



Cisco ASA 5508-X and 5516-X Getting Started Guide

Last Modified: 2021-05-26

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CHAPTER 1

Which Operating System and Manager is Right for You?

Your hardware platform can run one of two operating systems. For each operating system, you have a choice of managers. This chapter explains the operating system and manager choices.

- [Operating Systems, on page 1](#)
- [Managers, on page 1](#)

Operating Systems

You can use either ASA or Firepower Threat Defense (FTD) operating systems on your hardware platform:

- **ASA**—The ASA is a traditional, advanced stateful firewall and VPN concentrator.
You may want to use the ASA if you do not need the advanced capabilities of the FTD, or if you need an ASA-only feature that is not yet available on the FTD. Cisco provides ASA-to-FTD migration tools to help you convert your ASA to an FTD if you start with ASA and later reimage to FTD.
- **FTD**—FTD, also known as Firepower NGFW, is a next-generation firewall that combines an advanced stateful firewall, VPN concentrator, and next generation IPS. In other words, the FTD takes the best of ASA functionality and combines it with the best next-generation firewall and IPS functionality.

We recommend using the FTD over the ASA because it contains most of the major functionality of the ASA, plus additional next generation firewall and IPS functionality.

To reimage between the ASA and the FTD, see [Reimage the Cisco ASA or Firepower Threat Defense Device](#).

Managers

The FTD and ASA support multiple managers.

FTD Managers

Table 1: FTD Managers

Manager	Description
Firepower Device Manager (FDM)	<p>FDM is a web-based, simplified, on-device manager. Because it is simplified, some FTD features are not supported using FDM. You should use FDM if you are only managing a small number of devices and don't need a multi-device manager.</p> <p>Note Both FDM and CDO can discover the configuration on the firewall, so you can use FDM and CDO to manage the same firewall. FMC is not compatible with other managers.</p> <p>To get started with FDM, see Firepower Threat Defense Deployment with FDM, on page 5.</p>
Cisco Defense Orchestrator (CDO)	<p>CDO is a simplified, cloud-based multi-device manager. Because it is simplified, some FTD features are not supported using CDO. You should use CDO if you want a multi-device manager that offers a simplified management experience (similar to FDM). And because CDO is cloud-based, there is no overhead of running CDO on your own servers. CDO also manages other security devices, such as ASAs, so you can use a single manager for all of your security devices.</p> <p>Note Both FDM and CDO can discover the configuration on the firewall, so you can use FDM and CDO to manage the same firewall. FMC is not compatible with other managers.</p> <p>CDO is not covered in this guide. To get started with CDO, see the CDO home page.</p>
Firepower Management Center (FMC)	<p>FMC is a powerful, web-based, multi-device manager that runs on its own server hardware, or as a virtual device on a hypervisor. You should use FMC if you want a multi-device manager, and you require all features on the FTD. FMC also provides powerful analysis and monitoring of traffic and events.</p> <p>In 6.7 and later, FMC can manage FTDs from the outside (or other data) interface instead of from the standard Management interface. This feature is useful for remote branch deployments.</p> <p>Note FMC is not compatible with other managers because the FMC owns the FTD configuration, and you are not allowed to configure the FTD directly, bypassing the FMC.</p> <p>To get started with FMC, see Firepower Threat Defense Deployment with FMC, on page 27.</p>
FTD REST API	<p>The FTD REST API lets you automate direct configuration of the FTD. This API is compatible with FDM and CDO use because they can both discover the configuration on the firewall. You cannot use this API if you are managing the FTD using FMC.</p> <p>The FTD REST API is not covered in this guide. For more information, see the FTD REST API guide.</p>

Manager	Description
FMC REST API	<p>The FMC REST API lets you automate configuration of FMC policies that can then be applied to managed FTDs. This API does not manage an FTD directly.</p> <p>The FMC REST API is not covered in this guide. For more information, see the FMC REST API guide.</p>

ASA Managers

Table 2: ASA Managers

Manager	Description
Adaptive Security Device Manager (ASDM)	<p>ASDM is a Java-based, on-device manager that provides full ASA functionality. You should use ASDM if you prefer using a GUI over the CLI, and you only need to manage a small number of ASAs. ASDM can discover the configuration on the firewall, so you can also use the CLI, CDO, or CSM with ASDM.</p> <p>To get started with ASDM, see ASA and ASA FirePOWER Module Deployment with ASDM, on page 63.</p>
CLI	<p>You should use the ASA CLI if you prefer CLIs over GUIs.</p> <p>The CLI is not covered in this guide. For more information, see the ASA configuration guides.</p>
Cisco Defense Orchestrator (CDO)	<p>CDO is a simplified, cloud-based multi-device manager. Because it is simplified, some ASA features are not supported using CDO. You should use CDO if you want a multi-device manager that offers a simplified management experience. And because CDO is cloud-based, there is no overhead of running CDO on your own servers. CDO also manages other security devices, such as FTDs, so you can use a single manager for all of your security devices. CDO can discover the configuration on the firewall, so you can also use the CLI or ASDM.</p> <p>CDO is not covered in this guide. To get started with CDO, see the CDO home page.</p>
Cisco Security Manager (CSM)	<p>CSM is a powerful, multi-device manager that runs on its own server hardware. You should use CSM if you need to manage large numbers of ASAs. CSM can discover the configuration on the firewall, so you can also use the CLI or ASDM. CSM does not support managing FTDs.</p> <p>CSM is not covered in this guide. For more information, see the CSM user guide.</p>
ASA REST API	<p>The ASA REST API lets you automate ASA configuration. However, the API does not include all ASA features, and is no longer being enhanced.</p> <p>The ASA REST API is not covered in this guide. For more information, see the ASA REST API guide.</p>



CHAPTER 2

Firepower Threat Defense Deployment with FDM



Note Firepower version 7.0 is the final supported version for the ASA 5508-X and 5516-X.

Is This Chapter for You?

This chapter explains how to complete the initial set up and configuration of your Firepower Threat Defense (FTD) device using the Firepower Device Manager (FDM) web-based device setup wizard.

FDM lets you configure the basic features of the software that are most commonly used for small networks. It is especially designed for networks that include a single device or just a few, where you do not want to use a high-powered multiple-device manager to control a large network containing many FDM devices.

If you are managing large numbers of devices, or if you want to use the more complex features and configurations that FTD allows, use the Firepower Management Center (FMC) instead.

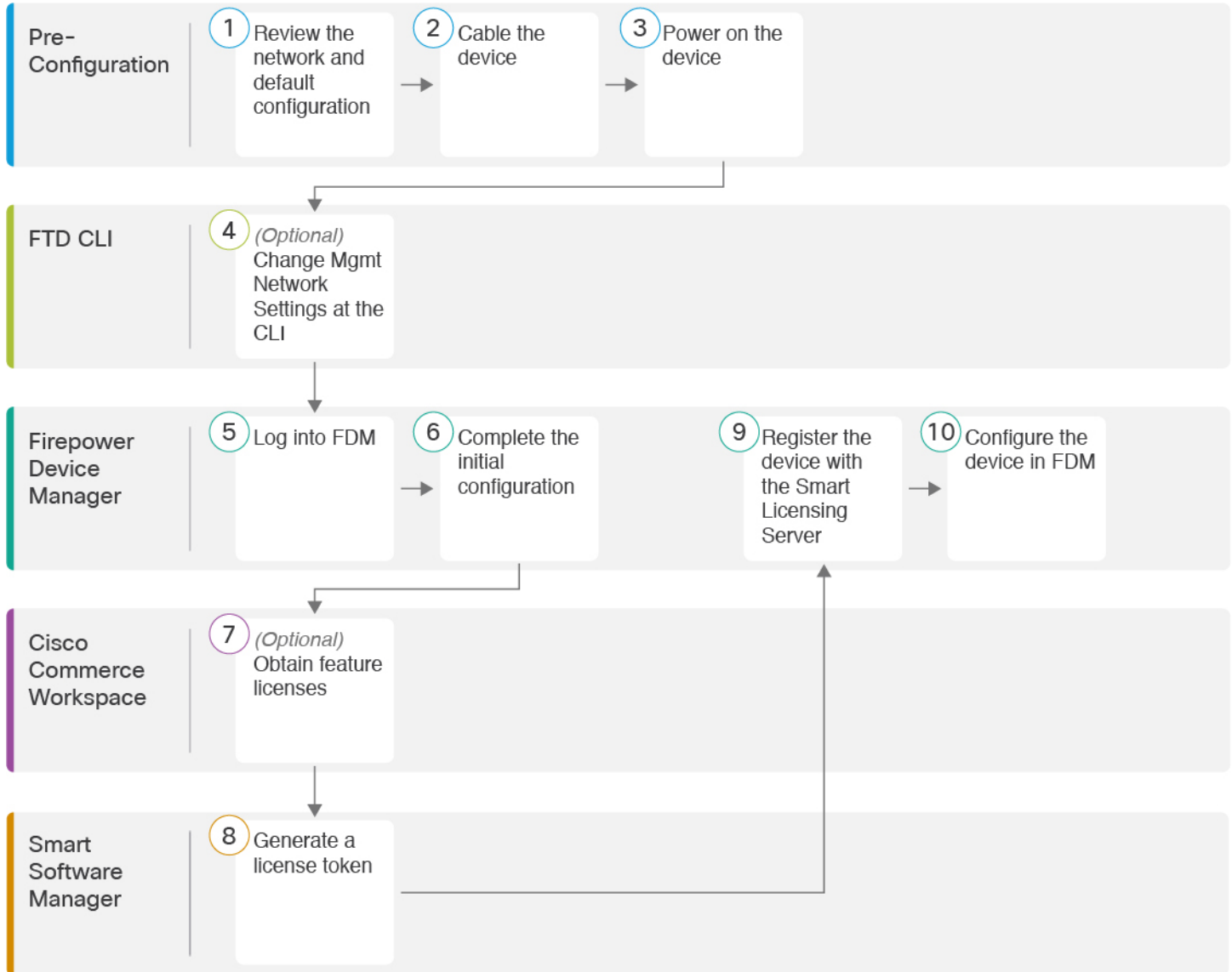
The Cisco ASA 5508-X and 5516-X hardware can run either FTD software or ASA software. Switching between FTD and ASA requires you to reimage the device. See [Reimage the Cisco ASA or Firepower Threat Defense Device](#).

Privacy Collection Statement—The ASA 5508-X and 5516-X does not require or actively collect personally-identifiable information. However, you can use personally-identifiable information in the configuration, for example for usernames. In this case, an administrator might be able to see this information when working with the configuration or when using SNMP.

- [End-to-End Procedure, on page 6](#)
- [Review the Network Deployment and Default Configuration, on page 7](#)
- [Cable the Device, on page 9](#)
- [Power on the Device, on page 10](#)
- [\(Optional\) Change Management Network Settings at the CLI, on page 11](#)
- [Log Into FDM, on page 13](#)
- [Complete the Initial Configuration, on page 13](#)
- [Configure Licensing, on page 15](#)
- [Configure the Firewall in Firepower Device Manager, on page 21](#)
- [Access the Firepower Threat Defense CLI, on page 24](#)
- [Power Off the Device, on page 25](#)
- [What's Next?, on page 26](#)

End-to-End Procedure

See the following tasks to deploy FTD with FDM on your chassis.



1	Pre-Configuration	Review the Network Deployment and Default Configuration, on page 7.
2	Pre-Configuration	Cable the Device, on page 9
3	Pre-Configuration	Power on the Device, on page 10.

4	FTD CLI	(Optional) Change Management Network Settings at the CLI, on page 11.
5	Firepower Device Manager	Log Into FDM, on page 13.
6	Firepower Device Manager	Complete the Initial Configuration, on page 13.
7	Cisco Commerce Workspace	Configure Licensing, on page 15: Obtain license features.
8	Smart Software Manager	Configure Licensing, on page 15: Generate a license token.
9	Firepower Device Manager	Configure Licensing, on page 15: Register the device with the Smart Licensing Server.
10	Firepower Device Manager	Configure the Firewall in Firepower Device Manager, on page 21.

Review the Network Deployment and Default Configuration

You can manage the FTD using FDM from either the Management 1/1 interface or the inside interface. The dedicated Management interface is a special interface with its own network settings.

The following figure shows the recommended network deployment. If you connect the outside interface directly to a cable modem or DSL modem, we recommend that you put the modem into bridge mode so the FTD performs all routing and NAT for your inside networks. If you need to configure PPPoE for the outside interface to connect to your ISP, you can do so after you complete initial setup in FDM.



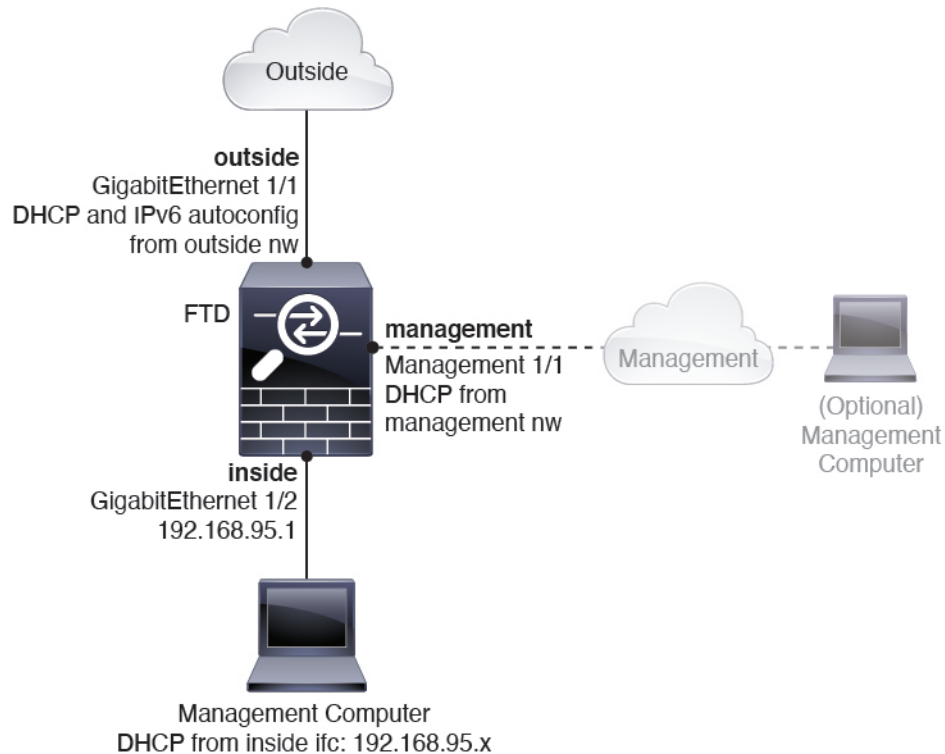
Note If you cannot use the default management IP address (for example, your management network does not include a DHCP server), then you can connect to the console port and perform initial setup at the CLI, including setting the Management IP address, gateway, and other basic networking settings.

If you need to change the inside IP address, you can do so after you complete initial setup in FDM. For example, you may need to change the inside IP address in the following circumstances:

- (7.0 and later) The inside IP address is 192.168.95.1. (6.7 and earlier) The inside IP address is 192.168.1.1. If the outside interface tries to obtain an IP address on the 192.168.1.0 network, which is a common default network, the DHCP lease will fail, and the outside interface will not obtain an IP address. This problem occurs because the FTD cannot have two interfaces on the same network. In this case you must change the inside IP address to be on a new network.
- If you add the FTD to an existing inside network, you will need to change the inside IP address to be on the existing network.

The following figure shows the default network deployment for FTD using FDM with the default configuration.

Figure 1: Suggested Network Deployment



Note For 6.7 and earlier, the GigabitEthernet 1/2 inside IP address is 192.168.1.1.
For 6.5 and earlier, the Management 1/1 default IP address is 192.168.45.45.

