Cisco Firepower Threat Defense for the ASA 5506-X Series Using Firepower Management Center Quick Start Guide

First Published: August 10, 2016

Last Updated: December 3, 2018

Warning: You cannot install Firepower Threat Defense 6.3 or subsequent releases on the ASA 5506-X, 5506W-X, and 5506H-X. The final supported Firepower Threat Defense release for these platforms is 6.2.3.

1. Is This Guide for You?

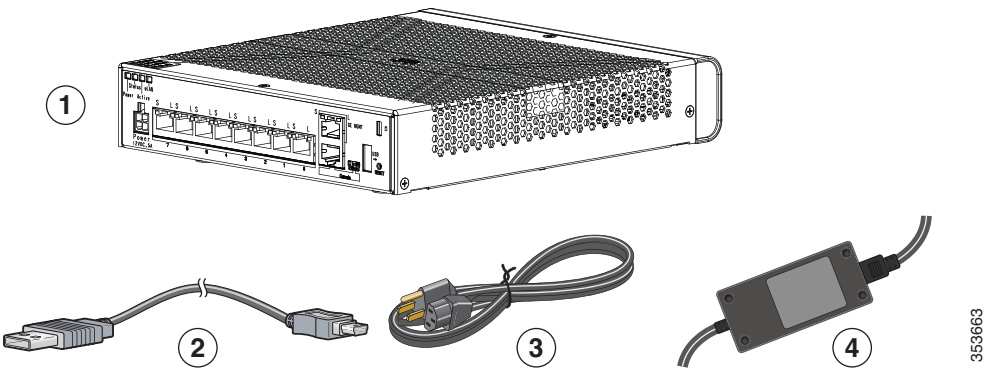
This guide explains how to complete the initial configuration of your Firepower Threat Defense device and how to register the device to a Firepower Management Center. In a typical deployment on a large network, multiple managed devices are installed on network segments, monitor traffic for analysis, and report to a managing Firepower Management Center. The Firepower Management Center provides a centralized management console with web interface that you can use to perform administrative, management, analysis, and reporting tasks.

For networks that include only a single device or just a few, where you do not need to use a high-powered multiple-device manager like the Firepower Management Center, you can use the integrated Firepower Device Manager. Use the Firepower Device Manager web-based device setup wizard to configure the basic features of the software that are most commonly used for small network deployments as described in http://www.cisco.com/go/fdm-quick.

2. Package Contents

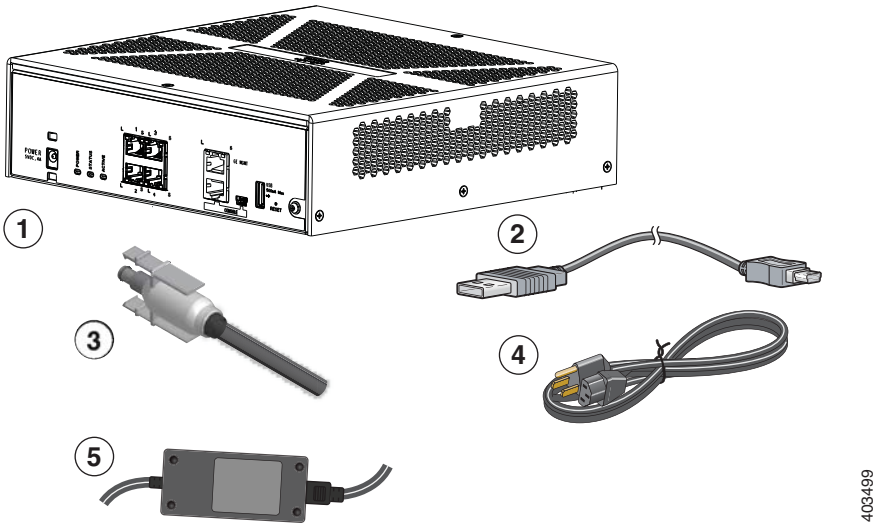
This section lists the package contents of the chassis. Note that contents are subject to change, and your exact contents might contain additional or fewer items.

