Getting Started

This chapter describes how to get started with your ASA. This chapter includes the following sections:

Accessing the Appliance Command-Line Interface

For initial configuration, access the CLI directly from the console port. Later, you can configure remote access using Telnet or SSH according to Chapter 1, "Configuring Management Access." If your system is already in multiple context mode, then accessing the console port places you in the system execution space. See Chapter 1, "Configuring Multiple Context Mode," for more information about multiple context mode.

Detailed Steps

Step 1 Connect a PC to the console port using the provided console cable, and connect to the console using a terminal emulator set for 9600 baud, 8 data bits, no parity, 1 stop bit, no flow control.

See the hardware guide for your ASA for more information about the console cable.

Step 2 Press the **Enter** key to see the following prompt:

hostname>

This prompt indicates that you are in user EXEC mode. Only basic commands are available from user EXEC mode.

Step 3 To access privileged EXEC mode, enter the following command:

```
hostname> enable
```

The following prompt appears:

```
Password:
```

All non-configuration commands are available in privileged EXEC mode. You can also enter configuration mode from privileged EXEC mode.

Step 4 Enter the enable password at the prompt.

By default, the password is blank, and you can press the **Enter** key to continue. See the "Configuring the Hostname, Domain Name, and Passwords" section on page 1-1 to change the enable password.

The prompt changes to:

```
hostname#
```

To exit privileged mode, enter the **disable**, **exit**, or **quit** command.

Step 5 To access global configuration mode, enter the following command:

```
hostname# configure terminal
```

The prompt changes to the following:

```
hostname(config)#
```

You can begin to configure the ASA from global configuration mode. To exit global configuration mode, enter the **exit**, **quit**, or **end** command.

Accessing the ASA Services Module Command-Line Interface

For initial configuration, access the command-line interface by connecting to the switch (either to the console port or remotely using Telnet or SSH) and then connecting to the ASASM. This section describes how to access the ASASM CLI, and includes the following sections:

- Logging Into the ASA Services Module, page 1-2
- Logging Out of a Console Session, page 1-5
- Logging Out of a Telnet Session, page 1-6

Logging Into the ASA Services Module

For initial configuration, access the command-line interface by connecting to the switch (either to the switch console port or remotely using Telnet or SSH) and then connecting to the ASASM.

If your system is already in multiple context mode, then accessing the ASASM from the switch places you in the system execution space. See Chapter 1, "Configuring Multiple Context Mode," for more information about multiple context mode.

Later, you can configure remote access directly to the ASASM using Telnet or SSH according to the "Configuring ASA Access for ASDM, Telnet, or SSH" section on page 1-1.

This section includes the following topics:

- Information About Connection Methods, page 1-3

- Logging In, page 1-4

Information About Connection Methods

From the switch CLI, you can use two methods to connect to the ASASM:

- Virtual console connection—Using the **service-module session** command, you create a virtual console connection to the ASASM, with all the benefits and limitations of an actual console connection.

  Benefits include:

  – The connection is persistent across reloads and does not time out.

  – You can stay connected through ASASM reloads and view startup messages.

  – You can access ROMMON if the ASASM cannot load the image.

  – No initial password configuration is required.

  Limitations include:

  – The connection is slow (9600 baud).

  – You can only have one console connection active at a time.

  – You cannot use this command in conjunction with a terminal server where **Ctrl-Shift-6**, **x** is the escape sequence to return to the terminal server prompt. **Ctrl-Shift-6**, **x** is also the sequence to escape the ASASM console and return to the switch prompt. Therefore, if you try to exit the ASASM console in this situation, you instead exit all the way to the terminal server prompt. If you reconnect the terminal server to the switch, the ASASM console session is still active; you can never exit to the switch prompt. You must use a direct serial connection to return the console to the switch prompt. In this case, either change the terminal server or switch escape character in Cisco IOS, or use the Telnet **session** command instead.

  Note Because of the persistence of the console connection, if you do not properly log out of the ASASM, the connection may exist longer than intended. If someone else wants to log in, they will need to kill the existing connection. See the "Logging Out of a Console Session" section on page 1-5 for more information.

- Telnet connection—Using the **session** command, you create a Telnet connection to the ASASM.

  Note You cannot connect using this method for a new ASASM; this method requires you to configure a Telnet login password on the ASASM (there is no default password). After you set a password using the **passwd** command, you can use this method.

  Benefits include:

  – You can have multiple sessions to the ASASM at the same time.

  – The Telnet session is a fast connection.

  Limitations include:

  – The Telnet session is terminated when the ASASM reloads, and can time out.

  – You cannot access the ASASM until it completely loads; you cannot access ROMMON.

  – You must first set a Telnet login password; there is no default password.

Logging In

Perform the following steps to log into the ASASM and access global configuration mode.

Detailed Steps

	Command	Purpose
Step 1	From the switch, perform one of the following:	

	(Available for initial access.)
	service-module session [**switch** {**1** | **2**}] **slot** *number*
	Example:
	`Router# service-module session slot 3`
	`hostname>`
		From the switch CLI, enter this command to gain console access to the ASASM.
		For a switch in a VSS, enter the **switch** argument.
		To view the module slot numbers, enter the **show module** command at the switch prompt.
		You access user EXEC mode.

