



## 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). The procedures in this chapter describe how to configure the adaptive security appliance using ASDM.

This chapter includes the following sections:

- [About the Factory Default Configuration, page 5-1](#)
- [Using the CLI for Configuration, page 5-3](#)
- [Using the Adaptive Security Device Manager for Configuration, page 5-3](#)
- [Running the ASDM Startup Wizard, page 5-10](#)
- [What to Do Next, page 5-11](#)

## About the Factory Default Configuration

Cisco adaptive security appliances are shipped with a factory-default configuration that enables quick startup. The ASA 5505 comes preconfigured with the following:

- Two VLANs: VLAN 1 and VLAN2
- VLAN 1 has the following properties:
  - Named “inside”

- Allocated switch ports Ethernet 0/1 through Ethernet 0/7
- Security level of 100
- Allocated switch ports Ethernet 0/1 through 0/7
- IP address of 192.168.1.1 255.255.255.0
- VLAN2 has the following properties:
  - Named “outside”
  - Allocated switch port Ethernet 0/0
  - Security level of 0
  - Configured to obtain its IP address using DHCP
- Inside interface to connect to the device and use ASDM to complete your configuration.

By default, the adaptive security appliance Inside 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.

The default configuration that ships with the adaptive security appliance, in most cases, is sufficient for your basic deployment. However, you can modify the default configuration so that you can customize the security policy to suit your deployment. To modify the default settings, you can use the ASDM or the CLI. In ASDM, run the Startup Wizard to change the following settings from their factory default settings:

- Hostname
- Domain name
- Administrative passwords
- IP address of the outside interface
- Interfaces such as DMZ interfaces
- Address translation rules
- Dynamic IP address settings for the inside interface

For more information about configuring the adaptive security appliance by using ASDM, see the online Help.

For more information about using the CLI configuration, see the *Cisco Security Appliance Command Line Configuration Guide*.

## Using the CLI for Configuration

In addition to the ASDM web configuration tool, you can configure the adaptive security appliance by using the command-line interface.

You can get step-by-step examples of how to configure basic remote access and LAN-to-LAN connections in the CLI itself by using the `vpnsetup ipsec-remote-access` steps and `vpnsetup site-to-site` steps commands. For more information about these commands, see the *Cisco Security Appliance Command Reference*.

For step-by-step configuration procedures for all functional areas of the adaptive security appliance, see the *Cisco Security Appliance Command Line Configuration Guide*.

## Using the Adaptive Security Device Manager for Configuration

The Adaptive Security Device Manager (ASDM) is a feature-rich graphical interface that allows you to manage and monitor the adaptive security appliance. The 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.

This section includes the following topics:

- [Preparing to Use ASDM, page 5-5](#)
- [Gathering Configuration Information for Initial Setup, page 5-5](#)
- [Installing the ASDM Launcher, page 5-6](#)
- [Starting ASDM with a Web Browser, page 5-9](#)

## Preparing to Use ASDM

Before you can use ASDM, 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), which enables the PC to communicate with the ASA 5505 and the Internet as well as to run ASDM for configuration and management tasks.

Alternatively, you can assign a static IP address to your PC by selecting an address in the 192.168.1.0 subnet. (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.)

When you connect other devices to any of the inside ports, make sure that they do not have the same IP address.



---

**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.
- 

## Gathering Configuration Information for Initial Setup

Gather the following information:

- A unique hostname to identify the adaptive security appliance on your network.
- The domain name.

- The IP addresses of your outside interface, inside interface, and any other interfaces to be configured.
  - IP addresses for hosts that should have administrative access to this device using HTTPS for ASDM, SSH, or Telnet.
  - The privileged mode password for administrative access.
  - The IP addresses to use for NAT or PAT address translation, if any.
  - The IP address range for the DHCP server.
  - The IP address for the WINS server.
  - Static routes to be configured.
  - If you want to create a DMZ, you must create a third VLAN and assign ports to that VLAN. (By default, there are two VLANs configured.)
  - Interface configuration information: whether traffic is permitted between interfaces at the same security level, and whether traffic is permitted between hosts on the same interface.
  - If you are configuring an Easy VPN hardware client, the IP addresses of primary and secondary Easy VPN servers; whether the client is to run in client or network extension mode; and user and group login credentials to match those configured on the primary and secondary Easy VPN servers.
- 

## Installing the ASDM Launcher

You can launch ASDM in either of two ways: by downloading the ASDM Launcher software so that ASDM runs locally on your PC, or by enabling Java and JavaScript in your web browser and accessing ASDM remotely from your PC. This procedure describes how to set up your system to run ASDM locally.

To install the ASDM Launcher, perform the following steps:

- 
- Step 1** On the PC connected to the switch or hub, launch an Internet browser.
- a. In the address field of the browser, enter this URL:  
**`https://192.168.1.1/admin`**.