ASA 5506-X and 5506W-X



1	ASA 5506-X or ASA 5506W-X chassis	2	USB Console Cable (Type A to Type B)
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		

3. License Requirements

Firepower Threat Defense devices require Cisco Smart Licensing. Smart Licensing lets you purchase and manage a pool of licenses centrally. Unlike product authorization key (PAK) licenses, Smart Licenses are not tied to a specific serial number or license key. Smart Licensing lets you assess your license usage and needs at a glance.

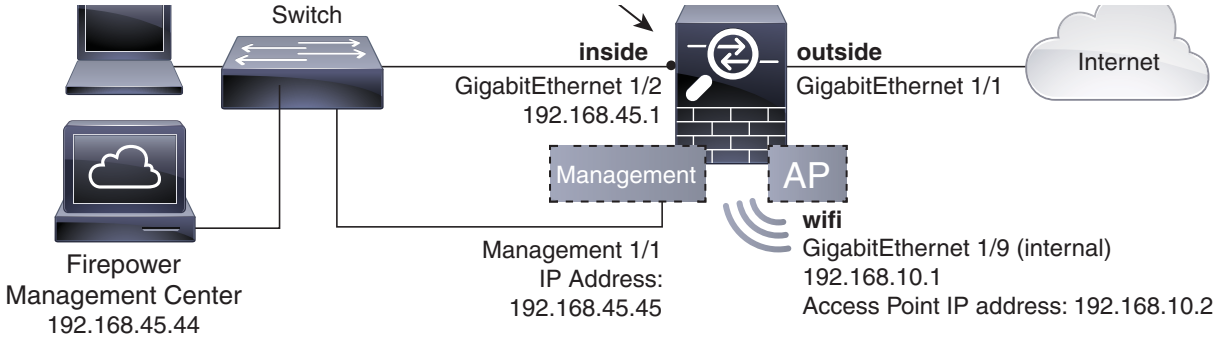
In addition, Smart Licensing does not prevent you from using product features that you have not yet purchased. You can start using a license immediately, as long as you are registered with the Cisco Smart Software Manager, and purchase the license later. This allows you to deploy and use a feature, and avoid delays due to purchase order approval.

When you purchase one or more Smart Licenses for Firepower features, you manage them in the Cisco Smart Software Manager: http://www.cisco.com/web/ordering/smart-software-manager/index.html. The Smart Software Manager lets you create a master account for your organization. For more information about the Cisco Smart Software Manager, see the *Cisco Smart Software Manager User Guide*.

Your purchase of a Firepower Threat Defense device or Firepower Threat Defense Virtual automatically includes a Base license. All additional licenses (Threat, Malware, or URL Filtering) are optional. For more information about Firepower Threat Defense licensing, see the Licensing the System chapter of the *Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager*.

4. Deploy the Firepower Threat Defense in Your Network

The following figure shows the recommended network deployment for Firepower Threat Defense on the ASA 5506-X series of appliances and the built-in wireless access point (ASA 5506W-X).



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

The example 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** is used to set up and register the Firepower Threat Defense device to the Firepower Management Center.

