

Getting Started

This chapter describes how to get started with your ASA.

- Access the Console for the Command-Line Interface, on page 1
- Enable FIPS Mode, on page 8
- Configure ASDM Access, on page 10
- Start ASDM, on page 13
- Customize ASDM Operation, on page 14
- Factory Default Configurations, on page 16
- Set the Firepower 2100 to Appliance or Platform Mode, on page 33
- Get Started with the Configuration, on page 35
- Use the Command Line Interface Tool in ASDM, on page 36
- Apply Configuration Changes to Connections, on page 37

Access the Console for the Command-Line Interface

In some cases, you may need to use the CLI to configure basic settings for ASDM access.

For initial configuration, access the CLI directly from the console port. Later, you can configure remote access using Telnet or SSH according to Management Access. If your system is already in multiple context mode, then accessing the console port places you in the system execution space.

If you get unreadable characters when connecting to the console port, verify the port settings. If they are correct, try the cable with another device using the same settings. If the cable is good, you might need to replace the hardware for the console port. Also consider trying a different workstation to make the connection.

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

Access the ASA Hardware or ISA 3000 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 Platform Mode Console

The Firepower 2100 console port connects you to the Secure Firewall eXtensible Operating System (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 Firepower 1000, 2100 Appliance Mode Console

The Firepower 1000, 2100 Appliance Mode console port connects you to the ASA CLI (unlike the Firepower 2100 Platform mode console, which connects you to the FXOS CLI). From the ASA CLI, you can then connect to the FXOS CLI using Telnet for troubleshooting purposes.

Procedure

Step 1 Connect your management computer to the console port. Be sure to install any necessary 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 ASA CLI. There are no user credentials required for console access by default.

Step 2 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#
```

The enable password that you set on the ASA is also the FXOS **admin** user password if the ASA fails to boot up, and you enter FXOS failsafe mode.

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

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

Step 3 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 4 (Optional) Connect to the FXOS CLI.

connect fxos [**admin**]

- **admin**—Provides admin-level access. Without this option, users have read-only access. Note that no configuration commands are available even in admin mode.

You are not prompted for user credentials. The current ASA username is passed through to FXOS, and no additional login is required. To return to the ASA CLI, enter **exit** or type **Ctrl-Shift-6**, **x**.

Within FXOS, you can view user activity using the **scope security/show audit-logs** command.

Example:

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

Enable FIPS Mode

FIPS, or Federal Information Processing Standard, is a U.S. and Canadian government certification standard. It defines requirements that cryptographic modules must follow. Certain versions of ASA are FIPS 140-3 compliant, in accordance with the U.S. National Institute of Standards (NIST).

In addition to enabling FIPS on the ASA, you must also configure FIPS-compliant ciphers.

You cannot enable FIPS for clustering.

Before you begin

- FIPS mode is only supported on releases that have been through FIPS compliance. You should disable FIPS mode before you upgrade to a non-FIPS compliance version.

For information about which releases are FIPS compliant and to view their certifications, see https://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications/fips-140.html?flt0_general-table0=asa.

- For failover, both units must be in FIPS mode.

Procedure

Step 1 Enable FIPS on the ASA.

fips enable

Example:

```
ciscoasa(config)# fips enable
WARNING: FIPS mode change will not take effect until you save configuration and reboot the
 device
```

When FIPS is enabled, FIPS POST will run and print the following console message at startup:

```
Copyright (c) 1996-2005 by Cisco Systems, Inc.
Restricted Rights Legend
Use, duplication, or disclosure by the Government is subject to restrictions as set forth
in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR
sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

               Cisco Systems, Inc.
               170 West Tasman Drive
               San Jose, California 95134-1706