	(Available after you configure a login password.)
	session [**switch** {**1** |**2**}] **slot** *number* **processor 1**
	You are prompted for the login password:
	`hostname passwd:`
	Example:
	`Router# session slot 3 processor 1`
	`hostname passwd: cisco`
	`hostname>`
		From the switch CLI, enter this command to Telnet to the ASASM over the backplane.
		For a switch in a VSS, enter the **switch** argument.
		Note The **session** *slot* **processor 0** command, which is supported on other services modules, is not supported on the ASASM; the ASASM does not have a processor 0.
		To view the module slot numbers, enter the **show module** command at the switch prompt.
		Enter the login password to the ASASM. Set the password using the **passwd** command. 9.0(1): The default password is "cisco." 9.0(2) and later: There is no default password.
		You access user EXEC mode.

Step 2	**enable**
	Example:
	`hostname> enable`
	`Password:`
	`hostname#`
		Accesses privileged EXEC mode, which is the highest privilege level.
		Enter the enable password at the prompt. By default, the password is blank. To change the enable password, see the "Configuring the Hostname, Domain Name, and Passwords" section on page 1-1.
		To exit privileged EXEC mode, enter the **disable**, **exit**, or **quit** command.

Step 3	**configure terminal**
	Example:
	`hostname# configure terminal`
	`hostname(config)#`
		Accesses global configuration mode.
		To exit global configuration mode, enter the **disable**, **exit**, or **quit** command.

Logging Out of a Console Session

This section includes the following topics:

- Logging Out, page 1-5
- Killing an Active Console Connection, page 1-5

Logging Out

If you do not log out of the ASASM, the console connection persists; there is no timeout. To end the ASASM console session and access the switch CLI, perform the following steps.

To kill another user's active connection, which may have been unintentionally left open, see the "Killing an Active Console Connection" section on page 1-5.

Detailed Steps

Step 1 To return to the switch CLI, type the following:

Ctrl-Shift-6, **x**

You return to the switch prompt:

```
asasm# [Ctrl-Shift-6, x]
Router#
```

Note Shift-6 on US and UK keyboards issues the caret (^) character. If you have a different keyboard and cannot issue the caret (^) character as a standalone character, you can temporarily or permanently change the escape character to a different character. In Cisco IOS, before you session to the ASASM, use the **terminal escape-character** *ascii_number* command (to change temporarily) or the **default escape-character** *ascii_number* command (to change permanently). For example, to temporarily change the sequence to **Ctrl-w**, **x**, enter **terminal escape-character 23**. The next time you log into the switch, the escape character reverts back to the default.

Killing an Active Console Connection

Because of the persistence of a console connection, if you do not properly log out of the ASASM, the connection may exist longer than intended. If someone else wants to log in, they will need to kill the existing connection.

Detailed Steps

Step 1 From the switch CLI, show the connected users using the **show users** command. A console user is called "con". The Host address shown is 127.0.0.*slot*0, where *slot* is the slot number of the module.

```
Router# show users
```

For example, the following command output shows a user "con" on line 0 on a module in slot 2:

```
Router# show users
```

```
Line       User       Host(s)              Idle       Location
*  0       con 0     127.0.0.20            00:00:02
```

Step 2 To clear the line with the console connection, enter the following command:

```
Router# clear line number
```

For example:

```
Router# clear line 0
```

Logging Out of a Telnet Session

To end the Telnet session and access the switch CLI, perform the following steps.

Detailed Steps

Step 1 To return to the switch CLI, type **exit** from the ASASM privileged or user EXEC mode. If you are in a configuration mode, enter **exit** repeatedly until you exit the Telnet session.

You return to the switch prompt:

```
asasm# exit
Router#
```

Note You can alternatively escape the Telnet session using the escape sequence **Ctrl-Shift-6**, **x**; this escape sequence lets you resume the Telnet session by pressing the **Enter** key at the switch prompt. To disconnect your Telnet session from the switch, enter **disconnect** at the switch CLI. If you do not disconnect the session, it will eventually time out according to the ASASM configuration.

Configuring ASDM Access for Appliances

ASDM access requires some minimal configuration so you can communicate over the network with a management interface. This section includes the following topics:

- Accessing ASDM Using the Factory Default Configuration, page 1-6
- Accessing ASDM Using a Non-Default Configuration (ASA 5505), page 1-7
- Accessing ASDM Using a Non-Default Configuration (ASA 5510 and Higher), page 1-9

Accessing ASDM Using the Factory Default Configuration

With a factory default configuration (see the "Factory Default Configurations" section on page 1-18), ASDM connectivity is pre-configured with default network settings. Connect to ASDM using the following interface and network settings:

- The management interface depends on your model:
  - 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.
- The default management address is 192.168.1.1.
- The clients allowed to access ASDM must be on the 192.168.1.0/24 network. The default configuration enables DHCP so your management station can be assigned an IP address in this range. To allow other client IP addresses to access ASDM, see the "Configuring ASA Access for ASDM, Telnet, or SSH" section on page 1-1.

To launch ASDM, see the "Starting ASDM" section on page 1-14.