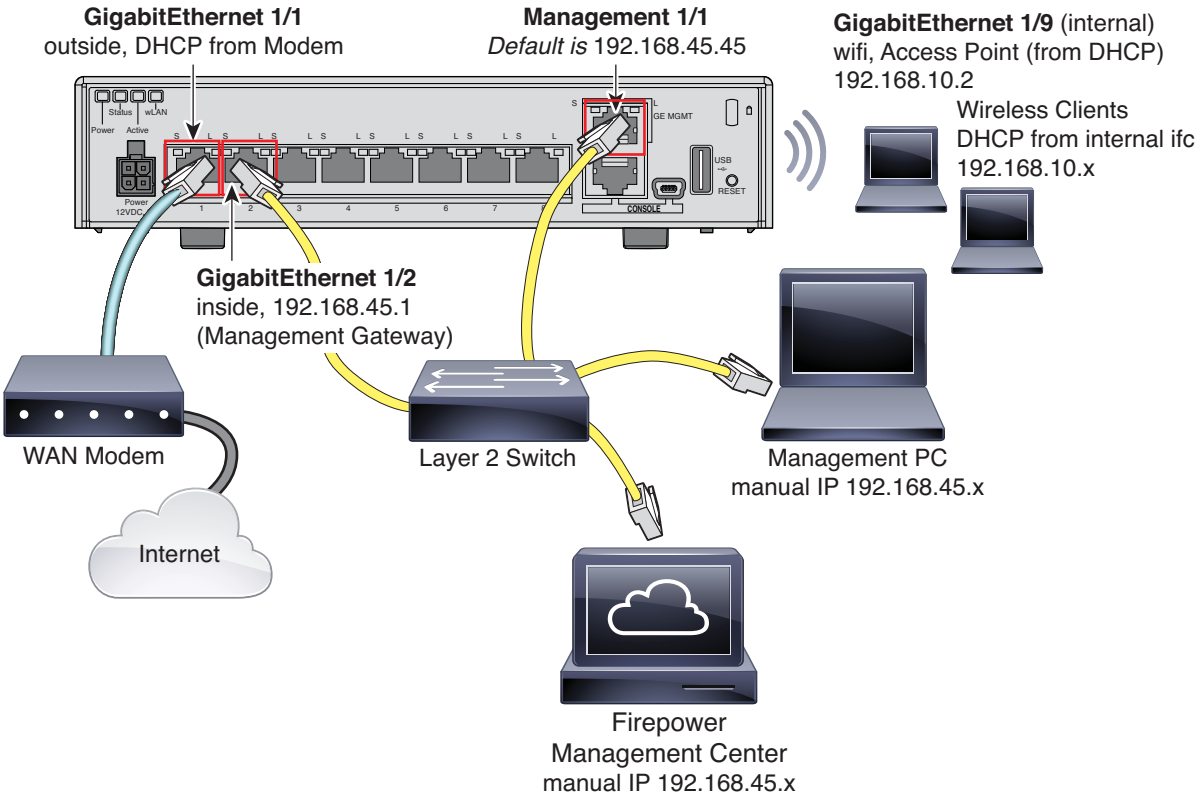
  The Management interface requires Internet access for updates. When you put Management on the same network as an inside interface, you can deploy the Firepower Threat Defense device with only a switch on the inside and point to the inside interface as its gateway.

  The physical management interface is shared between the Management logical interface and the Diagnostic logical interface; see the Interfaces for Firepower Threat Defense chapter of the *Firepower Management Center Configuration Guide*.
- **Firepower Management Center 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; see the Interfaces for Firepower Threat Defense chapter of the *Firepower Management Center Configuration Guide* for examples of alternate deployment configurations.

To cable the above scenario on the ASA 5506-X series, see the following illustration.

Note: The following illustration shows a simple topology using a Layer 2 switch. Other topologies can be used and your deployment will vary depending on your basic logical network connectivity, ports, addressing, and configuration requirements.



Procedure

1. Cable the following to a Layer 2 Ethernet switch:
   - GigabitEthernet 1/2 interface (inside)
   - Management 1/1 interface (for the Firepower Management Center)
   - A local management 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 Firepower Management.
2. Connect the GigabitEthernet 1/1 (outside) interface to your ISP/WAN modem or other outside device. By default, the IP address is obtained using DHCP, but you can set a static address during initial configuration.

5. Power on the Firepower Threat Defense Device

Procedure

1. Attach the power cable to the Firepower Threat Defense device 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 Firepower Threat Defense device; if it is solid green, the device is powered on.
3. Check the Status LED on the back of the Firepower Threat Defense device; after it is solid green, the system has passed power-on diagnostics.