....
Cryptochecksum (unchanged): 6c6d2f77 ef13898e 682c9f94 9c2d5ba9

INFO: FIPS Power-On Self-Test in process.  Estimated completion in 90 seconds.
.................................................
INFO: FIPS Power-On Self-Test complete.
Type help or '?' for a list of available commands.
ciscoasa>
```

Step 2 Save your configuration and reload.

write memory

reload

Step 3 (Optional) Execute power-on self-tests.

fips self-test poweron

Tests include the cryptographic algorithm test, software integrity test, and critical functions test.

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

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 1010—Management 1/1 (192.168.45.1), or inside Ethernet 1/2 through 1/8 (192.168.1.1). Management hosts are limited to the 192.168.45.0/24 network, and inside hosts are limited to the 192.168.1.0/24 network.
  - Firepower 1100, 2100 in Appliance Mode—Inside Ethernet 1/2 (192.168.1.1), or Management 1/1 (from DHCP). Inside hosts are limited to the 192.168.1.0/24 network. Management hosts are allowed from any network.
  - Firepower 2100 in Platform Mode—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.
  - 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 16
Enable or Disable Multiple Context Mode

Start ASDM, on page 13

Customize ASDM Access

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

- You do not have a factory default configuration
- 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 17
Set the Firewall Mode (Single Mode)
Access the ASA Hardware or ISA 3000 Console, on page 1
Start ASDM, on page 13

Start ASDM

You can start ASDM using two methods:

- ASDM 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 Client 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 and start ASDM:

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 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.

Customize ASDM Operation

You can install an identity certificate to successfully launch ASDM as well as increase the ASDM heap memory so it can handle larger configurations.

Install an Identity Certificate for ASDM

When using Java 7 update 51 and later, the ASDM Launcher requires a trusted certificate. An easy approach to fulfill the certificate requirements is to install a self-signed identity certificate. You can use Java Web Start to launch ASDM until you install a certificate.

See the following document to install a self-signed identity certificate on the ASA for use with ASDM and to register the certificate with Java.

http://www.cisco.com/go/asdm-certificate

Increase the ASDM Configuration Memory

ASDM supports a maximum configuration size of 512 KB. If you exceed this amount you may experience performance issues. For example, when you load the configuration, the status dialog box shows the percentage of the configuration that is complete, yet with large configurations it stops incrementing and appears to suspend operation, even though ASDM might still be processing the configuration. If this situation occurs, we recommend that you consider increasing the ASDM system heap memory. To confirm that you are experiencing memory exhaustion, monitor the Java console for the "java.lang.OutOfMemoryError" message.

In addition, we recommend reducing your configuration size if possible, for example, by removing unused objects.

Increase the ASDM Configuration Memory in Windows

To increase the ASDM heap memory size, edit the **run.bat** file by performing the following procedure.

Procedure

Step 1 Go to the ASDM installation directory, for example C:\Program Files (x86)\Cisco Systems\ASDM.

Step 2 Edit the **run.bat** file with any text editor.

Step 3 In the line that starts with “start javaw.exe”, change the argument prefixed with “-Xmx” to specify your desired heap size. For example, change it to -Xmx768M for 768 MB or -Xmx1G for 1 GB.

For very large configurations, you may need to specify a heap size up to 2 GB.

Step 4 Save the **run.bat** file.

Increase the ASDM Configuration Memory in Mac OS

To increase the ASDM heap memory size, edit the **Info.plist** file by performing the following procedure.

Procedure

Step 1 Right-click the **Cisco ASDM-IDM** icon, and choose **Show Package Contents**.

Step 2 In the **Contents** folder, double-click the **Info.plist** file. If you have Developer tools installed, it opens in the **Property List Editor**. Otherwise, it opens in **TextEdit**.

Step 3 Under **Java** > **VMOptions**, change the string prefixed with "-Xmx" to specify your desired heap size. For example, change it to -Xmx768M for 768 MB or -Xmx1G for 1 GB.

```
<key>CFBundleIconFile</key>
<string>asdm32.icns</string>

<key>VMOptions</key>
<string>-Xms64m -Xmx512m</string>


<key>CFBundleDocumentTypes</key>
  <array>
```

For very large configurations, you may need to specify a heap size up to 2 GB.

Step 4 If this file is locked, you see an error such as the following:



Step 5 Click **Unlock** and save the file.

If you do not see the **Unlock** dialog box, exit the editor, right-click the **Cisco ASDM-IDM** icon, choose **Copy Cisco ASDM-IDM**, and paste it to a location where you have write permissions, such as the Desktop. Then change the heap size from this copy.

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/5516-X—The factory default configuration enables a functional inside/outside configuration. You can manage the ASA using ASDM from the inside interface.
- Firepower 1010—The factory default configuration enables a functional inside/outside configuration. You can manage the ASA using ASDM from either the management interface or the inside switch ports.
- Firepower 1100—The factory default configuration enables a functional inside/outside configuration. You can manage the ASA using ASDM from either the management interface or the inside interface.

- Firepower 2100—Platform mode (the default):The factory default configuration enables a functional inside/outside configuration. You can manage the ASA using the Secure Firewall Chassis Manager and ASDM from the management interface.

  Appliance mode—If you change to appliance mode, the factory default configuration enables a functional inside/outside configuration. You can manage the ASA using ASDM from either the management interface or the inside 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.

- 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. Both CLI and ASDM procedures are provided. For the ASAv, this procedure erases the deployment configuration and applies the following configuration:

```
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
```



Note 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
```

Note
This command does not clear the currently-set mode, Appliance or Platform, for the Firepower 2100.

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 1010—Sets the **management** interface IP address.
- Firepower 1100—Sets the **inside** interface IP address.
- Firepower 2100 in Appliance mode—Sets the **inside** interface IP address.
- Firepower 2100 in Platform mode—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.
- ISA 3000—Sets the **management** interface IP address.

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 1000, and the Firepower 2100 in Appliance mode, 6100: This command clears the **boot system** command, if present, along with the rest of the configuration. This configuration change does not affect the image at bootup: the currently-loaded image continues to be used.

For the Firepower 2100 in Platform mode: 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.

Step 3 (ASDM procedure.) In the main ASDM application window, do the following:

a) Choose **File** > **Reset Device to the Factory Default Configuration**.

The **Reset Device to the Default Configuration** dialog box appears.

b) (Optional) Enter the **Management IP address** of the management or inside interface, instead of using the default address.

See the previous CLI step for details about which interface IP is set per model.

c) (Optional) Choose the **Management Subnet Mask** from the drop-down list.
d) Click **OK**.

A confirmation dialog box appears.

Note
For the Firepower 1000, and the Firepower 2100 in Appliance mode: This command clears the location of the boot image, if present, along with the rest of the configuration. This configuration change does not affect the image at bootup: the currently-loaded image continues to be used.

For the Firepower 2100 in Platform mode: This model does not use the boot image location; packages are managed by FXOS.

For all other models: This action also clears the location of the boot image, if present, along with the rest of the configuration. The **Configuration > Device Management > System Image/Configuration > Boot Image/Configuration** pane lets you boot from a specific image, including an image on the external memory. 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.

e) Click **Yes**.
f) After you restore the default configuration, save this configuration to internal flash memory. Choose **File > Save Running Configuration to Flash**.

Choosing this option saves the running configuration to the default location for the startup configuration, even if you have previously configured a different location. When the configuration was cleared, this path was also cleared.

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
```

Firepower 1010 Default Configuration

The default factory configuration for the Firepower 1010 configures the following:

- **Hardware switch**—Ethernet 1/2 through 1/8 belong to VLAN 1
- **inside→outside** traffic flow—Ethernet 1/1 (outside), VLAN1 (inside)
- **management**—Management 1/1 (management), IP address 192.168.45.1
- **outside IP address** from DHCP, **inside IP address**—192.168.1.1
- **DHCP server** on inside interface, management interface
- **Default route** from outside DHCP
- **ASDM** access—Management and inside hosts allowed. Management hosts are limited to the 192.168.45.0/24 network, and inside hosts are limited to the 192.168.1.0/24 network.
- **NAT**—Interface PAT for all traffic from inside to outside.
- **DNS** servers—OpenDNS servers are pre-configured.

The configuration consists of the following commands:

```
interface Vlan1
nameif inside
security-level 100
ip address 192.168.1.1 255.255.255.0
no shutdown
!
interface Management1/1
managment-only
nameif management
no shutdown
security-level 100
ip address 192.168.45.1 255.255.255.0
!
interface Ethernet1/1
nameif outside
ip address dhcp setroute
no shutdown
!
interface Ethernet1/2
```