Note To change to multiple context mode, see the "Enabling or Disabling Multiple Context Mode" section on page 1-15. After changing to multiple context mode, you can access ASDM from the admin context using the network settings above.

Accessing ASDM Using a Non-Default Configuration (ASA 5505)

If you do not have a factory default configuration, want to change the configuration, or want to change to transparent firewall mode, perform the following steps. See also the sample configurations in the "ASA 5505 Default Configuration" section on page 1-19.

Prerequisites

Access the CLI according to the "Accessing the Appliance Command-Line Interface" section on page 1-1.

Detailed Steps

	Command	Purpose
Step 1	(Optional) **firewall transparent** **Example:** `hostname(config)# firewall transparent`	Enables transparent firewall mode. This command clears your configuration.
Step 2	Do one of the following to configure a management interface, depending on your mode:	

	Command	Purpose

	Routed mode:
	`interface vlan number`
	`   ip address ip_address [mask]`
	`   nameif name`
	`   security-level level`
	Example:
	`hostname(config)# interface vlan 1`
	`hostname(config-if)# ip address 192.168.1.1 255.255.255.0`
	`hostname(config-if)# nameif inside`
	`hostname(config-if)# security-level 100`
		Configures an interface in routed mode. The **security-level** is a number between 1 and 100, where 100 is the most secure.

	Transparent mode:
	`interface bvi number`
	`   ip address ip_address [mask]`
	
	`interface vlan number`
	`   bridge-group bvi_number`
	`   nameif name`
	`   security-level level`
	Example:
	`hostname(config)# interface bvi 1`
	`hostname(config-if)# ip address 192.168.1.1 255.255.255.0`
	
	`hostname(config)# interface vlan 1`
	`hostname(config-if)# bridge-group 1`
	`hostname(config-if)# nameif inside`
	`hostname(config-if)# security-level 100`
		Configures a bridge virtual interface and assigns a management VLAN to the bridge group. The **security-level** is a number between 1 and 100, where 100 is the most secure.

Step 3	`interface ethernet 0/n`
	`   switchport access vlan number`
	`   no shutdown`
	Example:
	`hostname(config)# interface ethernet 0/1`
	`hostname(config-if)# switchport access vlan 1`
	`hostname(config-if)# no shutdown`
		Enables the management switchport and assigns it to the management VLAN.

Step 4	`dhcpd address ip_address-ip_address interface_name`
	`dhcpd enable interface_name`
	Example:
	`hostname(config)# dhcpd address 192.168.1.5-192.168.1.254 inside`
	`hostname(config)# dhcpd enable inside`
		Enables DHCP for the management host on the management interface network. Make sure you do not include the management address in the range.
		Note By default, the IPS module, if installed, uses 192.168.1.2 for its internal management address, so be sure not to use this address in the DHCP range. You can later change the IPS module management address using the ASA if required.

Step 5	`http server enable`
	Example:
	`hostname(config)# http server enable`
		Enables the HTTP server for ASDM.

	Command	Purpose
Step 6	**http** *ip_address mask interface_name* **Example:** `hostname(config)# http 192.168.1.0 255.255.255.0 inside`	Allows the management host to access ASDM.
Step 7	**write memory** **Example:** `hostname(config)# write memory`	Saves the configuration.
Step 8	To launch ASDM, see the "Starting ASDM" section on page 1-14.	

Examples

The following configuration converts the firewall mode to transparent mode, configures the VLAN 1 interface and assigns it to BVI 1, enables a switchport, and enables ASDM for a management host:

```
firewall transparent
interface bvi 1
    ip address 192.168.1.1 255.255.255.0
interface vlan 1
    bridge-group 1
    nameif inside
    security-level 100
interface ethernet 0/1
    switchport access vlan 1
    no shutdown
dhcpd address 192.168.1.5-192.168.1.254 inside
dhcpd enable inside
http server enable
http 192.168.1.0 255.255.255.0 inside
```

Accessing ASDM Using a Non-Default Configuration (ASA 5510 and Higher)

If you do not have a factory default configuration, or want to change the firewall or context mode, perform the following steps.

Prerequisites

Access the CLI according to the "Accessing the Appliance Command-Line Interface" section on page 1-1.

Detailed Steps

	Command	Purpose
Step 1	(Optional) **firewall transparent** **Example:** `hostname(config)# firewall transparent`	Enables transparent firewall mode. This command clears your configuration.

Step 2	**interface management 0/0**
	   ip address *ip_address mask*
	   nameif *name*
	   security-level *number*
	   no shutdown
	Example:
	`hostname(config)# interface management 0/0`
	`hostname(config-if)# ip address 192.168.1.1 255.255.255.0`
	`hostname(config-if)# nameif management`
	`hostname(config-if)# security-level 100`
	`hostname(config-if)# no shutdown`
		Configures the Management 0/0 interface. The **security-level** is a number between 1 and 100, where 100 is the most secure.

Step 3	(For directly-connected management hosts)
	dhcpd address *ip_address*-*ip_address interface_name*
	dhcpd enable *interface_name*
	Example:
	`hostname(config)# dhcpd address 192.168.1.2-192.168.1.254 management`
	`hostname(config)# dhcpd enable management`
		Enables DHCP for the management host on the management interface network. Make sure you do not include the Management 0/0 address in the range.