6. Configure the Device for Firepower Management

The first time you access the CLI, a setup wizard prompts you for basic network configuration parameters that are required to setup your Firepower Threat Defense device and to register with a Firepower Management Center. Note that the management IP address and associated gateway route **are not** included on the Firepower Management Center web interface in the list of interfaces or static routes for the device; they can only be set by the setup script and at the CLI.

Before You Begin

Ensure that you connect a data interface to your gateway device, for example, a cable modem or router. For edge deployments, this would be your Internet-facing gateway. For data center deployments, this would be a back-bone router.

The Management interface must also be connected to a gateway through which the Internet is accessible. System licensing and database updates require Internet access.

Procedure

1. Connect to the device, either from the console port or using SSH, for example.
   - For a device attached to a monitor and keyboard, log in at the console.
   - For access to the management interface of the device, SSH to the Management interface's default IPv4 address: 192.168.45.45.
2. Log in with the username **admin** and the password **Admin123**.
3. When the Firepower Threat Defense system boots, a setup wizard prompts you for the following information required to configure the system:
   - Accept EULA
   - New admin password
   - IPv4 or IPv6 configuration
   - IPv4 or IPv6 DHCP settings
   - Management port IPv4 address and subnet mask, or IPv6 address and prefix
   - System name
   - Default gateway IPv4, IPv6, or both
   - DNS setup
   - HTTP proxy
   - Management mode
4. Review the setup wizard settings. Defaults or previously entered values appear in brackets. To accept previously entered values, press **Enter**.

   Example:

```
Please enter 'YES' or press <ENTER> to AGREE to the EULA:

System initialization in progress.  Please stand by.
You must change the password for 'admin' to continue.
Enter new password:
Confirm new password:
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]: y
```

```
Do you want to configure IPv6? (y/n) [n]: n
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]: manual
Enter an IPv4 address for the management interface [192.168.45.45]: 10.133.128.47
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.248.0
Enter the IPv4 default gateway for the management interface []: 10.133.128.1
Enter a fully qualified hostname for this system [firepower]: laurel.example.com
Enter a comma-separated list of DNS servers or 'none' []: 10.33.16.6
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to reconnect.

For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: no
```

5. Reconnect to your appliance using the new log in credentials.
6. Configure the firewall mode. For example:

```
Configure firewall mode? (routed/transparent) [routed]
```

Note: We recommend that you set the firewall mode at initial configuration. Note that the default mode is *routed*. Changing the firewall mode after initial setup erases your running configuration. For more information, see the Transparent or Routed Firewall Mode chapter in the *Firepower Management Center Configuration Guide*.

7. Wait for the default system configuration to be processed. This may take a few minutes.

```
Update policy deployment information
    - add device configuration

You can register the sensor to a Management Center and use the Management Center
to manage it. Note that registering the sensor to a Management Center disables
on-sensor FirePOWER Services management capabilities.

When registering the sensor to a Management Center, a unique alphanumeric
registration key is always required.  In most cases, to register a sensor
to a Management Center, you must provide the hostname or the IP address along
with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'

However, if the sensor and the Management Center are separated by a NAT device,
you must enter a unique NAT ID, along with the unique registration key.
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'

Later, using the web interface on the Management Center, you must use the same
registration key and, if necessary, the same NAT ID when you add this
sensor to the Management Center.
```

8. Register the Firepower Threat Device device to a Firepower Management Center:

```
> configure manager add {hostname | IPv4_address | IPv6_address | DONTRESOLVE} reg_key
[nat_id]
```

where:

- {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} specifies either the fully qualified host name or IP address of the Firepower Management Center. If the Firepower Management Center is not directly addressable, use DONTRESOLVE.
- *reg_key* is the unique alphanumeric registration key required to register a Firepower Threat Defense module to the Firepower Management Center.

Note: The registration key is a user-generated one-time use key that must not exceed 37 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-). You will need to remember this registration key when you add the device to the Firepower Management Center.

