



Cisco ASA 5506-X Series Quick Start Guide

Cisco ASA 5506-X Series Quick Start Guide	2
License Requirements	2
ASA 5506W-X Wireless Access Point	3
Deploy the ASA 5506-X in Your Network	3
Power On the ASA	8
Enable the Wireless Access Point (ASA 5506W-X)	8
Launch ASDM	9
Run Other ASDM Wizards and Advanced Configuration	12
Configure the ASA FirePOWER Module (supported with ASA 9.9(x) and earlier)	12
Where to Go Next	13

Revised: November 30, 2021

Cisco ASA 5506-X Series Quick Start Guide

The Cisco ASA 5506-X series is a powerful desktop firewall.



Note ASA version 9.16 is the final supported version for the ASA 5506-X.



Note The ASA 5506-X only supports the ASA FirePOWER module in version 9.9(x) and earlier.

License Requirements

Licenses are required to enable special features.

ASA Licenses

The ASA 5506-X includes the **Base** or **Security Plus** license, depending on the version you ordered. The **Security Plus** license provides more firewall connections, VPN connections, failover capability, and VLANs.

It also comes pre-installed with the **Strong Encryption (3DES/AES)** license if you qualify for its use; this license is not available for some countries depending on United States export control policy. The Strong Encryption license allows traffic with strong encryption, such as VPN traffic. If you need to manually request the Strong Encryption license (which is free), see <https://www.cisco.com/go/license>.

You can optionally purchase an **AnyConnect Plus** or **Apex** license, which allows AnyConnect VPN client connections.

If you want to upgrade from the Base license to the Security Plus license, or purchase an AnyConnect license, see <http://www.cisco.com/go/ccw>. See also the [Cisco AnyConnect Ordering Guide](#) and the [AnyConnect Licensing Frequently Asked Questions \(FAQ\)](#). You will then receive an email with a Product Authorization Key (PAK) so you can obtain the license activation key. For the AnyConnect licenses, you receive a multi-use PAK that you can apply to multiple ASAs that use the same pool of user sessions.



Note The serial number used for licensing is different from the chassis serial number printed on the outside of your hardware. The chassis serial number is used for technical support, but not for licensing. To view the licensing serial number, enter the **show version | grep Serial** command or see the [ASDM Configuration > Device Management > Licensing Activation Key](#) page.

ASA FirePOWER Licenses (supported with ASA 9.9(x) and earlier)

The ASA FirePOWER module uses a separate licensing mechanism from the ASA. No licenses are pre-installed, but the box includes a PAK on a printout that lets you obtain a license activation key for the following licenses:

- **Control and Protection**—Control is also known as “Application Visibility and Control (AVC)” or “Apps”. Protection is also known as “IPS”. In addition to the activation key for these licenses, you also need “right-to-use” subscriptions for automated updates for these features.

The **Control** (AVC) updates are included with a Cisco support contract.

The **Protection** (IPS) updates require you to purchase the IPS subscription from <http://www.cisco.com/go/ccw>. This subscription includes entitlement to Rule, Engine, Vulnerability, and Geolocation updates. **Note:** This right-to-use subscription does not generate or require a PAK/license activation key for the ASA FirePOWER module; it just provides the right to use the updates.

Other licenses that you can purchase include the following:

- **Advanced Malware Protection (AMP)**
- **URL Filtering**

These licenses generate a PAK/license activation key for the ASA FirePOWER module. See the [Cisco Firepower System Feature Licenses](#) for more information.

To install the Control and Protection licenses and other optional licenses, see [Install the Licenses, on page 12](#).

ASA 5506W-X Wireless Access Point

The ASA 5506W-X includes a Cisco Aironet 702i wireless access point integrated into the ASA. The access point connects to the ASA internally over the GigabitEthernet 1/9 interface. All wifi clients belong to the GigabitEthernet 1/9 network. The ASA security policy determines how the wifi network can access any networks on other interfaces. The access point does not contain any external interfaces or switch ports.

The access point includes an *autonomous* Cisco IOS image, which enables individual device management. You can install the *lightweight* image if you want to add the ASA 5506W-X to a Cisco Unified Wireless Network and use a wireless LAN controller. See the [Converting Autonomous Access Points to Lightweight Mode](#) chapter in the Cisco Wireless Control Configuration Guide for more information about using the lightweight image in unified mode.