Step 4	(For remote management hosts) **route** *management_ifc management_host_ip mask gateway_ip* **1** **Example:** `hostname(config)# route management 10.1.1.0 255.255.255.0 192.168.1.50`	Configures a route to the management hosts.
Step 5	**http server enable** **Example:** `hostname(config)# http server enable`	Enables the HTTP server for ASDM.
Step 6	**http** *ip_address mask interface_name* **Example:** `hostname(config)# http 192.168.1.0 255.255.255.0 management`	Allows the management host to access ASDM.

	Command	Purpose
Step 7	**write memory** **Example:** `hostname(config)# write memory`	Saves the configuration.
Step 8	(Optional) **mode multiple** **Example:** `hostname(config)# mode multiple`	Sets the mode to multiple mode. When prompted, confirm that you want to convert the existing configuration to be the admin context. You are then prompted to reload the ASASM. See Chapter 1, "Configuring Multiple Context Mode," for more information.
Step 9	To launch ASDM, see the "Starting ASDM" section on page 1-14.	

Examples

The following configuration converts the firewall mode to transparent mode, configures the Management 0/0 interface, and enables ASDM for a management host:

```
firewall transparent
interface management 0/0
    ip address 192.168.1.1 255.255.255.0
    nameif management
    security-level 100
    no shutdown
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
http server enable
http 192.168.1.0 255.255.255.0 management
```

Configuring ASDM Access for the ASA Services Module

Because the ASASM does not have physical interfaces, it does not come pre-configured for ASDM access; you must configure ASDM access using the CLI on the ASASM. To configure the ASASM for ASDM access, perform the following steps.

Prerequisites

- Assign a VLAN interface to the ASASM according to the "Assigning VLANs to the ASA Services Module" section on page 1-4.
- Connect to the ASASM and access global configuration mode according to the "Accessing the ASA Services Module Command-Line Interface" section on page 1-2.

Detailed Steps

	Command	Purpose
Step 1	(Optional) **firewall transparent** **Example:** hostname(config)# firewall transparent	Enables transparent firewall mode. This command clears your configuration.
Step 2	Do one of the following to configure a management interface, depending on your mode:	
	Routed mode: **interface vlan** *number* **ip address** *ip_address* [*mask*] **nameif** *name* **security-level** *level* **Example:** hostname(config)# interface vlan 1 hostname(config-if)# ip address 192.168.1.1 255.255.255.0 hostname(config-if)# nameif inside hostname(config-if)# security-level 100	Configures an interface in routed mode. The **security-level** is a number between 1 and 100, where 100 is the most secure.
	Transparent mode: **interface bvi** *number* **ip address** *ip_address* [*mask*] **interface vlan** *number* **bridge-group** *bvi_number* **nameif** *name* **security-level** *level* **Example:** hostname(config)# interface bvi 1 hostname(config-if)# ip address 192.168.1.1 255.255.255.0 hostname(config)# interface vlan 1 hostname(config-if)# bridge-group 1 hostname(config-if)# nameif inside hostname(config-if)# security-level 100	Configures a bridge virtual interface and assigns a management VLAN to the bridge group. The **security-level** is a number between 1 and 100, where 100 is the most secure.
Step 3	(For directly-connected management hosts) **dhcpd address** *ip_address-ip_address interface_name* **dhcpd enable** *interface_name* **Example:** hostname(config)# dhcpd address 192.168.1.2-192.168.1.254 inside hostname(config)# dhcpd enable inside	Enables DHCP for the management host on the management interface network. Make sure you do not include the management address in the range.

	Command	Purpose
Step 4	(For remote management hosts) **route** *management_ifc management_host_ip mask gateway_ip* **1** **Example:** `hostname(config)# route management 10.1.1.0 255.255.255.0 192.168.1.50`	Configures a route to the management hosts.
Step 5	**http server enable** **Example:** `hostname(config)# http server enable`	Enables the HTTP server for ASDM.
Step 6	**http** *ip_address mask interface_name* **Example:** `hostname(config)# http 192.168.1.0 255.255.255.0 management`	Allows the management host to access ASDM.
Step 7	**write memory** **Example:** `hostname(config)# write memory`	Saves the configuration.
Step 8	(Optional) **mode multiple** **Example:** `hostname(config)# mode multiple`	Sets the mode to multiple mode. When prompted, confirm that you want to convert the existing configuration to be the admin context. You are then prompted to reload the ASASM. See Chapter 1, "Configuring Multiple Context Mode," for more information.
Step 9	To launch ASDM, see the "Starting ASDM" section on page 1-14.	

