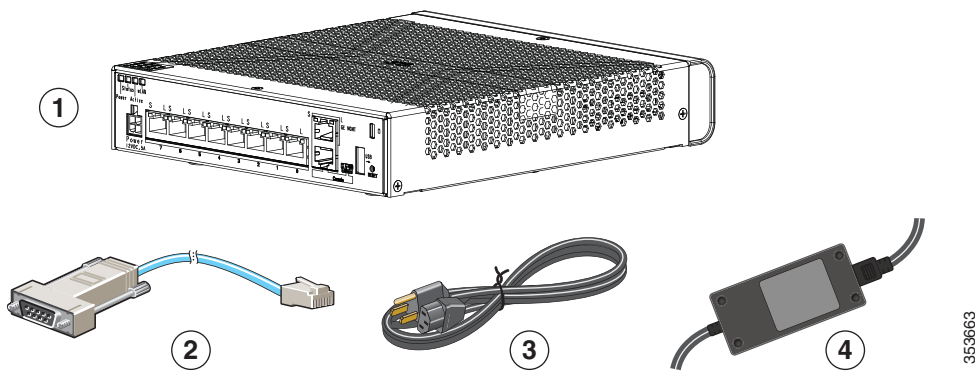# Cisco ASA 5506-X Series Quick Start Guide

**Last Updated:** October 20, 2015

1. Package Contents

This section lists the package contents of the chassis. Note that contents are subject to change, and your exact contents might contain additional or fewer items.

ASA 5506-X and 5506W-X

1	ASA 5506-X or ASA 5506W-X chassis	2	Blue Console Cable and Serial PC Terminal Adapter (DB-9 to RJ-45)
3	Power cable	4	Power supply

ASA 5506H-X
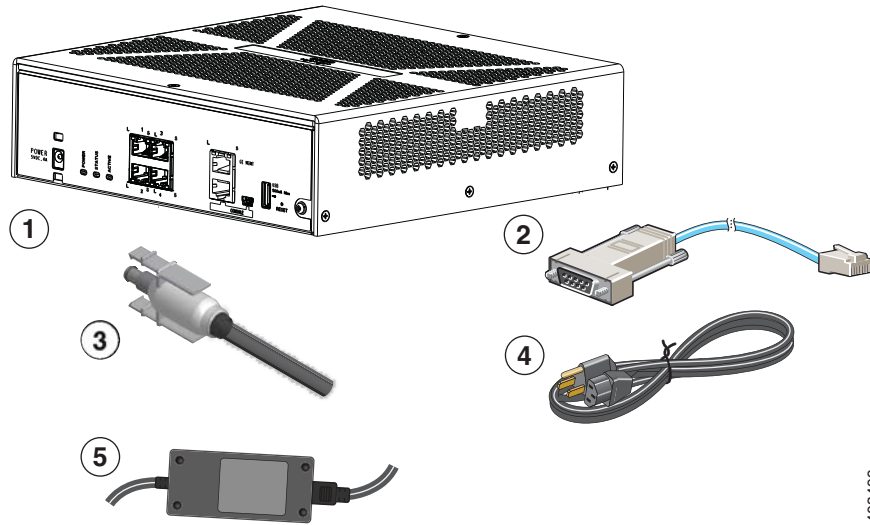
1	ASA 5506H-X chassis	2	Blue Console Cable and Serial PC Terminal Adapter (DB-9 to RJ-45)
3	Power cord retention lock	4	Power cable
5	Power supply		