- For supported access point software, see [Cisco ASA Compatibility](#).
- For details about using the wireless LAN controller, see the [Cisco Wireless LAN Controller Software documentation](#).
- For details about the wireless access point hardware and software, see the [Cisco Aironet 700 Series documentation](#).

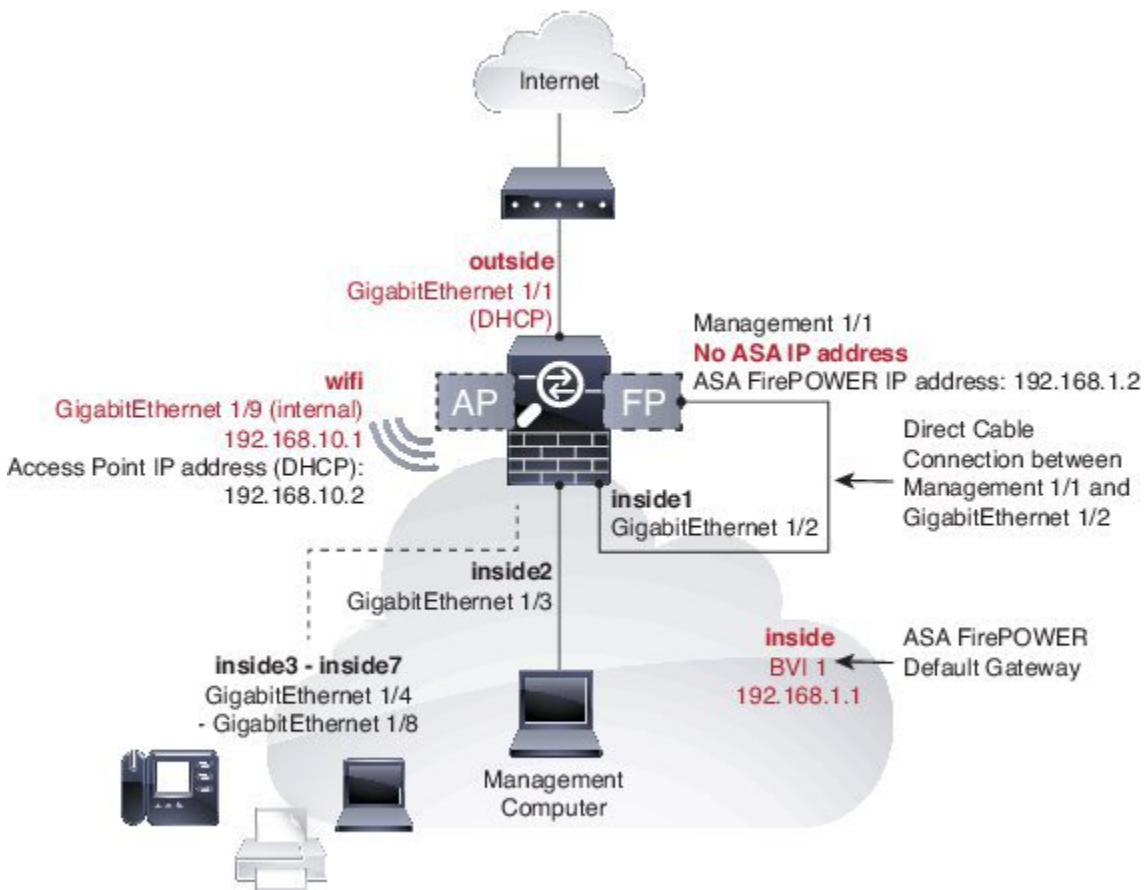
Deploy the ASA 5506-X in Your Network

See the procedure for your version.

ASA 9.7 and Later

The following figure shows the recommended network deployment for the ASA 5506-X with the ASA FirePOWER module (supported with ASA 9.9(x) and earlier) and the built-in wireless access point (ASA 5506W-X). This deployment includes an inside bridge group (also known as a software switch) that includes all but the outside and wifi interfaces so that you can use these interfaces as an alternative to an external switch.

Figure 1: ASA 5506-X 9.7 and Later Network



The default configuration enables the above network deployment with the following behavior.