Default Configuration

The configuration for the f after initial setup includes the following:

- **inside**—GigabitEthernet 1/2, IP address (7.0 and later) 192.168.95.1; (pre-7.0) 192.168.1.1.
- **outside**—Ethernet 1/1, IP address from IPv4 DHCP and IPv6 autoconfiguration
- **inside**→**outside** traffic flow
- **management**—Management 1/1 (management)
 - (6.6 and later) IP address from DHCP
 - (6.5 and earlier) IP address 192.168.45.45

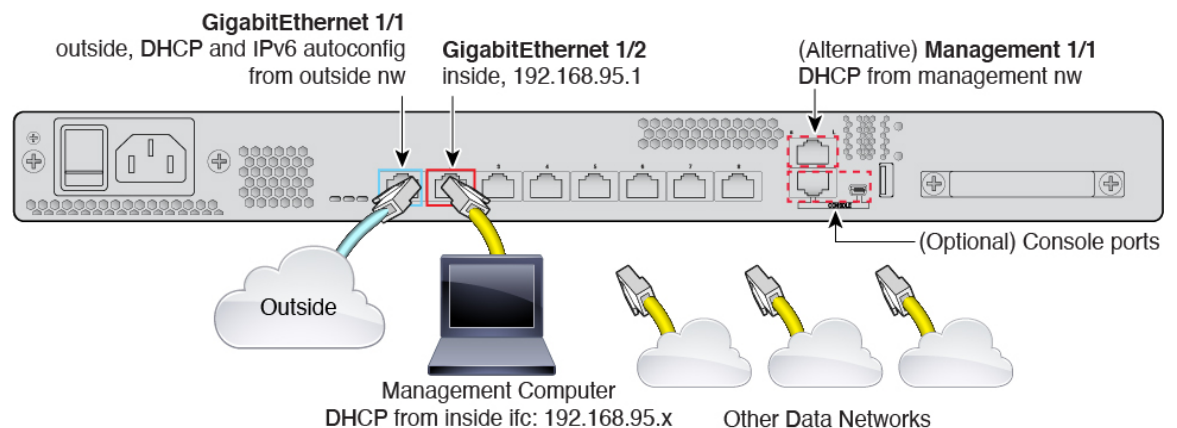


Note The Management 1/1 interface is a special interface separate from data interfaces that is used for management, Smart Licensing, and database updates. The physical interface is shared with a second logical interface, the Diagnostic interface. Diagnostic is a data interface, but is limited to other types of management traffic (to-the-device and from-the-device), such as syslog or SNMP. The Diagnostic interface is not typically used. See the [FDM configuration guide](#) for more information.

- **DNS server for management**—OpenDNS: (IPv4) 208.67.222.222, 208.67.220.220; (IPv6) 2620:119:35::35, or servers you specify during setup. DNS servers obtained from DHCP are never used.
- **NTP**—Cisco NTP servers: 0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org, 2.sourcefire.pool.ntp.org, or servers you specify during setup
- **Default routes**
 - **Data interfaces**—Obtained from outside DHCP, or a gateway IP address you specify during setup
 - **Management interface**—(6.6 and later) Obtained from management DHCP. If you do not receive a gateway, then the default route is over the backplane and through the data interfaces. (6.5 and earlier) Over the backplane and through the data interfaces

Note that the Management interface requires internet access for licensing and updates, either over the backplane or using a separate internet gateway. Note that only traffic originating on the Management interface can go over the backplane; otherwise, Management does not allow through traffic for traffic entering Management from the network.
- **DHCP server**—Enabled on the inside interface and (6.5 and earlier only) management interface
- **FDM access**—All hosts allowed on Management and inside interfaces.
- **NAT**—Interface PAT for all traffic from inside to outside

Cable the Device





Note For 6.7 and earlier, the GigabitEthernet 1/2 inside IP address is 192.168.1.1.
For 6.5 and earlier, the Management 1/1 default IP address is 192.168.45.45.

Manage the ASA 5508-X or 5516-X on either Management 1/1 or GigabitEthernet 1/2. The default configuration also configures GigabitEthernet 1/1 as outside.

Procedure

- Step 1** Connect your management computer to one of the following interfaces:
- GigabitEthernet 1/2—Connect your management computer directly to GigabitEthernet 1/2 for initial configuration, or connect GigabitEthernet 1/2 to your inside network. GigabitEthernet 1/2 has a default IP address (192.168.95.1) and also runs a DHCP server to provide IP addresses to clients (including the management computer), so make sure these settings do not conflict with any existing inside network settings
 - Management 1/1—Connect your management computer to the management network. The Management 1/1 interface obtains an IP address from DHCP, so make sure your network includes a DHCP server.
- If you need to change the Management 1/1 IP address from the default to configure a static IP address, you must also cable your management PC to the console port. See [\(Optional\) Change Management Network Settings at the CLI, on page 11](#).

You can later configure FDM management access from other interfaces; see the [FDM configuration guide](#).

- Step 2** Connect the outside network to the GigabitEthernet 1/1 interface.
- By default, the IP address is obtained using IPv4 DHCP and IPv6 autoconfiguration, but you can set a static address during initial configuration.

- Step 3** Connect other networks to the remaining interfaces.
-

Power on the Device

System power is controlled by a rocker power switch located on the rear of the device.

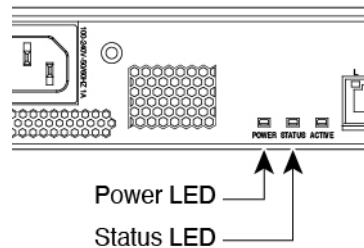
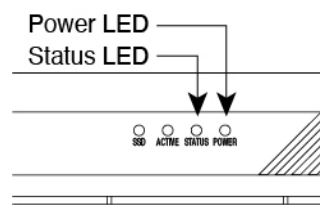
Before you begin

It's important that you provide reliable power for your device (for example, using an uninterruptible power supply (UPS)). Loss of power without first shutting down can cause serious file system damage. There are many processes running in the background all the time, and losing power does not allow the graceful shutdown of your system.

Procedure

- Step 1** Attach the power cord to the device, and connect it to an electrical outlet.

- Step 2** Turn the power on using the standard rocker-type power on/off switch located on the rear of the chassis, adjacent to the power cord.
- Step 3** Check the Power LED on the front or rear of the device; if it is solid green, the device is powered on.

Figure 2: Rear Panel*Figure 3: Front Panel*

- Step 4** Check the Status LED on the front or rear of the device; after it is solid green, the system has passed power-on diagnostics.

(Optional) Change Management Network Settings at the CLI

If you cannot use the default management IP address, then you can connect to the console port and perform initial setup at the CLI, including setting the Management IP address, gateway, and other basic networking settings. You can only configure the Management interface settings; you cannot configure inside or outside interfaces, which you can later configure in the GUI.



Note You cannot repeat the CLI setup script unless you clear the configuration; for example, by reimaging. However, all of these settings can be changed later at the CLI using **configure network** commands. See the [threat defense command reference](#).

Procedure

- Step 1** Connect to the FTD console port. See [Access the Firepower Threat Defense CLI, on page 24](#) for more information.
- Log in with the **admin** user and the default password, **Admin123**.

Note If the password was already changed, and you do not know it, you must reimage the device to reset the password to the default. See the [reimage guide](#) for instructions.

Step 2 The first time you log in to FTD, you are prompted to accept the End User License Agreement (EULA) and to change the admin password. You are then presented with the CLI setup script.

Defaults or previously-entered values appear in brackets. To accept previously entered values, press **Enter**.

See the following guidelines:

- **Enter the IPv4 default gateway for the management interface**—If you set a manual IP address, enter either **data-interfaces** or the IP address of the gateway router. The **data-interfaces** setting sends outbound management traffic over the backplane to exit a data interface. This setting is useful if you do not have a separate Management network that can access the internet. Traffic originating on the Management interface includes license registration and database updates that require internet access. If you use **data-interfaces**, you can still use the FDM (or SSH) on the Management interface if you are directly-connected to the Management network, but for remote management for specific networks or hosts, you should add a static route using the **configure network static-routes** command. Note that FDM management on data interfaces is not affected by this setting. If you use DHCP, the system uses the gateway provided by DHCP and uses the **data-interfaces** as a fallback method if DHCP doesn't provide a gateway.
- **If your networking information has changed, you will need to reconnect**—If you are connected with SSH to the default IP address but you change the IP address at initial setup, you will be disconnected. Reconnect with the new IP address and password. Console connections are not affected.
- **Manage the device locally?**—Enter **yes** to use the FDM or the CDO. A **no** answer means you intend to use the FMC to manage the device.

Example:

```

You must accept the EULA to continue.
Press <ENTER> to display the EULA:
End User License Agreement
[...]

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]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.10.15
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]: 10.10.10.1
Enter a fully qualified hostname for this system [firepower]: ftd-1.cisco.com
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]:
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]: yes

>

```

Step 3 Log into the FDM on the new Management IP address.

Log Into FDM

Log into FDM to configure your FTD.

Before you begin

- Use a current version of Firefox, Chrome, Safari, Edge, or Internet Explorer.

Procedure

- Step 1** Enter the following URL in your browser.
- (7.0 and later) Inside (GigabitEthernet 1/2)—**https://192.168.95.1**.
 - (6.7 and earlier) Inside (GigabitEthernet 1/2)—**https://192.168.1.1**.
 - (6.6 and later) Management—**https://management_ip**. The Management interface is a DHCP client, so the IP address depends on your DHCP server. If you changed the Management IP address at the CLI setup, then enter that address.
 - (6.5 and earlier) Management—**https://192.168.45.45**. If you changed the Management IP address at the CLI setup, then enter that address.
- Step 2** Log in with the username **admin**, and the default password **Admin123**.
-

What to do next

- Run through the FDM setup wizard; see [Complete the Initial Configuration, on page 13](#).

Complete the Initial Configuration

Use the setup wizard when you first log into FDM to complete the initial configuration. After you complete the setup wizard, you should have a functioning device with a few basic policies in place:

- An outside (GigabitEthernet1/1) and an inside interface (GigabitEthernet1/2).
- Security zones for the inside and outside interfaces.
- An access rule trusting all inside to outside traffic.
- An interface NAT rule that translates all inside to outside traffic to unique ports on the IP address of the outside interface.
- A DHCP server running on the inside interface.



Note If you performed the [\(Optional\) Change Management Network Settings at the CLI, on page 11](#) procedure, then some of these tasks, specifically changing the admin password and configuring the outside and management interfaces, should have already been completed.

Procedure

Step 1 You are prompted to read and accept the End User License Agreement and change the admin password. You must complete these steps to continue.

Step 2 Configure the following options for the outside and management interfaces and click **Next**.

Note Your settings are deployed to the device when you click **Next**. The interface will be named “outside” and it will be added to the “outside_zone” security zone. Ensure that your settings are correct.

a) **Outside Interface**—This is the data port that you connected to your gateway router. You cannot select an alternative outside interface during initial device setup. The first data interface is the default outside interface.

Configure IPv4—The IPv4 address for the outside interface. You can use DHCP or manually enter a static IP address, subnet mask, and gateway. You can also select **Off** to not configure an IPv4 address. You cannot configure PPPoE using the setup wizard. PPPoE may be required if the interface is connected to a DSL modem, cable modem, or other connection to your ISP, and your ISP uses PPPoE to provide your IP address. You can configure PPPoE after you complete the wizard.

Configure IPv6—The IPv6 address for the outside interface. You can use DHCP or manually enter a static IP address, prefix, and gateway. You can also select **Off** to not configure an IPv6 address.

b) **Management Interface**

DNS Servers—The DNS server for the system's management address. Enter one or more addresses of DNS servers for name resolution. The default is the OpenDNS public DNS servers. If you edit the fields and want to return to the default, click **Use OpenDNS** to reload the appropriate IP addresses into the fields.

Firewall Hostname—The hostname for the system's management address.

Step 3 Configure the system time settings and click **Next**.

a) **Time Zone**—Select the time zone for the system.

b) **NTP Time Server**—Select whether to use the default NTP servers or to manually enter the addresses of your NTP servers. You can add multiple servers to provide backups.

Step 4 (Optional) Configure the smart licenses for the system.

Your purchase of a Firepower Threat Defense device automatically includes a Base license. All additional licenses are optional.

You must have a smart license account to obtain and apply the licenses that the system requires. Initially, you can use the 90-day evaluation license and set up smart licensing later.

To register the device now, click the link to log into your Smart Software Manager account, and see [Configure Licensing, on page 15](#).

To use the evaluation license, select **Start 90 day evaluation period without registration**.

Step 5 Click **Finish**.

What to do next

- Although you can continue using the evaluation license, we recommend that you register and license your device; see [Configure Licensing, on page 15](#).
- You can also choose to configure the device using FDM; see [Configure the Firewall in Firepower Device Manager, on page 21](#).

Configure Licensing

The FTD uses Smart Software Licensing, which lets you purchase and manage a pool of licenses centrally.

When you register the chassis, the Smart Software Manager issues an ID certificate for communication between the chassis and the Smart Software Manager. It also assigns the chassis to the appropriate virtual account.

For a more detailed overview on Cisco Licensing, go to cisco.com/go/licensingguide

The Base license is included automatically. 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 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. See the following licenses:

- **Threat**—Security Intelligence and Next-Generation IPS
- **Malware**—Malware
- **URL**—URL Filtering
- **RA VPN**—AnyConnect Plus, AnyConnect Apex, or AnyConnect VPN Only

Before you begin

- Have a master account on the [Smart Software Manager](#).

If you do not yet have an account, click the link to [set up a new account](#). The Smart Software Manager lets you create a master account for your organization.

- Your Smart Software Licensing account must qualify for the Strong Encryption (3DES/AES) license to use some features (enabled using the export-compliance flag).

Procedure

Step 1 Make sure your Smart Licensing account contains the available licenses you need.

When you bought your device from Cisco or a reseller, your licenses should have been linked to your Smart Software License account. However, if you need to add licenses yourself, use the **Find Products and Solutions** search field on the [Cisco Commerce Workspace](#). Search for the following license PIDs:

Figure 4: License Search

Note If a PID is not found, you can add the PID manually to your order.

- Threat, Malware, and URL license combination:

- L-ASA5508T-TMC=

- L-ASA5516T-TMC=

When you add one of the above PIDs to your order, you can then choose a term-based subscription corresponding with one of the following PIDs:

- L-ASA5508T-TMC-1Y

- L-ASA5508T-TMC-3Y

- L-ASA5508T-TMC-5Y

- L-ASA5516T-TMC-1Y

- L-ASA5516T-TMC-3Y

- L-ASA5516T-TMC-5Y

- RA VPN—See the [Cisco AnyConnect Ordering Guide](#).

Step 2

In the [Smart Software Manager](#), request and copy a registration token for the virtual account to which you want to add this device.

- Click **Inventory**.

[Cisco Software Central](#) > [Smart Software Licensing](#)

Smart Software Licensing

[Alerts](#) | **[Inventory](#)** | [License Conversion](#) | [Reports](#) | [Email Notification](#) | [Satellites](#) | [Activity](#)

- On the **General** tab, click **New Token**.

General Licenses Product Instances Event Log

Virtual Account

Description: [REDACTED]

Default Virtual Account: No

Product Instance Registration Tokens

The registration tokens below can be used to register new product instances to this virtual account.

New Token...

Token	Expiration Date	Description
NWU1MzY1MzEtZjNmOS00MjF.	2018-Jul-06 14:20:13 (in 354 days)	FTD-5506

- c) On the **Create Registration Token** dialog box enter the following settings, and then click **Create Token**:

Create Registration Token

This dialog will generate the token required to register your product instances with your Smart Account.

Virtual Account: [REDACTED]

Description: [REDACTED]

* Expire After: 30 Days

Enter the value between 1 and 365, but Cisco recommends a maximum of 30 days.

Allow export-controlled functionality on the products registered with this token

Create Token Cancel

- **Description**

- **Expire After**—Cisco recommends 30 days.

- **Allow export-controlled functionality on the products registered with this token**—Enables the export-compliance flag if you are in a country that allows for strong encryption. You must select this option now if you plan to use this functionality. If you enable this functionality later, you will need to re-register your device with a new product key and reload the device. If you do not see this option, your account does not support export-controlled functionality.

The token is added to your inventory.

- d) Click the arrow icon to the right of the token to open the **Token** dialog box so you can copy the token ID to your clipboard. Keep this token ready for later in the procedure when you need to register the FTD.

Figure 5: View Token

General Licenses Product Instances Event Log

Virtual Account

Description: [Redacted]

Default Virtual Account: No

Product Instance Registration Tokens

The registration tokens below can be used to register new product instances to this virtual account.

New Token...

Token	Expiration Date	Description	Export-Controlled	Created By	Actions
MJM3ZjYhYtIiZGQ4OS00Yjk2LT...	2017-Aug-16 19:41:53 (in 30 days)	ASA FP 2110 1	Allowed	[Redacted]	Actions

Figure 6: Copy Token

Token ? X

MJM3ZjYhYtIiZGQ4OS00Yjk2LTgzMGltMThmZTUyYjkyNmVhLTE1MDI5MTI1%0AMTMxMzh8YzdQdmgzMjA2VmFJN2dYQjI5QWRhOEpscDU4cWl5NFNWRUtsa2wz%0AMNdnST0%3D%0A

Press ctrl + c to copy selected text to clipboard.

MJM3ZjYhYtIiZGQ4OS00Yjk2LT... 2017-Aug-16 19:41:53

Step 3 In the FDM, click **Device**, and then in the **Smart License** summary, click **View Configuration**. You see the **Smart License** page.

Step 4 Click **Register Device**.

Device Summary

Smart License

LICENSE ISSUE
EVALUATION PERIOD
You are in Evaluation mode now.

