.</td>
</tr>
<tr>
<td>show module</td>
<td>Shows the AIP SSC-5 status information.</td>
</tr>
</tbody>
</table>

**hw-module module ip**

To configure the AIP SSC-5 management parameters, use the `hw-module module ip` command in privileged EXEC mode.

```
hw-module module slot_number ip ip_address netmask gateway
```

Syntax Description

- `gateway` Specifies the AIP SSC-5 management gateway IP address.
- `ip ip_address` Specifies the AIP SSC-5 management IP address.
- `netmask` Specifies the AIP SSC-5 management network mask.
- `slot_num` Specifies the slot number, which is always 1.

Defaults

No default behavior or values.
Command Modes

The following table shows the modes in which you can enter the command:

<table>
<thead>
<tr>
<th>Command Mode</th>
<th>Firewall Mode</th>
<th>Security Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privileged EXEC</td>
<td>•</td>
<td>•</td>
</tr>
</tbody>
</table>

Command History

Release  Modification
8.2(1)  This command was introduced.

Usage Guidelines

This command is only valid when the AIP SSC-5 status is Up. Default values that are currently in effect are provided. To obtain these values, use the show module details command. These settings are saved as part of the AIP SSC-5 configuration.

Examples

The following example shows how to configure management parameters for the AIP SSC-5:

```
hostname# hw-module module 1 ip 209.165.200.30 255.255.255.0 209.165.200.254
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hw-module module allow-ip</td>
<td>Allows you to configure the AIP SSC-5 host parameters.</td>
</tr>
<tr>
<td>show module</td>
<td>Shows the AIP SSC-5 status information.</td>
</tr>
</tbody>
</table>