- **outside** GigabitEthernet 1/1 interface, IP address from DHCP
- **inside** bridge group with GigabitEthernet 1/2 through 1/8 member interfaces (GigabitEthernet 1/2 through 1/4 for the ASA 5506H-X), 192.168.1.1
- (ASA 5506W-X) **wifi** GigabitEthernet 1/9 internal interface, 192.168.10.1
- **inside** --> **outside** traffic flow, which allows inside users to access the outside (internet)
- **inside** --> **inside** traffic flow for member interfaces, which allows all inside bridge group member interfaces to communicate
- (ASA 5506W-X) **wifi** <--> **inside**, **wifi** --> **outside** traffic flow, which allows free communication between the wifi network and the inside network, and allows the wifi network to access the outside (internet)
- **DHCP** for clients on **inside** and **wifi**. Clients receive IP addresses from the ASA. The access point itself and all its clients use the ASA as the DHCP server.
- **Management 1/1** interface belongs to the **ASA FirePOWER module** (supported with ASA 9.9(x) and earlier); this usage requires ASA management from the inside or wifi interface. The interface is Up, *but otherwise unconfigured* on the ASA. 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**.



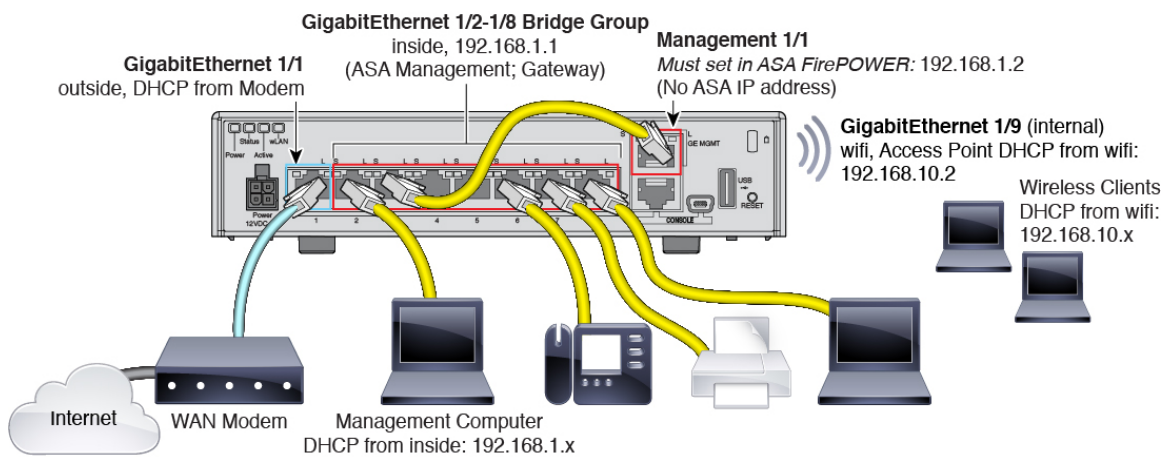
Note Do not configure an IP address for this interface in the ASA configuration. Only configure an IP address in the FirePOWER configuration. You should **consider this interface as completely separate from the ASA** in terms of routing.

- **Adaptive Security Device Manager (ASDM) HTTPS access** on the **inside** interface and the **wifi** interface
- **Network Address Translation (NAT):** Interface Port Address Translation (PAT) for all traffic from inside, wifi, and management to outside. IP addresses from the private inside, wifi, and management networks will be translated to the public outside IP address plus a unique port number. You cannot route private IP addresses on the internet, so NAT is required.



Note If you want to deploy a separate router on the inside network, then you can route between management and inside. In this case, you can manage both the ASA and ASA FirePOWER module on Management 1/1 with the appropriate configuration changes. Many network and routing setups are possible using alternative configurations. However, you cannot manage the FirePOWER module using ASDM if you use NAT between your management computer and the FirePOWER management IP address (at least, not without configuring a more complicated VPN setup). When you run ASDM on your computer, ASDM communicates with the FirePOWER module using the real IP address configured on the module, and it does not have the ability to specify a NAT address instead.