69/90 days left. REGISTER DEVICE

Then follow the instructions on the **Smart License Registration** dialog box to paste in your token:

Smart License Registration
✕

- 1 Create or log in into your [Cisco Smart Software Manager](#) account.
 - 2 On your assigned virtual account, under “General tab”, click on “New Token” to create token.
 - 3 Copy the token and paste it here:

MGY2NzMwOGitODJiZi00NzFiLWJiNiltYWMwNzU0ODY2ZGVlTE1NlUz
 Nzlv%0AODg5Mzh8SUQ5Vm5XbzZiSmN5M3I6K3owZ3ovVmpmc3Vtal
 JLQ2FFeGhFWmlW%0AWC9WTT0%3D%0A
 - 4 Select Region

When you register the device, you are also registered with Cisco Security Services Exchange (SSE). Please select the region in which your device is operating. You will be able to see your device in the device list of the regional SSE portal.

Region

SSE US Region
▼
i
 - 5 Cisco Success Network

Cisco Success Network enablement provides usage information and statistics to Cisco which are essential for Cisco to provide technical support. This information also allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product in your network.

Check out the [Sample Data](#) that will be sent to Cisco. [See more](#) ▼

Enable Cisco Success Network

CANCEL
REGISTER DEVICE

Step 5 Click **Register Device**.

You return to the **Smart License** page. While the device registers, you see the following message:

Registration request sent on 10 Jul 2019. Please wait. Normally, it takes about one minute to complete the registration. You can check the task status in [Task List](#). Refresh this page to see the updated status.

After the device successfully registers and you refresh the page, you see the following:

Device Summary

Smart License

✓
CONNECTED
 SUFFICIENT LICENSE

Last sync: 10 Jul 2019 11:39 AM
 Next sync: 10 Jul 2019 11:49 AM

i

Step 6 Click the **Enable/Disable** control for each optional license as desired.

SUBSCRIPTION LICENSES INCLUDED

Threat ENABLE

Disabled by user

This License allows you to perform intrusion detection and prevention and file control. You must have this license to apply intrusion policies in access rules. You also must have this license to apply file policies that control files based on file type.

Includes: Intrusion Policy

Malware ENABLE

Disabled by user

This License allows you to perform Cisco Advanced Malware Protection (AMP) with AMP for Firepower and AMP Threat Grid. You must have this license to apply file policies that detect and block malware in files transmitted over your network.

Includes: File Policy

URL License ENABLE

Disabled by user

This license allows you to control web access based on URL categories and reputations, rather than by individual URL alone. You must have this license to deploy access rules that filter web traffic based on category and reputation.

Includes: URL Reputation

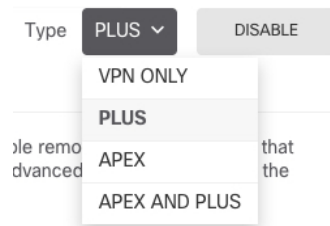
RA VPN License Type PLUS ▾ ENABLE

Disabled by user

Please select the license type that you purchased to enable remote access VPN. Note that Firepower Device Manager does not support any of the advanced features covered by the Apex license.

Includes: RA-VPN

- **Enable**—Registers the license with your Cisco Smart Software Manager account and enables the controlled features. You can now configure and deploy policies controlled by the license.
- **Disable**—Unregisters the license with your Cisco Smart Software Manager account and disables the controlled features. You cannot configure the features in new policies, nor can you deploy policies that use the feature.
- If you enabled the **RA VPN** license, select the type of license you want to use: **Plus**, **Apex**, **VPN Only**, or **Plus and Apex**.



After you enable features, if you do not have the licenses in your account, you will see the following non-compliance message after you refresh the page:

Device Summary

Smart License

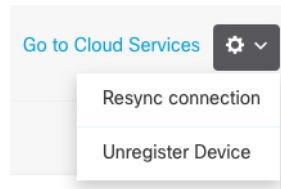
LICENSE ISSUE Last sync: 10 Jul 2019 11:47 AM

OUT OF COMPLIANCE Next sync: 10 Jul 2019 11:57 AM

There is no available license for the device. Licensed features continue to work. However, you must either purchase or free up additional licenses to be in compliance.

[GO TO LICENSE MANAGER](#) [Need help?](#)

- Step 7** Choose **Resync Connection** from the gear drop-down list to synchronize license information with Cisco Smart Software Manager.



Configure the Firewall in Firepower Device Manager

The following steps provide an overview of additional features you might want to configure. Please click the help button (?) on a page to get detailed information about each step.

Procedure

Step 1 If you wired other interfaces, choose **Device**, and then click the link in the **Interfaces** summary.

Click the edit icon (🔗) for each interface to set the mode and define the IP address and other settings.

The following example configures an interface to be used as a “demilitarized zone” (DMZ), where you place publicly-accessible assets such as your web server. Click **Save** when you are finished.

Figure 7: Edit Interface

 A screenshot of the "Edit Physical Interface" configuration page. The page has a blue header with the title "Edit Physical Interface". Below the header, there are several fields:

- Interface Name:** A text input field containing "dmz".
- Status:** A toggle switch that is currently turned on (blue).
- Description:** A large, empty text area.
- Navigation tabs:** Three tabs are visible: "IPv4 Address" (selected), "IPv6 Address", and "Advanced Options".
- Type:** A dropdown menu set to "Static".
- IP Address and Subnet Mask:** Two input fields. The first contains "192.168.6.1" and the second contains "24".
- Example text:** Below the IP fields, there is small text: "e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0".

Step 2 If you configured new interfaces, choose **Objects**, then select **Security Zones** from the table of contents.

Edit or create new zones as appropriate. Each interface must belong to a zone, because you configure policies based on security zones, not interfaces. You cannot put the interfaces in zones when configuring them, so you must always edit the zone objects after creating new interfaces or changing the purpose of existing interfaces.

The following example shows how to create a new dmz-zone for the dmz interface.

Figure 8: Security Zone Object

Step 3

If you want internal clients to use DHCP to obtain an IP address from the device, choose **Device > System Settings > DHCP Server**, then select the **DHCP Servers** tab.

There is already a DHCP server configured for the inside interface, but you can edit the address pool or even delete it. If you configured other inside interfaces, it is very typical to set up a DHCP server on those interfaces. Click + to configure the server and address pool for each inside interface.

You can also fine-tune the WINS and DNS list supplied to clients on the **Configuration** tab. The following example shows how to set up a DHCP server on the inside2 interface with the address pool 192.168.4.50-192.168.4.240.

Figure 9: DHCP Server

Step 4

Choose **Device**, then click **View Configuration** (or **Create First Static Route**) in the **Routing** group and configure a default route.

The default route normally points to the upstream or ISP router that resides off the outside interface. A default IPv4 route is for any-ipv4 (0.0.0.0/0), whereas a default IPv6 route is for any-ipv6 (::0/0). Create routes for each IP version you use. If you use DHCP to obtain an address for the outside interface, you might already have the default routes that you need.

Note The routes you define on this page are for the data interfaces only. They do not impact the management interface. Set the management gateway on **Device > System Settings > Management Interface**.

The following example shows a default route for IPv4. In this example, `isp-gateway` is a network object that identifies the IP address of the ISP gateway (you must obtain the address from your ISP). You can create this object by clicking **Create New Network** at the bottom of the **Gateway** drop-down list.

Figure 10: Default Route

The screenshot shows the 'Add Static Route' configuration interface. It includes the following fields and options:

- Protocol:** Radio buttons for IPv4 (selected) and IPv6.
- Gateway:** A text input field containing 'isp-gateway'.
- Interface:** A text input field containing 'outside'.
- Metric:** A text input field containing '1'.
- Networks:** A '+' icon and a text input field containing 'any-ipv4'.

Step 5 Choose **Policies** and configure the security policies for the network.

The device setup wizard enables traffic flow between the inside-zone and outside-zone, and interface NAT for all interfaces when going to the outside interface. Even if you configure new interfaces, if you add them to the inside-zone object, the access control rule automatically applies to them.

However, if you have multiple inside interfaces, you need an access control rule to allow traffic flow from inside-zone to inside-zone. If you add other security zones, you need rules to allow traffic to and from those zones. These would be your minimum changes.

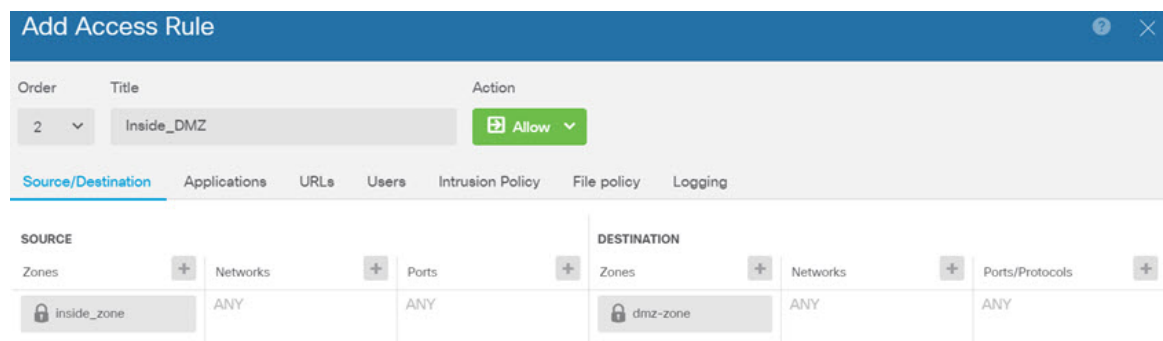
In addition, you can configure other policies to provide additional services, and fine-tune NAT and access rules to get the results that your organization requires. You can configure the following policies:

- **SSL Decryption**—If you want to inspect encrypted connections (such as HTTPS) for intrusions, malware, and so forth, you must decrypt the connections. Use the SSL decryption policy to determine which connections need to be decrypted. The system re-encrypts the connection after inspecting it.
- **Identity**—If you want to correlate network activity to individual users, or control network access based on user or user group membership, use the identity policy to determine the user associated with a given source IP address.
- **Security Intelligence**—Use the Security Intelligence policy to quickly drop connections from or to blacklisted IP addresses or URLs. By blacklisting known bad sites, you do not need to account for them in your access control policy. Cisco provides regularly updated feeds of known bad addresses and URLs so that the Security Intelligence blacklist updates dynamically. Using feeds, you do not need to edit the policy to add or remove items in the blacklist.
- **NAT (Network Address Translation)**—Use the NAT policy to convert internal IP addresses to externally routeable addresses.

- **Access Control**—Use the access control policy to determine which connections are allowed on the network. You can filter by security zone, IP address, protocol, port, application, URL, user or user group. You also apply intrusion and file (malware) policies using access control rules. Use this policy to implement URL filtering.
- **Intrusion**—Use the intrusion policies to inspect for known threats. Although you apply intrusion policies using access control rules, you can edit the intrusion policies to selectively enable or disable specific intrusion rules.


The following example shows how to allow traffic between the inside-zone and dmz-zone in the access control policy. In this example, no options are set on any of the other tabs except for **Logging**, where **At End of Connection** is selected.

Figure 11: Access Control Policy



- Step 6** Choose **Device**, then click **View Configuration** in the **Updates** group and configure the update schedules for the system databases.

If you are using intrusion policies, set up regular updates for the Rules and VDB databases. If you use Security Intelligence feeds, set an update schedule for them. If you use geolocation in any security policies as matching criteria, set an update schedule for that database.

- Step 7** Click the **Deploy** button in the menu, then click the Deploy Now button (), to deploy your changes to the device.

Changes are not active on the device until you deploy them.

Access the Firepower Threat Defense CLI

Use the command-line interface (CLI) to set up the system and do basic system troubleshooting. You cannot configure policies through a CLI session. You can access the CLI by connecting to the console port.

You can SSH to the management interface of the FTD device. You can also connect to the address on a data interface if you open the interface for SSH connections. SSH access to data interfaces is disabled by default.

Procedure

- Step 1** To log into the CLI, connect your management computer to the console port.. The ASA 5508-X and 5516-X ship with a USB A-to-B serial cable. Be sure to install any necessary USB serial drivers for your operating system (see the [hardware guide](#)). Use the following serial settings:
- 9600 baud
 - 8 data bits
 - No parity
 - 1 stop bit
- Step 2** Log in to the FTD CLI using the **admin** username and the password you set at initial setup (the default is **Admin123**).
- After logging in, for information on the commands available in the CLI, enter **help** or **?**. For usage information, see the [Cisco Firepower Threat Defense Command Reference](#).
-

Power Off the Device

It's important that you shut down your system properly. Simply unplugging the power or pressing the power switch can cause serious file system damage. Remember that there are many processes running in the background all the time, and unplugging or shutting off the power does not allow the graceful shutdown of your Firepower system.

Procedure

- Step 1** Connect to the console port to access the FTD CLI, and then shut down the FTD.

shutdown

Example:

```
> shutdown
This command will shutdown the system. Continue?
Please enter 'YES' or 'NO': yes
INIT: Stopping Cisco Threat Defense.....ok
Shutting down sfid... [ OK ]
Clearing static routes
Unconfiguring default route [ OK ]
Unconfiguring address on br1 [ OK ]
Unconfiguring IPv6 [ OK ]
Downing interface [ OK ]
Stopping xinetd:
Stopping nscd... [ OK ]
Stopping system log daemon... [ OK ]
Stopping Threat Defense ...
Stopping system message bus: dbus. [ OK ]
Un-mounting disk partitions ...
device-mapper: remove ioctl on root failed: Device or resource busy
```

```
[...]  
mdadm: Cannot get exclusive access to /dev/md0:Perhaps a running process, mounted filesystem  
or active volume group?  
Stopping OpenBSD Secure Shell server: sshd  
stopped /usr/sbin/sshd (pid 3520)  
done.  
Stopping Advanced Configuration and Power Interface daemon: stopped /usr/sbin/acpid (pid  
3525)  
acpid.  
Stopping system message bus: dbus.  
Stopping internet superserver: xinetd.  
no /etc/sysconfig/kdump.conf  
Deconfiguring network interfaces... ifdown: interface br1 not configured  
done.  
SSP-Security-Module is shutting down ...  
Sending ALL processes the TERM signal ...  
acpid: exiting  
Sending ALL processes the KILL signal ...  
Deactivating swap...  
Unmounting local filesystems...  
  
Firepower Threat Defense stopped.  
It is safe to power off now.  
  
Do you want to reboot instead? [y/N]
```

- Step 2** After the FTD shuts down, and the console shows that "It is safe to power off now", you can then turn off the power switch and unplug the power to physically remove power from the chassis if necessary.
- Alternatively, you can reboot the system by typing `y` at the prompt.
-

What's Next?

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

For information related to using FDM, see [Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager](#).



CHAPTER 3

Firepower Threat Defense Deployment with FMC



Note Firepower version 7.0 is the final supported version for the ASA 5508-X and 5516-X.

Is This Chapter for You?

This chapter explains how to complete the initial configuration of your Firepower Threat Defense (FTD) and how to register the device to a Firepower Management Center (FMC). In a typical deployment on a large network, you install multiple managed devices on network segments. Each device controls, inspects, monitors, and analyzes traffic, and then reports to a managing FMC. The FMC provides a centralized management console with a web interface that you can use to perform administrative, management, analysis, and reporting tasks in service to securing your local network.

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 FMC, you can use the integrated Firepower Device Manager (FDM). Use the FDM web-based device setup wizard to configure the basic features of the software that are most commonly used for small network deployments.



Note The Cisco ASA 5508-X and 5516-X can run either FTD software or ASA software. Switching between FTD and ASA requires you to reimage the device. See [Reimage the Cisco ASA or Firepower Threat Defense Device](#).



Note **Privacy Collection Statement**—The ASA 5508-X and 5516-X do not require or actively collect personally-identifiable information. However, you can use personally-identifiable information in the configuration, for example for usernames. In this case, an administrator might be able to see this information when working with the configuration or when using SNMP.

