CHAPTER 58

Managing Services Modules

This chapter describes how to manage the following module types:

- Security Services Cards (SSCs)
- Security Services Modules (SSMs)
- Security Services Processors (SSPs)

Modules run advanced security applications, such as IPS and Content Security and Control. See the *Cisco ASA 5500 Series Hardware and Software Compatibility Matrix* for a list of supported modules and ASA models:

http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html

Note For information about the 4GE SSM, which is an interface module and does not run intelligent software, see Chapter 6, "Starting Interface Configuration (ASA 5510 and Higher)."

The core SSP for the ASA 5585-X runs ASA software, and is not covered in this chapter.

This chapter includes the following sections:

Information About Modules

This section describes SSMs and SSCs, and includes the following topics:

Supported Applications

The following applications are supported on the SSM:

- IPS software (on the AIP SSM)
- Content Security and Control software (on the CSC SSM)

The following applications are supported on the SSC:

- IPS software (on the AIP SSC)

The following applications are supported on the SSP:

- IPS software (on the IPS SSP)

Note You cannot change the software type installed on the SSM/SSC; if you purchase an AIP SSM, you cannot later install CSC software on it.

Information About Management Access

You can manage the module application using ASDM or by using the module application CLI. This section includes the following topics:

Sessioning to the Module

If you have CLI access to the ASA, then you can session to the module over the backplane and access the module CLI. See the "Sessioning to the Module" section on page 58-6.

Using ASDM

After you launch ASDM on the ASA, ASDM connects to the module management interface to configure the module application.

- On the SSM and SSP—ASDM connects to an external Gigabit Ethernet port. If you cannot use the default address, you can change the interface IP address and other network parameters by sessioning to the module and setting the parameters at the module CLI. See the documentation for the module application for more information.
- On the SSC—You can configure a VLAN as a management VLAN to allow access to an internal management IP address over the backplane. To change the network parameters, see the "Configuring the SSC Management Interface" section on page 58-4.

See the "Default Settings" section on page 58-4 for information about the default management interface parameters.

Using SSH or Telnet

You can access the module CLI directly using SSH or Telnet to the module management interface. (Telnet access requires additional configuration in the module application). See the "Using ASDM" section on page 58-2 for more information about the management interface.

Other Uses for the Module Management Interface

The module management interface can be used for sending syslog messages or allowing updates for the module application, such as signature database updates on the AIP SSM or SSC.

Routing Considerations for Accessing the Management Interface

To make sure ASDM can manage the module, be sure that the ASA can access the module management interface address.

- For the SSC—Be sure to configure an IP address for the ASA VLAN that you are also using for the SSC management interface, and assign that VLAN to a switch port so the SSC interface is physically connected to the network. The SSC management interface will then be on a directly-connected network for the ASA, so ASDM can access the management interface without any additional routing configuration.
- For the SSM and SSP—The external management interface is not considered to be an ASA interface, so it is not automatically on a directly-connected network. Depending on how you cable your network, the module external interface can be on the same network as an ASA interface (through a switch), or you can put it on a different network (through a router).

Guidelines and Limitations

This section includes the guidelines and limitations for this feature.

Context Mode Guidelines

See the chapter for each SSM or SSC application for context mode guidelines.

Firewall Mode Guidelines

See the chapter for each SSM or SSC application for firewall mode guidelines.

Failover Guidelines

For the SSC, make sure you configure the management IP addresses on both units to be on the same subnet and VLAN.

Model Guidelines

For a complete list of supported ASA software, models, and modules, see *Cisco ASA 5500 Series Hardware and Software Compatibility*:

http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html

Additional Guidelines

- You cannot change the software type installed on the module; if you purchase an IPS module, you cannot later install CSC software on it.

- You cannot set up the SSC in ASDM if you use an IP address that goes through NAT.
- The AIP SSC-5 does not support virtualization, unretiring default retired signatures, creating custom signatures, adding signatures, cloning signatures, or anomaly detection.

Default Settings

Table 58-1 lists the default network settings for modules.

Table 58-1 Default Network Parameters

Parameters	Default
Management VLAN (SSC only)	VLAN 1
Management IP address	192.168.1.2/24
Management hosts (SSC only)	192.168.1.0/24
Gateway	192.168.1.1

Note The default management IP address on the ASA is 192.168.1.1/24.

Configuring the SSC Management Interface

An SSC does not have any external interfaces. You can 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 SSC management address. You can only assign one VLAN as the SSC management VLAN. This section describes how to change the management VLAN. It also describes how to change the default management IP address, allowed hosts, and gateway. See the "Default Settings" section on page 58-4 for more information about defaults.

