



CHAPTER 2

Getting Started

This chapter describes how to get started with your adaptive security appliance. This chapter includes the following sections:

- [Configuring the Security Appliance for ASDM Access, page 2-1](#)
- [Starting ASDM, page 2-1](#)
- [Factory Default Configurations, page 2-5](#)
- [Getting Started With the Configuration, page 2-8](#)
- [Using the Command Line Interface, page 2-8](#)

Configuring the Security Appliance for ASDM Access

If you want to use ASDM to configure the adaptive security appliance and you have a factory default configuration, you can connect to the default management address by pointing your browser or the ASDM launcher to the IP address in the following URL:

```
https://192.168.1.1/admin
```

With the factory default configuration, clients on the 192.168.1.0/24 inside network can access ASDM. To allow other clients to access ASDM, see the [“Configuring Device Access for ASDM, Telnet, or SSH” section on page 33-1](#).

See the following Ethernet connection guidelines when using the factory default configurations:

- ASA 5505—The switch port to which you connect to ASDM can be any port, except for Ethernet 0/0.
- ASA 5510 and higher —The interface to which you connect to ASDM is Management 0/0.

For more information, see the [“Factory Default Configurations” section on page 2-5](#). If you do not have a factory default configuration, see the *Cisco ASA 5500 Series Configuration Guide using the CLI* for instructions to access the CLI and the **setup** command to perform minimum initial configuration.

Starting ASDM

This section describes how to start ASDM according to one of the following methods:

- [Downloading the ASDM Launcher, page 2-2](#)
- [Starting ASDM from the ASDM Launcher, page 2-2](#)

- [Using ASDM in Demo Mode, page 2-3](#)
- [Starting ASDM from a Web Browser, page 2-4](#)

Downloading the ASDM Launcher

The ASDM Launcher is for Windows only. The ASDM Launcher avoids double authentication and certificate dialog boxes, launches more quickly, and caches previously entered IP addresses and usernames.

To download the ASDM launcher, perform the following steps:

Step 1 On the ASDM Welcome screen, click the applicable button to download the ASDM Launcher installation file.

Step 2 Double-click the **asdm-launcher.exe** file.



Note In transparent firewall mode, enter the management IP address. Be sure to enter **https**, not **http**.

Step 3 Click **OK** or **Yes** to all prompts, including the name and password prompt. Leave the name and password blank.

The installer downloads to your computer.

Step 4 Run the installer to install the ASDM Launcher.

Starting ASDM from the ASDM Launcher

To start ASDM from the ASDM Launcher, perform the following steps:

Step 1 Double-click the Cisco ASDM Launcher shortcut on your desktop, or open it from the **Start** menu. Alternatively, from the ASDM Welcome screen, you can click **Run Startup Wizard** to configure ASDM.

Step 2 Enter or choose the adaptive adaptive security appliance IP address or hostname to which you want to connect. To clear the list of IP addresses, click the trash can icon next to the Device/IP Address/Name field.

Step 3 Enter your username and your password, and then click **OK**.

If there is a new version of ASDM on the adaptive adaptive security appliance, the ASDM Launcher automatically downloads the new version and requests that you update the current version before starting ASDM.



Note If you are using the factory default configuration, you do not need to have a username or password. Leave these fields blank to login to ASDM.

Using ASDM in Demo Mode

The ASDM Demo Mode, a separately installed application, lets you run ASDM without having a live device available. In this mode, you can do the following:

- Perform configuration and selected monitoring tasks via ASDM as though you were interacting with a real device.
- Demonstrate ASDM or adaptive security appliance features using the ASDM interface.
- Perform configuration and monitoring tasks with the CSC SSM.
- Obtain simulated monitoring and logging data, including real-time syslog messages. The data shown is randomly generated; however, the experience is identical to what you would see when you are connected to a real device.

