

Getting Started

This chapter describes how to get started with your Cisco ASA.

- Access the Console for the Command-Line Interface, on page 1
- Configure ASDM Access, on page 11
- Start ASDM, on page 17
- Factory Default Configurations, on page 18
- Work with the Configuration, on page 31
- Apply Configuration Changes to Connections, on page 35
- Reload the ASA, on page 36

Access the Console for the 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 #unique_35. If your system is already in multiple context mode, then accessing the console port places you in the system execution space.

Note For ASAv console access, see the ASAv quick start guide.

Access the Appliance Console

Follow these steps to access the appliance console.

Procedure

Step 1 Connect a computer 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:

```
ciscoasa>
```

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

Step 3 Access privileged EXEC mode.

enable

You are prompted to change the password the first time you enter the **enable** command:

Example:

```
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
ciscoasa#
```

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

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

Step 4 Access global configuration mode.

configure terminal

Example:

```
ciscoasa# configure terminal
ciscoasa(config)#
```

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

Access the Firepower 2100 Console

The Firepower 2100 console port connects you to the FXOS CLI. From the FXOS CLI, you can then connect to the ASA console, and back again. If you SSH to FXOS, you can also connect to the ASA CLI; a connection from SSH is not a console connection, so you can have multiple ASA connections from an FXOS SSH connection. Similarly, if you SSH to the ASA, you can connect to the FXOS CLI.

Before you begin

You can only have one console connection at a time. When you connect to the ASA console from the FXOS console, this connection is a persistent console connection, not like a Telnet or SSH connection.

Procedure

Step 1 Connect your management computer to the console port. The Firepower 2100 ships with a DB-9 to RJ-45 serial cable, so you will need a third party serial-to-USB cable to make the connection. Be sure to install any necessary USB serial drivers for your operating system. Use the following serial settings:

- 9600 baud
- 8 data bits
- No parity
- 1 stop bit

You connect to the FXOS CLI. Enter the user credentials; by default, you can log in with the **admin** user and the default password, **Admin123**.

Step 2 Connect to the ASA:

connect asa

Example:

```
firepower-2100# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
ciscoasa>
```

Step 3 Access privileged EXEC mode.

enable

You are prompted to change the password the first time you enter the **enable** command.

Example:

```
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
ciscoasa#
```

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

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

Step 4 Access global configuration mode.

configure terminal

Example:

```
ciscoasa# configure terminal
ciscoasa(config)#
```

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

Step 5 To return to the FXOS console, enter **Ctrl+a**, **d**.

Step 6 If you SSH to the ASA (after you configure SSH access in the ASA), connect to the FXOS CLI.

connect fxos

You are prompted to authenticate for FXOS; use the default username: **admin** and password: **Admin123**. To return to the ASA CLI, enter **exit** or type **Ctrl-Shift-6**, **x**.

Example:

```
ciscoasa# connect fxos
Connecting to fxos.
Connected to fxos. Escape character sequence is 'CTRL-^X'.

FXOS 2.2(2.32) kp2110

kp2110 login: admin
Password: Admin123
Last login: Sat Jan 23 16:20:16 UTC 2017 on pts/1
Successful login attempts for user 'admin' : 4
Cisco Firepower Extensible Operating System (FX-OS) Software

[…]

kp2110#
kp2110# exit
Remote card closed command session. Press any key to continue.
Connection with fxos terminated.
Type help or '?' for a list of available commands.
ciscoasa#
```

Access the ASA Console on the Firepower 4100/9300 Chassis

For initial configuration, access the command-line interface by connecting to the Firepower 4100/9300 chassis supervisor (either to the console port or remotely using Telnet or SSH) and then connecting to the ASA security module.

Procedure

Step 1 Connect to the Firepower 4100/9300 chassis supervisor CLI (console or SSH), and then session to the ASA:

connect module *slot* {**console** | **telnet**}

The benefits of using a Telnet connection is that you can have multiple sessions to the module at the same time, and the connection speed is faster.

The first time you access the module, you access the FXOS module CLI. You must then connect to the ASA application.

connect asa

Example:

```
Firepower# connect module 1 console
Firepower-module1> connect asa

asa>
```

Step 2 Access privileged EXEC mode, which is the highest privilege level.

enable

You are prompted to change the password the first time you enter the **enable** command.

Example:

```
asa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
asa#
```

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

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

Step 3 Enter global configuration mode.

configure terminal

Example:

```
asa# configure terminal
asa(config)#
```

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

Step 4 Exit the application console to the FXOS module CLI by entering **Ctrl-a, d**

You might want to use the FXOS module CLI for troubleshooting purposes.

Step 5 Return to the supervisor level of the FXOS CLI.