Figure 2: Cabling



Procedure

Step 1 (ASA 9.9(x) and earlier) Cable Management 1/1 (for the ASA FirePOWER module) directly to one of: GigabitEthernet 1/2 through GigabitEthernet 1/8.

Note You can connect inside and management on the same network, because the management interface acts like a separate device that belongs only to the ASA FirePOWER module.

Step 2 Cable your computer to one of: GigabitEthernet 1/2 through GigabitEthernet 1/8 (GigabitEthernet 1/2 through 1/4 for the ASA 5506H-X).

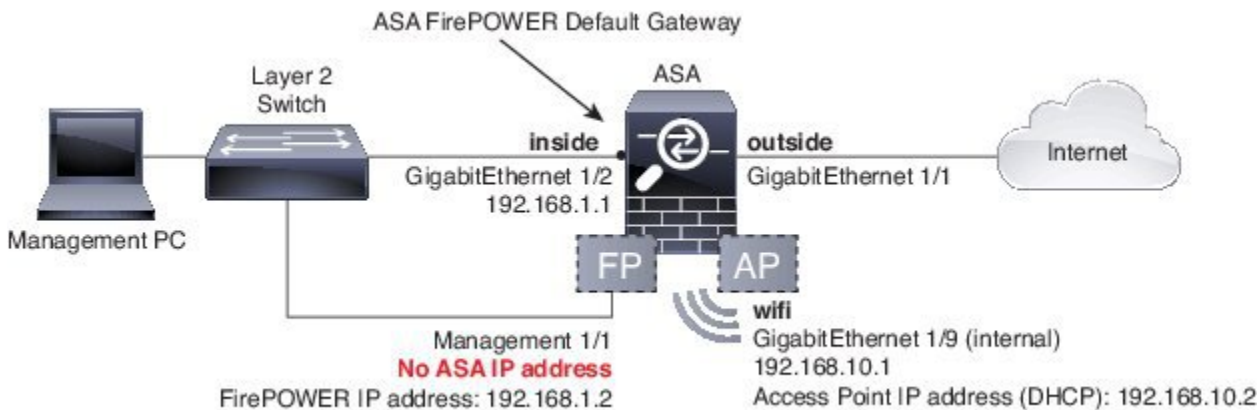
Step 3 Cable GigabitEthernet 1/1 (outside) to your WAN device, for example, your cable modem.

Note If the cable modem supplies an outside IP address that is on 192.168.1.0/24 or 192.168.10.0/24, then you must change the ASA configuration to use a different IP address. Interface IP addresses, HTTPS (ASDM) access, and DHCP server settings can all be changed using the Startup Wizard. If you change the IP address to which you are connected to ASDM, you will be disconnected when you finish the wizard. You must reconnect to the new IP address.

ASA 9.6 and Earlier

The following figure shows the recommended network deployment for the ASA 5506-X with the ASA FirePOWER module and the built-in wireless access point (ASA 5506W-X):

Figure 3: ASA 5506-X 9.6 and Earlier Network



Note You must use a separate inside switch in your deployment.

The default configuration enables the above network deployment with the following behavior.

- **outside** GigabitEthernet 1/1 interface, IP address from DHCP
- **inside** GigabitEthernet 1/2 interface, 192.168.1.1
- (ASA 5506W-X) **wifi** GigabitEthernet 1/9 internal interface, 192.168.10.1
- **inside** --> **outside** traffic flow, which allows inside users to access the outside (internet)
- (ASA 5506W-X) **wifi** <--> **inside**, **wifi** --> **outside** traffic flow, which allows free communication between the wifi network and the inside network, and allows the wifi network to access the outside (internet)
- **DHCP** for clients on **inside** and **wifi**. Clients receive IP addresses from the ASA. The access point itself and all its clients use the ASA as the DHCP server.
- **Management 1/1** belongs to the **ASA FirePOWER module**; this usage requires ASA management from the inside or wifi interface. The interface is Up, *but otherwise unconfigured* on the ASA. 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**.