- [Before You Start](#), on page 28
- [End-to-End Procedure](#), on page 28
- [Review the Network Deployment](#), on page 29
- [Cable the Device](#), on page 34
- [Power on the Device](#), on page 38
- [Complete the FTD Initial Configuration Using the CLI](#), on page 39

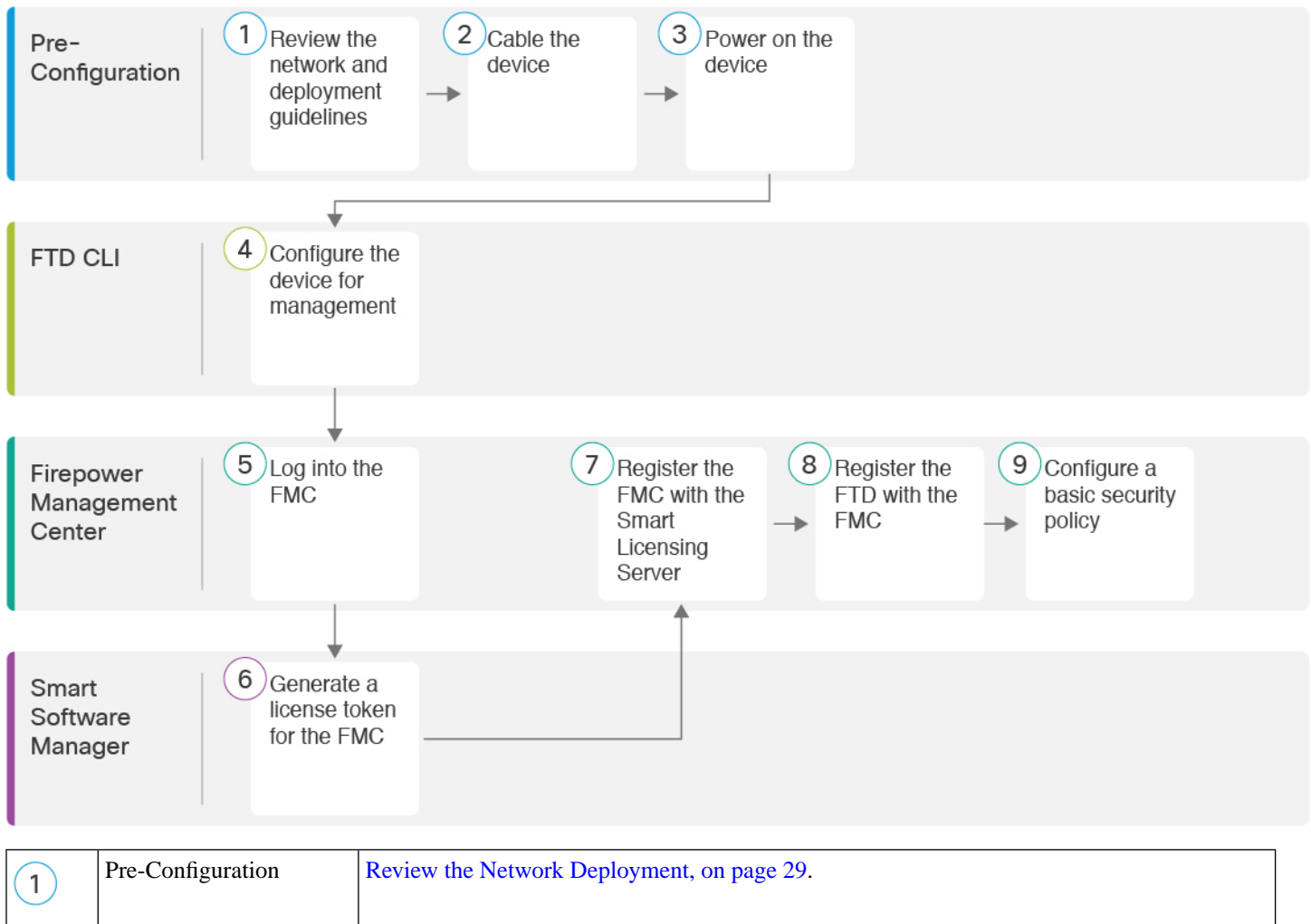
- [Log Into the Firepower Management Center](#), on page 44
- [Obtain Licenses for the FMC](#), on page 45
- [Register the FTD with the FMC](#), on page 46
- [Configure a Basic Security Policy](#), on page 49
- [Access the Firepower Threat Defense CLI](#), on page 59
- [Power Off the Device](#), on page 59
- [What's Next?](#), on page 61

Before You Start

Deploy and perform initial configuration of the FMC. See the [FMC getting started guide](#).

End-to-End Procedure

See the following tasks to deploy the FTD with FMC on your chassis.



2	Pre-Configuration	Cable the Device, on page 34.
3	Pre-Configuration	Power on the Device, on page 38.
4	FTD CLI	Complete the FTD Initial Configuration Using the CLI, on page 39.
5	Firepower Management Center	Log Into the Firepower Management Center, on page 44.
6	Smart Software Manager	Obtain Licenses for the FMC, on page 45: Generate a license token for the FMC.
7	Firepower Management Center	Obtain Licenses for the FMC, on page 45: Register the FMC with the Smart Licensing server.
8	Firepower Management Center	Register the FTD with the FMC, on page 46.
9	Firepower Management Center	Configure a Basic Security Policy, on page 49.

Review the Network Deployment

You can manage the FTD using FMC from the Management 1/1 interface, or in 6.7 and later, a data interface. By default, the Management 1/1 interface is enabled and configured as a DHCP client. You can configure the Management interface and an FMC access data interface during initial setup at the console port. You can configure other data interfaces after you connect the FTD to the FMC.



Note FMC access from a data interface has the following limitations:

- You can only enable FMC access on one physical, data interface. You cannot use a subinterface or EtherChannel.
- This interface cannot be management-only.
- Routed firewall mode only, using a routed interface.
- High Availability is not supported. You must use the Management interface in this case.
- PPPoE is not supported. If your ISP requires PPPoE, you will have to put a router with PPPoE support between the FTD and the WAN modem.
- The interface must be in the global VRF only.
- You cannot use separate management and event-only interfaces.
- SSH is not enabled by default for data interfaces, so you will have to enable SSH later using FMC. Because the Management interface gateway will be changed to be the data interfaces, you also cannot SSH to the Management interface from a remote network unless you add a static route for the Management interface using the **configure network static-routes** command.



Note In 6.5 and earlier, the Management interface is configured with an IP address (192.168.45.45).

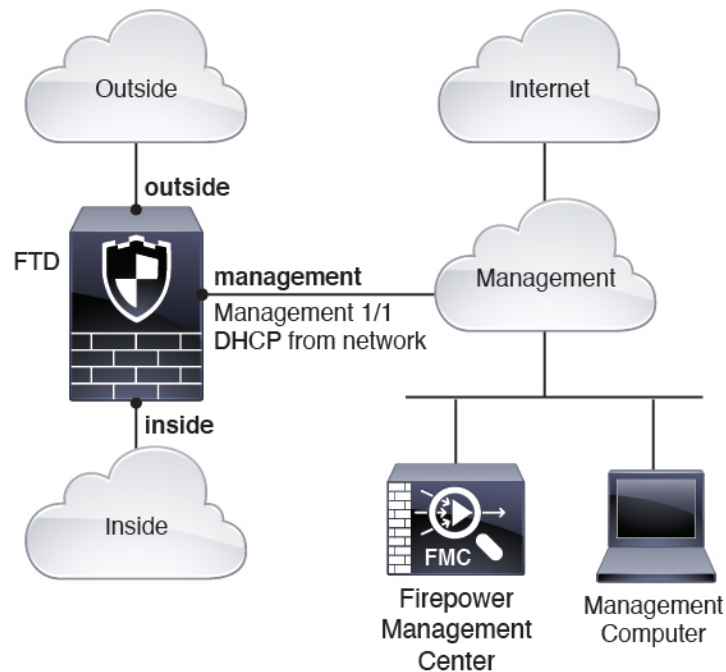
See the following sample network deployments for ideas on how to place your FTD device in your network.

Separate Management Network

Both the FMC and FTD require internet access from management for licensing and updates.

The following figure shows a possible network deployment for the ASA 5508-X or 5516-X where the FMC and management computer connect to the management network. The management network has a path to the internet for licensing and updates.

Figure 12: Separate Management Network



6.7 and Later Remote Management Deployment

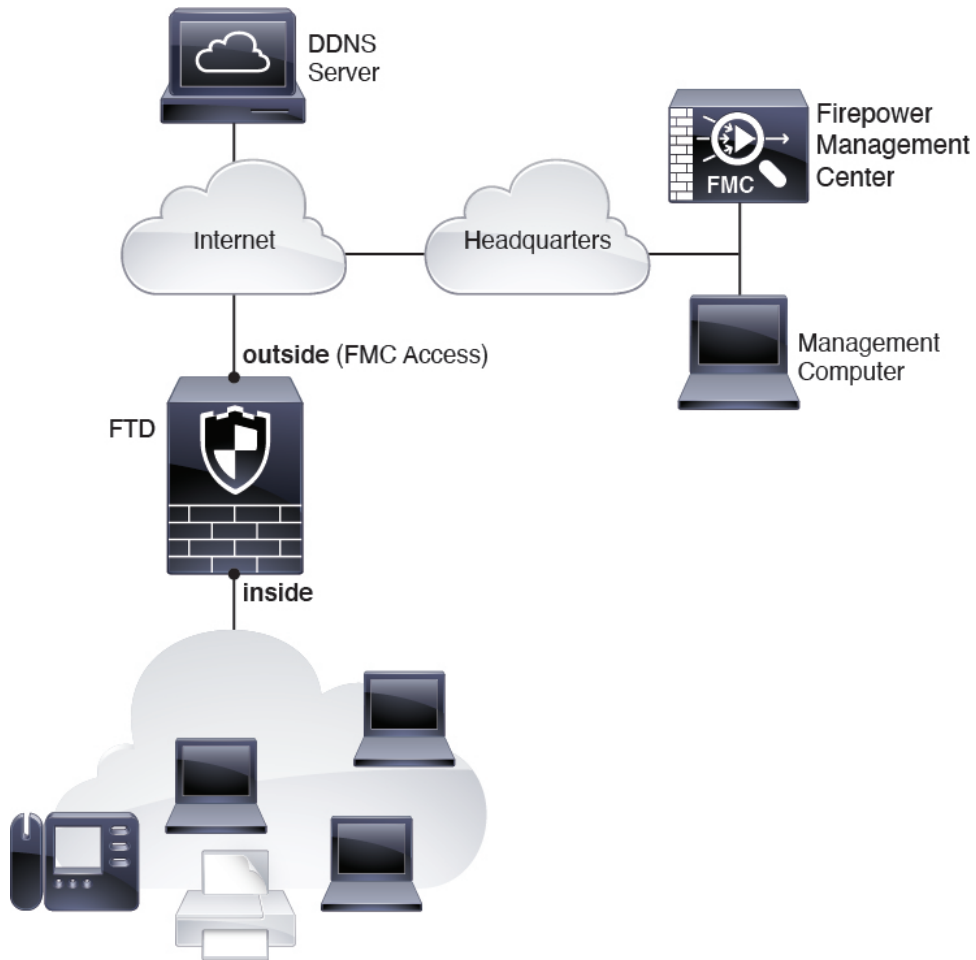


Note For a remote branch setup, we recommend that you use the [standalone document](#) specific to that deployment.

The following figure shows the recommended network deployment for the ASA 5508-X or 5516-X using the outside interface for management. This scenario is ideal for managing branch offices from a central headquarters. You can perform initial setup of the FTD at headquarters and then send a pre-configured device to a branch location.

Either the FTD or FMC needs a public IP address or hostname. If the FTD receives a public IP address using DHCP, then you can optionally configure Dynamic DNS (DDNS) for the outside interface. DDNS ensures the FMC can reach the FTD at its Fully-Qualified Domain Name (FQDN) if the FTD's IP address changes. If the FTD receives a private IP address, then the FMC needs to have a public IP address or hostname.

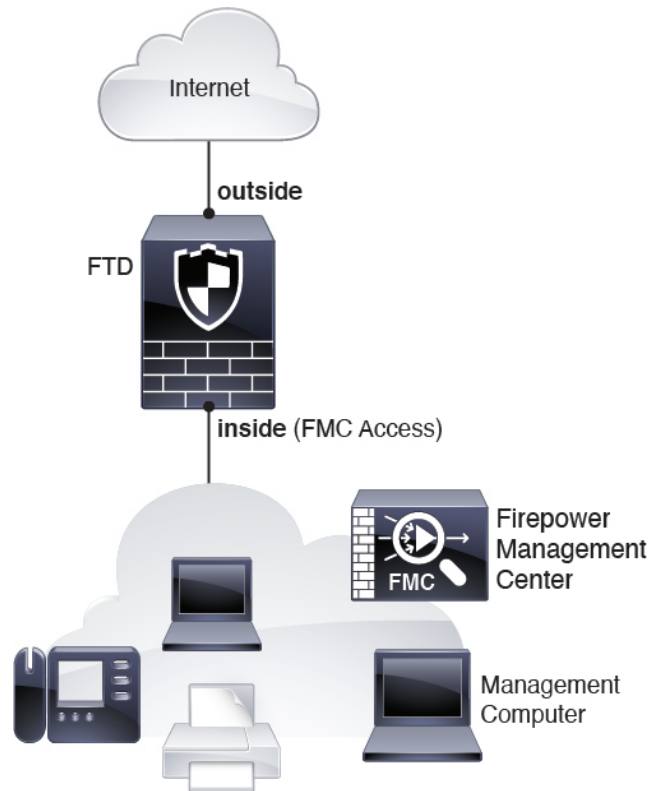
Figure 13: Remote Management Deployment



6.7 and Later Inside Management Deployment

The following figure shows the recommended network deployment for the ASA 5508-X or 5516-X using the inside interface for management.

Figure 14: Inside Management Deployment



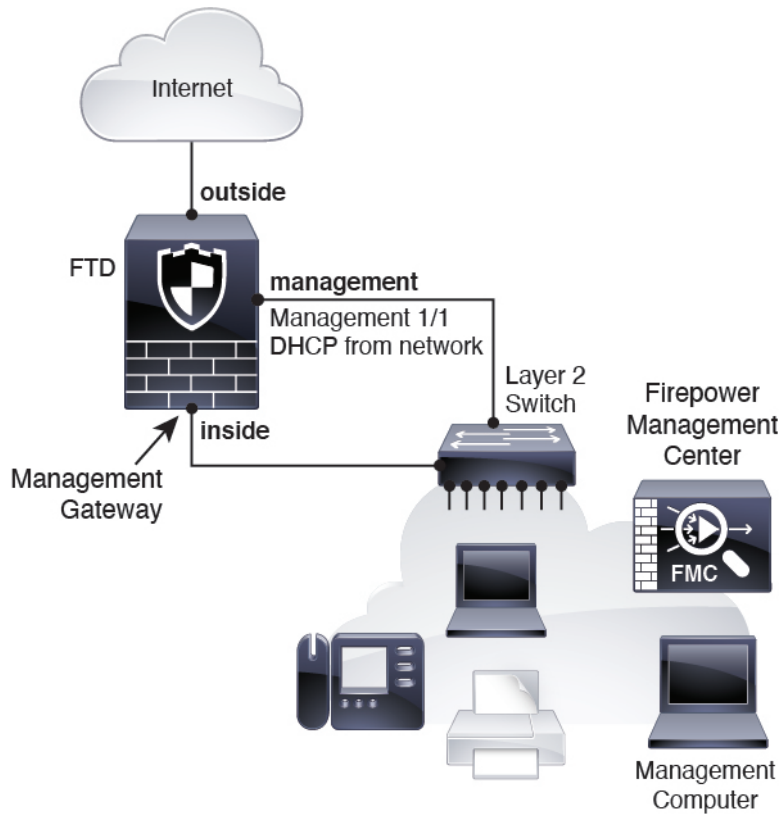
6.6 and Earlier Edge Network Deployment

The FMC can only communicate with the FTD on the management interface in 6.6 and earlier. Moreover, both the FMC and FTD require internet access from management for licensing and updates.

The following figure shows a possible network deployment for the ASA 5508-X or 5516-X where the ASA acts as the internet gateway for the FMC and FTD management. You can also use this scenario in 6.7 and later for a High Availability deployment, for example.

In the following diagram, the ASA 5508-X or 5516-X acts as the internet gateway for the management interface and the FMC by connecting Management 1/1 to an inside interface through a Layer 2 switch, and by connecting the FMC and management computer to the switch. (This direct connection is allowed because the management interface is separate from the other interfaces on the FTD.)

Figure 15: Edge Network Deployment



Cable the Device

To cable one of the above scenarios on the ASA 5508-X or 5516-X, see the following steps.