Exit the console:

a) Enter **~**

You exit to the Telnet application.

b) To exit the Telnet application, enter:

telnet>**quit**

Exit the Telnet session:

a) Enter **Ctrl-], .**

Access the ASA Services Module Console

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.

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 software, 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.

- 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.

Log 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.

Later, you can configure remote access directly to the ASASM using Telnet or SSH.

Procedure

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

- Available for initial access—From the switch CLI, enter this command to gain console access to the ASASM:

  service-module session [**switch** {**1** | **2**}] **slot** *number*

  Example:

  ```
  Router# service-module session slot 3
  ciscoasa>
  ```

  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—From the switch CLI, enter this command to Telnet to the ASASM over the backplane:

  session [**switch** {**1** | | **2**}] **slot** *number* **processor 1**

  You are prompted for the login password:

  ```
  ciscoasa passwd:
  ```

  Example:

  ```
  Router# session slot 3 processor 1
  ciscoasa passwd: cisco
  ciscoasa>
  ```

  For a switch in a VSS, enter the **switch** argument.

  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. There is no default password.

You access user EXEC mode.

Step 2 Access privileged EXEC mode, which is the highest privilege level.

enable

You are prompted to change the password the first time you enter the **enable** command.

Example:

```
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
ciscoasa#
```

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

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

Step 3 Access global configuration mode:

configure terminal

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

Related Topics

Guidelines for Management Access
Set the Hostname, Domain Name, and the Enable and Telnet Passwords

Log Out of a Console Session

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 Kill an Active Console Connection, on page 9.

Procedure

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. Use the **terminal escape-character** *ascii_number* command (to change for this session) or the **default escape-character** *ascii_number* command (to change permanently). For example, to change the sequence for the current session to **Ctrl-w**, **x**, enter **terminal escape-character 23**.

Kill 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.

Procedure

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.

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:

clear *line number*

For example:

```
Router# clear line 0
```

Log Out of a Telnet Session

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

Procedure

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.

Access the Software Module Console

If you have a software module installed, such as the ASA FirePOWER module on the ASA 5506-X, you can session to the module console.



Note You cannot access the *hardware* module CLI over the ASA backplane using the **session** command.

Procedure

From the ASA CLI, session to the module:

session {**sfr** | **cxsc** | **ips**} **console**

Example:

```
ciscoasa# session sfr console
Opening console session with module sfr.
Connected to module sfr. Escape character sequence is 'CTRL-^X'.

Cisco ASA SFR Boot Image 5.3.1
asasfr login: admin
Password: Admin123
```

Access the ASA 5506W-X Wireless Access Point Console

To access the wireless access point console, perform the following steps.

Procedure

Step 1 From the ASA CLI, session to the access point:

session wlan console

Example:

```
ciscoasa# session wlan console
```

```
opening console session with module wlan
connected to module wlan. Escape character sequence is 'CTRL-^X'

ap>
```

Step 2 See the Cisco IOS Configuration Guide for Autonomous Aironet Access Points for information about the access point CLI.

Configure ASDM Access

This section describes how to access ASDM with a default configuration and how to configure access if you do not have a default configuration.

Use the Factory Default Configuration for ASDM Access (Appliances, ASAv)

With a factory default configuration, ASDM connectivity is pre-configured with default network settings.

Procedure

Connect to ASDM using the following interface and network settings:

- The management interface depends on your model:
  - Firepower 2100—Management 1/1 (192.168.45.1). Management hosts are limited to the 192.168.45.0/24 network.
  - Firepower 4100/9300—The Management type interface and IP address of your choice defined when you deployed. Management hosts are allowed from any network.
  - ASA 5506-X, ASA 5506W-X—Inside GigabitEthernet 1/2 through 1/8, and wifi GigabitEthernet 1/9 (192.168.10.1). Inside hosts are limited to the 192.168.1.0/24 network, and wifi hosts are limited to 192.168.10.0/24.
  - ASA 5508-X, and ASA 5516-X—Inside GigabitEthernet 1/2 (192.168.1.1). Inside hosts are limited to the 192.168.1.0/24 network.
  - ASA 5512-X and higher—Management 0/0 (192.168.1.1). Management hosts are limited to the 192.168.1.0/24 network.
  - ASAv—Management 0/0 (set during deployment). Management hosts are limited to the management network.
  - ISA 3000—Management 1/1 (192.168.1.1). Management hosts are limited to the 192.168.1.0/24 network.

Note If you change to multiple context mode, you can access ASDM from the admin context using the network settings above.

Related Topics

Factory Default Configurations, on page 18
Enable or Disable Multiple Context Mode
Start ASDM, on page 17

Customize ASDM Access

This procedure applies to all models except the ASA Services Module.