2. 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.
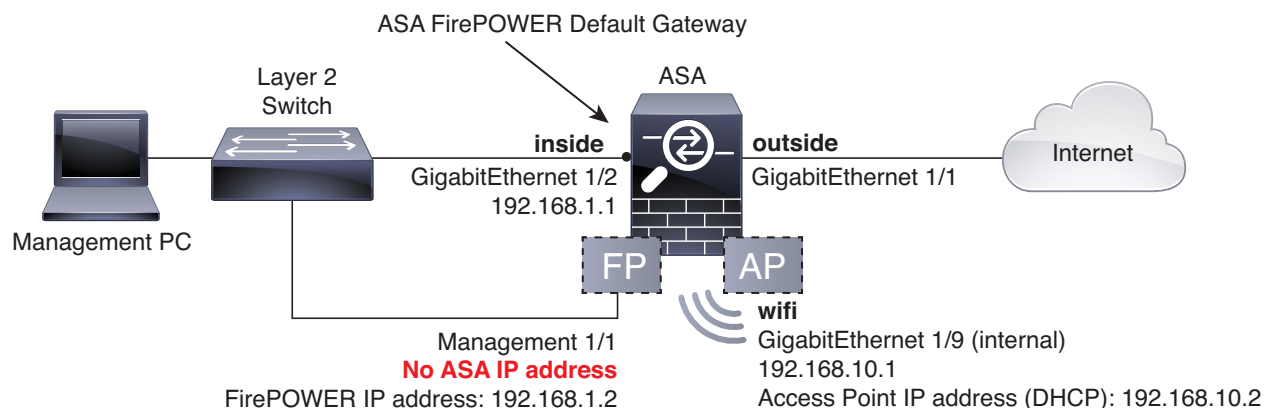
The access point includes either an autonomous image or a Cisco Unified Wireless image (depending on your order). Autonomous mode lets you manage each access point individually. Unified mode lets you use a separate Wireless LAN Controller device so you can manage multiple access points centrally.

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.

3. Deploy the ASA 5506-X in Your Network

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):

ASA FirePOWER Default Gateway

Layer 2
Switch   ASA

inside   outside   Internet
GigabitEthernet 1/2   GigabitEthernet 1/1
192.168.1.1

Management PC

FP   AP

wifi
Management 1/1   GigabitEthernet 1/9 (internal)
No ASA IP address   192.168.10.1
FirePOWER IP address: 192.168.1.2   Access Point IP address (DHCP): 192.168.10.2

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

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

- **inside --> outside** traffic flow

- **outside IP** address from **DHCP**

- (ASA 5506W-X) **wifi <--> inside**, **wifi --> outside** traffic flow

- **DHCP** for clients on **inside** and **wifi**. The access point itself and all its clients use the ASA as the DHCP server.

- **Management 1/1** belongs to the **ASA Firepower module**. 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.

- **ASDM access** on the **inside** interface and the **wifi** interface

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.

Procedure
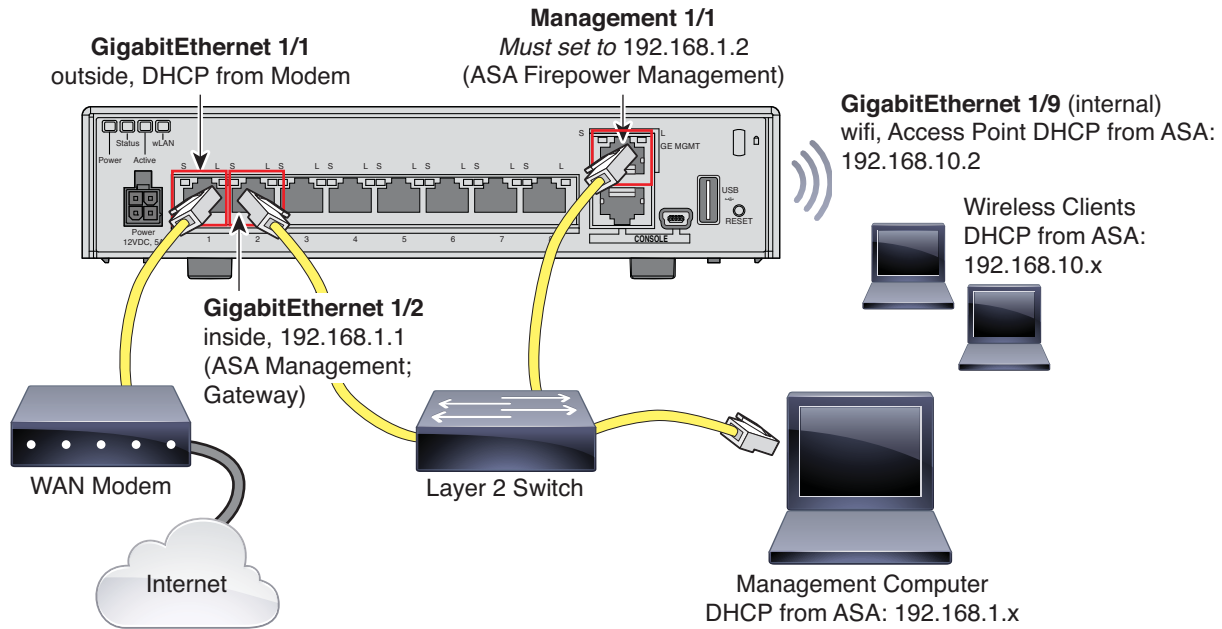
1. Cable the following to a Layer 2 Ethernet switch:

   – 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.

2. Connect the GigabitEthernet 1/1 (outside) interface 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.

4. Power On the ASA

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.

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

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

5. 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

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

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**.

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

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

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)

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

7. Click the **Settings** tab.

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

9. Repeat for the 5 GHz radio.

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.

6. Launch ASDM

See the ASDM release notes on Cisco.com for the requirements to run ASDM.

This procedure assumes you want to use ASDM to manage the ASA Firepower Module. If you want to use the FireSIGHT System, then you need to connect to the module CLI and run the setup script; see the ASA Firepower quick start guide.

Procedure

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

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**.

3. Click one of the available options: **Install ASDM Launcher**, **Run ASDM**, or **Run Startup Wizard**.

4. Follow the onscreen instructions to launch ASDM according to the option you chose. The **Cisco ASDM-IDM Launcher** appears.

   If you click **Install ASDM Launcher**, in some cases you need to install an identity certificate for the ASA and a separate certificate for the ASA Firepower module according to Install an Identity Certificate for ASDM.

5. Leave the username and password fields empty, and click **OK**. The main ASDM window appears.

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.

7. Choose **Wizards > Startup Wizard**.

8. Configure additional ASA settings as desired, or skip screens until you reach the ASA Firepower Basic Configuration screen.
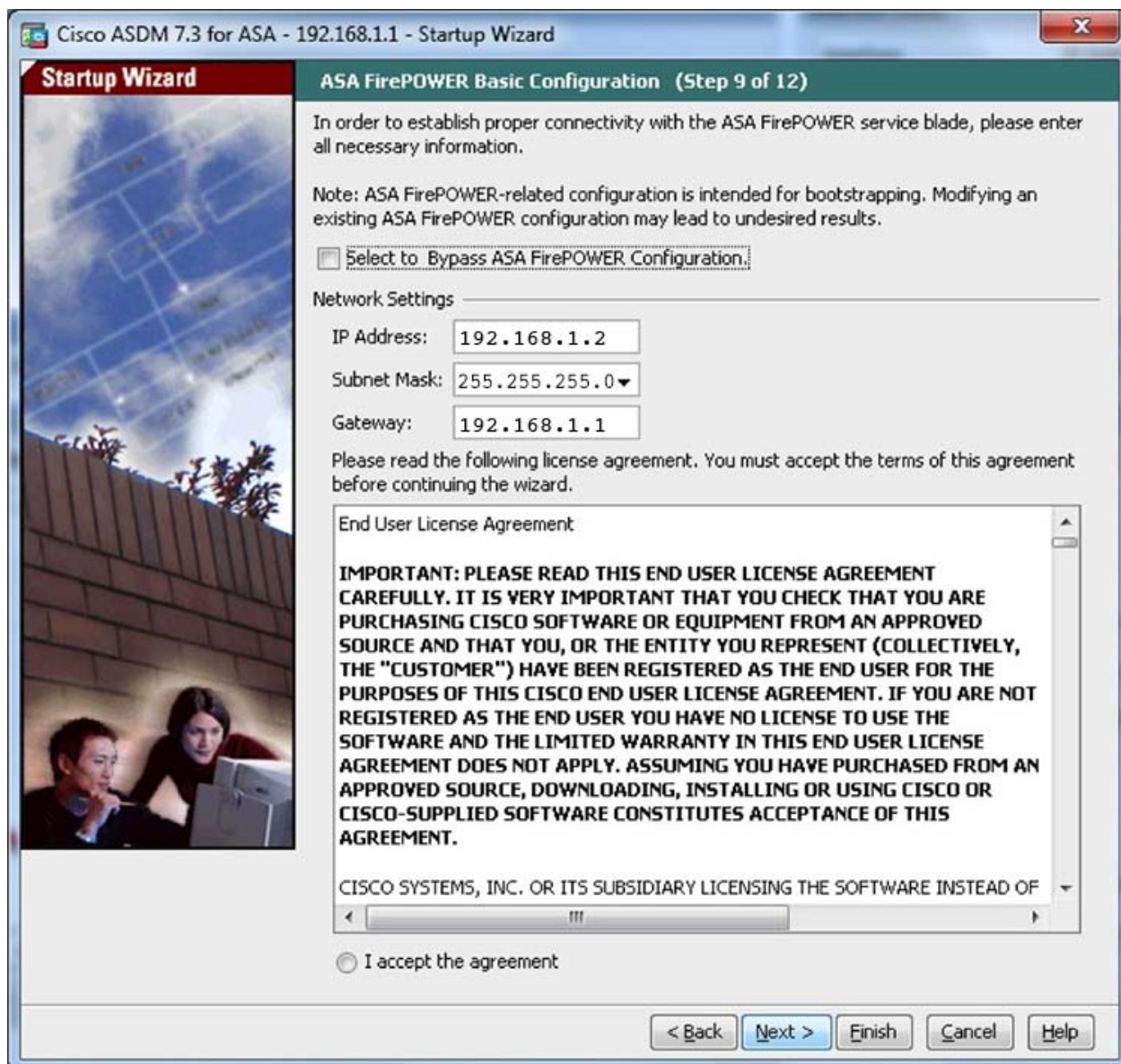
Set the following values to work with the default configuration:

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

9. Click **I accept the agreement**, and click **Next** or **Finish** to complete the wizard.

10. Quit ASDM, and then relaunch. You should see ASA Firepower tabs on the Home page.

7. 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.

8.Configure the ASA Firepower Module

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

Note: You can alternatively use the FireSIGHT Management Center to manage the ASA Firepower module. See the ASA Firepower Module Quick Start Guide for more information.

Configure the ASA FirePOWER Security Policy

Procedure

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

2. Certain areas of ASA Firepower module functionality may require additional licenses. Enable licenses using the ASA Firepower pages in ASDM. See the licensing chapter of the *ASA FirePOWER Module User Guide* or the online help for more information.

   The ASA itself does not require any additional licenses.

Configure the ASA Security Policy

Procedure

1. To send traffic to the module, choose **Configuration > Firewall > Service Policy Rules**.

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

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

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**.

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

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

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.

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

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

   Repeat this procedure to configure additional traffic flows as desired.

9. Where to Go Next

- 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. You can find links to all ASA/ASDM documentation at Navigating the Cisco ASA Series Documentation.

- For more information about ASA Firepower configuration, see the online help or the ASA Firepower Module User Guide or FireSIGHT System User Guide.