- *nat_id* is an optional alphanumeric string used during the registration process between the Firepower Management Center and the Firepower Threat Defense. It is required if the hostname is set to DONTRESOLVE.

9. Identify the Firepower Management Center appliance that will manage this device using the **configure manager add** command.

   Remember that the registration key is a user-generated one-time use key which you need to add the Firepower Threat Defense device to the Firepower Management Center's inventory. The following example shows the simple case:

   ```
   > configure manager add MC.example.com 123456
   Manager successfully configured.
   ```

   If the device and the Firepower Management Center are separated by a NAT device, enter a unique NAT ID along with the registration key, and specify DONTRESOLVE instead of the hostname, for example:

   ```
   >configure manager add DONTRESOLVE my_reg_key my_nat_id
   Manager successfully configured.
   ```

   The Firepower Management Center and the security appliance use the registration key and NAT ID (instead of IP addresses) to authenticate and authorize for initial registration. The NAT ID **must** be unique among all NAT IDs used to register managed appliances to establish trust for the initial communication and to look up the correct registration key.

   Note: At least one of the security appliances, either the Firepower Management Center or the Firepower Threat Defense, must have a public IP address to establish the two-way, SSL-encrypted communication channel between the two appliances.

10. Close the CLI.

    ```
    > exit
    ```

What To Do Next

- Register your device to a Firepower Management Center as described in the next section.

7. Register the Device with the Firepower Management Center and Assign Smart Licenses

Before You Begin

- Set up Smart Licensing on your Firepower Management Center. Make sure you have the following a Cisco Smart Account. You can create one at Cisco Software Central (https://software.cisco.com/).
- Make sure you have a base Firepower Threat Defense license added to your Smart Account; for example, L-ASA5516T-BASE=.

Procedure

1. Log into the Firepower Management Center using an HTTPS connection in a browser, using the hostname or address entered above. For example, https://MC.example.com.

2. Use the Device Management (**Devices** > **Device Management**) page to add the device. For more information, see the online help or the Managing Devices chapter in the *Firepower Management Center Configuration Guide*.
3. Enter the management IP address configured on the device during the CLI setup.
4. Use the same registration key as specified on the device during the CLI setup.
5. Select your **Smart Licensing** options (Threat, URL, Advanced Malware).

   These licenses need to be present in your Smart Account already. You should have a base license for your appliance in your Smart Account.
6. Click **Register** and confirm a successful device registration.

What To Do Next

- If you have a ASA 5506W-X with the built-in wireless access point, enable the access point as described in the next section; or
- Configure policies and device settings for your device.

8. Configure the Wireless Access Point (ASA 5506W-X)

The ASA 5506W-X includes a Cisco Aironet 702i wireless access point integrated into the device. The wireless access point is disabled by default. Connect to the access point web interface so that you can enable the wireless radios and configure the SSID and security settings.

The access point connects internally over the GigabitEthernet1/9 interface. All Wi-Fi clients belong to the GigabitEthernet1/9 network. Your security policy determines how the Wi-Fi network can access any networks on other interfaces. The access point does not contain any external interfaces or switch ports.

The following procedure explains how to configure the access point.

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.

Before You Begin

- Log into the Firepower Management Center that is managing the ASA 5506W-X device. This procedure only covers a small subset of Interface settings. Refrain from setting other parameters at this point.

Procedure

1. Select **Devices > Device Management** and click the edit icon ( ) for your Firepower Threat Defense device.

   The Interfaces tab is selected by default.
2. Click the edit icon ( ) next for the interface you want to edit, in this case GigabitEthernet1/9:
   a. In the Mode drop-down list, choose **None**.
   b. Optionally, add a **Name**. For example, AP-FTD.
   c. Enable the interface by checking the **Enabled** check box.
   d. Add GigabitEthernet1/9 to the same zone as inside interface.

e. Optionally, add a **Description**.

f. Set an IP address. For example, 192.168.10.2-254.

