



# CHAPTER 5

## Configuring the Adaptive Security Appliance

---

This chapter describes the initial configuration of the adaptive security appliance. You can perform the configuration steps using either the browser-based Cisco Adaptive Security Device Manager (ASDM) or the command-line interface (CLI). However, the procedures in this chapter refer to the method using ASDM.



### Note

---

To use ASDM, you must have a DES license or a 3DES-AES license. For more information, see [Appendix A, “Obtaining a DES License or a 3DES-AES License.”](#)

---

This chapter includes the following sections:

- [About the Factory-Default Configuration, page 5-2](#)
- [About the Adaptive Security Device Manager, page 5-2](#)
- [Using the Startup Wizard, page 5-3](#)
- [Setting the Media Type for Fiber Interfaces, page 5-6](#)
- [What to Do Next, page 5-7](#)

## About the Factory-Default Configuration

Cisco adaptive security appliances are shipped with a factory-default configuration that enables quick startup. The factory-default configuration automatically configures an interface for management so you can quickly connect to the device and use ASDM to complete your configuration.

By default, the adaptive security appliance Management interface is configured with a default DHCP address pool. This configuration enables a client on the inside network to obtain a DHCP address from the adaptive security appliance to connect to the appliance. Administrators can then configure and manage the adaptive security appliance using ASDM.

## About the Adaptive Security Device Manager



The Adaptive Security Device Manager (ASDM) is a feature-rich graphical interface that enables you to manage and monitor the adaptive security appliance. Its web-based design provides secure access so that you can connect to and manage the adaptive security appliance from any location by using a web browser.

In addition to its complete configuration and management capability, ASDM features intelligent wizards to simplify and accelerate the deployment of the adaptive security appliance.

In addition to the ASDM web configuration tool, you can configure the adaptive security appliance by using the command-line interface. For more information, see the *Cisco Security Appliance Command Line Configuration Guide* and the *Cisco Security Appliance Command Reference*.

## Using the Startup Wizard

ASDM includes a Startup Wizard to simplify the initial configuration of your adaptive security appliance. With a few steps, the Startup Wizard enables you to configure the adaptive security appliance so that it allows packets to flow securely between the inside network and the outside network.



---

**Note** You must use a port in Slot 0 for the inside interface and a port in Slot 1 for the outside interface.

---

This section describes how to use the Startup Wizard to set basic configuration parameters. This section includes the following topics:

- [Before Launching the Startup Wizard, page 5-4](#)
- [Running the Startup Wizard, page 5-4](#)

## Before Launching the Startup Wizard

Before you launch the Startup Wizard, perform the following steps:

---

**Step 1** Obtain a DES license or a 3DES-AES license.

To run ASDM, you must have a DES license or a 3DES-AES license. If you did not purchase one of these licenses with the adaptive security appliance, see [Appendix A, “Obtaining a DES License or a 3DES-AES License”](#) for information about how to obtain and activate one.

**Step 2** Enable Java and Javascript in your web browser.

**Step 3** Gather the following information:

- A unique hostname to identify the adaptive security appliance on your network.
  - The IP addresses of your outside interface, inside interface, and any other interfaces to be configured.
  - The IP addresses to use for NAT or PAT configuration.
  - The IP address range for the DHCP server.
- 

## Running the Startup Wizard

To use the Startup Wizard to set up a basic configuration for the adaptive security appliance, perform the following steps:

---

**Step 1** If you have not already done so, connect to the management port.

- a. Locate an Ethernet cable, which has an RJ-45 connector on each end.
- b. Connect one RJ-45 connector to the Management0/0 port.
- c. Connect the other end of the Ethernet cable to the Ethernet port on your computer or to your management network.
- d. If you connected to your management network, connect a PC for configuring the adaptive security appliance to your management network.

- Step 2** Launch the Startup Wizard.
- a. On the PC connected to the switch, hub, or management network, launch an Internet browser.
  - b. In the address field of the browser, enter this URL: **https://192.168.1.1/**.



---

**Note** The adaptive security appliance ships with a default IP address of 192.168.1.1. Remember to add the “s” in “**https**” or the connection fails. HTTPS (HTTP over SSL) provides a secure connection between your browser and the adaptive security appliance.

---

- c. In the window that requires you to choose the method you want to use to run the ASDM software, choose either to download the ASDM launcher or to run the ASDM software as a Java applet.

**Step 3** In the dialog box that requires a username and password, leave both fields empty. Press **Enter**.

**Step 4** Click **Yes** to accept the certificates. Click **Yes** for all subsequent authentication and certificate dialog boxes.

ASDM starts.

**Step 5** From the Wizards menu, choose Startup Wizard.

**Step 6** Follow the instructions in the Startup Wizard to set up your adaptive security appliance.

For information about any field in the Startup Wizard, click **Help** at the bottom of the window.

---



---

**Note** Based on your network security policy, you should also consider configuring the adaptive security appliance to deny all ICMP traffic through the outside interface or any other interface that is necessary. You can configure this access control policy using the **icmp** command. For more information about the **icmp** command, see the *Cisco Security Appliance Command Reference*.

---

# Setting the Media Type for Fiber Interfaces

If you are using any fiber connections in Slot 1, you must change the media type setting from the default setting to Fiber Connector.

**Note**

---

Because the default media type setting is for a copper Ethernet port, you do not need to set the media type setting for copper Ethernet ports you use.

---

To set the media type for fiber interfaces using ASDM, perform the following steps starting from the main ASDM window:

- 
- Step 1** In the ASDM window, click **Configuration**.
  - Step 2** In the Features pane, click **Interfaces**.
  - Step 3** Click the **4GE SSM** interface and click **Edit**. The Edit Interface dialog box appears.
  - Step 4** Click **Configure Hardware Properties**. The Hardware Properties dialog box appears.
  - Step 5** From the Media Type drop-down list, choose **Fiber Connector**.
  - Step 6** Click **OK** to return to the Edit Interfaces dialog box, then click **OK** to return to the interfaces configuration dialog box.
  - Step 7** Repeat this procedure for each fiber interface.
- 

You can also set the media type from the command line. For more information, see *Configuring Ethernet Settings and Subinterfaces in the Cisco Security Appliance Command Line Configuration Guide*.

# What to Do Next

Next, configure the adaptive security appliance for your deployment using one or more of the following chapters:

To Do This ...	See ...
Configure the adaptive security appliance to protect a DMZ web server	<a href="#">Chapter 6, “Scenario: DMZ Configuration”</a>
Configure the adaptive security appliance for remote-access VPN	<a href="#">Chapter 7, “Scenario: Remote-Access VPN Configuration”</a>
Configure the adaptive security appliance for Site-to-Site VPN	<a href="#">Chapter 8, “Scenario: Site-to-Site VPN Configuration”</a>