This mode has been updated to support the following features:

- For global policies, an adaptive security appliance in single, routed mode and intrusion prevention
- For object NAT, an adaptive security appliance in single, routed mode and a firewall DMZ.
- For the Botnet Traffic Filter, an adaptive security appliance in single, routed mode and security contexts.
- Site-to-Site VPN with IPv6 (Clientless SSL VPN and IPsec VPN)
- Promiscuous IDS (intrusion prevention)
- Unified Communication Wizard

This mode does not support the following:

- Saving changes made to the configuration that appear in the GUI.
- File or disk operations.
- Historical monitoring data.
- Non-administrative users.
- These features:
 - File menu:
 - Save Running Configuration to Flash
 - Save Running Configuration to TFTP Server
 - Save Running Configuration to Standby Unit
 - Save Internal Log Buffer to Flash
 - Clear Internal Log Buffer
 - Tools menu:
 - Command Line Interface
 - Ping
 - File Management
 - Update Software
 - File Transfer
 - Upload Image from Local PC
 - System Reload

- Toolbar/Status bar > Save
- Configuration > Interface > Edit Interface > Renew DHCP Lease
- Configuring a standby device after failover
- Operations that cause a rereading of the configuration, in which the GUI reverts to the original configuration:
 - Switching contexts
 - Making changes in the Interface pane
 - NAT pane changes
 - Clock pane changes

To run ASDM in Demo Mode, perform the following steps:

-
- Step 1** Download the ASDM Demo Mode installer, `asdm-demo-version.msi`, from the following location:
<http://www.cisco.com/cisco/software/navigator.html?a=a&i=rpm>
- Step 2** Double-click the installer to install the software.
- Step 3** Double-click the Cisco ASDM Launcher shortcut on your desktop, or open it from the **Start** menu.
- Step 4** Check the **Run in Demo Mode** check box.
The Demo Mode window appears.
-

Starting ASDM from a Web Browser

To start ASDM from a web browser, perform the following steps:

-
- Step 1** From a supported web browser on the adaptive security appliance network, enter the following URL:
`https://interface_ip_address`
- Where `interface_ip_address` is the IP address of ASDM on the adaptive security appliance network.



Note In transparent firewall mode, enter the management IP address. Be sure to enter `https`, not `http`.

- Step 2** Click **OK** or **Yes** to all browser prompts, including the username and password, which you should leave blank.
- The Cisco ASDM 6.3(1) Welcome page displays with the following buttons:
- **Install ASDM Launcher and Run ASDM**
 - **Run ASDM**
 - **Run Startup Wizard**
- Step 3** Click **Run ASDM**.
- Step 4** Click **OK** or **Yes** to all the browser prompts.
-

Multiple ASDM Session Support

ASDM allows multiple PCs or workstations to each have one browser session open with the same adaptive security appliance software. A single adaptive security appliance can support up to five concurrent ASDM sessions in single, routed mode. Only one session per browser per PC or workstation is supported for a specified adaptive security appliance. In multiple context mode, five concurrent ASDM sessions are supported per context, up to a maximum of 32 total connections for each adaptive security appliance.

Factory Default Configurations

The factory default configuration is the configuration applied by Cisco to new adaptive security appliances.

For the ASA 5510 and higher adaptive security appliances, the factory default configuration configures an interface for management so you can connect to it using ASDM, with which you can then complete your configuration.

For the ASA 5505 adaptive security appliance, the factory default configuration configures interfaces and NAT so that the adaptive security appliance is ready to use in your network immediately.

The factory default configuration is available only for routed firewall mode and single context mode. See [Chapter 6, “Configuring Multiple Context Mode,”](#) for more information about multiple context mode. See [Chapter 5, “Configuring the Transparent or Routed Firewall,”](#) for more information about routed and transparent firewall mode.

**Note**

In addition to the image files and the (hidden) default configuration, the following folders and files are standard in flash memory: log/, crypto_archive/, and coredumpinfo/coredump.cfg. The date on these files may not match the date of the image files in flash memory. These files aid in potential troubleshooting; they do not indicate that a failure has occurred.

This section includes the following topics:

- [Restoring the Factory Default Configuration, page 2-5](#)
- [ASA 5505 Default Configuration, page 2-6](#)
- [ASA 5510 and Higher Default Configuration, page 2-7](#)

Restoring the Factory Default Configuration

This section describes how to restore the factory default configuration.

Limitations

This feature is available only in routed firewall mode; transparent mode does not support IP addresses for interfaces. In addition, this feature is available only in single context mode; an adaptive security appliance with a cleared configuration does not have any defined contexts to configure automatically using this feature.