This will provide IP addresses for the access point itself and for any clients on the access point.

g. Click **OK**.

3. Click **Save**.

4. Click **DHCP**.

a. Select the GigabitEthernet1/9 interface in the **Add Server** dialog box.

b. Add the same IP address pool as previously specified for this interface. For example, 192.168.10.2-254.

c. Enable the DHCP server by checking the **Enable DHCP Server** check box.

d. Click **OK**.

5. Click **Save**.

6. Configure the wireless access point.

The wireless access point obtains its address from the DHCP pool defined for the wireless interface. It should get the first address in the pool. If you used the example addresses, this is 192.168.10.2. (Try the next address in the pool if the first one does not work.)

a. Use a new browser window to go to the wireless access point IP address, for example, **http://192.168.10.2**. The access point web interface should appear.

You must be on the inside network, or a network that can route to it, to open this address.

b. Log in with the username **cisco** and password **Cisco**.

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

d. In the **Radio Configuration** area, for each of the **Radio 2.4GHz** and **Radio 5GHz** sections, set at least the following parameters and click **Apply** for each section.

- **SSID**—The Service Set Identifier. This is the name of the wireless network. Users will see this name when selecting a wireless network for their Wi-Fi connection.
- **Broadcast SSID in Beacon**—Select this option.
- **Universal Admin Mode**: **Disable**.
- **Security**—Select whichever security option you want to use.

7. While in the wireless access point web interface, enable the radios.

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

b. Click the **Settings** tab.

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

d. Repeat the process for the 5 GHz radio.

What To Do Next

- Configure policies and device settings for your device. After you add the device to the Firepower Management Center, you can use the Firepower Management Center user interface to configure device management settings and to configure and apply access control policies and other related policies to manage traffic using your Firepower Threat Defense system.

Restore the Wireless Access Point Configuration (ASA 5506W-X)

If you are unable to reach the access point, and the Firepower Threat Defense has the suggested configuration and other networking issues are not found, then you may want to restore the access point default configuration. You must access the Firepower Threat Defense CLI (connect to the console port, or configure Telnet or SSH access).

Procedure

1. From the Firepower Threat Defense CLI, navigate to the system support CLI menu:

   ```
   > system support diagnostic-cli
   ```

   Example:

   ```
   > system support diagnostic-cli
   Attaching to ASA console ... Press 'Ctrl+a then d' to detach.
   Type help or '?' for a list of available commands.
   firepower>
   ```

2. Enter the **enable** command to turn on privileged commands:

   ```
   firepower> enable
   ```

   After issuing the **enable** command, the system will prompt you for a password. By default, the password is blank.

   Example:

   ```
   firepower> enable
   Password: <by default, the password is blank>
   firepower#
   ```

3. Enter the command to restore the access point default configuration:

   ```
   firepower# hw-module module wlan recover configuration
   ```

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

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

You can configure and monitor the wireless access point using the command-line interface (CLI), which you access from the Firepower Threat Defense CLI (connect to the console port, or configure Telnet or SSH access).

Procedure

1. From the Firepower Threat Defense CLI, navigate to the system support CLI menu:

   ```
   > system support diagnostic-cli
   ```

   Example:

   ```
   > system support diagnostic-cli
   Attaching to ASA console ... Press 'Ctrl+a then d' to detach.
   Type help or '?' for a list of available commands.
   firepower>
   ```

2. Enter the **enable** command to turn on privileged commands:

   ```
   firepower> enable
   ```

   After issuing the **enable** command, the system will prompt you for a password. By default, the password is blank.

Example:

```
firepower> enable
Password: <by default, the password is blank>
firepower#
```

3. Session to the access point:

```
firepower# session wlan console
```

Example:

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

ap>
```

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

8. Where to Go Next

- For more information about managing the Firepower Threat Defense with the Firepower Management Center, see the Firepower Management Center configuration guide, or the Firepower Management Center online help.