Use this procedure if *one or more* of the following conditions applies:

- You do not have a factory default configuration
- You want to change the management IP address
- You want to change to transparent firewall mode
- You want to change to multiple context mode

For routed, single mode, for quick and easy ASDM access, we recommend applying the factory default configuration with the option to set your own management IP address. Use the procedure in this section only if you have special needs such as setting transparent or multiple context mode, or if you have other configuration that you need to preserve.

Note For the ASAv, you can configure transparent mode when you deploy, so this procedure is primarily useful after you deploy if you need to clear your configuration, for example.

Procedure

Step 1 Access the CLI at the console port.

Step 2 (Optional) Enable transparent firewall mode:

This command clears your configuration.

firewall transparent

Step 3 Configure the management interface:

```
interface interface_id
   nameif name
   security-level level
   no shutdown
   ip address ip_address mask
```

Example:

```
ciscoasa(config)# interface management 0/0
ciscoasa(config-if)# nameif management
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# no shutdown
```

```
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
```

The **security-level** is a number between 1 and 100, where 100 is the most secure.

Step 4 (For directly-connected management hosts) Set the DHCP pool for the management network:

```
dhcpd address ip_address-ip_address interface_name
dhcpd enable interface_name
```

Example:

```
ciscoasa(config)# dhcpd address 192.168.1.2-192.168.1.254 management
ciscoasa(config)# dhcpd enable management
```

Make sure you do not include the interface address in the range.

Step 5 (For remote management hosts) Configure a route to the management hosts:

route *management_ifc management_host_ip mask gateway_ip* **1**

Example:

```
ciscoasa(config)# route management 10.1.1.0 255.255.255.0 192.168.1.50 1
```

Step 6 Enable the HTTP server for ASDM:

http server enable

Step 7 Allow the management host(s) to access ASDM:

http *ip_address mask interface_name*

Example:

```
ciscoasa(config)# http 192.168.1.0 255.255.255.0 management
```

Step 8 Save the configuration:

write memory

Step 9 (Optional) Set the mode to multiple mode:

mode multiple

When prompted, confirm that you want to convert the existing configuration to be the admin context. You are then prompted to reload the ASA.

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
```

Related Topics

Restore the Factory Default Configuration, on page 19
Set the Firewall Mode
Access the Appliance Console, on page 1
Start ASDM, on page 17

Configure 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.

Before you begin

Assign a VLAN interface to the ASASM according to ASASM quick start guide.

Procedure

Step 1 Connect to the ASASM and access global configuration mode.

Step 2 (Optional) Enable transparent firewall mode:

firewall transparent

This command clears your configuration.

Step 3 Do one of the following to configure a management interface, depending on your mode:

- Routed mode—Configure an interface in routed mode:

```
interface vlan number
   ip address ip_address [mask]
   nameif name
   security-level level
```

Example:

```
ciscoasa(config)# interface vlan 1
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
ciscoasa(config-if)# nameif inside
```

```
ciscoasa(config-if)# security-level 100
```

The **security-level** is a number between 1 and 100, where 100 is the most secure.

- Transparent mode—Configure a bridge virtual interface and assigns a management VLAN to the bridge group:

```
interface bvi number
   ip address ip_address [mask]

interface vlan number
   bridge-group bvi_number
   nameif name
   security-level level
```

Example:

```
ciscoasa(config)# interface bvi 1
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0

ciscoasa(config)# interface vlan 1
ciscoasa(config-if)# bridge-group 1
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
```

The **security-level** is a number between 1 and 100, where 100 is the most secure.

Step 4 (For directly-connected management hosts) Enable DHCP for the management host on the management interface network:

```
dhcpd address ip_address-ip_address interface_name
dhcpd enable interface_name
```

Example:

```
ciscoasa(config)# dhcpd address 192.168.1.2-192.168.1.254 inside
ciscoasa(config)# dhcpd enable inside
```

Make sure you do not include the management address in the range.

Step 5 (For remote management hosts) Configure a route to the management hosts:

route *management_ifc management_host_ip mask gateway_ip* **1**

Example:

```
ciscoasa(config)# route management 10.1.1.0 255.255.255.0 192.168.1.50
```

Step 6 Enable the HTTP server for ASDM:

http server enable

Step 7 Allow the management host to access ASDM:

http *ip_address mask interface_name*

Example:

```
ciscoasa(config)# http 192.168.1.0 255.255.255.0 management
```

Step 8 Save the configuration:

write memory

Step 9 (Optional) Set the mode to multiple mode:

mode multiple

When prompted, confirm that you want to convert the existing configuration to be the admin context. You are then prompted to reload the ASASM.

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
```

Related Topics

Access the ASA Services Module Console, on page 5
About Connection Methods, on page 6
Log Out of a Console Session, on page 8

Kill an Active Console Connection, on page 9
Log Out of a Telnet Session, on page 9
Set the Firewall Mode

Start 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.
- 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 shortcut to your computer; however you need separate shortcuts for each ASA IP address.