Examples

The following routed mode configuration configures the VLAN 1 interface and enables ASDM for a management host:

```
interface vlan 1
    nameif inside
    ip address 192.168.1.1 255.255.255.0
    security-level 100
dhcpd address 192.168.1.3-192.168.1.254 inside
dhcpd enable inside
http server enable
http 192.168.1.0 255.255.255.0 inside
```

The following configuration converts the firewall mode to transparent mode, configures the VLAN 1 interface and assigns it to BVI 1, and enables ASDM for a management host:

```
firewall transparent
interface bvi 1
    ip address 192.168.1.1 255.255.255.0
interface vlan 1
    bridge-group 1
    nameif inside
    security-level 100
dhcpd address 192.168.1.3-192.168.1.254 inside
dhcpd enable inside
http server enable
http 192.168.1.0 255.255.255.0 inside
```

Starting ASDM

You can start ASDM using two methods:

- ASDM-IDM Launcher—The Launcher is an application downloaded from the ASA using a web browser that you can use to connect to any ASA IP address. You do not need to re-download the launcher if you want to connect to other ASAs. The Launcher also lets you run a virtual ASDM in Demo mode using files downloaded locally.
- Java Web Start—For each ASA that you manage, you need to connect with a web browser and then save or launch the Java Web Start application. You can optionally save the application to your PC; however you need separate applications for each ASA IP address.

Note Within ASDM, you can choose a different ASA IP address to manage; the difference between the Launcher and Java Web Start application functionality rests primarily in how you initially connect to the ASA and launch ASDM.

This section describes how to connect to ASDM initially, and then launch ASDM using the Launcher or the Java Web Start application. This section includes the following topics:

- Connecting to ASDM for the First Time, page 1-14
- Starting ASDM from the ASDM-IDM Launcher, page 1-15
- Starting ASDM from the Java Web Start Application, page 1-16
- Using ASDM in Demo Mode, page 1-16

Note ASDM allows multiple PCs or workstations to each have one browser session open with the same ASA software. A single ASA 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 ASA. In multiple context mode, five concurrent ASDM sessions are supported per context, up to a maximum of 32 total connections for each ASA.

Connecting to ASDM for the First Time

To connect to ASDM for the first time to download the ASDM-IDM Launcher or Java Web Start application, perform the following steps:

Step 1 From a supported web browser on the ASA network, enter the following URL:

https://*interface_ip_address***/admin**

Where *interface_ip_address* is the management IP address of the ASA. See the "Configuring ASDM Access for Appliances" section on page 1-6 or the "Configuring ASDM Access for the ASA Services Module" section on page 1-11 for more information about management access.

See the ASDM release notes for your release for the requirements to run ASDM.

The ASDM launch page appears with the following buttons:

- **Install ASDM Launcher and Run ASDM**
- **Run ASDM**
- **Run Startup Wizard**

Step 2 To download the Launcher:

a. Click **Install ASDM Launcher and Run ASDM**.

b. Enter the username and password, and click **OK**. For a factory default configuration, leave these fields empty. With no HTTPS authentication configured, you can gain access to ASDM with no username and the **enable** password, which is blank by default. With HTTPS authentication enabled, enter your username and associated password.

c. Save the installer to your PC, and then start the installer. The ASDM-IDM Launcher opens automatically after installation is complete.

d. See the "Starting ASDM from the ASDM-IDM Launcher" section on page 1-15 to use the Launcher to connect to ASDM.

Step 3 To use the Java Web Start application:

a. Click **Run ASDM** or **Run Startup Wizard**.

b. Save the application to your PC when prompted. You can optionally open it instead of saving it.

c. See the "Starting ASDM from the Java Web Start Application" section on page 1-16 to use the Java Web Start application to connect to ASDM.

Starting ASDM from the ASDM-IDM Launcher

To start ASDM from the ASDM-IDM Launcher, perform the following steps.

Prerequisites

Download the ASDM-IDM Launcher according to the "Connecting to ASDM for the First Time" section on page 1-14.

Detailed Steps

Step 1 Start the ASDM-IDM Launcher application.

Step 2 Enter or choose the ASA 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**.

For a factory default configuration, leave these fields empty. With no HTTPS authentication configured, you can gain access to ASDM with no username and the **enable** password, which is blank by default. With HTTPS authentication enabled, enter your username and associated password.

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

The main ASDM window appears.

Starting ASDM from the Java Web Start Application

To start ASDM from the Java Web Start application, perform the following steps.

Prerequisites

Download the Java Web Start application according to the "Connecting to ASDM for the First Time" section on page 1-14.

Detailed Steps

Step 1 Start the Java Web Start application.

Step 2 Accept any certificates according to the dialog boxes that appear. The Cisco ASDM-IDM Launcher appears.

Step 3 Enter the username and password, and click **OK**. For a factory default configuration, leave these fields empty. With no HTTPS authentication configured, you can gain access to ASDM with no username and the **enable** password, which is blank by default. With HTTPS authentication enabled, enter your username and associated password.

The main ASDM window appears.

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 ASA 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 ASA in single, routed mode and intrusion prevention
- For object NAT, an ASA in single, routed mode and a firewall DMZ.
- For the Botnet Traffic Filter, an ASA 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/web/download/index.html.

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.

Factory Default Configurations

The factory default configuration is the configuration applied by Cisco to new ASAs.

- ASA 5505—The factory default configuration configures interfaces and NAT so that the ASA is ready to use in your network immediately.
- ASA 5510 and higher—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.

The factory default configuration is available only for routed firewall mode and single context mode. See Chapter 1, "Configuring Multiple Context Mode," for more information about multiple context mode. See Chapter 1, "Configuring the Transparent or Routed Firewall," for more information about routed and transparent firewall mode. For the ASA 5505, a sample transparent mode configuration is provided in this section.