Detailed Steps

Step 1 In the main ASDM application window, choose **File > Reset Device to the Factory Default Configuration**.

The Reset Device to the Default Configuration dialog box appears.

Step 2 (Optional) Enter the Management IP address of the management interface, instead of using the default address, 192.168.1.1. For an adaptive security appliance with a dedicated management interface, the interface is called “Management0/0.” For other adaptive security appliance, the configured interface is Ethernet 1 and called “inside.”

Step 3 Choose the Management (or Inside) Subnet Mask from the drop-down list.

Step 4 To save this configuration to internal flash memory, choose **File > Save Running Configuration to Flash**.

Choosing this option saves the running configuration to the default location for the startup configuration, even if you have previously configured a different location. When the configuration was cleared, this path was also cleared. The next time you reload the adaptive security appliance after restoring the factory configuration, the device boots from the first image in internal flash memory. If an image in internal flash memory does not exist, the adaptive security appliance does not boot.

What to Do Next

See the [“Getting Started With the Configuration”](#) section on page 2-8 to start configuring the adaptive security appliance.

ASA 5505 Default Configuration

The default factory configuration for the ASA 5505 adaptive security appliance configures the following:

- An inside VLAN 1 interface that includes the Ethernet 0/1 through 0/7 switch ports. If you did not set the IP address, then the VLAN 1 IP address and mask are 192.168.1.1 and 255.255.255.0.
- An outside VLAN 2 interface that includes the Ethernet 0/0 switch port. VLAN 2 derives its IP address using DHCP.
- The default route is also derived from DHCP.
- All inside IP addresses are translated when accessing the outside using interface PAT.
- By default, inside users can access the outside, and outside users are prevented from accessing the inside.
- The DHCP server is enabled on the adaptive security appliance, so a PC connecting to the VLAN 1 interface receives an address between 192.168.1.2 and 192.168.1.254.
- The HTTP server is enabled for ASDM and is accessible to users on the 192.168.1.0 network.

The configuration consists of the following commands:

```
interface Ethernet 0/0
  switchport access vlan 2
  no shutdown
interface Ethernet 0/1
```

```

        switchport access vlan 1
        no shutdown
interface Ethernet 0/2
        switchport access vlan 1
        no shutdown
interface Ethernet 0/3
        switchport access vlan 1
        no shutdown
interface Ethernet 0/4
        switchport access vlan 1
        no shutdown
interface Ethernet 0/5
        switchport access vlan 1
        no shutdown
interface Ethernet 0/6
        switchport access vlan 1
        no shutdown
interface Ethernet 0/7
        switchport access vlan 1
        no shutdown
interface vlan2
        nameif outside
        no shutdown
        ip address dhcp setroute
interface vlan1
        nameif inside
        ip address 192.168.1.1 255.255.255.0
        security-level 100
        no shutdown
object network obj_any
        subnet 0 0
        nat (inside,outside) dynamic interface
http server enable
http 192.168.1.0 255.255.255.0 inside
dhcpd address 192.168.1.2-192.168.1.254 inside
dhcpd auto_config outside
dhcpd enable inside
logging asdm informational

```

ASA 5510 and Higher Default Configuration

The default factory configuration for the ASA 5510 and higher adaptive security appliance configures the following:

- The management interface, Management 0/0. If you did not set the IP address, then the IP address and mask are 192.168.1.1 and 255.255.255.0.
- The DHCP server is enabled on the adaptive security appliance, so a PC connecting to the interface receives an address between 192.168.1.2 and 192.168.1.254.
- The HTTP server is enabled for ASDM and is accessible to users on the 192.168.1.0 network.

The configuration consists of the following commands:

```

interface management 0/0
        ip address 192.168.1.1 255.255.255.0
        nameif management
        security-level 100
        no shutdown
asdm logging informational 100
asdm history enable

```

```
http server enable
http 192.168.1.0 255.255.255.0 management
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd enable management
```

Getting Started With the Configuration

To configure and monitor the adaptive adaptive security appliance, perform the following steps:

-
- Step 1** For initial configuration using the Startup Wizard, choose **Wizards > Startup Wizard**.
 - Step 2** To use the IPsec [VPN Wizard](#) to configure IPsec VPN connections, choose **Wizards > IPsec VPN Wizard** and complete each screen that appears.
 - Step 3** To use the SSL [VPN Wizard](#) to configure SSL VPN connections, choose **Wizards > SSL VPN Wizard** and complete each screen that appears.
 - Step 4** To configure high availability and scalability settings, choose **Wizards > High Availability and Scalability Wizard**. See the “[Configuring Failover with the High Availability and Scalability Wizard](#)” section on page 59-2 for more information.
 - Step 5** To use the Packet Capture Wizard to configure packet capture, choose **Wizards > Packet Capture Wizard**.
 - Step 6** To display different colors and styles available in the ASDM GUI, choose **View > Office Look and Feel**.
 - Step 7** To configure features, click the **Configuration** button on the toolbar and then click one of the feature buttons to display the associated configuration pane.



Note If the Configuration screen is blank, click **Refresh** on the toolbar to display the screen content.

- Step 8** To monitor the adaptive adaptive security appliance, click the **Monitoring** button on the toolbar and then click a feature button to display the associated monitoring pane.



Note ASDM supports up to a maximum of a 512 KB configuration. If you exceed this amount, you may experience performance issues.

Using the Command Line Interface

This section tells how to enter commands using ASDM, and how to work with the command line interface. This section includes the following topics:

- [Using the Command Line Interface Tool, page 2-9](#)
- [Handling Command Errors, page 2-9](#)
- [Using Interactive Commands, page 2-9](#)
- [Avoiding Conflicts with Other Administrators, page 2-10](#)

- [Showing Commands Ignored by ASDM on the Device, page 2-10](#)

Using the Command Line Interface Tool

This feature provides a text-based tool for sending commands to the adaptive security appliance and viewing the results.

The commands you can enter with the CLI tool depend on your user privileges. See the [“About Authorization” section on page 32-2](#) for more information. Review your privilege level in the status bar at the bottom of the main ASDM application window to ensure that you have the required privileges to execute privileged-level CLI commands.

**Note**

Commands entered via the ASDM CLI tool might function differently from those entered through a terminal connection to the adaptive security appliance.

To use the CLI tool, perform the following steps:

-
- Step 1** In the main ASDM application window, choose **Tools > Command Line Interface**.
The Command Line Interface dialog box appears.
 - Step 2** Choose the type of command (single line or multiple line) that you want, and then choose the command from the drop-down list, or type it in the field provided.
 - Step 3** Click **Send** to execute the command.
 - Step 4** To enter a new command, click **Clear Response**, and then choose (or type) another command to execute.
 - Step 5** Check the **Enable context-sensitive help (?)** check box to provide context-sensitive help for this feature. Uncheck this check box to disable the context-sensitive help.
 - Step 6** After you have closed the Command Line Interface dialog box, if you changed the configuration, click **Refresh** to view the changes in ASDM.
-

Handling Command Errors

If an error occurs because you entered an incorrect command, the incorrect command is skipped and the remaining commands are processed. A message appears in the Response area to inform you whether or not any error occurred, as well as other related information.

**Note**

ASDM supports almost all CLI commands. See the *Cisco ASA 5500 Series Command Reference* for a list of commands.

Using Interactive Commands

Interactive commands are not supported in the CLI tool. To use these commands in ASDM, use the **noconfirm** keyword if available, as shown in the following command:

```
crypto key generate rsa modulus 1024 noconfirm
```

Avoiding Conflicts with Other Administrators

Multiple administrative users can update the running configuration of the adaptive security appliance. Before using the ASDM CLI tool to make configuration changes, check for other active administrative sessions. If more than one user is configuring the adaptive security appliance at the same time, the most recent changes take effect.

To view other administrative sessions that are currently active on the same adaptive security appliance, choose **Monitoring > Properties > Device Access**.

Showing Commands Ignored by ASDM on the Device

This feature lets you show the list of commands that ASDM does not support. Typically, ASDM ignores them. ASDM does not change or remove these commands from your running configuration. See the [“Unsupported Commands” section on page 1-13](#) for more information.

To display the list of unsupported commands for ASDM, perform the following steps:

-
- Step 1** In the main ASDM application window, choose **Tools > Show Commands Ignored by ASDM on Device**.
- Step 2** Click **OK** when you are done.
-