



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 [“Obtaining a DES License or a 3DES-AES License”](#) section on page A-1.

About the Factory Default Configuration

Cisco adaptive security appliances are shipped with a factory-default configuration that enables quick startup. This configuration meets the needs of most small and medium business networking environments.

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.

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*.

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

To use ASDM, you must have a DES license or a 3DES-AES license. In addition, Java and JavaScript must be enabled in your web browser.

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*.

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.
 - The IP addresses to use for NAT or PAT configuration.
 - The IP address range for the DHCP server.
-

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 (GigabitEthernet0/1) and the outside network (GigabitEthernet0/0).

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 the MGMT interface to a switch or hub by using the Ethernet cable. To this same switch, connect a PC for configuring the adaptive security appliance.

Step 2 Configure your PC to use DHCP (to receive an IP address automatically from the adaptive security appliance), or assign a static IP address to your PC by selecting an address out of the 192.168.1.0 network. (Valid addresses are 192.168.1.2 through 192.168.1.254, with a mask of 255.255.255.0 and default route of 192.168.1.1.)



Note The MGMT interface of the adaptive security appliance is assigned 192.168.1.1 by default, so this address is unavailable.

Step 3 Check the LINK LED on the MGMT interface.

When a connection is established, the LINK LED interface on the adaptive security appliance and the corresponding LINK LED on the switch or hub turn solid green.

Step 4 Launch the Startup Wizard.

- a. On the PC connected to the switch or hub, 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.

Step 5 In the dialog box that requires a username and password, leave both fields empty. Press **Enter**.

Step 6 Click **Yes** to accept the certificates. Click **Yes** for all subsequent authentication and certificate dialog boxes.

ASDM starts.

Step 7 From the Wizards menu at the top of the ASDM window, choose Startup Wizard.

Step 8 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.

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	Chapter 6, “Scenario: DMZ Configuration”
Configure the adaptive security appliance for remote-access VPN	Chapter 7, “Scenario: Remote-Access VPN Configuration”
Configure the adaptive security appliance for Site-to-Site VPN	Chapter 8, “Scenario: Site-to-Site VPN Configuration”
Configure the AIP SSM for intrusion prevention	Chapter 9, “Configuring the AIP SSM”
Configure the CSC SSM for content security	Chapter 10, “Configuring the CSC SSM”