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 1-18
- ASA 5505 Default Configuration, page 1-19
- ASA 5510 and Higher Default Configuration, page 1-23

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 ASA with a cleared configuration does not have any defined contexts to configure automatically using this feature.

Detailed Steps

	Command	Purpose
Step 1	**configure factory-default** [*ip_address* [*mask*]] **Example:** `hostname(config)# `**`configure factory-default 10.1.1.1 255.255.255.0`**	Restores the factory default configuration. If you specify the *ip_address*, then you set the inside or management interface IP address, depending on your model, instead of using the default IP address of 192.168.1.1. The **http** command uses the subnet you specify. Similarly, the **dhcpd address** command range consists of addresses within the subnet that you specify. **Note** This command also clears the **boot system** command, if present, along with the rest of the configuration. The **boot system** command lets you boot from a specific image, including an image on the external flash memory card. The next time you reload the ASA after restoring the factory configuration, it boots from the first image in internal flash memory; if you do not have an image in internal flash memory, the ASA does not boot.
Step 2	**write memory** **Example:** `active(config)# write memory`	Saves the default configuration to flash memory. This command saves the running configuration to the default location for the startup configuration, even if you previously configured the **boot config** command to set a different location; when the configuration was cleared, this path was also cleared.

What to Do Next

See the "Working with the Configuration" section on page 1-23 to start configuring the ASA.

ASA 5505 Default Configuration

The default configuration is available for routed mode only. This section describes the default configuration and also provides a sample transparent mode configuration that you can copy and paste as a starting point. This section includes the following topics:

- ASA 5505 Routed Mode Default Configuration, page 1-19
- ASA 5505 Transparent Mode Sample Configuration, page 1-21

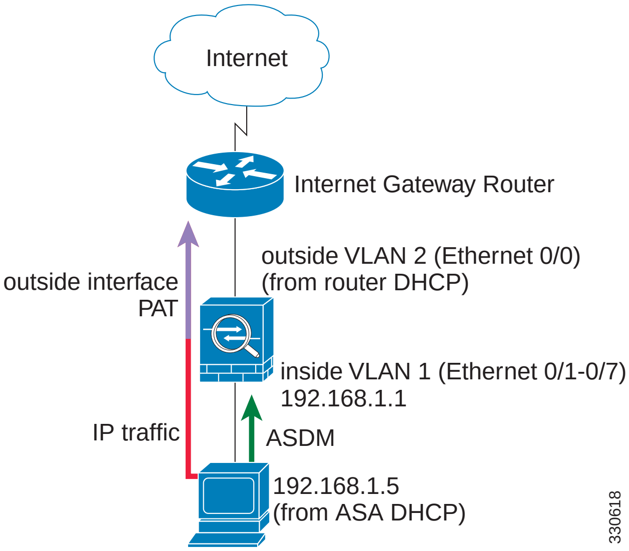
ASA 5505 Routed Mode Default Configuration

The default factory configuration for the ASA 5505 configures the following:

- Interfaces—Inside (VLAN 1) and outside (VLAN 2).
- Switchports enabled and assigned—Ethernet 0/1 through 0/7 switch ports assigned to inside. Ethernet 0/0 assigned to outside.
- IP addresses— Outside address from DHCP; inside address set manually to 192.168.1.1/24.
- Network address translation (NAT)—All inside IP addresses are translated when accessing the outside using interface PAT.

- Traffic flow—IPv4 and IPv6 traffic allowed from inside to outside (this behavior is implicit on the ASA). Outside users are prevented from accessing the inside.
- DHCP server—Enabled for inside hosts, so a PC connecting to the inside interface receives an address between 192.168.1.5 and 192.168.1.254. DNS, WINS, and domain information obtained from the DHCP client on the outside interface is passed to the DHCP clients on the inside interface.
- Default route—Derived from DHCP.
- ASDM access—Inside hosts allowed.

Figure 1-1 ASA 5505 Routed Mode



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 192.168.1.5-192.168.1.254 inside
dhcpd auto_config outside
dhcpd enable inside
logging asdm informational
```

Note For testing purposes, you can allow ping from inside to outside by enabling ICMP inspection. Add the following commands to the default configuration:

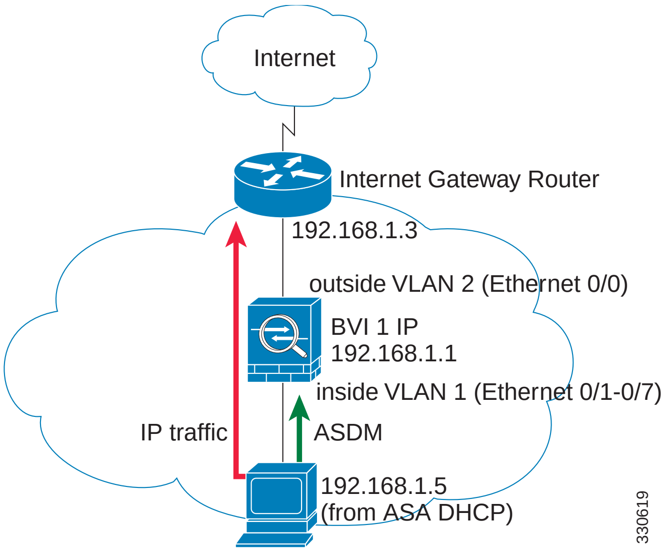
```
policy-map global_policy
   class inspection_default
      inspect icmp
```

ASA 5505 Transparent Mode Sample Configuration

When you change the mode to transparent mode, the configuration is erased. You can copy and paste the following sample configuration at the CLI to get started. This configuration uses the default configuration as a starting point. Note the following areas you may need to modify:

- IP addresses—The IP addresses configured should be changed to match the network to which you are connecting.
- Static routes—For some kinds of traffic, static routes are required. See the "MAC Address vs. Route Lookups" section on page 1-6.

Figure 1-2 ASA 5505 Transparent Mode