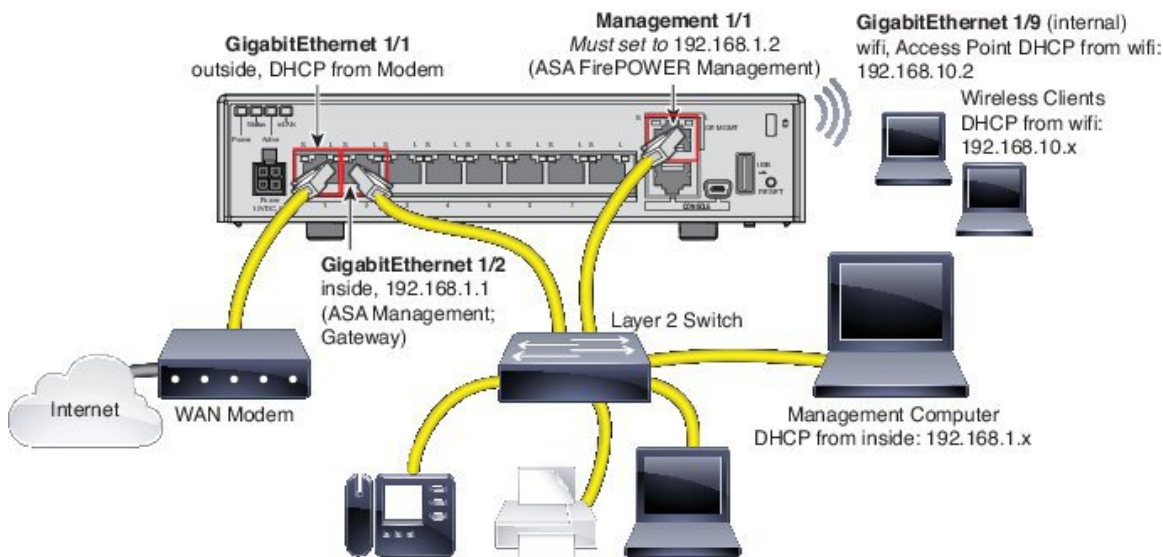
Note Do not configure an IP address for this interface in the ASA configuration. Only configure an IP address in the FirePOWER configuration. You should **consider this interface as completely separate from the ASA** in terms of routing.

- **Adaptive Security Device Manager (ASDM) HTTPS access** on the **inside** interface and the **wifi** interface
- **Network Address Translation (NAT):** Interface Port Address Translation (PAT) for all traffic from inside, wifi, and management to outside. IP addresses from the private inside, wifi, and management networks will be translated to the public outside IP address plus a unique port number. You cannot route private IP addresses on the internet, so NAT is required.



Note If you want to deploy a separate router on the inside network, then you can route between management and inside. In this case, you can manage both the ASA and ASA FirePOWER module on Management 1/1 with the appropriate configuration changes. Many network and routing setups are possible using alternative configurations. However, you cannot manage the FirePOWER module using ASDM if you use NAT between your management computer and the FirePOWER management IP address (at least, not without configuring a more complicated VPN setup). When you run ASDM on your computer, ASDM communicates with the FirePOWER module using the real IP address configured on the module, and it does not have the ability to specify a NAT address instead.

Figure 4: Cabling



Procedure

Step 1 Cable the following to a Layer 2 Ethernet switch:

- GigabitEthernet 1/2 interface (inside)

- Management 1/1 interface (for the ASA FirePOWER module)
- Your computer

Note You can connect inside and management on the same network, because the management interface acts like a separate device that belongs only to the ASA FirePOWER module.

Step 2 Cable GigabitEthernet 1/1 (outside) to your WAN device, for example, your cable modem.

Note If the cable modem supplies an outside IP address that is on 192.168.1.0/24 or 192.168.10.0/24, then you must change the ASA configuration to use a different IP address. Interface IP addresses, HTTPS (ASDM) access, and DHCP server settings can all be changed using the Startup Wizard. If you change the IP address to which you are connected to ASDM, you will be disconnected when you finish the wizard. You must reconnect to the new IP address.

Power On the ASA

Power on the ASA, and check the power up progress.

Procedure

Step 1 Attach the power cable to the ASA and connect it to an electrical outlet.

The power turns on automatically when you plug in the power cable. There is no power button.

Step 2 Check the Power LED on the back of the ASA; if it is solid green, the device is powered on.

Step 3 Check the Status LED on the back of the ASA; after it is solid green, the system has passed power-on diagnostics.