Note If you use web start, clear the Java cache or you might lose changes to some pre-login policies such as Hostscan. This problem does not occur if you use the launcher.

Within ASDM, you can choose a different ASA IP address to manage; the difference between the Launcher and Java Web Start 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.

ASDM stores files in the local \Users\<user_id>\.asdm directory, including cache, log, and preferences, and also in the Temp directory, including AnyConnect profiles.

Procedure

Step 1 On the computer that you specified as the ASDM client, enter the following URL:

https://*asa_ip_address***/admin**

Note Be sure to specify **https://**, and not **http://** or just the IP address (which defaults to HTTP); the ASA does not automatically forward an HTTP request to HTTPS.

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) Leave the username and password fields empty (for a new installation), and click **OK**. With no HTTPS authentication configured, you can gain access to ASDM with no username and the **enable** password,

which is blank by default. When you enter the **enable** command at the CLI for the first time, you are prompted to change the password; this behavior is not enforced when you log into ASDM. We suggest that you change the enable password as soon as possible so that it does not remain blank; see Set the Hostname, Domain Name, and the Enable and Telnet Passwords. **Note**: If you enabled HTTPS authentication, enter your username and associated password. Even without authentication, if you enter a username and password at the login screen (instead of leaving the username blank), ASDM checks the local database for a match.

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

d) Enter the management IP address, the same username and password (blank for a new installation), and then click **OK**.

Step 3 To use Java Web Start:

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

b) Save the shortcut to your computer when prompted. You can optionally open it instead of saving it.

c) Start Java Web Start from the shortcut.

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

e) Leave the username and password fields empty (for a new installation), and click **OK**. With no HTTPS authentication configured, you can gain access to ASDM with no username and the **enable** password, which is blank by default. When you enter the **enable** command at the CLI for the first time, you are prompted to change the password; this behavior is not enforced when you log into ASDM. We suggest that you change the enable password as soon as possible so that it does not remain blank; see Set the Hostname, Domain Name, and the Enable and Telnet Passwords. **Note**: If you enabled HTTPS authentication, enter your username and associated password. Even without authentication, if you enter a username and password at the login screen (instead of leaving the username blank), ASDM checks the local database for a match.

Factory Default Configurations

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

- ASA 5506-X—The factory default configuration enables a functional inside/outside configuration. You can manage the ASA using ASDM from the inside interfaces, which are placed in a bridge group using Integrated Routing and Bridging.
- ASA 5508-X and 5516-X—The factory default configuration enables a functional inside/outside configuration. You can manage the ASA using ASDM from the inside interface.
- ASA 5512-X through ASA 5585-X—The factory default configuration configures an interface for management so that you can connect to it using ASDM, with which you can then complete your configuration.
- Firepower 2100—The factory default configuration enables a functional inside/outside configuration. You can manage the ASA using the Firepower Chassis Manager and ASDM from the management interface.
- Firepower 4100/9300 chassis—When you deploy the standalone or cluster of ASAs, the factory default configuration configures an interface for management so that you can connect to it using ASDM, with which you can then complete your configuration.

- ASAv—Depending on your hypervisor, as part of deployment, the deployment configuration (the initial virtual deployment settings) configures an interface for management so that you can connect to it using ASDM, with which you can then complete your configuration. You can also configure failover IP addresses. You can also apply a "factory default" configuration if desired.
- ASASM—No default configuration. See Access the ASA Services Module Console, on page 5 to start configuration.
- ISA 3000—The factory default configuration is an almost-complete transparent firewall mode configuration with all inside and outside interfaces on the same network; you can connect to the management interface with ASDM to set the IP address of your network. Hardware bypass is enabled for two interface pairs, and all traffic is sent to the ASA FirePOWER module in Inline Tap Monitor-Only Mode. This mode sends a duplicate stream of traffic to the ASA Firepower module for monitoring purposes only.

For appliances, the factory default configuration is available only for routed firewall mode and single context mode, except for the ISA 3000, where the factory default configuration is only available in transparent mode. For the ASAv and the Firepower 4100/9300 chassis, you can choose transparent or routed mode at deployment.

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.

Restore the Factory Default Configuration

This section describes how to restore the factory default configuration. For the ASAv, this procedure erases the deployment configuration and applies the same factory default configuration as for the ASA 5525-X.

Note On the ASASM, restoring the factory default configuration simply erases the configuration; there is no factory default configuration.

On the Firepower 4100/9300, restoring the factory default configuration simply erases the configuration; to restore the default configuration, you must re-deploy the ASA from the supervisor.

Before you begin

This feature is available only in routed firewall mode, except for the ISA 3000, where this command is only supported in transparent mode. 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.