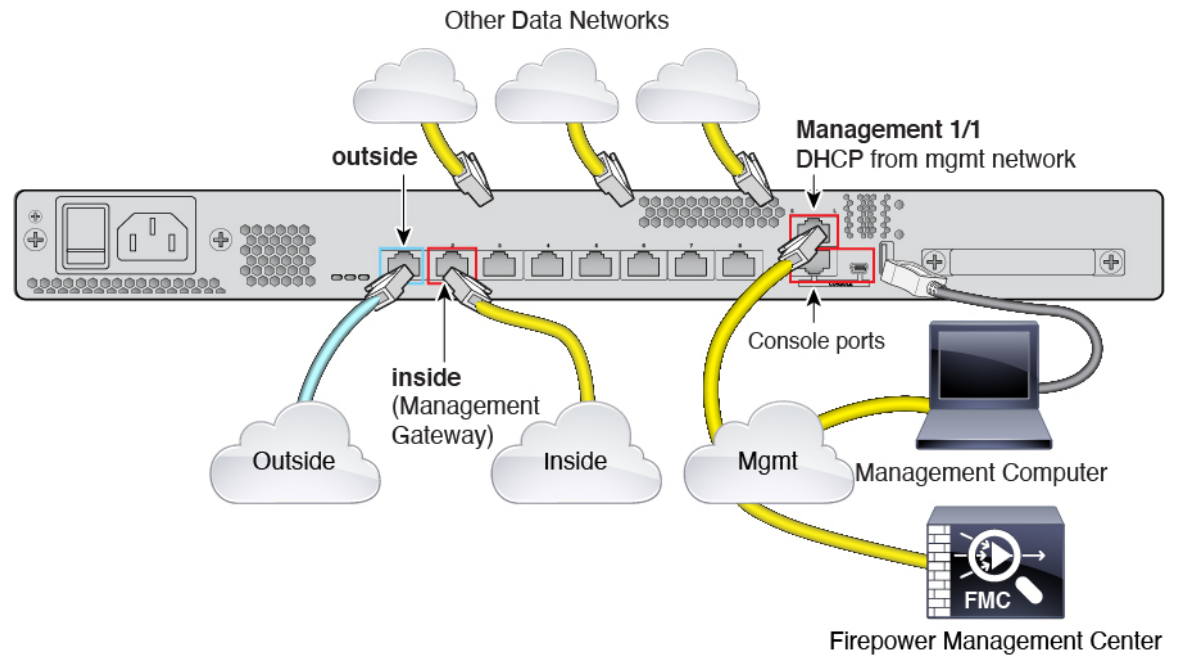
Note

Other topologies can be used, and your deployment will vary depending on your basic logical network connectivity, ports, addressing, and configuration requirements.

Procedure

Step 1 Cable for a separate management network.

Figure 16: Cabling a Separate Management Network

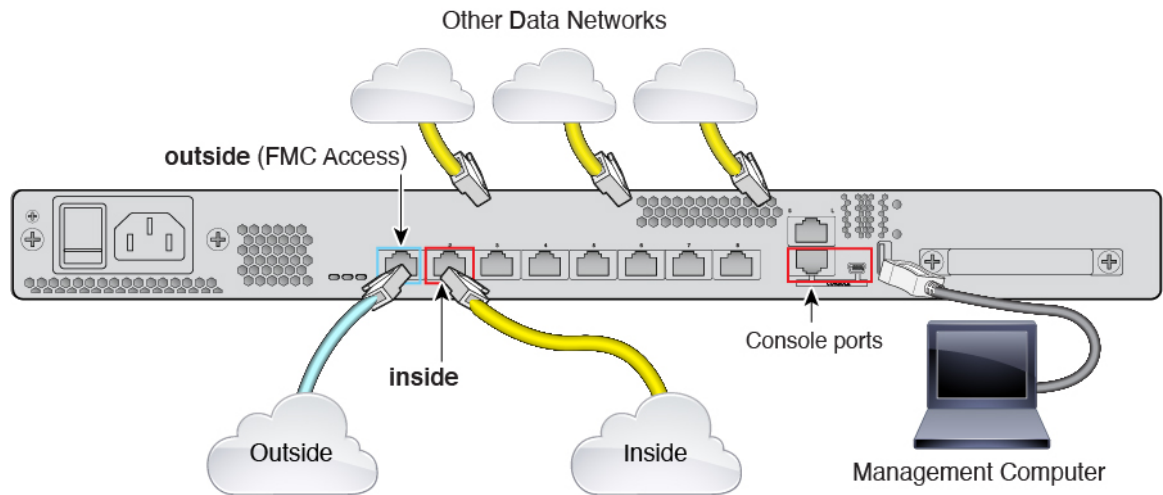


Note For version 6.5 and earlier, the Management 1/1 default IP address is 192.168.45.45.

- a) Cable the following to your management network:
 - Management 1/1 interface
 - Firepower Management Center
 - Management computer
- b) Connect the management computer to the console port. You need to use the console port to access the CLI for initial setup if you do not use SSH to the Management interface.
- c) Connect the inside interface (for example, GigabitEthernet 1/2) to your inside router.
- d) Connect the outside interface (for example, GigabitEthernet 1/1) to your outside router.
- e) Connect other networks to the remaining interfaces.

Step 2 (6.7 and later) Cable for a remote management deployment:

Figure 17: Cabling a Remote Management Deployment



The FMC and your management computer reside at a remote headquarters, and can reach the FTD over the internet.

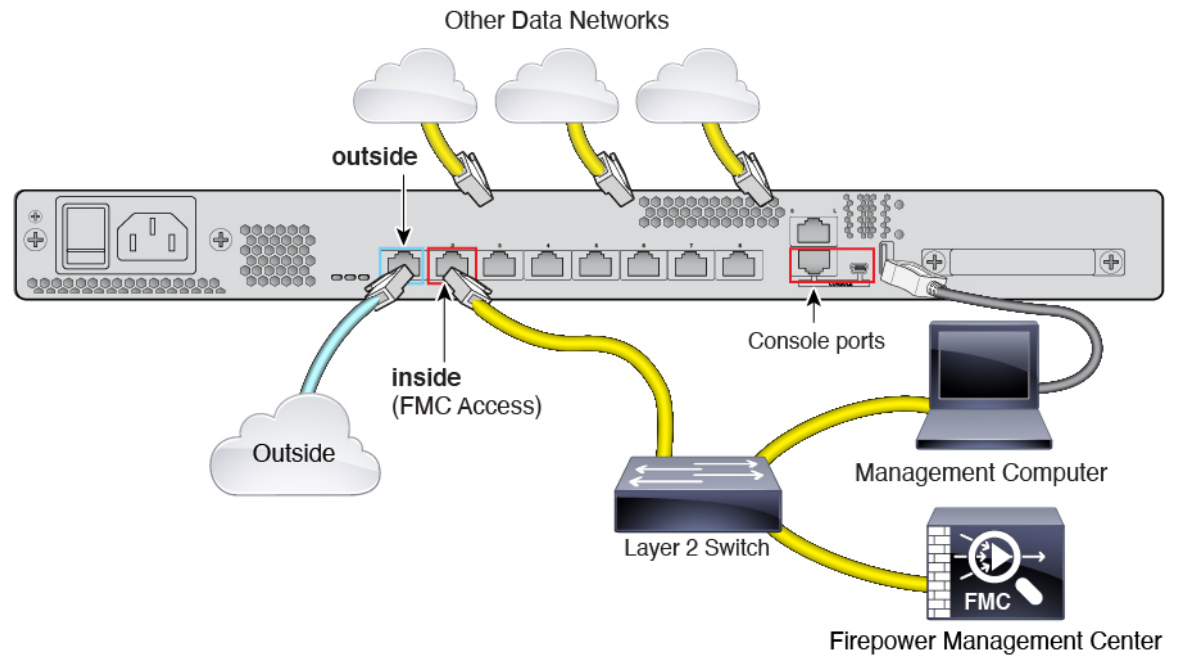
- a) Connect the management computer to the console port. You need to use the console port to access the CLI for initial setup.

You can perform initial CLI setup at headquarters, and then send the FTD to the remote branch office. At the branch office, the console connection is not required for everyday use; it may be required for troubleshooting purposes.

- b) Cable your inside network (for example, GigabitEthernet 1/2).
- c) Connect the outside interface (for example, GigabitEthernet 1/1) to your outside router.
- d) Connect other networks to the remaining interfaces.

Step 3 (6.7 and later) Cable for an inside management deployment:

Figure 18: Cabling an Inside Management Deployment

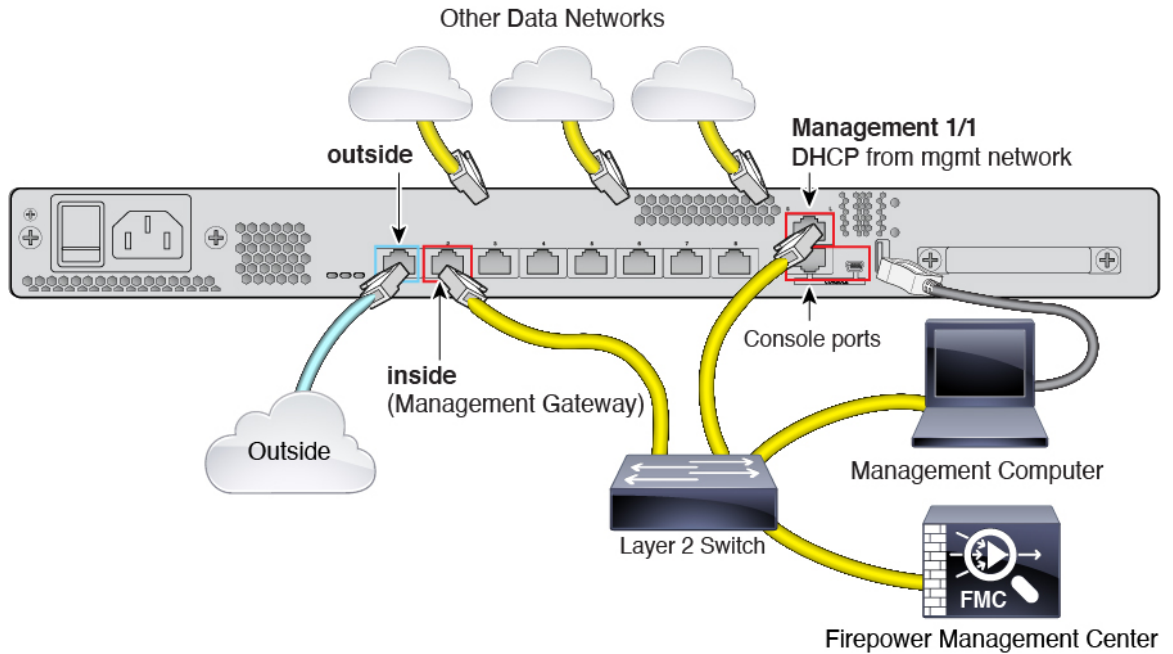


The FMC and your management computer reside on the inside network with your other inside end points.

- a) Connect the management computer to the console port. You need to use the console port to access the CLI for initial setup.
- b) Cable the following to the inside network (for example, GigabitEthernet 1/2):
 - Firepower Management Center
 - Management computer
- c) Connect the outside interface (for example, GigabitEthernet 1/1) to your outside router.
- d) Connect other networks to the remaining interfaces.

Step 4 (6.6 and earlier) Cable for an edge deployment.

Figure 19: Cabling an Edge Deployment



Note For version 6.5 and earlier, the Management 1/1 default IP address is 192.168.45.45.

- a) Cable the following to a Layer 2 Ethernet switch:
 - Inside interface (for example, GigabitEthernet 1/2)
 - Management 1/1 interface
 - Firepower Management Center
 - Management computer
- b) Connect the management computer to the console port. You need to use the console port to access the CLI for initial setup if you do not use SSH to the Management interface.
- c) Connect the outside interface (for example, GigabitEthernet 1/1) to your outside router.
- d) Connect other networks to the remaining interfaces.

Power on the Device

System power is controlled by a rocker power switch located on the rear of the device.

Before you begin

It's important that you provide reliable power for your device (for example, using an uninterruptable power supply (UPS)). Loss of power without first shutting down can cause serious file system damage. There are many processes running in the background all the time, and losing power does not allow the graceful shutdown of your system.

Procedure

-
- Step 1** Attach the power cord to the device, and connect it to an electrical outlet.
 - Step 2** Turn the power on using the standard rocker-type power on/off switch located on the rear of the chassis, adjacent to the power cord.
 - Step 3** Check the Power LED on the front or rear of the device; if it is solid green, the device is powered on.

Figure 20: Rear Panel

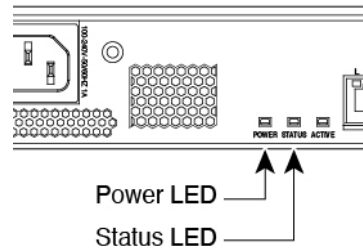
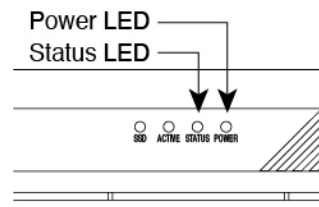


Figure 21: Front Panel



- Step 4** Check the Status LED on the front or rear of the device; after it is solid green, the system has passed power-on diagnostics.
-

Complete the FTD Initial Configuration Using the CLI

Connect to the FTD CLI to perform initial setup, including setting the Management IP address, gateway, and other basic networking settings using the setup wizard. The dedicated Management interface is a special interface with its own network settings. In 6.7 and later: If you do not want to use the Management interface for FMC access, you can use the CLI to configure a data interface instead. You will also configure FMC communication settings.

Procedure

-
- Step 1** Connect to the FTD CLI, either from the console port or using SSH to the Management interface, which obtains an IP address from a DHCP server by default. If you intend to change the network settings, we recommend using the console port so you do not get disconnected.
 - Step 2** Log in with the username **admin** and the password **Admin123**.

Note If the password was already changed, and you do not know it, you must reimage the device to reset the password to the default. See the [reimage guide](#) for instructions.

Step 3

The first time you log in to FTD, you are prompted to accept the End User License Agreement (EULA) and to change the admin password. You are then presented with the CLI setup script.

Note You cannot repeat the CLI setup wizard unless you clear the configuration; for example, by reimaging. However, all of these settings can be changed later at the CLI using **configure network** commands. See the [FTD command reference](#).

Defaults or previously entered values appear in brackets. To accept previously entered values, press **Enter**.

Note In 6.7 and later: The Management interface settings are used even when you enable FMC access on a data interface. For example, the management traffic that is routed over the backplane through the data interface will resolve FQDNs using the Management interface DNS servers, and not the data interface DNS servers.

See the following guidelines:

- **Configure IPv4 via DHCP or manually?**—In 6.7 and later: If you want to use a data interface for FMC access instead of the management interface, choose **manual**. Although you do not plan to use the Management interface, you must set an IP address, for example, a private address. You cannot configure a data interface for management if the management interface is set to DHCP, because the default route, which must be **data-interfaces** (see the next bullet), might be overwritten with one received from the DHCP server.
- **Enter the IPv4 default gateway for the management interface**—In 6.7 and later: If you want to use a data interface for FMC access instead of the management interface, set the gateway to be **data-interfaces**. This setting forwards management traffic over the backplane so it can be routed through the FMC access data interface. If you want to use the Management interface for FMC access, you should set a gateway IP address on the Management 1/1 network.
- **If your networking information has changed, you will need to reconnect**—If you are connected with SSH but you change the IP address at initial setup, you will be disconnected. Reconnect with the new IP address and password. Console connections are not affected.
- **Manage the device locally?**—Enter **no** to use FMC. A **yes** answer means you will use Firepower Device Manager instead.
- **Configure firewall mode?**—We recommend that you set the firewall mode at initial configuration. Changing the firewall mode after initial setup erases your running configuration. Note that data interface FMC access is only supported in routed firewall mode.

Example:

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
End User License Agreement
[...]

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]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.10.15
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]: 10.10.10.1
Enter a fully qualified hostname for this system [firepower]: ftd-1.cisco.com
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]:
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
Configure firewall mode? (routed/transparent) [routed]:
Configuring firewall mode ...