Enable the Wireless Access Point (ASA 5506W-X)

The ASA 5506W-X wireless access point is disabled by default. Connect to the access point GUI so you can enable the wireless radios and configure the SSID and security settings.

Before you begin

This procedure requires you to use the default configuration.

Procedure

Step 1 On the computer connected to the ASA inside network, launch a web browser.

Step 2 In the **Address** field, enter <http://192.168.10.2>. You are prompted for the username and password.

Note If you are unable to reach the access point, and the ASA has the default configuration and other networking issues are not found, then you may want to restore the access point default configuration. You must access the ASA CLI (connect to the ASA console port, or configure Telnet or SSH access using ASDM). From the ASA CLI, enter **hw-module module wlan recover configuration**. If you need to troubleshoot the access point further, connect to the access point CLI using the **session wlan console** command.

Step 3 Enter the username **cisco** and the password **Cisco**. The access point GUI appears.

Step 4 On the left, click **Easy Setup > Network Configuration**.

Step 5 In the **Radio Configuration** area, for each of the **Radio 2.4GHz** and **Radio 5GHz** sections, set the following parameters and click **Apply** for each section:

- **SSID**
- **Broadcast SSID in Beacon**
- **Universal Admin Mode: Disable**
- **Security** (of your choosing)

Step 6 On the left, click **Summary**, and then on the main page under **Network Interfaces**, click the hotlink for the **2.4 GHz** radio.

Step 7 Click the **Settings** tab.

Step 8 For the **Enable Radio** setting, click the **Enable** radio button, and then click **Apply** at the bottom of the page.

Step 9 Repeat for the **5 GHz** radio.

Step 10 For more information, see the following manuals:

- For details about using the wireless LAN controller, see the [Cisco Wireless LAN Controller Software documentation](#).
- For details about the wireless access point hardware and software, see the [Cisco Aironet 700 Series documentation](#).

Launch ASDM

This procedure assumes you want to use ASDM to manage the ASA FirePOWER Module (supported with ASA 9.9(x) and earlier). If you want to use the Firepower Management Center, then you need to connect to the module CLI and run the setup script; see the [ASA FirePOWER quick start guide](#). For ASA 9.10(x) and later, ignore any steps related to the FirePOWER module.

Before you begin

See the [ASDM release notes](#) on Cisco.com for the requirements to run ASDM.