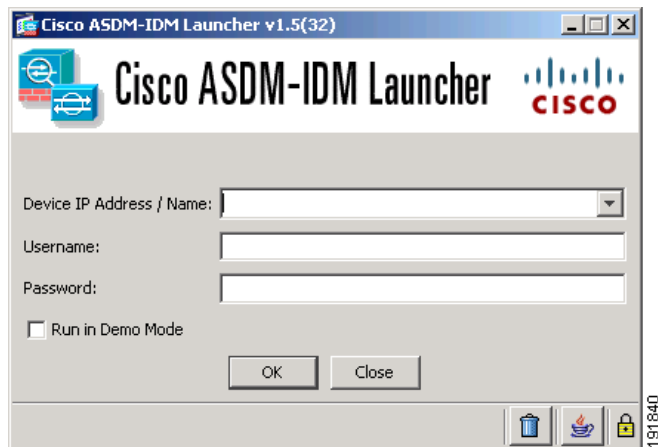
**Note** The adaptive security appliance ships with a default IP address of 192.168.1.1. Remember to add the “s” in “**https**” or the connection fails. HTTPS (HTTP over SSL) provides a secure connection between your browser and the adaptive security appliance.

The Cisco ASDM splash screen appears.

- b.** Click **Install ASDM Launcher and Run ASDM**.
- c.** In the dialog box that requires a username and password, leave both fields empty. Click **OK**.
- d.** Click **Yes** to accept the certificates. Click **Yes** for all subsequent authentication and certificate dialog boxes.
- e.** When the File Download dialog box opens, click **Open** to run the installation program directly. It is not necessary to save the installation software to your hard drive.
- f.** When the InstallShield Wizard appears, follow the instructions to install the ASDM Launcher software.

**Step 2** From your desktop, start the Cisco ASDM Launcher software.

A dialog box appears.



**Step 3** Enter the IP address or the host name of your adaptive security appliance.

**Step 4** Leave the Username and Password fields blank.



---

**Note** By default, there is no Username and Password set for the Cisco ASDM Launcher.

---

**Step 5** Click OK.

**Step 6** If you receive a security warning containing a request to accept a certificate, click **Yes**.

The ASA checks to see if there is updated software and if so, downloads it automatically.

The main ASDM window appears.

The screenshot displays the Cisco ASDM 6.1 for ASA web interface. The main window is titled "Cisco ASDM 6.1 for ASA - 10.86.194.224". The interface is divided into several sections:

- Device Information:** Shows general device details such as Host Name (asa2.cisco.com), ASA Version (8.0(4)), ASDM Version (6.1(3)), Firewall Mode (Routed), Total Flash (64 MB), Total Memory (256 MB), Device Uptime (46d 15h 59m 34s), Device Type (ASA 5510), and Context Mode (Single).
- Interface Status:** A table showing the status of various interfaces:
 

Interface	IP Address/Mask	Line	Link	Kbps
fa/0/24	192.168.3.4/24	down	down	0
inside	no ip address	down	down	0
management	192.168.1.1/24	down	down	0
outside	10.86.194.224/23	up	up	120
- System Resources Status:** Displays CPU usage (3%) and Memory usage (132MB).
- Traffic Status:** Includes a "Connections Per Second Usage" graph and an "outside" Interface Traffic Usage (Kbps) graph.
- Latest ASDM Syslog Messages:** A table showing recent system messages:
 

Severity	Date	Time	Syslog ID	Source IP	Source	Destination IP	Destination	Description
6	Oct 14 2008	13:55:31	725007	171.69.39.67	1748			SSL session with client outside:171.69.39.67/1748 terminated.
6	Oct 14 2008	13:55:31	605005	171.69.39.67	1748	10.86.194.224	https	Login permitted from 171.69.39.67/1748 to outside:10.86.194.224/https for user "enable_15"
6	Oct 14 2008	13:55:31	725002	171.69.39.67	1748			Device completed SSL handshake with client outside:171.69.39.67/1748
6	Oct 14 2008	13:55:31	725003	171.69.39.67	1748			SSL client outside:171.69.39.67/1748 permit to resume previous session

The status bar at the bottom indicates "Device configuration loaded successfully." and the user is logged in as "admin".

ASDM starts and the main window appears.

## Starting ASDM with a Web Browser

To run ASDM in a web browser, enter the factory default IP address in the address field: <https://192.168.1.1/admin/>.

**Note**

---

Remember to add the “s” in “**https**” or the connection fails. HTTP over SSL (HTTP) provides a secure connection between your browser and the adaptive security appliance.

---

The Main ASDM window appears.

## Running the ASDM 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.

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

---

**Step 1** From the Wizards menu at the top of the ASDM window, choose Startup Wizard.

**Step 2** 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**

---

If you get an error requesting a DES license or a 3DES-AES license, see [Appendix A, “Obtaining a 3DES/AES License”](#) for information.

---

**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 ASDM. From the ASDM main page, click **Configuration > Properties > ICMP Rules**. Add an entry for the outside interface. Set the IP address to 0.0.0.0, the netmask to 0.0.0.0, and Action to deny.

---

# What to Do 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: IPsec Remote-Access VPN Configuration”</a>
Configure the adaptive security appliance for SSL VPN connections using software clients	<a href="#">Chapter 8, “Scenario: Configuring Connections for a Cisco AnyConnect VPN Client”</a>
Configure the adaptive security appliance for SSL VPN connections using a web browser	<a href="#">Chapter 9, “Scenario: SSL VPN Clientless Connections”</a>
Configure the adaptive security appliance for site-to-site VPN	<a href="#">Chapter 10, “Scenario: Site-to-Site VPN Configuration”</a>
Configure the adaptive security appliance as an Easy VPN remote device	<a href="#">Chapter 11, “Scenario: Easy VPN Hardware Client Configuration”</a>

■ What to Do Next