Procedure

Step 1 Restore the factory default configuration:

configure factory-default [*ip_address* [*mask*]]

Example:

```
ciscoasa(config)# configure factory-default 10.1.1.1 255.255.255.0
```

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. See the following model guidelines for which interface is set by the *ip_address* option:

- Firepower 2100—Sets the **management** interface IP address.
- Firepower 4100/9300—No effect.
- ASAv—Sets the **management** interface IP address.
- ASA 5506-X—Sets the **inside** interface IP address.
- ASA 5508-X and 5516-X—Sets the **inside** interface IP address.
- ASA 5512-X, 5515-X, 5525-X, 5545-X, 5555-X—Sets the **management** interface IP address.
- ASA 5585-X—Sets the **management** interface IP address.
- ISA 3000—Sets the **management** interface IP address.
- ASASM—No effect.

The **http** command uses the subnet you specify. Similarly, the **dhcpd address** command range consists of all available addresses higher than the IP address you specify. For example, if you specify 10.5.6.78 with a subnet mask of 255.255.255.0, then the DHCP address range will be 10.5.6.79-10.5.6.254.

For the Firepower 2100: This model does not use the **boot system** command; packages are managed by FXOS.

For all other models: This command 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. 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.

Example:

```
docs-bxb-asa3(config)# configure factory-default 10.86.203.151 255.255.254.0
Based on the management IP address and mask, the DHCP address
pool size is reduced to 103 from the platform limit 256

WARNING: The boot system configuration will be cleared.
The first image found in disk0:/ will be used to boot the
system on the next reload.
Verify there is a valid image on disk0:/ or the system will
not boot.

Begin to apply factory-default configuration:
Clear all configuration
WARNING: The new maximum-session limit will take effect after the running-config is saved
and the system boots next time. Command accepted
WARNING: Local user database is empty and there are still 'aaa' commands for 'LOCAL'.
Executing command: interface management0/0
Executing command: nameif management
INFO: Security level for "management" set to 0 by default.
Executing command: ip address 10.86.203.151 255.255.254.0
Executing command: security-level 100
Executing command: no shutdown
```

```
Executing command: exit
Executing command: http server enable
Executing command: http 10.86.202.0 255.255.254.0 management
Executing command: dhcpd address 10.86.203.152-10.86.203.254 management
Executing command: dhcpd enable management
Executing command: logging asdm informational
Factory-default configuration is completed
ciscoasa(config)#
```

Step 2 Save the default configuration to flash memory:

write 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.

Restore the ASAv Deployment Configuration

This section describes how to restore the ASAv deployment (Day 0) configuration.

Procedure

Step 1 For failover, power off the standby unit.

To prevent the standby unit from becoming active, you must power it off. If you leave it on, when you erase the active unit configuration, then the standby unit becomes active. When the former active unit reloads and reconnects over the failover link, the old configuration will sync from the new active unit, wiping out the deployment configuration you wanted.

Step 2 Restore the deployment configuration after you reload. For failover, enter this command on the active unit:

write erase

Note The ASAv boots the current running image, so you are not reverted to the original boot image. To use the original boot image, see the **boot image** command.

Do not save the configuration.

Step 3 Reload the ASAv and load the deployment configuration:

reload

Step 4 For failover, power on the standby unit.

After the active unit reloads, power on the standby unit. The deployment configuration will sync to the standby unit.

ASA 5506-X Series Default Configuration

The default factory configuration for the ASA 5506-X series configures the following:

- Integrated Routing and Bridging functionality—GigabitEthernet 1/2 through 1/8 belong to bridge group 1; Bridge Virtual Interface (BVI) 1
- inside --> outside traffic flow—GigabitEthernet 1/1 (outside), BVI 1 (inside)
- outside IP address from DHCP, inside IP address—192.168.1.1
- (ASA 5506W-X) wifi <--> inside, wifi --> outside traffic flow—GigabitEthernet 1/9 (wifi)
- (ASA 5506W-X) wifi IP address—192.168.10.1
- DHCP for clients on inside and wifi. The access point itself and all its clients use the ASA as the DHCP server.
- ASDM access—inside and wifi hosts allowed.
- NAT—Interface PAT for all traffic from inside, wifi, and management to outside.