Update policy deployment information
- add device configuration
- add network discovery
- add system policy

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

When registering the sensor to a Firepower Management Center, a unique
alphanumeric registration key is always required. In most cases, to register
a sensor to a Firepower 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 Firepower 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 Firepower Management Center, you must
use the same registration key and, if necessary, the same NAT ID when you add
this sensor to the Firepower Management Center.
>

```

Step 4 Identify the FMC that will manage this FTD.

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

- {hostname | IPv4_address | IPv6_address | **DONTRESOLVE**}—Specifies either the FQDN or IP address of the FMC. If the FMC is not directly addressable, use **DONTRESOLVE** and also specify the *nat_id*. At least one of the devices, either the FMC or the FTD, must have a reachable IP address to establish the two-way, SSL-encrypted communication channel between the two devices. If you specify **DONTRESOLVE** in this command, then the FTD must have a reachable IP address or hostname.
- *reg_key*—Specifies a one-time registration key of your choice that you will also specify on the FMC when you register the FTD. The registration key must not exceed 37 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-).
- *nat_id*—Specifies a unique, one-time string of your choice that you will also specify on the FMC when you register the FTD when one side does not specify a reachable IP address or hostname. It is required if you set the FMC to **DONTRESOLVE**. The NAT ID must not exceed 37 characters. Valid characters

include alphanumeric characters (A–Z, a–z, 0–9) and the hyphen (-). This ID cannot be used for any other devices registering to the FMC.

Note If you use a data interface for management, then you must specify the NAT ID on both the FTD and FMC for registration.

Example:

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

If the FMC is behind a NAT device, enter a unique NAT ID along with the registration key, and specify DONTRESOLVE instead of the hostname, for example:

Example:

```
> configure manager add DONTRESOLVE regk3y78 natid90
Manager successfully configured.
```

If the FTD is behind a NAT device, enter a unique NAT ID along with the FMC IP address or hostname, for example:

Example:

```
> configure manager add 10.70.45.5 regk3y78 natid56
Manager successfully configured.
```

Step 5 (Optional) (6.7 and Later) Configure a data interface for FMC access.

configure network management-data-interface

You are then prompted to configure basic network settings for the data interface.

Note You should use the console port when using this command. If you use SSH to the Management interface, you might get disconnected and have to reconnect to the console port. See below for more information about SSH usage.

See the following details for using this command:

- The original Management interface cannot use DHCP if you want to use a data interface for management. If you did not set the IP address manually during initial setup, you can set it now using the **configure network {ipv4 | ipv6} manual** command. If you did not already set the Management interface gateway to **data-interfaces**, this command will set it now.
- FMC access from a data interface has the following limitations:
 - You can only enable FMC access on one physical, data interface. You cannot use a subinterface or EtherChannel.
 - This interface cannot be management-only.
 - Routed firewall mode only, using a routed interface.
 - High Availability is not supported. You must use the Management interface in this case.
 - PPPoE is not supported. If your ISP requires PPPoE, you will have to put a router with PPPoE support between the FTD and the WAN modem.
 - The interface must be in the global VRF only.

- You cannot use separate management and event-only interfaces.
- SSH is not enabled by default for data interfaces, so you will have to enable SSH later using FMC. Because the Management interface gateway will be changed to be the data interfaces, you also cannot SSH to the Management interface from a remote network unless you add a static route for the Management interface using the **configure network static-routes** command.
- When you add the FTD to the FMC, the FMC discovers and maintains the interface configuration, including the following settings: interface name and IP address, static route to the gateway, DNS servers, and DDNS server. For more information about the DNS server configuration, see below. In FMC, you can later make changes to the FMC access interface configuration, but make sure you don't make changes that can prevent the FTD or FMC from re-establishing the management connection. If the management connection is disrupted, the FTD includes the **configure policy rollback** command to restore the previous deployment.
- If you configure a DDNS server update URL, the FTD automatically adds certificates for all of the major CAs from the Cisco Trusted Root CA bundle so that the FTD can validate the DDNS server certificate for the HTTPS connection. The FTD supports any DDNS server that uses the DynDNS Remote API specification (<https://help.dyn.com/remote-access-api/>).
- This command sets the *data* interface DNS server. The Management DNS server that you set with the setup script (or using the **configure network dns servers** command) is used for management traffic. The data DNS server is used for DDNS (if configured) or for security policies applied to this interface.

On the FMC, the data interface DNS servers are configured in the Platform Settings policy that you assign to this FTD. When you add the FTD to the FMC, the local setting is maintained, and the DNS servers are *not* added to a Platform Settings policy. However, if you later assign a Platform Settings policy to the FTD that includes a DNS configuration, then that configuration will overwrite the local setting. We suggest that you actively configure the DNS Platform Settings to match this setting to bring the FMC and the FTD into sync.

Also, local DNS servers are only retained by FMC if the DNS servers were discovered at initial registration. For example, if you registered the device using the Management interface, but then later configure a data interface using the **configure network management-data-interface** command, then you must manually configure all of these settings in FMC, including the DNS servers, to match the FTD configuration.

- You can change the management interface after you register the FTD to the FMC, to either the Management interface or another data interface.
- The FQDN that you set in the setup wizard will be used for this interface.
- You can clear the entire device configuration as part of the command; you might use this option in a recovery scenario, but we do not suggest you use it for initial setup or normal operation.
- To disable data management, enter the **configure network management-data-interface disable** command.

Example:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]:
IP address (manual / dhcp) [dhcp]:
DDNS server update URL [none]:
https://jcrichon:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
```

Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow FMC access from any network, if you wish to change the FMC access network use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>

Example:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:
```

Configuration done with option to allow FMC access from any network, if you wish to change the FMC access network use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>

Step 6 (Optional) (6.7 and Later) Limit data interface access to an FMC on a specific network.

configure network management-data-interface client *ip_address netmask*

By default, all networks are allowed.

What to do next

Register your device to a FMC.

Log Into the Firepower Management Center

Use the FMC to configure and monitor the FTD.

Before you begin

For information on supported browsers, refer to the release notes for the version you are using (see <https://www.cisco.com/go/firepower-notes>).

Procedure

Step 1 Using a supported browser, enter the following URL.

`https://fmc_ip_address`

- Step 2** Enter your username and password.
- Step 3** Click **Log In**.
-

Obtain Licenses for the FMC

All licenses are supplied to the FTD by the FMC. You can purchase the following licenses:

- **Threat**—Security Intelligence and Next-Generation IPS
- **Malware**—Malware
- **URL**—URL Filtering
- **RA VPN**—AnyConnect Plus, AnyConnect Apex, or AnyConnect VPN Only

For a more detailed overview on Cisco Licensing, go to cisco.com/go/licensingguide

Before you begin

- Have a master account on the [Smart Software Manager](#).

If you do not yet have an account, click the link to [set up a new account](#). The Smart Software Manager lets you create a master account for your organization.

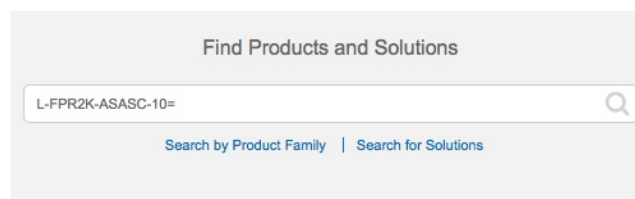
- Your Smart Software Licensing account must qualify for the Strong Encryption (3DES/AES) license to use some features (enabled using the export-compliance flag).

Procedure

- Step 1** Make sure your Smart Licensing account contains the available licenses you need.

When you bought your device from Cisco or a reseller, your licenses should have been linked to your Smart Software License account. However, if you need to add licenses yourself, use the **Find Products and Solutions** search field on the [Cisco Commerce Workspace](#). Search for the following license PIDs:

Figure 22: License Search



Note If a PID is not found, you can add the PID manually to your order.

- Threat, Malware, and URL license combination:
 - L-ASA5508T-TMC=

- L-ASA5516T-TMC=

When you add one of the above PIDs to your order, you can then choose a term-based subscription corresponding with one of the following PIDs:

- L-ASA5508T-TMC-1Y
 - L-ASA5508T-TMC-3Y
 - L-ASA5508T-TMC-5Y
 - L-ASA5516T-TMC-1Y
 - L-ASA5516T-TMC-3Y
 - L-ASA5516T-TMC-5Y
- RA VPN—See the [Cisco AnyConnect Ordering Guide](#).

Step 2 If you have not already done so, register the FMC with the Smart Licensing server.

Registering requires you to generate a registration token in the Smart Software Manager. See the [FMC configuration guide](#) for detailed instructions.

Register the FTD with the FMC

Register the FTD to the FMC.

Before you begin

- Gather the following information that you set in the FTD initial configuration:
 - The FTD management IP address or hostname, and NAT ID
 - The FMC registration key

Procedure

Step 1 In the FMC, choose **Devices > Device Management**.

Step 2 From the **Add** drop-down list, choose **Add Device**.

Add Device ?

Host:†

Display Name:

Registration Key:†*

Group:

Access Control Policy:†*

Smart Licensing

- Malware
- Threat
- URL Filtering

Advanced

Unique NAT ID:†

- Transfer Packets

Set the following parameters:

- **Host**—Enter the IP address or hostname of the FTD you want to add. You can leave this field blank if you specified both the FMC IP address and a NAT ID in the FTD initial configuration.
- **Display Name**—Enter the name for the FTD as you want it to display in the FMC.
- **Registration Key**—Enter the same registration key that you specified in the FTD initial configuration.
- **Domain**—Assign the device to a leaf domain if you have a multidomain environment.
- **Group**—Assign it to a device group if you are using groups.
- **Access Control Policy**—Choose an initial policy. Unless you already have a customized policy you know you need to use, choose **Create new policy**, and choose **Block all traffic**. You can change this later to allow traffic; see [Allow Traffic from Inside to Outside, on page 57](#).

Figure 23: New Policy

New Policy

Name:
ftd-ac-policy

Description:

Select Base Policy:
None

Default Action:
 Block all traffic
 Intrusion Prevention
 Network Discovery

Cancel Save

- **Smart Licensing**—Assign the Smart Licenses you need for the features you want to deploy: **Malware** (if you intend to use malware inspection), **Threat** (if you intend to use intrusion prevention), and **URL** (if you intend to implement category-based URL filtering). **Note:** You can apply an AnyConnect remote access VPN license after you add the device, from the **System > Licenses > Smart Licenses** page.
- **Unique NAT ID**—Specify the NAT ID that you specified in the FTD initial configuration.
- **Transfer Packets**—Allow the device to transfer packets to the FMC. When events like IPS or Snort are triggered with this option enabled, the device sends event metadata information and packet data to the FMC for inspection. If you disable it, only event information will be sent to the FMC, but packet data is not sent.

Step 3 Click **Register**, and confirm a successful registration.

If the registration succeeds, the device is added to the list. If it fails, you will see an error message. If the FTD fails to register, check the following items:

- Ping—Access the FTD CLI, and ping the FMC IP address using the following command:

```
ping system ip_address
```

If the ping is not successful, check your network settings using the **show network** command. If you need to change the FTD Management IP address, use the **configure network {ipv4 | ipv6} manual** command. If you configured a data interface for FMC access, use the **configure network management-data-interface** command.

- Registration key, NAT ID, and FMC IP address—Make sure you are using the same registration key, and if used, NAT ID, on both devices. You can set the registration key and NAT ID on the FMC using the **configure manager add** command.

For more troubleshooting information, see <https://cisco.com/go/fmc-reg-error>.

Configure a Basic Security Policy

This section describes how to configure a basic security policy with the following settings:

- Inside and outside interfaces—Assign a static IP address to the inside interface, and use DHCP for the outside interface.
- DHCP server—Use a DHCP server on the inside interface for clients.
- Default route—Add a default route through the outside interface.
- NAT—Use interface PAT on the outside interface.
- Access control—Allow traffic from inside to outside.

To configure a basic security policy, complete the following tasks.

1	Configure Interfaces, on page 49.
2	Configure the DHCP Server, on page 52.
3	Add the Default Route, on page 53.
4	Configure NAT, on page 55.
5	Allow Traffic from Inside to Outside, on page 57.
6	Deploy the Configuration, on page 58.

Configure Interfaces

Enable FTD interfaces, assign them to security zones, and set the IP addresses. Typically, you must configure at least a minimum of two interfaces to have a system that passes meaningful traffic. Normally, you would have an outside interface that faces the upstream router or internet, and one or more inside interfaces for your organization's networks. Some of these interfaces might be "demilitarized zones" (DMZs), where you place publically-accessible assets such as your web server.

A typical edge-routing situation is to obtain the outside interface address through DHCP from your ISP, while you define static addresses on the inside interfaces.

The following example configures a routed mode inside interface with a static address and a routed mode outside interface using DHCP.

Procedure

Step 1 Choose **Devices > Device Management**, and click the **Edit** (✎) for the firewall.

Step 2 Click **Interfaces**.

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
Ethernet1/2		Physical			
Ethernet1/3.1		Subinterface			
Ethernet1/4	diagnostic	Physical			
Ethernet1/5		Physical			

Step 3 Click **Edit** (✎) for the interface that you want to use for *inside*.

The **General** tab appears.

Edit Physical Interface

General | IPv4 | IPv6 | Advanced | Hardware Configuration

Name: Enabled Management Only

Description:

Mode: ▼

Security Zone: ▼

Interface ID:

MTU: (64 - 9000)

OK Cancel

- Enter a **Name** up to 48 characters in length.
For example, name the interface **inside**.
- Check the **Enabled** check box.
- Leave the **Mode** set to **None**.
- From the **Security Zone** drop-down list, choose an existing inside security zone or add a new one by clicking **New**.

For example, add a zone called **inside_zone**. Each interface must be assigned to a security zone and/or interface group. An interface can belong to only one security zone, but can also belong to multiple interface groups. You apply your security policy based on zones or groups. For example, you can assign the inside interface to the inside zone; and the outside interface to the outside zone. Then you can configure your access control policy to enable traffic to go from inside to outside, but not from outside to inside. Most policies only support security zones; you can use zones or interface groups in NAT policies, prefilter policies, and QoS policies.

e) Click the **IPv4** and/or **IPv6** tab.

- **IPv4**—Choose **Use Static IP** from the drop-down list, and enter an IP address and subnet mask in slash notation.

For example, enter **192.168.1.1/24**

- **IPv6**—Check the **Autoconfiguration** check box for stateless autoconfiguration.

f) Click **OK**.

Step 4 Click the **Edit** (✎) for the interface that you want to use for *outside*.
The **General** tab appears.

Note If you pre-configured this interface for FMC access management, then the interface will already be named, enabled, and addressed. You should not alter any of these basic settings because doing so will disrupt the FMC management connection. You can still configure the Security Zone on this screen for through traffic policies.

a) Enter a **Name** up to 48 characters in length.

For example, name the interface **outside**.

b) Check the **Enabled** check box.

c) Leave the **Mode** set to **None**.

d) From the **Security Zone** drop-down list, choose an existing outside security zone or add a new one by clicking **New**.

For example, add a zone called **outside_zone**.

e) Click the **IPv4** and/or **IPv6** tab.

- **IPv4**—Choose **Use DHCP**, and configure the following optional parameters:

- **Obtain default route using DHCP**—Obtains the default route from the DHCP server.

- **DHCP route metric**—Assigns an administrative distance to the learned route, between 1 and 255. The default administrative distance for the learned routes is 1.

The screenshot shows the 'Edit Physical Interface' configuration window with the 'IPv4' tab selected. The 'IP Type' dropdown is set to 'Use DHCP'. Below it, the 'Obtain default route using DHCP' checkbox is checked. The 'DHCP route metric' is set to '1' in a text input field, with '(1 - 255)' indicating the valid range.

- **IPv6**—Check the **Autoconfiguration** check box for stateless autoconfiguration.

f) Click **OK**.

Step 5 Click **Save**.

Configure the DHCP Server

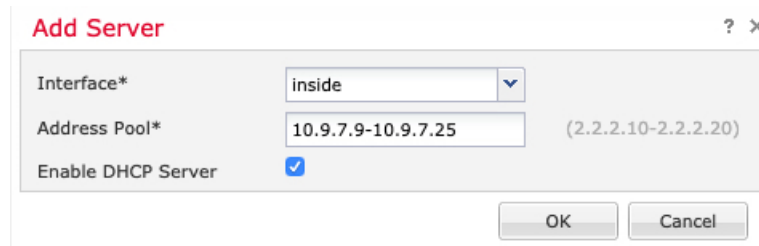
Enable the DHCP server if you want clients to use DHCP to obtain IP addresses from the FTD.

Procedure

Step 1 Choose **Devices > Device Management**, and click the **Edit** (✎) for the device.

Step 2 Choose **DHCP > DHCP Server**.

Step 3 On the **Server** page, click **Add**, and configure the following options:



- **Interface**—Choose the interface from the drop-down list.
- **Address Pool**—Set the range of IP addresses from lowest to highest that are used by the DHCP server. The range of IP addresses must be on the same subnet as the selected interface and cannot include the IP address of the interface itself.
- **Enable DHCP Server**—Enable the DHCP server on the selected interface.

Step 4 Click **OK**.

Step 5 Click **Save**.

Add the Default Route

The default route normally points to the upstream router reachable from the outside interface. If you use DHCP for the outside interface, your device might have already received a default route. If you need to manually add the route, complete this procedure. If you received a default route from the DHCP server, it will show in the **IPv4 Routes** or **IPv6 Routes** table on the **Devices > Device Management > Routing > Static Route** page.

Procedure

Step 1 Choose **Devices > Device Management**, and click the **Edit** (✎) for the device.

Step 2 Choose **Routing > Static Route**, click **Add Route**, and set the following:

Add the Default Route

- **Type**—Click the **IPv4** or **IPv6** radio button depending on the type of static route that you are adding.
- **Interface**—Choose the egress interface; typically the outside interface.
- **Available Network**—Choose **any-ipv4** for an IPv4 default route, or **any-ipv6** for an IPv6 default route and click **Add** to move it to the **Selected Network** list.
- **Gateway** or **IPv6 Gateway**—Enter or choose the gateway router that is the next hop for this route. You can provide an IP address or a Networks/Hosts object.
- **Metric**—Enter the number of hops to the destination network. Valid values range from 1 to 255; the default value is 1.

Step 3 Click **OK**.

The route is added to the static route table.

Network	Interface	Gateway	Tunneled	Metric	Tracked
▼ IPv4 Routes					
any-ipv4	outside	10.99.10.1	false	1	
▼ IPv6 Routes					

Step 4 Click **Save**.

Configure NAT

A typical NAT rule converts internal addresses to a port on the outside interface IP address. This type of NAT rule is called *interface Port Address Translation (PAT)*.

Procedure

Step 1 Choose **Devices > NAT**, and click **New Policy > Threat Defense NAT**.

Step 2 Name the policy, select the device(s) that you want to use the policy, and click **Save**.

The screenshot shows the 'New Policy' dialog box. The 'Name' field contains 'interface_PAT'. Below it is a 'Description' field. The 'Targeted Devices' section is divided into 'Available Devices' and 'Selected Devices'. In the 'Available Devices' list, the IP address '192.168.0.16' is selected. This IP address has been moved to the 'Selected Devices' list, which is highlighted with a red oval. An 'Add to Policy' button is located between the two lists. At the bottom of the dialog are 'Save' and 'Cancel' buttons.

The policy is added to the FMC. You still have to add rules to the policy.

Step 3 Click **Add Rule**.

The **Add NAT Rule** dialog box appears.

Step 4 Configure the basic rule options:

The screenshot shows the 'Add NAT Rule' dialog box. The 'NAT Rule' dropdown menu is set to 'Auto NAT Rule'. The 'Type' dropdown menu is set to 'Dynamic'. The 'Enable' checkbox is checked. At the bottom, there are four tabs: 'Interface Objects', 'Translation' (which is selected and highlighted in blue), 'PAT Pool', and 'Advanced'.

- **NAT Rule**—Choose **Auto NAT Rule**.

- **Type**—Choose **Dynamic**.

Step 5 On the **Interface Objects** page, add the outside zone from the **Available Interface Objects** area to the **Destination Interface Objects** area.

Step 6 On the **Translation** page, configure the following options:

- **Original Source**—Click **Add (+)** to add a network object for all IPv4 traffic (0.0.0.0/0).

Note You cannot use the system-defined **any-ipv4** object, because Auto NAT rules add NAT as part of the object definition, and you cannot edit system-defined objects.

- **Translated Source**—Choose **Destination Interface IP**.

Step 7 Click **Save** to add the rule.

The rule is saved to the **Rules** table.

The screenshot shows the FMC interface with the 'Rules' tab selected. The 'interface_PAT' rule is highlighted in the 'Auto NAT Rules' section. The rule configuration is as follows:

#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options
1	→	Dynamic	any	outside_zone	any-ipv4			Interface			Dns:false

Step 8 Click **Save** on the NAT page to save your changes.

Allow Traffic from Inside to Outside

If you created a basic **Block all traffic** access control policy when you registered the FTD with the FMC, then you need to add rules to the policy to allow traffic through the device. The following procedure adds a rule to allow traffic from the inside zone to the outside zone. If you have other zones, be sure to add rules allowing traffic to the appropriate networks.

See the [FMC configuration guide](#) to configure more advanced security settings and rules.

Procedure

Step 1 Choose **Policy > Access Policy > Access Policy**, and click the **Edit** (✎) for the access control policy assigned to the FTD.

Step 2 Click **Add Rule**, and set the following parameters:

The screenshot shows the 'Add Rule' configuration page with the following settings:

- Name:** inside_to_outside
- Enabled:**
- Action:** Allow
- Insert:** into Mandatory
- Zones:** Selected
- Available Zones:** inside_zone, outside_zone
- Source Zones (1):** inside_zone
- Destination Zones (1):** outside_zone

- **Name**—Name this rule, for example, **inside_to_outside**.
- **Source Zones**—Select the inside zone from **Available Zones**, and click **Add to Source**.
- **Destination Zones**—Select the outside zone from **Available Zones**, and click **Add to Destination**.

Leave the other settings as is.

Step 3 Click Add.

The rule is added to the **Rules** table.

The screenshot shows the FMC interface with the 'Policies' tab selected. The 'Rules' table is displayed, showing a rule named 'inside_to_outside' with source zone 'inside_zone' and destination zone 'outside_zone'. The rule is set to 'Allow' action. The table has columns for Name, Source Zo..., Dest Zones, Source Ne..., Dest Netw..., VLAN Tags, Users, Applications, Source Po..., Dest Ports, URLs, ISE/SGT A..., and Action.

#	Name	Source Zo...	Dest Zones	Source Ne...	Dest Netw...	VLAN Tags	Users	Applications	Source Po...	Dest Ports	URLs	ISE/SGT A...	Action
1	inside_to_outside	inside_zone	outside_zone	Any	Any	Any	Any	Any	Any	Any	Any	Any	Allow

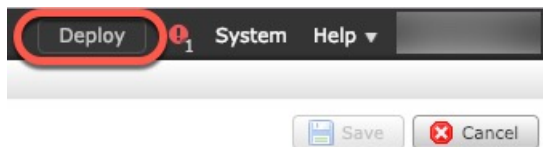
Step 4 Click Save.

Deploy the Configuration

Deploy the configuration changes to the FTD; none of your changes are active on the device until you deploy them.

Procedure

Step 1 Click **Deploy** in the upper right.

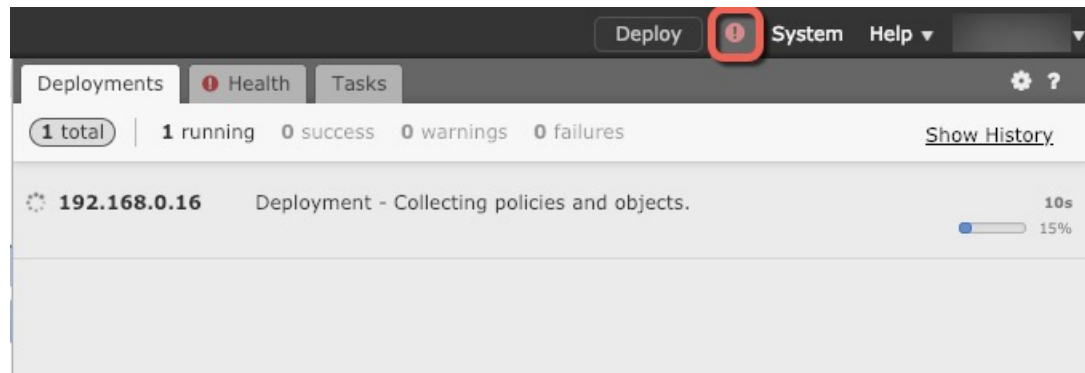


Step 2 Select the device in the **Deploy Policies** dialog box, then click **Deploy**.

The screenshot shows the 'Deploy Policies' dialog box in the FMC interface. The dialog has a title bar with 'Deploy Policies' and a version timestamp 'Version: 2019-03-05 03:17 PM'. Below the title bar is a table with columns for Device, Inspect Interruption, Type, Group, and Current Version. A device with IP 192.168.0.16 is selected, and the 'Deploy' button is highlighted.

Device	Inspect Interruption	Type	Group	Current Version
192.168.0.16	No	FTD		2019-02-28 07:11 AM

Step 3 Ensure that the deployment succeeds. Click the icon to the right of the **Deploy** button in the menu bar to see status for deployments.



Access the Firepower Threat Defense CLI

Use the command-line interface (CLI) to set up the system and do basic system troubleshooting. You cannot configure policies through a CLI session. You can access the CLI by connecting to the console port.

You can SSH to the management interface of the FTD device. You can also connect to the address on a data interface if you open the interface for SSH connections. SSH access to data interfaces is disabled by default.

Procedure

- Step 1** To log into the CLI, connect your management computer to the console port.. The ASA 5508-X and 5516-X ship with a USB A-to-B serial cable. Be sure to install any necessary USB serial drivers for your operating system (see the [hardware guide](#)). Use the following serial settings:
- 9600 baud
 - 8 data bits
 - No parity
 - 1 stop bit
- Step 2** Log in to the FTD CLI using the **admin** username and the password you set at initial setup (the default is **Admin123**).
- After logging in, for information on the commands available in the CLI, enter **help** or **?**. For usage information, see the [Cisco Firepower Threat Defense Command Reference](#).

Power Off the Device

It's important that you shut down your system properly. Simply unplugging the power or pressing the power switch can cause serious file system damage. Remember that there are many processes running in the background all the time, and unplugging or shutting off the power does not allow the graceful shutdown of your Firepower system.

Procedure

Step 1 Connect to the console port to access the FTD CLI, and then shut down the FTD.

shutdown

Example:

```
> shutdown
This command will shutdown the system. Continue?
Please enter 'YES' or 'NO': yes
INIT: Stopping Cisco Threat Defense.....ok
Shutting down sfidf... [ OK ]
Clearing static routes
Unconfiguring default route [ OK ]
Unconfiguring address on br1 [ OK ]
Unconfiguring IPv6 [ OK ]
Downing interface [ OK ]
Stopping xinetd:
Stopping nscd... [ OK ]
Stopping system log daemon... [ OK ]
Stopping Threat Defense ...
Stopping system message bus: dbus. [ OK ]
Un-mounting disk partitions ...
device-mapper: remove ioctl on root failed: Device or resource busy
[...]
mdadm: Cannot get exclusive access to /dev/md0:Perhaps a running process, mounted filesystem
or active volume group?
Stopping OpenBSD Secure Shell server: sshd
stopped /usr/sbin/sshd (pid 3520)
done.
Stopping Advanced Configuration and Power Interface daemon: stopped /usr/sbin/acpid (pid
3525)
acpid.
Stopping system message bus: dbus.
Stopping internet superserver: xinetd.
no /etc/sysconfig/kdump.conf
Deconfiguring network interfaces... ifdown: interface br1 not configured
done.
SSP-Security-Module is shutting down ...
Sending ALL processes the TERM signal ...
acpid: exiting
Sending ALL processes the KILL signal ...
Deactivating swap...
Unmounting local filesystems...

Firepower Threat Defense stopped.
It is safe to power off now.

Do you want to reboot instead? [y/N]
```

Step 2 After the FTD shuts down, and the console shows that "It is safe to power off now", you can then turn off the power switch and unplug the power to physically remove power from the chassis if necessary.

Alternatively, you can reboot the system by typing **y** at the prompt.

What's Next?

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

For information related to using FMC, see the [Firepower Management Center Configuration Guide](#).



CHAPTER 4

ASA and ASA FirePOWER Module Deployment with ASDM



Note ASA version 9.16 is the final supported version for the ASA 5508-X and 5516-X.

Is This Chapter for You?

This chapter describes how to deploy the ASA 5508-X or 5516-X in your network with the ASA FirePOWER module and how to perform initial configuration. This chapter does not cover the following deployments, for which you should refer to the [ASA configuration guide](#):

- Failover
- Clustering (ASA 5516-X only)
- CLI configuration

This chapter also walks you through configuring a basic security policy; if you have more advanced requirements, refer to the configuration guide.

The ASA 5508-X and 5516-X hardware can run either ASA software or FTD software. Switching between ASA and FTD requires you to reimage the device. See [Reimage the Cisco ASA or Firepower Threat Defense Device](#).

Privacy Collection Statement—The ASA 5508-X or 5516-X do not require or actively collect personally-identifiable information. However, you can use personally-identifiable information in the configuration, for example for usernames. In this case, an administrator might be able to see this information when working with the configuration or when using SNMP.

- [About the ASA, on page 64](#)
- [End-to-End Procedure, on page 64](#)
- [Review the Network Deployment and Default Configuration, on page 66](#)
- [Cable the Device, on page 69](#)
- [Power on the ASA, on page 69](#)
- [\(Optional\) Change the IP Address, on page 70](#)
- [Log Into ASDM, on page 71](#)
- [\(Optional\) Configure ASA Licensing, on page 72](#)
- [Configure the ASA, on page 73](#)

- [Configure the ASA FirePOWER Module, on page 76](#)
- [Access the ASA CLI, on page 78](#)
- [What's Next?, on page 79](#)

About the ASA

The ASA provides advanced stateful firewall and VPN concentrator functionality in one device, and with the included ASA FirePOWER module, next-generation firewall services including Next-Generation Intrusion Prevention System (NGIPS), Application Visibility and Control (AVC), URL filtering, and Advanced Malware Protection (AMP).

You can manage the ASA using one of the following managers:

- ASDM (covered in this guide)—A single device manager included on the device.
- CLI
- Cisco Defense Orchestrator—A simplified, cloud-based multi-device manager
- Cisco Security Manager—A multi-device manager on a separate server.

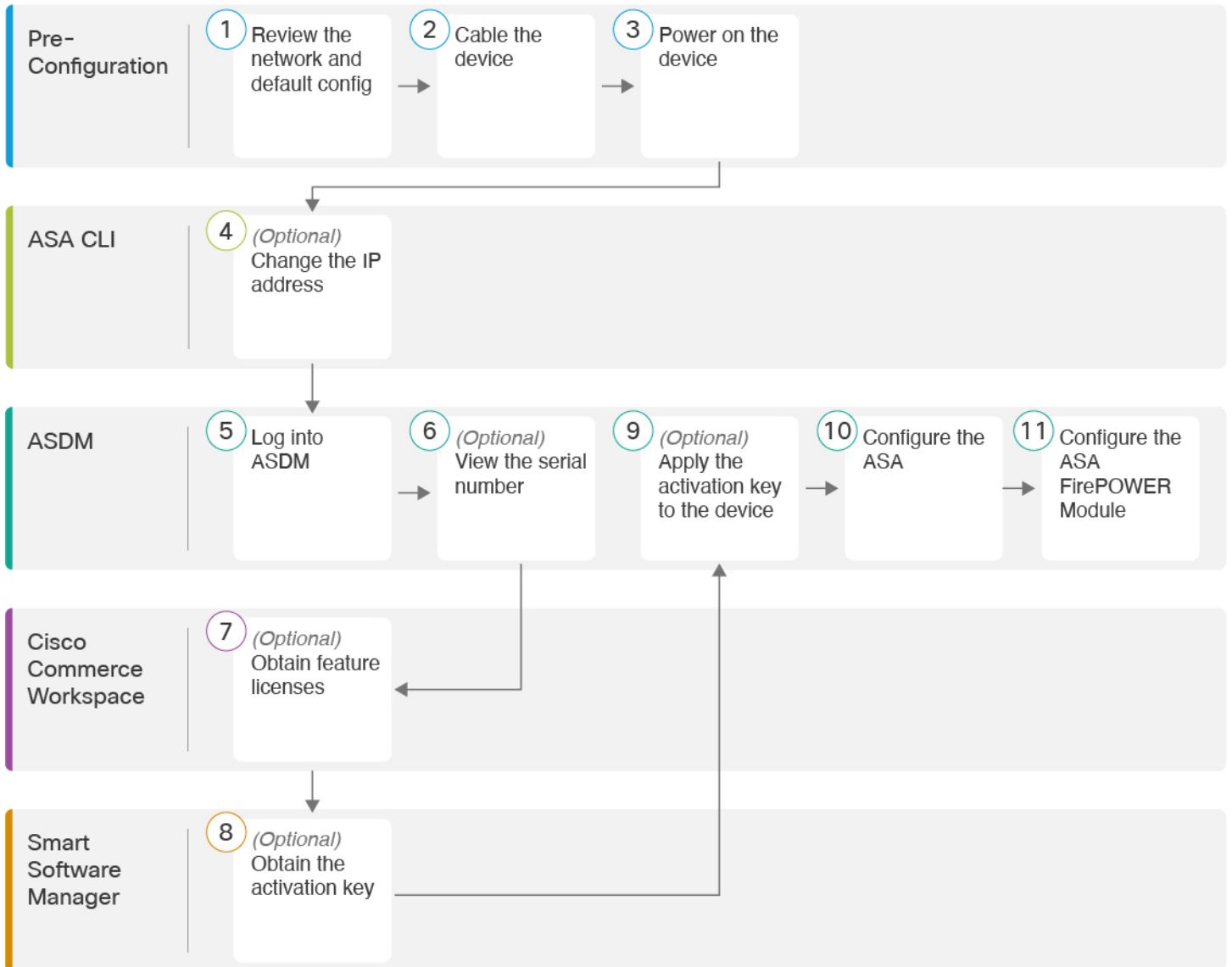
You can manage the ASA FirePOWER module using one of the following managers:

- ASDM (Covered in this guide)—A single device manager included on the device.
- Firepower Management Center (FMC)—A full-featured, multidevice manager on a separate server.

You can also access the FirePOWER CLI for troubleshooting purposes.

End-to-End Procedure

See the following tasks to deploy and configure the ASA on your chassis.



1	Pre-Configuration	Review the Network Deployment and Default Configuration, on page 66.
2	Pre-Configuration	Cable the Device, on page 69.
3	Pre-Configuration	Power on the ASA, on page 69.
4	ASA CLI	(Optional) Change the IP Address, on page 70.
5	ASDM	Log Into ASDM, on page 71.

6	ASDM	(Optional) Configure ASA Licensing, on page 72 : View the serial number.
7	Cisco Commerce Workspace	(Optional) Configure ASA Licensing, on page 72 : Obtain feature licenses.
8	Smart Software Manager	(Optional) Configure ASA Licensing, on page 72 : Obtain the activation key.
9	ASDM	(Optional) Configure ASA Licensing, on page 72 : Apply the activation key to the device.
10	ASDM	Configure the ASA, on page 73 .
11	ASDM	Configure the ASA FirePOWER Module, on page 76 .

Review the Network Deployment and Default Configuration

The following figure shows a typical edge deployment for the ASA 5508-X and 5516-X using the default configuration. In this deployment, the ASA acts as the internet gateway for the ASA FirePOWER module, which needs internet access for database updates. You can connect the Management 1/1 interface to the same network (through a switch) as the inside interface if you do not set the Management 1/1 IP address for the ASA. (You can set the Management 1/1 IP address for the ASA FirePOWER module to be on the same network as inside because it is a separate system from the ASA.)

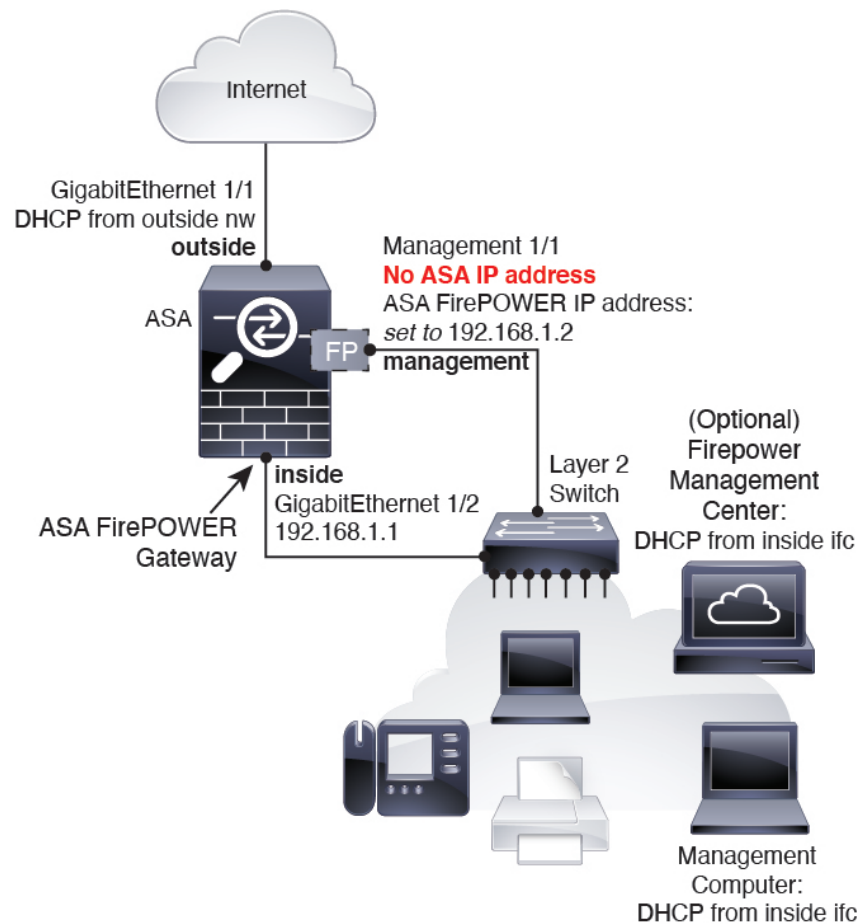
If you connect the outside interface directly to a cable modem or DSL modem, we recommend that you put the modem into bridge mode so the ASA performs all routing and NAT for your inside networks. If you need to configure PPPoE for the outside interface to connect to your ISP, you can do so as part of the ASDM Startup Wizard.



Note

If you cannot use the default inside IP address for ASDM access, you can set the inside IP address at the ASA CLI. See [\(Optional\) Change the IP Address, on page 70](#). For example, you may need to change the inside IP address in the following circumstances:

- If the outside interface tries to obtain an IP address on the 192.168.1.0 network, which is a common default network, the DHCP lease will fail, and the outside interface will not obtain an IP address. This problem occurs because the ASA cannot have two interfaces on the same network. In this case you must change the inside IP address (and later, the ASA FirePOWER IP address) to be on a new network.
- If you add the ASA to an existing inside network, you will need to change the inside IP address (and later, the ASA FirePOWER IP address) to be on the existing network.



ASA 5506-X, 5508-X, and 5516-X Default Configuration

The default factory configuration for the ASA 5506-X series, 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
- (ASA 5506W-X) **wifi <--> inside, wifi --> outside** traffic flow—GigabitEthernet 1/9 (wifi)
- (ASA 5506W-X) **wifi IP address**—192.168.10.1
- **DHCP server** on inside and wifi. The access point itself and all its clients use the ASA as the DHCP server.
- **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 and wifi hosts allowed.

- **NAT**—Interface PAT for all traffic from inside, wifi, and management to outside.

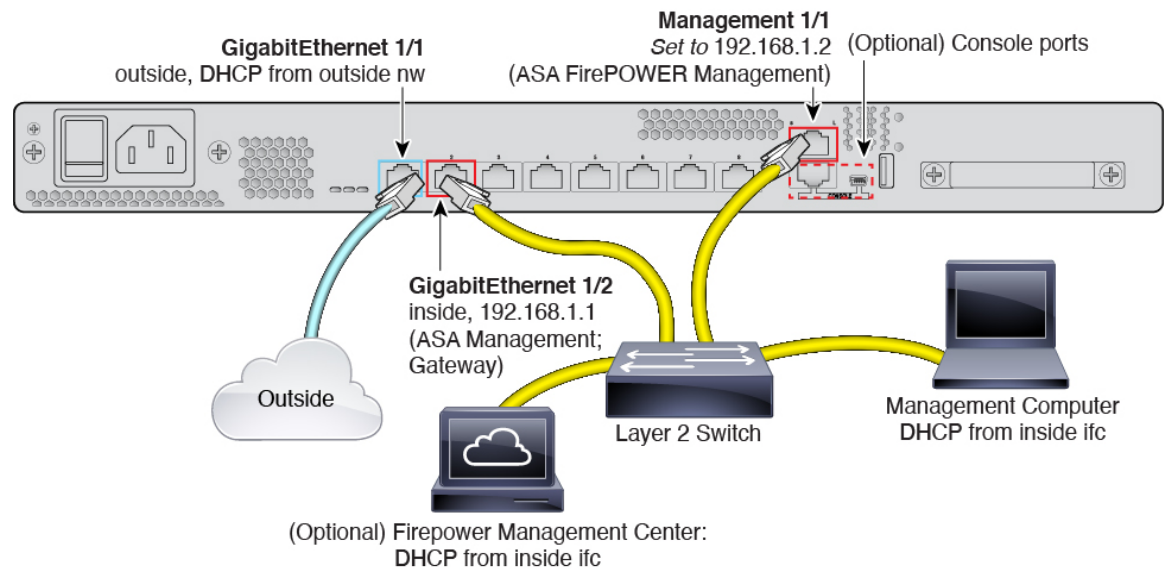
The configuration consists of the following commands:

