



CHAPTER 10

Configuring Management Access to the SSC

This chapter describes how to configure management access to a Security Services Card (SSC) that is installed in the security appliance. The SSC runs the IPS application. For information about configuring IPS, see [Configuring the IPS Application on the AIP SSM and SSC, page 30-1](#).

This chapter includes the following sections:

- [Information About Management Access to the SSC, page 10-1](#)
- [Guidelines and Limitations, page 10-2](#)
- [Default Settings, page 10-2](#)
- [Configuring the SSC Management Interface, page 10-3](#)
- [Where to Go Next, page 10-5](#)

Information About Management Access to the SSC

You can manage the module application using ASDM or by using the module application CLI. For information about using the CLI, see the *Cisco ASA 5500 Series Configuration Guide using the CLI*.

This section includes the following topics:

- [Information About Using ASDM to Manage the SSC, page 10-1](#)
- [Other Uses for the SSC Management Interface, page 10-2](#)
- [Routing Considerations for Accessing the Management Interface, page 10-2](#)

Information About Using ASDM to Manage the SSC

After you launch ASDM on the security appliance, ASDM connects to the SSC management interface to configure the module application. 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, page 10-3](#).

See the [Default Settings, page 10-2](#) for information about the default management interface parameters.

Other Uses for the SSC 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 SSC.

Routing Considerations for Accessing the Management Interface

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

Be sure to configure an IP address for the security appliance VLAN that you are also using for the SSC management interface, and assign that VLAN to a switch port so that the SSC interface is physically connected to the network. The SSC management interface will then be on a directly-connected network for the security appliance, so ASDM can access the management interface without any additional routing configuration.



Note

If the default gateway is set to the security appliance, traffic from the SSC to devices directly connected to the security appliance go through; however, if the destination is a hop away (that is, on a different gateway), the traffic does not go through.

If you have multiple networks on an internal link, make sure that you change the default gateway to an internal router instead of leaving it at the default setting of the security appliance.

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

Make sure you configure the management IP addresses on both units to be on the same subnet and VLAN.

Model Guidelines

For model support for the SSC, see the [“SSM and SSC Support Per Model”](#) section on page 3-2.

Additional Guidelines

You cannot set up the SSC in ASDM if you use an IP address that goes through NAT.

Default Settings

[Table 10-1](#) lists the default network settings for SSCs.

Table 10-1 Default Network Parameters

Parameters	Default
Management VLAN	VLAN 1
Management IP address	192.168.1.2/24
Gateway	192.168.1.1

**Note**

The default management IP address on the security appliance is 192.168.1.5/24.

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 10-2 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. This is required so the SSC interface is physically connected to the network. You must create and assign VLANs to an interface before you can go to the SSC Setup pane and select one for the SSC.

Restrictions

Do not configure NAT for the management address. For initial setup with ASDM, you need to access the real address. After initial setup (where you set the password in the SSC), you can configure NAT and supply ASDM with the translated address when you want to access the SSC on the Configuration > IPS pane.

Detailed Steps

- Step 1** If you are configuring the SSC for the first time, in the ASDM main window, choose **Configuration > Device Setup > SSC Setup**.

**Note**

If you click the **IPS** tab before you have configured the SSC, the Stop dialog box appears. Click **OK** to have ASDM redirect you to the SSC Setup pane. You must define the settings in the SSC Setup pane before you can access any part of the GUI.

- Step 2** In the Management Interface area, do the following:
- a. Choose the Interface VLAN from the drop-down list.
This setting allows you to manage the SSC using this VLAN.



Note The following settings are written to the SSC application configuration, not the security appliance configuration.

- b. Enter the IP address.
- c. Choose the subnet mask from the drop-down list.
- d. Enter the default gateway IP address.

If the management station is on a directly-connected security appliance 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.

Step 3 In the Management Access List area, do the following.



Note The following settings are written to the SSC application configuration, not the security appliance configuration.

- a. Enter the IP address for the host network.
- b. Choose the subnet mask from the drop-down list.
- c. Click **Add** to add these settings to the Allowed Hosts/Networks list.



Note After you click **Add**, make sure you save the management settings you have just defined by clicking **Apply**. If you decide to remove these settings, continue to the next substep. Otherwise, go to [Step 4](#).

- d. To delete these settings, in the ASDM main window, click the **IPS** tab. Choose **Configuration > IPS > Sensor Setup > Allowed Hosts/Networks**. Choose the host or network that you want to remove from the list, and click **Delete**. To add new management settings, you can either click **Add** in the existing pane or return to the SSC Setup pane by choosing **Configuration > Device Setup > SSC Setup**.

Step 4 In the IPS Password area, do the following:



Note The following settings are written to the SSC application configuration, not the security appliance configuration.

- a. Enter the password. The default password is “cisco.”
- b. Enter the new password, and confirm the change.

Step 5 Click **Apply** to save the settings to the running configuration.

The SSC Setup completed dialog box appears only after the initial configuration.

Step 6 To complete the SSC application configuration and have ASDM go directly to the Configuration > IPS > Sensor Setup > Startup Wizard screen, do one of the following:

- Click the **IPS** button in the navigation pane.
- Click the **Configure the IPS SSC module** link.



Note If you want to change the SSC configuration settings at a later date, click the **IPS** tab.

Troubleshooting

To reset the password, choose **Tools > IPS Password Reset**. If you change the password, the Status dialog box appears, indicating that the new sensor password is being saved to the SSC application configuration.

After you have logged in and defined a new password, you do not need to log in to the IPS SSC application again. If you cannot connect to the IPS SSC application with the new password, restart ASDM and try to log in again.

If you have defined a new password and still have an existing password that is different than the new password, clear the password cache by choosing **File > Clear ASDM Password Cache**, then restart ASDM and try to log in again.

If you upgrade the ASA 5505 and add an SSC, make sure that the factory default IP address of the ASA 5505 starts at 192.168.1.5, because the factory default IP address of the SSC is 192.168.1.2. If a conflict occurs during configuration, a warning message appears.

At startup, make sure that the TFTP URL download location is valid, because if the ASA 5505 cannot detect a valid image to download, the SSC application does not start and the following error message appears:

```
Autoboot Error\System Halt
```



Note

If you restart the security appliance, the SSC is not automatically restarted. For more information, see the “Managing SSMs and SSCs” section in the *Cisco ASA 5500 Series Configuration Guide using the CLI*.

Where to Go Next

See [Chapter 30, “Configuring the IPS Application on the AIP SSM and SSC.”](#)