Procedure

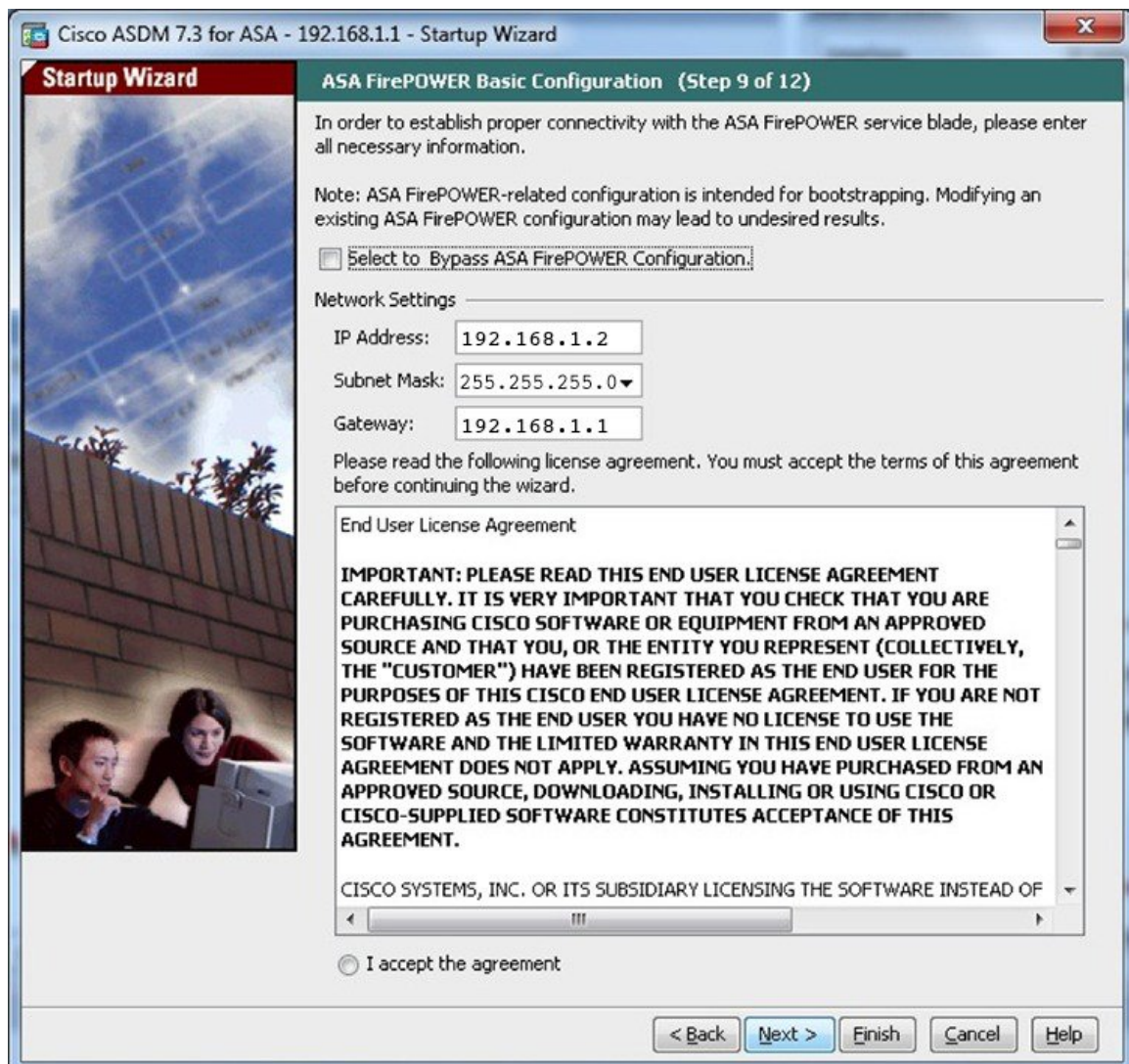
Step 1 On the computer connected to the ASA, launch a web browser.

Step 2 In the Address field, enter the following URL: <https://192.168.1.1/admin>. The **Cisco ASDM** web page appears.

If you connected your management computer to the ASA as a wireless client, you can access ASDM at <https://192.168.10.1/admin>.

- Step 3** Click one of the available options: **Install ASDM Launcher**, **Run ASDM**, or **Run Startup Wizard**.
- Step 4** Follow the onscreen instructions to launch ASDM according to the option you chose. The **Cisco ASDM-IDM Launcher** appears.
- Step 5** Leave the username and password fields empty, and click **OK**. The main ASDM window appears.
- Note** Change your privileged (enable) mode password after you log in on the **Configuration > Device Setup > Device Name/Password** page.
- Step 6** If you are prompted to provide the IP address of the installed ASA FirePOWER module, cancel out of the dialog box. You must first set the module IP address to the correct IP address using the Startup Wizard.
- ASDM can change the ASA FirePOWER module IP address settings over the ASA backplane; but for ASDM to then manage the module, ASDM must be able to reach the module (and its new IP address) on the Management 1/1 interface over the network. The recommended deployment allows this access because the module IP address is on the inside network. If ASDM cannot reach the module on the network after you set the IP address, then you will see an error.
- Step 7** Choose **Wizards > Startup Wizard**.
- Step 8** Configure additional ASA settings as desired, or skip screens until you reach the **ASA FirePOWER Basic Configuration** screen.

Figure 5: ASDM Startup Wizard



Set the following values to work with the default configuration:

- **IP Address**—192.168.1.2
- **Subnet Mask**—255.255.255.0
- **Gateway**—192.168.1.1

- Step 9** Click **I accept the agreement**, and click **Next** or **Finish** to complete the wizard.
- Step 10** Quit ASDM, and then relaunch. You should see **ASA FirePOWER** tabs on the **Home** page.

Run Other ASDM Wizards and Advanced Configuration

ASDM includes many wizards to configure your security policy. See the **Wizards** menu for all available wizards.

To continue configuring your ASA, see the documents available for your software version at [Navigating the Cisco ASA Series Documentation](#).