```
firewall transparent
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 bvi 1
   ip address 192.168.1.1 255.255.255.0
interface vlan2
   nameif outside
   security-level 0
   bridge-group 1
   no shutdown
interface vlan1
   nameif inside
   security-level 100
   bridge-group 1
   no shutdown
http server enable
http 192.168.1.0 255.255.255.0 inside
dhcpd address 192.168.1.5-192.168.1.254 inside
dhcpd enable inside
```

Note For testing purposes, you can allow ping from inside to outside by enabling ICMP inspection. Add the following commands to the sample configuration:

```
policy-map global_policy
   class inspection_default
      inspect icmp
```

ASA 5510 and Higher Default Configuration

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

- Management interface—Management 0/0 (management).
- IP address—The management address is 192.168.1.1/24.
- DHCP server—Enabled for management hosts, so a PC connecting to the management interface receives an address between 192.168.1.2 and 192.168.1.254.
- ASDM access—Management hosts allowed.

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
```

Working with the Configuration

This section describes how to work with the configuration. The ASA loads the configuration from a text file, called the startup configuration. This file resides by default as a hidden file in internal flash memory. You can, however, specify a different path for the startup configuration. (For more information, see Chapter 1, “Managing Software and Configurations.”)

When you enter a command, the change is made only to the running configuration in memory. You must manually save the running configuration to the startup configuration for your changes to remain after a reboot.

The information in this section applies to both single and multiple security contexts, except where noted. Additional information about contexts is in Chapter 1, “Configuring Multiple Context Mode.”

This section includes the following topics:

- Saving Configuration Changes, page 1-24
- Copying the Startup Configuration to the Running Configuration, page 1-25

- Viewing the Configuration, page 1-26
- Clearing and Removing Configuration Settings, page 1-26
- Creating Text Configuration Files Offline, page 1-27

Saving Configuration Changes

This section describes how to save your configuration and includes the following topics:

- Saving Configuration Changes in Single Context Mode, page 1-24
- Saving Configuration Changes in Multiple Context Mode, page 1-24

Saving Configuration Changes in Single Context Mode

To save the running configuration to the startup configuration, enter the following command:

Command	Purpose
write memory **Example:** `hostname# write memory`	Saves the running configuration to the startup configuration. **Note** The **copy running-config startup-config** command is equivalent to the **write memory** command.

Saving Configuration Changes in Multiple Context Mode

You can save each context (and system) configuration separately, or you can save all context configurations at the same time. This section includes the following topics:

- Saving Each Context and System Separately, page 1-24
- Saving All Context Configurations at the Same Time, page 1-25

Saving Each Context and System Separately

To save the system or context configuration, enter the following command within the system or context:

Command	Purpose
write memory **Example:** `hostname# write memory`	Saves the running configuration to the startup configuration. For multiple context mode, context startup configurations can reside on external servers. In this case, the ASA saves the configuration back to the server you identified in the context URL, except for an HTTP or HTTPS URL, which do not let you save the configuration to the server. **Note** The **copy running-config startup-config** command is equivalent to the **write memory** command.

Saving All Context Configurations at the Same Time

To save all context configurations at the same time, as well as the system configuration, enter the following command in the system execution space:

Command	Purpose
write memory all [**/noconfirm**] **Example:** `hostname# write memory all /noconfirm`	Saves the running configuration to the startup configuration for all contexts and the system configuration. If you do not enter the **/noconfirm** keyword, you see the following prompt: `Are you sure [Y/N]:` After you enter **Y**, the ASA saves the system configuration and each context. Context startup configurations can reside on external servers. In this case, the ASA saves the configuration back to the server you identified in the context URL, except for an HTTP or HTTPS URL, which do not let you save the configuration to the server.

After the ASA saves each context, the following message appears:

```
'Saving context 'b' ... ( 1/3 contexts saved ) '
```

Sometimes, a context is not saved because of an error. See the following information for errors:

- For contexts that are not saved because of low memory, the following message appears:

  ```
  The context 'context a' could not be saved due to Unavailability of resources
  ```

- For contexts that are not saved because the remote destination is unreachable, the following message appears:

  ```
  The context 'context a' could not be saved due to non-reachability of destination
  ```

- For contexts that are not saved because the context is locked, the following message appears:

  ```
  Unable to save the configuration for the following contexts as these contexts are
  locked.
  context 'a' , context 'x' , context 'z' .
  ```

  A context is only locked if another user is already saving the configuration or in the process of deleting the context.