The configuration consists of the following commands:

```
interface Management1/1
  management-only
  no nameif
  no security-level
  no ip address
  no shutdown
interface GigabitEthernet1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface GigabitEthernet1/2
  nameif inside_1
  security-level 100
  bridge-group 1
  no shutdown
interface GigabitEthernet1/3
  nameif inside_2
  security-level 100
  no shutdown
  bridge-group 1
interface GigabitEthernet1/4
  nameif inside_3
  security-level 100
  no shutdown
  bridge-group 1
interface GigabitEthernet1/5
  nameif inside_4
  security-level 100
  no shutdown
  bridge-group 1
interface GigabitEthernet1/6
  nameif inside_5
  security-level 100
  no shutdown
  bridge-group 1
interface GigabitEthernet1/7
  nameif inside_6
  security-level 100
  no shutdown
  bridge-group 1
```

```
interface GigabitEthernet1/8
  nameif inside_7
  security-level 100
  no shutdown
  bridge-group 1
!
interface bvi 1
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
!
object network obj_any1
 subnet 0.0.0.0 0.0.0.0
 nat (inside_1,outside) dynamic interface
object network obj_any2
 subnet 0.0.0.0 0.0.0.0
 nat (inside_2,outside) dynamic interface
object network obj_any3
 subnet 0.0.0.0 0.0.0.0
 nat (inside_3,outside) dynamic interface
object network obj_any4
 subnet 0.0.0.0 0.0.0.0
 nat (inside_4,outside) dynamic interface
object network obj_any5
 subnet 0.0.0.0 0.0.0.0
 nat (inside_5,outside) dynamic interface
object network obj_any6
 subnet 0.0.0.0 0.0.0.0
 nat (inside_6,outside) dynamic interface
object network obj_any7
 subnet 0.0.0.0 0.0.0.0
 nat (inside_7,outside) dynamic interface
!
same-security-traffic permit inter-interface
!
http server enable
http 192.168.1.0 255.255.255.0 inside_1
http 192.168.1.0 255.255.255.0 inside_2
http 192.168.1.0 255.255.255.0 inside_3
http 192.168.1.0 255.255.255.0 inside_4
http 192.168.1.0 255.255.255.0 inside_5
http 192.168.1.0 255.255.255.0 inside_6
http 192.168.1.0 255.255.255.0 inside_7
!
dhcpd auto_config outside
dhcpd address 192.168.1.5-192.168.1.254 inside
dhcpd enable inside
!
logging asdm informational
```

For the ASA 5506W-X, the following commands are also included:

```
interface GigabitEthernet 1/9
  security-level 100
  nameif wifi
  ip address 192.168.10.1 255.255.255.0
  no shutdown
!
object network obj_any_wifi
 subnet 0.0.0.0 0.0.0.0
 nat (wifi,outside) dynamic interface
!
http 192.168.10.0 255.255.255.0 wifi
```

```
!
dhcpd address 192.168.10.2-192.168.10.254 wifi
dhcpd enable wifi
```

ASA 5508-X and 5516-X Default Configuration

The default factory configuration for the ASA 5508-X and 5516-X configures the following:

- **inside --> outside** traffic flow—GigabitEthernet 1/1 (outside), GigabitEthernet 1/2 (inside)
- **outside IP address** from DHCP
- **inside IP address**—192.168.1.1
- **DHCP server** on inside.
- **Default route** from outside DHCP
- **Management 1/1 interface** is Up, but otherwise unconfigured. The ASA FirePOWER module can then use this interface to access the ASA inside network and use the inside interface as the gateway to the Internet.
- **ASDM** access—inside hosts allowed.
- **NAT**—Interface PAT for all traffic from inside and management to outside.

The configuration consists of the following commands:

```
interface Management1/1
  management-only
  no nameif
  no security-level
  no ip address
  no shutdown
interface GigabitEthernet1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
interface GigabitEthernet1/2
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
  no shutdown
!
object network obj_any
  subnet 0.0.0.0 0.0.0.0
  nat (any,outside) dynamic interface
!
http server enable
http 192.168.1.0 255.255.255.0 inside
!
dhcpd auto_config outside
dhcpd address 192.168.1.5-192.168.1.254 inside
dhcpd enable inside
!
logging asdm informational
```

ASA 5512-X through ASA 5585-X Default Configuration

The default factory configuration for the ASA 5512-X through ASA 5585-X 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 that a computer 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
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 enable management
```

Firepower 2100 Default Configuration

ASA Configuration

The default factory configuration for the ASA on the Firepower 2100 configures the following:

- **inside→outside traffic flow**—Ethernet 1/1 (outside), Ethernet 1/2 (inside)
- **outside IP address** from DHCP, inside IP address—192.168.1.1
- **DHCP server** on inside interface
- **Default route** from outside DHCP
- **management**—Management 1/1 (management), IP address 192.168.45.1
- **ASDM** access—Management hosts allowed.
- **NAT**—Interface PAT for all traffic from inside to outside.
- **FXOS management** traffic initiation—The FXOS chassis can initiate management traffic on the ASA outside interface.
- **DNS** servers—OpenDNS servers are pre-configured.

The configuration consists of the following commands:

```
interface Management1/1
  management-only
  nameif management
  security-level 100
  ip address 192.168.45.1 255.255.255.0
  no shutdown
!
interface Ethernet1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/2
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
  no shutdown
!
object network obj_any
  subnet 0.0.0.0 0.0.0.0
  nat (any,outside) dynamic interface
!
http server enable
http 192.168.45.0 255.255.255.0 management
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd enable inside
!
ip-client outside
!
dns domain-lookup outside
dns server-group DefaultDNS
   name-server 208.67.222.222 outside
   name-server 208.67.220.220 outside
```

FXOS Configuration

The default factory configuration for FXOS on the Firepower 2100 configures the following:

- **Management 1/1**—IP address 192.168.45.45
- **Default gateway**—ASA data interfaces
- **Firepower Chassis Manager and SSH access**—From the management network only.
- **Default Username**—**admin**, with the default password **Admin123**
- **DHCP server**—Client IP address range 192.168.45.10-192.168.45.12
- **NTP** server—Cisco NTP servers: 0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org, 2.sourcefire.pool.ntp.org
- **DNS** Servers—OpenDNS: 208.67.222.222, 208.67.220.220
- **Ethernet 1/1 and Ethernet 1/2**—Enabled

Firepower 4100/9300 Chassis Default Configuration

When you deploy the ASA on the Firepower 4100/9300 chassis, you can pre-set many parameters that let you connect to the Management interface using ASDM. A typical configuration includes the following settings:

- Management interface:
  - Management type interface of your choice defined on the Firepower 4100/9300 Chassis supervisor
  - Named “management”
  - IP address of your choice
  - Security level 0
  - Management-only
- Default route through the management interface
- ASDM access—All hosts allowed.

The configuration for a standalone unit consists of the following commands. For additional configuration for clustered units, see Create an ASA Cluster.

```
interface <management_ifc>
  management-only
  ip address <ip_address> <mask>
  ipv6 address <ipv6_address>
  ipv6 enable
  nameif management
  security-level 0
  no shutdown
!
http server enable
http 0.0.0.0 0.0.0.0 management
http ::/0 management
!
route management 0.0.0.0 0.0.0.0 <gateway_ip> 1
ipv6 route management ::/0 <gateway_ipv6>
```

ISA 3000 Default Configuration

The default factory configuration for the ISA 3000 configures the following:

- **Transparent firewall mode**—A transparent firewall is a Layer 2 firewall that acts like a “bump in the wire,” or a “stealth firewall,” and is not seen as a router hop to connected devices.
- **1 Bridge Virtual Interface**—All member interfaces are in the same network (**IP address *not* pre-configured; you must set to match your network**): GigabitEthernet 1/1 (outside1), GigabitEthernet 1/2 (inside1), GigabitEthernet 1/3 (outside2), GigabitEthernet 1/4 (inside2)
- All **inside and outside** interfaces can communicate with each other.
- **Management 1/1** interface—192.168.1.1/24 for ASDM access.
- **DHCP** for clients on management.
- **ASDM** access—Management hosts allowed.

- **Hardware bypass** is enabled for the following interface pairs: GigabitEthernet 1/1 & 1/2; GigabitEthernet 1/3 & 1/4



Note When the ISA 3000 loses power and goes into hardware bypass mode, only the above interface pairs can communicate; inside1 and inside2, and outside1 and outside2 can no longer communicate. Any existing connections between these interfaces will be lost. When the power comes back on, there is a brief connection interruption as the ASA takes over the flows.

- **ASA FirePOWER module**—All traffic is sent to the module in Inline Tap Monitor-Only Mode. This mode sends a duplicate stream of traffic to the ASA Firepower module for monitoring purposes only.
- **Precision Time Protocol**—PTP traffic is not sent to the FirePOWER module.

The configuration consists of the following commands:

```
firewall transparent

interface GigabitEthernet1/1
  bridge-group 1
  nameif outside1
  security-level 0
  no shutdown
interface GigabitEthernet1/2
  bridge-group 1
  nameif inside1
  security-level 100
  no shutdown
interface GigabitEthernet1/3
  bridge-group 1
  nameif outside2
  security-level 0
  no shutdown
interface GigabitEthernet1/4
  bridge-group 1
  nameif inside2
  security-level 100
  no shutdown
interface Management1/1
  management-only
  no shutdown
  nameif management
  security-level 100
  ip address 192.168.1.1 255.255.255.0
interface BVI1
  no ip address

access-list allowAll extended permit ip any any
access-group allowAll in interface outside1
access-group allowAll in interface outside2