Configure the ASA FirePOWER Module (supported with ASA 9.9(x) and earlier)

Use ASDM to install licenses, configure the module security policy, and send traffic to the module.



Note You can alternatively use the Firepower Management Center to manage the ASA FirePOWER module. See the [ASA FirePOWER Module Quick Start Guide](#) for more information.

Procedure

- Step 1** [Install the Licenses, on page 12.](#)
 - Step 2** [Configure the ASA FirePOWER Security Policy, on page 13.](#)
 - Step 3** [Send Traffic from the ASA to the ASA FirePOWER Module, on page 13.](#)
-

Install the Licenses

The Control and Protection licenses are provided by default and the Product Authorization Key (PAK) is included on a printout in your box. If you ordered additional licenses, you should have PAKs for those licenses in your email.

Procedure

- Step 1** Obtain the License Key for your chassis by choosing **Configuration > ASA FirePOWER Configuration > Licenses** and clicking **Add New License**.
The License Key is near the top; for example, 72:78:DA:6E:D9:93:35.
- Step 2** Click **Get License** to launch the licensing portal. Alternatively, in your browser go to <https://www.cisco.com/go/license>
- Step 3** Enter the PAKs separated by commas in the **Get New Licenses** field, and click **Fulfill**.
- Step 4** Provide the License Key and email address and other fields.
- Step 5** Copy the resulting license activation key from either the website display or from the zip file attached to the licensing email that the system automatically delivers.
- Step 6** Return to the ASDM **Configuration > ASA FirePOWER Configuration > Licenses > Add New License** screen.
- Step 7** Paste the license activation key into the **License** box.
- Step 8** Click **Verify License** to ensure that you copied the text correctly, and then click **Submit License** after verification.

Step 9 Click **Return to License Page**.

Configure the ASA FirePOWER Security Policy

Configure the security policy for traffic that you send from the ASA to the ASA FirePOWER module.

Procedure

Choose **Configuration > ASA FirePOWER Configuration** to configure the ASA FirePOWER security policy.

Use the ASA FirePOWER pages in ASDM for information to learn about the ASA FirePOWER security policy. You can click **Help** in any page, or choose **Help > ASA FirePOWER Help Topics**, to learn more about how to configure policies.

See also the [ASA FirePOWER module configuration guide](#).

Send Traffic from the ASA to the ASA FirePOWER Module

Configure the ASA to send traffic to the ASA FirePOWER module.

Procedure

Step 1 Choose **Configuration > Firewall > Service Policy Rules**.

Step 2 Choose **Add > Add Service Policy Rule**.

Step 3 Choose whether to apply the policy to a particular interface or apply it globally and click **Next**.

Step 4 Configure the traffic match. For example, you could match **Any Traffic** so that all traffic that passes your inbound access rules is redirected to the module. Or, you could define stricter criteria based on ports, ACL (source and destination criteria), or an existing traffic class. The other options are less useful for this policy. After you complete the traffic class definition, click **Next**.

Step 5 On the **Rule Actions** page, click the **ASA FirePOWER Inspection** tab.

Step 6 Check the **Enable ASA FirePOWER for this traffic flow** check box.

Step 7 In the **If ASA FirePOWER Card Fails** area, click one of the following:

- **Permit traffic**—Sets the ASA to allow all traffic through, uninspected, if the module is unavailable.
- **Close traffic**—Sets the ASA to block all traffic if the module is unavailable.

Step 8 (Optional) Check **Monitor-only** to send a read-only copy of traffic to the module, i.e. passive mode.

Step 9 Click **Finish** and then **Apply**.

Step 10 Repeat this procedure to configure additional traffic flows as desired.

Where to Go Next

- To continue configuring your ASA, see the documents available for your software version at [Navigating the Cisco ASA Series Documentation](#).

- (ASA 9.9(x) and earlier) For more information about the ASA FirePOWER module and ASA operation, see the *ASA FirePOWER Module* chapter in the ASA/ASDM firewall configuration guide, or the ASDM online help.
- (ASA 9.9(x) and earlier) For more information about ASA FirePOWER configuration, see the online help or the [ASA FirePOWER module configuration guide](#) or the [Firepower Management Center configuration guide](#) for your version.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.