```
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/3
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/4
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/5
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/6
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/7
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/8
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
object network obj_any
   subnet 0.0.0.0 0.0.0.0
   nat (any,outside) dynamic interface
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd address 192.168.45.10-192.168.45.12 management
dhcpd enable inside
dhcpd enable management
!
http server enable
http 192.168.45.0 255.255.255.0 management
http 192.168.1.0 255.255.255.0 inside
!
dns domain-lookup outside
dns server-group DefaultDNS
   name-server 208.67.222.222 outside
   name-server 208.67.220.220 outside
!
```

Firepower 1100 Default Configuration

The default factory configuration for the Firepower 1100 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
- **management**—Management 1/1 (management), IP address from DHCP
- **DHCP server** on inside interface
- **Default routes** from outside DHCP, management DHCP
- **ASDM** access—Management and inside hosts allowed. Inside hosts are limited to the 192.168.1.0/24 network.
- **NAT**—Interface PAT for all traffic from inside to outside.
- **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 dhcp setroute
  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 0.0.0.0 0.0.0.0 management
http 192.168.1.0 255.255.255.0 inside
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd enable inside
!
dns domain-lookup outside
dns server-group DefaultDNS
   name-server 208.67.222.222 outside
   name-server 208.67.220.220 outside
!
```

Firepower 2100 Platform Mode Default Configuration

You can set the Firepower 2100 to run in Platform mode; Appliance mode is the default.

Note For pre-9.13(1) versions, Platform mode was the default and only option. If you upgrade from Platform mode, this mode is maintained.

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
- **Firewall 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 2100 Appliance Mode Default Configuration

The Firepower 2100 runs in Appliance mode by default.

Note For pre-9.13(1) versions, Platform mode was the default and only option. If you upgrade from Platform mode, Platform mode is maintained.

The default factory configuration for the Firepower 2100 in Appliance mode 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
- **management IP address** from DHCP—Management 1/1 (management)
- **DHCP server** on inside interface
- **Default routes** from outside DHCP, management DHCP
- **ASDM** access—Management and inside hosts allowed. Inside hosts are limited to the 192.168.1.0/24 network.

- **NAT**—Interface PAT for all traffic from inside to outside.
- **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 dhcp setroute
  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 0.0.0.0 0.0.0.0 management
http 192.168.1.0 255.255.255.0 management
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd enable inside
!
dns domain-lookup outside
dns server-group DefaultDNS
   name-server 208.67.222.222 outside
   name-server 208.67.220.220 outside
!
```

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

object-group service bypass_sfr_inspect
  service-object udp destination range 319 320
access-list sfrAccessList extended deny object-group bypass_sfr_inspect any any
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
```



Note The Essentials license used to be called “Standard” license.

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
```

Set the Firepower 2100 to Appliance or Platform Mode

The Firepower 2100 runs an underlying operating system called the FXOS. You can run the Firepower 2100 in the following modes:

- Appliance mode (the default)—Appliance mode lets you configure all settings in the ASA. Only advanced troubleshooting commands are available from the FXOS CLI.

- Platform mode—When in Platform mode, you must configure basic operating parameters and hardware interface settings in FXOS. These settings include enabling interfaces, establishing EtherChannels, NTP, image management, and more. You can use the Firewall Chassis Manager web interface or FXOS CLI. You can then configure your security policy in the ASA operating system using ASDM or the ASA CLI.

This procedure tells you how to change the mode.



Caution When you change the mode, you need to reload the system, and the configuration is cleared. The default configuration is applied upon reload. Be sure to keep a copy of the original configuration to refer to.

Note that the **clear configure all** and **configure factory-default** commands do not clear the current mode.

Before you begin

You can only change the mode at the CLI.

Procedure

Step 1 (Optional) Back up your current configuration. See Back Up and Restore Configurations or Other Files.

Although there are slight differences between an Appliance mode configuration and a Platform mode configuration, a copy of the old configuration can be a good starting point. For example, for Platform mode, the NTP, DNS, and EtherChannel configuration is not part of the ASA configuration, so it will not be included in your backup, but most other ASA settings are valid for both modes.

Step 2 View the current mode.

show fxos mode

Example:

```
ciscoasa(config)# show fxos mode
Mode is currently set to appliance
```

Step 3 Set the mode to Platform mode.

no fxos mode appliance

write memory

reload

After you set the mode, you need to save the configuration and reload the device. Prior to reloading, you can set the mode back to the original value without any disruption.

Caution
When you reload, the configuration is cleared. The default configuration is applied upon reload.

Example:

```
ciscoasa(config)# no fxos mode appliance
Mode set to platform mode
```

```
WARNING: This command will take effect after the running-config is saved and the system has
 been rebooted. Command accepted.
ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: c0532471 648dc7c2 4f2b4175 1f162684