same-security-traffic permit inter-interface

hardware-bypass GigabitEthernet 1/1-1/2
hardware-bypass GigabitEthernet 1/3-1/4

http server enable
http 192.168.1.0 255.255.255.0 management
```

```
dhcpd address 192.168.1.5-192.168.1.254 management
dhcpd enable management


access-list sfrAccessList extended permit ip any any
class-map sfrclass
  match access-list sfrAccessList
policy-map global_policy
  class sfrclass
  sfr fail-open monitor-only
service-policy global_policy global
```

ASAv Deployment Configuration

When you deploy the ASAv, you can pre-set many parameters that let you connect to the Management 0/0 interface using ASDM. A typical configuration includes the following settings:

- Routed or Transparent firewall mode
- Management 0/0 interface:
  - Named “management”
  - IP address or DHCP
  - Security level 0
- Static route for the management host IP address (if it is not on the management subnet)
- HTTP server enabled or disabled
- HTTP access for the management host IP address
- (Optional) Failover link IP addresses for GigabitEthernet 0/8, and the Management 0/0 standby IP address
- DNS server
- Smart licensing ID token
- Smart licensing Throughput Level and Standard Feature Tier
- (Optional) Smart Call Home HTTP Proxy URL and port
- (Optional) SSH management settings:
  - Client IP addresses
  - Local username and password
  - Authentication required for SSH using the LOCAL database
- (Optional) REST API enabled or disabled

Note To successfully register the ASAv with the Cisco Licensing Authority, the ASAv requires Internet access. You might need to perform additional configuration after deployment to achieve Internet access and successful license registration.

See the following sample configuration for a standalone unit:

```
interface Management0/0
  nameif management
  security-level 0
  ip address ip_address

  no shutdown
http server enable
http managemment_host_IP mask management
route management management_host_IP mask gateway_ip 1
dns server-group DefaultDNS
  name-server ip_address
call-home
  http-proxy ip_address port port
license smart
  feature tier standard
  throughput level {100M | 1G | 2G}
  license smart register idtoken id_token
aaa authentication ssh console LOCAL
username username password password
ssh source_IP_address mask management
rest-api image boot:/path
rest-api agent
```

See the following sample configuration for a primary unit in a failover pair:

```
nameif management
  security-level 0
  ip address ip_address standby standby_ip

  no shutdown
route management management_host_IP mask gateway_ip 1
http server enable
http managemment_host_IP mask management
dns server-group DefaultDNS
  name-server ip_address
call-home
  http-proxy ip_address port port
license smart
  feature tier standard
  throughput level {100M | 1G | 2G}
  license smart register idtoken id_token
aaa authentication ssh console LOCAL
username username password password
ssh source_IP_address mask management
rest-api image boot:/path
rest-api agent
failover
failover lan unit primary
failover lan interface fover gigabitethernet0/8
failover link fover gigabitethernet0/8
```

```
failover interface ip fover primary_ip mask standby standby_ip
```

Work 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.

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.

Save Configuration Changes

This section describes how to save your configuration.

Save Configuration Changes in Single Context Mode

To save the running configuration to the startup configuration, perform the following procedure.

Procedure

Save the running configuration to the startup configuration:

write memory

Note The **copy running-config startup-config** command is equivalent to the **write memory** command.

Save 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.

Save Each Context and System Separately

Use the following procedure to save the system or context configuration.

Procedure

From within the context or the system, save the running configuration to the startup configuration:

write memory

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.

Save All Context Configurations at the Same Time

Use the following procedure to save all context configurations at the same time, as well as the system configuration.

Procedure

From the system execution space, save the running configuration to the startup configuration for all contexts and the system configuration:

write memory all [**/noconfirm**]

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
```

Copy the Startup Configuration to the Running Configuration

Use one of the following commands to copy a new startup configuration to the running configuration:

- **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** and then **copy startup-config running-config**

  Loads the startup configuration and discards the running configuration without requiring a reload.

View the Configuration

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

- **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.

Clear and Remove Configuration Settings

To erase settings, enter one of the following commands:

- **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*.

For example, to clear the configuration for all **aaa** commands, enter the following command:

```
ciscoasa(config)# clear configure aaa
```

To clear the configuration for only **aaa authentication** commands, enter the following command:

```
ciscoasa(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*.

  For example, to remove a specific **access-list** command, enter enough of the command to identify it uniquely; you may have to enter the entire command:

```
ciscoasa(config)# no access-list abc extended permit icmp any any object-group obj_icmp_1
```

- **write erase**

  Erases the startup configuration.

  Note For the ASAv, this command restores the deployment configuration after a reload. To erase the configuration completely, use the **clear configure all** command.

- **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.

  Note For the Firepower 2100: This model does not use the **boot system** command; packages are managed by FXOS.

  For all other models: This command 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, 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.

Create 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 computer 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 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 "ciscoasa(config)#":

```
ciscoasa(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 Using the Command-Line Interface.

Apply 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 that they can reconnect using the new policy.

To disconnect connections, enter one of the following commands:

- **clear local-host** [*ip_address*] [**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*]]

  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.

Reload the ASA

To reload the ASA, complete the following procedure.

Procedure

Reload the ASA:

reload

Note In multiple context mode, you can only reload from the system execution space.