- For contexts that are not saved because the startup configuration is read-only (for example, on an HTTP server), the following message report is printed at the end of all other messages:

  ```
  Unable to save the configuration for the following contexts as these contexts have
  read-only config-urls:
  context 'a' , context 'b' , context 'c' .
  ```

- For contexts that are not saved because of bad sectors in the flash memory, the following message appears:

  ```
  The context 'context a' could not be saved due to Unknown errors
  ```

Copying the Startup Configuration to the Running Configuration

Copy a new startup configuration to the running configuration using one of the following options.

Command	Purpose
copy startup-config running-config	Merges the startup configuration with the running configuration. A merge adds any new commands from the new configuration to the running configuration. If the configurations are the same, no changes occur. If commands conflict or if commands affect the running of the context, then the effect of the merge depends on the command. You might get errors, or you might have unexpected results.
reload	Reloads the ASA, which loads the startup configuration and discards the running configuration.
clear configure all **copy startup-config running-config**	Loads the startup configuration and discards the running configuration without requiring a reload.

Viewing the Configuration

The following commands let you view the running and startup configurations.

Command	Purpose
show running-config	Views the running configuration.
show running-config *command*	Views the running configuration of a specific command.
show startup-config	Views the startup configuration.

Clearing and Removing Configuration Settings

To erase settings, enter one of the following commands.

Command	Purpose
clear configure *configurationcommand* [*level2configurationcommand*]	Clears all the configuration for a specified command. If you only want to clear the configuration for a specific version of the command, you can enter a value for *level2configurationcommand*.

Example:
`hostname(config)# clear configure aaa`
	For example, to clear the configuration for all **aaa** commands, enter the following command:
	`hostname(config)# clear configure aaa`
	To clear the configuration for only **aaa authentication** commands, enter the following command:
	`hostname(config)# clear configure aaa authentication`

no *configurationcommand* [*level2configurationcommand*] *qualifier*	Disables the specific parameters or options of a command. In this case, you use the **no** command to remove the specific configuration identified by *qualifier*.
Example: `hostname(config)# no nat (inside) 1`	For example, to remove a specific **nat** command, enter enough of the command to identify it uniquely as follows: `hostname(config)# no nat (inside) 1`

Command	Purpose
write erase **Example:** `hostname(config)# write erase`	Erases the startup configuration.
clear configure all **Example:** `hostname(config)# clear configure all`	Erases the running configuration. **Note** In multiple context mode, if you enter **clear configure all** from the system configuration, you also remove all contexts and stop them from running. The context configuration files are not erased, and remain in their original location.

Creating Text Configuration Files Offline

This guide describes how to use the CLI to configure the ASA; when you save commands, the changes are written to a text file. Instead of using the CLI, however, you can edit a text file directly on your PC and paste a configuration at the configuration mode command-line prompt in its entirety, or line by line. Alternatively, you can download a text file to the ASA internal flash memory. See Chapter 1, "Managing Software and Configurations," for information on downloading the configuration file to the ASA.

In most cases, commands described in this guide are preceded by a CLI prompt. The prompt in the following example is "hostname(config)#":

```
hostname(config)# context a
```

In the text configuration file you are not prompted to enter commands, so the prompt is omitted as follows:

```
context a
```

For additional information about formatting the file, see Appendix 1, "Using the Command-Line Interface."

Applying Configuration Changes to Connections

When you make security policy changes to the configuration, all *new* connections use the new security policy. Existing connections continue to use the policy that was configured at the time of the connection establishment. **show** command output for old connections reflect the old configuration, and in some cases will not include data about the old connections.

For example, if you remove a QoS **service-policy** from an interface, then re-add a modified version, then the **show service-policy** command only displays QoS counters associated with new connections that match the new service policy; existing connections on the old policy no longer show in the command output.

To ensure that all connections use the new policy, you need to disconnect the current connections so they can reconnect using the new policy.

To disconnect connections, enter one of the following commands.

Detailed Steps

Command	Purpose
clear local-host [*ip_address*] [**all**] **Example:** `hostname(config)# clear local-host all`	This command reinitializes per-client run-time states such as connection limits and embryonic limits. As a result, this command removes any connection that uses those limits. See the **show local-host all** command to view all current connections per host. With no arguments, this command clears all affected through-the-box connections. To also clear to-the-box connections (including your current management session), use the **all** keyword. To clear connections to and from a particular IP address, use the *ip_address* argument.
clear conn [**all**] [**protocol** {**tcp** | **udp**}] [**address** *src_ip*[-*src_ip*] [**netmask** *mask*]] [**port** *src_port*[-*src_port*]] [**address** *dest_ip*[-*dest_ip*] [**netmask** *mask*]] [**port** *dest_port*[-*dest_port*]] **Example:** `hostname(config)# clear conn all`	This command terminates connections in any state. See the **show conn** command to view all current connections. With no arguments, this command clears all through-the-box connections. To also clear to-the-box connections (including your current management session), use the **all** keyword. To clear specific connections based on the source IP address, destination IP address, port, and/or protocol, you can specify the desired options.

Reloading the ASA

To reload the ASA, enter the following command:

Command	Purpose
reload **Example:** `hostname (config)# reload`	Reloads the ASA. **Note** In multiple context mode, you can only reload from the system execution space.