Prerequisites

For the VLAN you want to use for the SSC management interface, configure the switch port and VLAN interface on the ASA 5505 according to the procedures listed in Chapter 6, "Starting Interface Configuration (ASA 5505)." This configuration is required so the SSC interface is physically connected to the network.

Restrictions

Do not configure NAT for the management address if you intend to access it using ASDM. For initial setup with ASDM, you need to access the real address. After initial setup (where you set the the password in the SSC), you can configure NAT and supply ASDM with the translated address when you want to access the SSC.

Detailed Steps

	Command	Purpose
Step 1	**interface vlan** *number* **Example:** `hostname(config)# interface vlan 1`	Specifies the current management VLAN for which you want to disable SSC management. By default, this is VLAN 1.
Step 2	**no allow-ssc-mgmt** **Example:** `hostname(config-if)# no allow-ssc-mgmt`	Disables SSC management for the old VLAN so that you can enable it for a different VLAN.
Step 3	**interface vlan** *number* **Example:** `hostname(config)# interface vlan 20`	Specifies the VLAN you want to use as the SSC management VLAN.
Step 4	**allow-ssc-mgmt** **Example:** `hostname(config-if)# allow-ssc-mgmt`	Sets this interface as the SSC management interface.
Step 5	**hw-module module 1 ip** *ip_address netmask gateway* **Example:** `hostname# hw-module module 1 ip 209.165.200.225 255.255.255.224 209.165.200.245`	Configures the management IP address for the SSC. Make sure this address is on the same subnet as the ASA 5505 VLAN interface. If the management station is on a directly-connected ASA network, then set the gateway to be the ASA 5505 VLAN interface address. If the management station is on a remote network, then set the gateway to the address of an upstream router on the management VLAN. **Note** These settings are written to the SSC application configuration, not the ASA 5505 configuration. You can view these settings from the ASA 5505 using the **show module details** command. You can alternatively use the SSC application **setup** command to configure this setting from the SSC CLI.
Step 6	**hw-module module 1 allow-ip** *ip_address netmask* **Example:** `hostname# hw-module module 1 allow-ip 209.165.201.29 255.255.255.224`	Sets the hosts that are allowed to access the management IP address. **Note** These settings are written to the SSC application configuration, not the ASA 5505 configuration. You can view these settings from the ASA 5505 using the **show module details** command. You can alternatively use the SSC application **setup** command to configure this setting from the SSC CLI.

Examples

The following example configures VLAN 20 as the SSC management VLAN. This VLAN is restricted to management traffic only. Only the host at 10.1.1.30 can access the SSC 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 SSC on 10.1.1.2.

```
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
```

Sessioning to the Module

To begin configuring the module, session to the module from the ASA. To session to the module from the ASA, enter the following command:

Command	Purpose

session 1
 	
Example:
`hostname# session 1`
 	
`Opening command session with slot 1.`
`Connected to slot 1. Escape character sequence is 'CTRL-^X'.`
	Accesses the module over the backplane. You are prompted for the username and password. The default username is “cisco” and the default password is “cisco.”
	
	Note The first time you log in to the module, you are prompted to change the default password. Passwords must be at least eight characters long and not a word in the dictionary.

Troubleshooting the Module

This section includes procedures that help you recover or troubleshoot the module, and includes the following topics:

Installing an Image on the Module

If the module suffers a failure and the module application image cannot run, you can transfer application images from a TFTP server to the module using the ASA CLI. The ASA can communicate with the module ROMMON application to transfer the image.

Note This process can take approximately 15 minutes to complete, depending on your network and the size of the image.

Do not use the **upgrade** command within the SSM or SSC software to install the image.

Prerequisites

Be sure the TFTP server that you specify can transfer files up to 60 MB in size.

Detailed Steps

	Command	Purpose

Step 1	**hw-module module 1 recover configure**
	
	Example:
	`hostname# hw-module module 1 recover configure`
	`Image URL [tftp://127.0.0.1/myimage]: tftp://10.1.1.1/ids-newimg`
	`Port IP Address [127.0.0.2]: 10.1.2.10`
	`Port Mask [255.255.255.254]: 255.255.255.0`
	`Gateway IP Address [1.1.2.10]: 10.1.2.254`
	`VLAN ID [0]: 100`
		Prompts you for the URL for the TFTP server, the management interface IP address and netmask, gateway address, and VLAN ID (the SSC uses the VLAN you configured for management in the "Configuring the SSC Management Interface" section on page 58-4.) These network parameters are configured in the ROMMON module; the network parameters you configured in the module application configuration (for example in the "Configuring the SSC Management Interface" section on page 58-4) are not available to ROMMON, so you must set them separately here.
		
		If you are modifying a configuration, you can keep the previously configured value by pressing **Enter** when prompted.
		