23736 bytes copied in 1.520 secs (23736 bytes/sec)
[OK]
ciscoasa(config)# reload
Proceed with reload? [confirm]
```

Step 4 Set the mode to Appliance mode.

fxos mode appliance

write memory

reload

After you set the mode, you need to save the configuration and reload the device. Prior to reloading, you can set the mode back to the original value without any disruption.

Caution
When you reload, the configuration is cleared. The default configuration is applied upon reload.

Example:

```
ciscoasa(config)# fxos mode appliance
Mode set to appliance mode
WARNING: This command will take effect after the running-config is saved and the system has
 been rebooted. Command accepted.
ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: c0532471 648dc7c2 4f2b4175 1f162684

23736 bytes copied in 1.520 secs (23736 bytes/sec)
[OK]
ciscoasa(config)# reload
Proceed with reload? [confirm]
```

Get Started with the Configuration

To configure and monitor the ASA, perform the following steps.

Note ASDM supports up to a maximum of a 512 KB configuration. If you exceed this amount, you may experience performance issues. See Increase the ASDM Configuration Memory, on page 15.

Procedure

Step 1 For initial configuration using the Startup Wizard, choose **Wizards** > **Startup Wizard**.

Step 2 To use the IPsec VPN Wizard to configure IPsec VPN connections, choose **Wizards** > **IPsec VPN Wizard** and complete each screen that appears.

Step 3 To use the SSL VPN Wizard to configure SSL VPN connections, choose **Wizards** > **SSL VPN Wizard** and complete each screen that appears.

Step 4 To configure high availability and scalability settings, choose **Wizards** > **High Availability and Scalability Wizard**.

Step 5 To use the Packet Capture Wizard to configure packet capture, choose **Wizards** > **Packet Capture Wizard**.

Step 6 To display different colors and styles available in the ASDM GUI, choose **View** > **Office Look and Feel**.

Step 7 To configure features, click the **Configuration** button on the toolbar and then click one of the feature buttons to display the associated configuration pane.

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

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

Use the Command Line Interface Tool in ASDM

This section tells how to enter commands using ASDM, and how to work with the CLI.

Use the Command Line Interface Tool

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

The commands you can enter with the CLI tool depend on your user privileges. Review your privilege level in the status bar at the bottom of the main ASDM application window to ensure that you have the required privileges to execute privileged-level CLI commands.

Before you begin

- Commands entered via the ASDM CLI tool might function differently from those entered through a terminal connection to the ASA.
- Command errors—If an error occurs because you entered an incorrect command, the incorrect command is skipped and the remaining commands are processed. A message appears in the Response area to inform you whether or not any error occurred, as well as other related information.
- Interactive commands—Interactive commands are not supported in the CLI tool. To use these commands in ASDM, use the **noconfirm** keyword if available, as shown in the following command:

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

- Avoid conflicts with other administrators—Multiple administrative users can update the running configuration of the ASA. Before using the ASDM CLI tool to make configuration changes, check for other active administrative sessions. If more than one user is configuring the ASA at the same time, the most recent changes take effect.

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

Procedure

Step 1 In the main ASDM application window, choose **Tools** > **Command Line Interface**.

The **Command Line Interface** dialog box appears.

Step 2 Choose the type of command (single line or multiple line) that you want, and then choose the command from the drop-down list, or type it in the field provided.

Step 3 Click **Send** to execute the command.

Step 4 To enter a new command, click **Clear Response**, and then choose (or type) another command to execute.

Step 5 Check the **Enable context-sensitive help (?)** check box to provide context-sensitive help for this feature. Uncheck this check box to disable the context-sensitive help.

Step 6 After you have closed the **Command Line Interface** dialog box, if you changed the configuration, click **Refresh** to view the changes in ASDM.

Show Commands Ignored by ASDM on the Device

This feature lets you show the list of commands that ASDM does not support. Typically, ASDM ignores them. ASDM does not change or remove these commands from your running configuration. See Unsupported Commands for more information.

Procedure

Step 1 In the main ASDM application window, choose **Tools** > **Show Commands Ignored by ASDM on Device**.

Step 2 Click **OK** when you are done.

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 the following command:

- **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.