		You can view the recovery configuration using the **show module 1 recover** command.
		
		In multiple context mode, enter this command in the system execution space.

Step 2	**hw-module module 1 recover boot** **Example:** `hostname# hw-module module 1 recover boot`	Transfers the image from the TFTP server to the module and restarts the module.
Step 3	**show module 1 details** **Example:** `hostname# show module 1 details`	Checks the progress of the image transfer and module restart process. The Status field in the output indicates the operational status of the module. A module operating normally shows a status of "Up." While the ASA transfers an application image to the module, the Status field in the output reads "Recover." When the ASA completes the image transfer and restarts the module, the newly transferred image is running.

Resetting the Password

To reset the module password to the default of "cisco," enter the following command:

Command	Purpose
hw-module module 1 password-reset **Example:** `hostname# hw-module module 1 password-reset`	Resets the module password to "cisco."

Reloading or Resetting the Module

To reload or reset the module, enter one of the following commands:

Command	Purpose
hw-module module 1 reload **Example:** `hostname# hw-module module 1 reload`	Reloads the module software.
hw-module module 1 reset **Example:** `hostname# hw-module module 1 reset`	Performs a hardware reset, and then reloads the module.

Shutting Down the Module

To shut down the module, enter the following command:

Command	Purpose
hw-module module 1 shutdown **Example:** `hostname# hw-module module 1 shutdown`	Shuts down the module.

Monitoring SSMs and SSCs

To check the status of an SSM or SSC, enter one of the following commands:

Command	Purpose
`show module`	Displays the status.
`show module 1 details`	Displays additional status information.
`show module 1 recover`	Displays the network parameters for transferring an image to the module.

Examples

The following is sample output from the **show module** command for an ASA with a CSC SSM installed.

```
hostname# show module
Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  0 ASA 5520 Adaptive Security Appliance         ASA5520            JMX1241L05S
  1 ASA 5500 Series Content Security Services Mo ASA-SSM-CSC-10     AF1234BQQL

Mod SSM Application Name           Status           SSM Application Version
--- ------------------------------ ---------------- --------------------------
  1 CSC SSM                        Down             6.2.1599.0
```

The following is sample output from the **show module details** command, which provides additional information about an ASA with a CSC SSM installed.

```
hostname# 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: 1.0
Serial Number: JAF10333331
Firmware version: 1.0(10)0
Software version: Trend Micro InterScan Security Module Version 6.2
App. name: Trend Micro InterScan Security Module
App. version: Version 6.2
Data plane Status: Up
Status: Up
HTTP Service: Up
Mail Service: Up
FTP Service: Up
Activated: Yes
Mgmt IP addr: 209.165.200.225
Mgmt web port: 8443
```

The following is sample output from the **show module recover** command, which includes recovery details for an ASA with a CSC SSM installed.

```
hostname# show module 1 recover
Module 1 recover parameters. . .
Boot Recovery Image: Yes
Image URL: tftp://10.21.18.1/ids-oldimg
Port IP Address: 209.165.200.230
Port Mask: 255.255.224.0
Gateway IP Address: 209.165.200.254
```

The following is sample output from the **show module details** command, which provides additional information for an ASA with an SSC installed.

```
hostname# 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)E2
MAC Address Range: 001d.45c2.e832 to 001d.45c2.e832
App. Name: IPS
App. Status: Up
App. Status Desc: Not Applicable
App. Version: 6.2(1)E2
Data plane Status: Up
Status: Up
```

```
Mgmt IP Addr: 209.165.201.29
Mgmt Network Mask: 255.255.224.0
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
```

Where to Go Next

To configure the IPS module, see Chapter 59, "Configuring the IPS Module."

To configure the CSC module, see Chapter 60, "Configuring the Content Security and Control Application on the CSC SSM."

Feature History for the Module

Table 58-2 lists the release history for this feature.

Table 58-2 Feature History for the SSM and SSC

Feature Name	Releases	Feature Information
AIP SSM and CSC SSM	ASA 7.0(1), ASDM 5.0(1)	SSMs were introduced to support IPS and CSC applications. The following commands were introduced to manage the SSM: **hw-module module {recover | reload | reset | shutdown}**, **show module**, and **session**.
Password reset	ASA 7.2(2), ASDM 5.2(2)	The **hw-module module password-reset** command was introduced.
AIP SSC	ASA 8.2(1), ASDM 6.2(1)	The AIP SSC was introduced. The following commands were introduced: **allow-ssc-mgmt**, **hw-module module ip**, and **hw-module module allow-ip**.
IPS SSP	ASA 8.2(4.4), ASDM 6.3(5)	The IPS SSP was introduced.