```
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
  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
```

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

```
same-security-traffic permit inter-interface
!
interface GigabitEthernet 1/9
  security-level 100
  nameif wifi
  ip address 192.168.10.1 255.255.255.0
  no shutdown
!
http 192.168.10.0 255.255.255.0 wifi
!
dhcpd address 192.168.10.2-192.168.10.254 wifi
dhcpd enable wifi
```

Cable the Device



Manage the ASA 5508-X or 5516-X on the GigabitEthernet 1/2 interface, and manage the ASA FirePOWER module on the Management 1/1 interface. The default configuration also configures GigabitEthernet 1/1 as outside.

Procedure

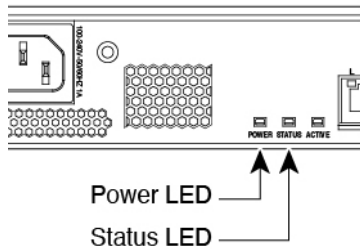
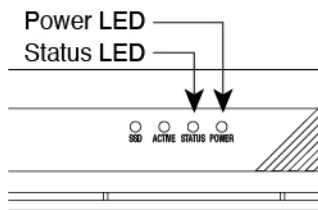
-
- Step 1** Cable the following to a Layer 2 Ethernet switch:
- GigabitEthernet 1/2 (inside)
 - Management 1/1
 - Management computer
 - (Optional) Firepower Management Center
- Step 2** (Optional) Connect the management computer to the console port.
- If you need to change the inside IP address from the default, you must also cable your management computer to the console port. See [\(Optional\) Change the IP Address, on page 70](#).
- Step 3** Connect the GigabitEthernet 1/1 interface (outside) to your outside router.
- Step 4** Connect other networks to the remaining interfaces.
-

Power on the ASA

System power is controlled by a rocker power switch located on the rear of the device.

(Optional) Change the IP Address**Procedure**

-
- Step 1** Attach the power cord to the device, and connect it to an electrical outlet.
- Step 2** Turn the power on using the standard rocker-type power on/off switch located on the rear of the chassis, adjacent to the power cord.
- Step 3** Check the Power LED on the front or rear of the device; if it is solid green, the device is powered on.

Figure 24: Rear Panel*Figure 25: Front Panel*

- Step 4** Check the Status LED on the front or rear of the device; after it is solid green, the system has passed power-on diagnostics.
-

(Optional) Change the IP Address

If you cannot use the default IP address for ASDM access, you can set the IP address of the inside interface at the ASA CLI.



-
- Note** This procedure restores the default configuration and also sets your chosen IP address, so if you made any changes to the ASA configuration that you want to preserve, do not use this procedure.
-

Procedure

-
- Step 1** Connect to the ASA console port, and enter global configuration mode. See [Access the ASA CLI, on page 78](#) for more information.
- Step 2** Restore the default configuration with your chosen IP address.

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

```
ciscoasa(config)# configure factory-default 10.1.1.151 255.255.255.0
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
Executing command: interface gigabitethernet1/2
Executing command: nameif inside
INFO: Security level for "inside" set to 100 by default.
Executing command: ip address 10.1.1.151 255.255.255.0
Executing command: security-level 100
Executing command: no shutdown
Executing command: exit
Executing command: http server enable
Executing command: http 10.1.1.0 255.255.255.0 management
Executing command: dhcpd address 10.1.1.152-10.1.1.254 management
Executing command: dhcpd enable management
Executing command: logging asdm informational
Factory-default configuration is completed
ciscoasa(config)#
```

Step 3 Save the default configuration to flash memory.

write memory

Log Into ASDM

Launch ASDM so you can configure the ASA.

Before you begin

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

Procedure

Step 1 Enter the following URL in your browser.

- **https://192.168.1.1**—Inside (GigabitEthernet 1/2) interface IP address.

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 **Cisco ASDM** web page appears. You may see browser security warnings because the ASA does not have a certificate installed; you can safely ignore these warnings and visit the web page.

- Step 2** Click one of these available options: **Install ASDM Launcher** or **Run ASDM**.
- Step 3** Follow the onscreen instructions to launch ASDM according to the option you chose.
- The **Cisco ASDM-IDM Launcher** appears.
- Step 4** Leave the username and password fields empty, and click **OK**.
- The main ASDM window appears.

(Optional) Configure ASA Licensing

The ASA 5508-X or ASA 5516-X includes the **Base** license by default.

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.

This procedure describes how to obtain and activate additional licenses. You do not need to follow this procedure unless you obtain new licenses.

If you need to manually request the Strong Encryption license (which is free), see <https://www.cisco.com/go/license>.

You can optionally purchase the following licenses:

- **5 Security Contexts**
- **AnyConnect Plus** or **Apex**

To install additional ASA licenses, perform the following steps.

Procedure

- Step 1** Obtain the serial number for your ASA in ASDM by choosing **Configuration > Device Management > Licensing > Activation Key**.
- 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.
- Step 2** See <http://www.cisco.com/go/ccw> to purchase the 5 Security Context license using the following PID: **L-ASA-SC-5=**. The ASA supports 2 contexts with the Base license.
- For AnyConnect License PIDs, see the [Cisco AnyConnect Ordering Guide](#) and the [AnyConnect Licensing Frequently Asked Questions \(FAQ\)](#).
- After you order a license, 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. The PAK email can take several days in some cases.

Step 3 Obtain the activation key from the following licensing website: <https://www.cisco.com/go/license>

Enter the following information, when prompted:

- Product Authorization Keys
- The serial number of your ASA
- Your e-mail address

An activation key is automatically generated and sent to the e-mail address that you provide. This key includes all features you have registered so far for permanent licenses.

Step 4 On the ASDM **Configuration > Device Management > Licensing > Activation Key** pane, enter the **New Activation Key**.

The key is a five-element hexadecimal string with one space between each element. The leading 0x specifier is optional; all values are assumed to be hexadecimal. For example:

```
ASA0xd11b3d48 0xa80a4c0a 0x48e0fd1c 0xb0443480 0x843fc490
```

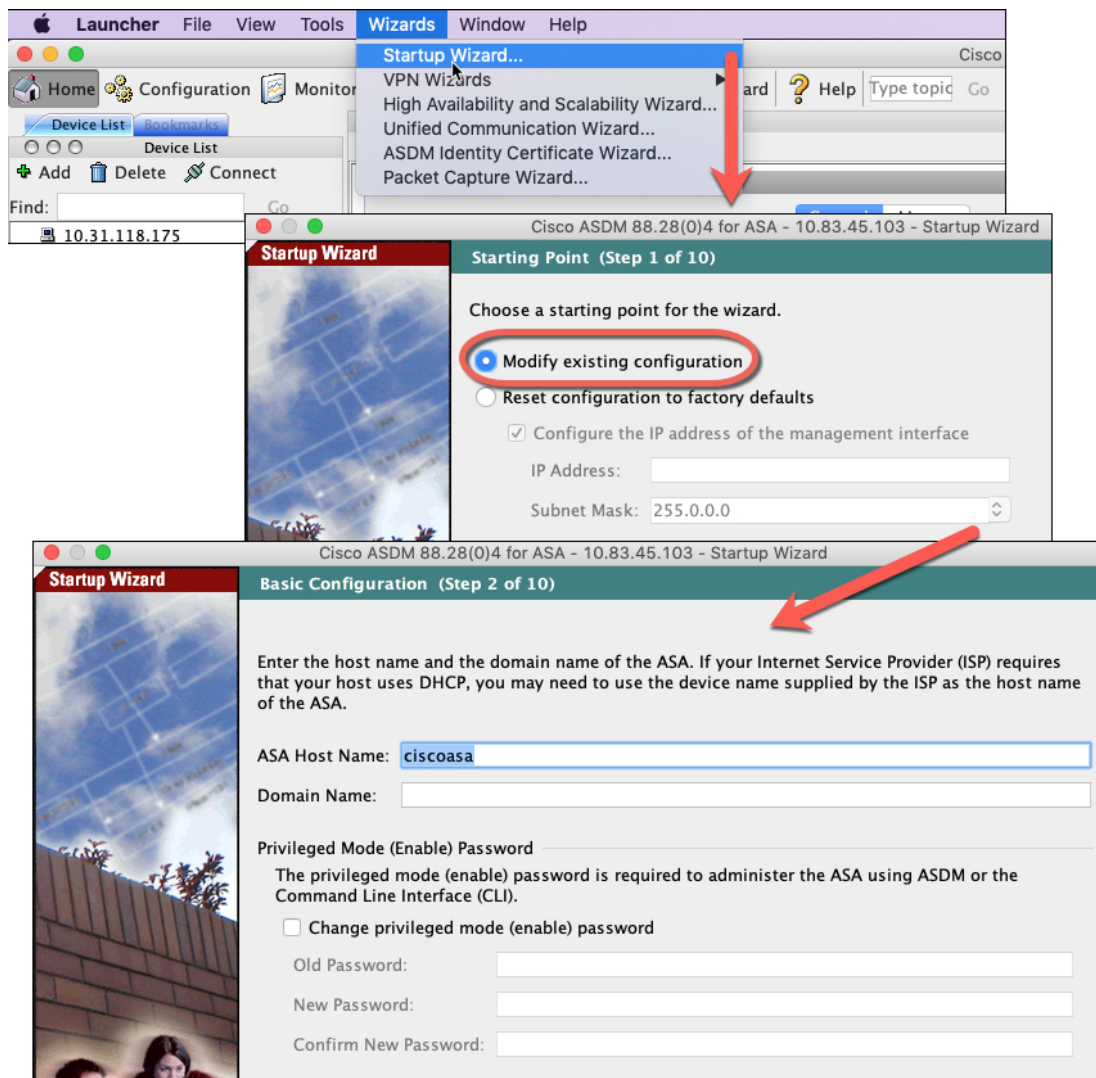
Step 5 Click **Update Activation Key**.

Configure the ASA

Using ASDM, you can use wizards to configure basic and advanced features. You can also manually configure features not included in wizards.

Procedure

Step 1 Choose **Wizards > Startup Wizard**, and click the **Modify existing configuration** radio button.



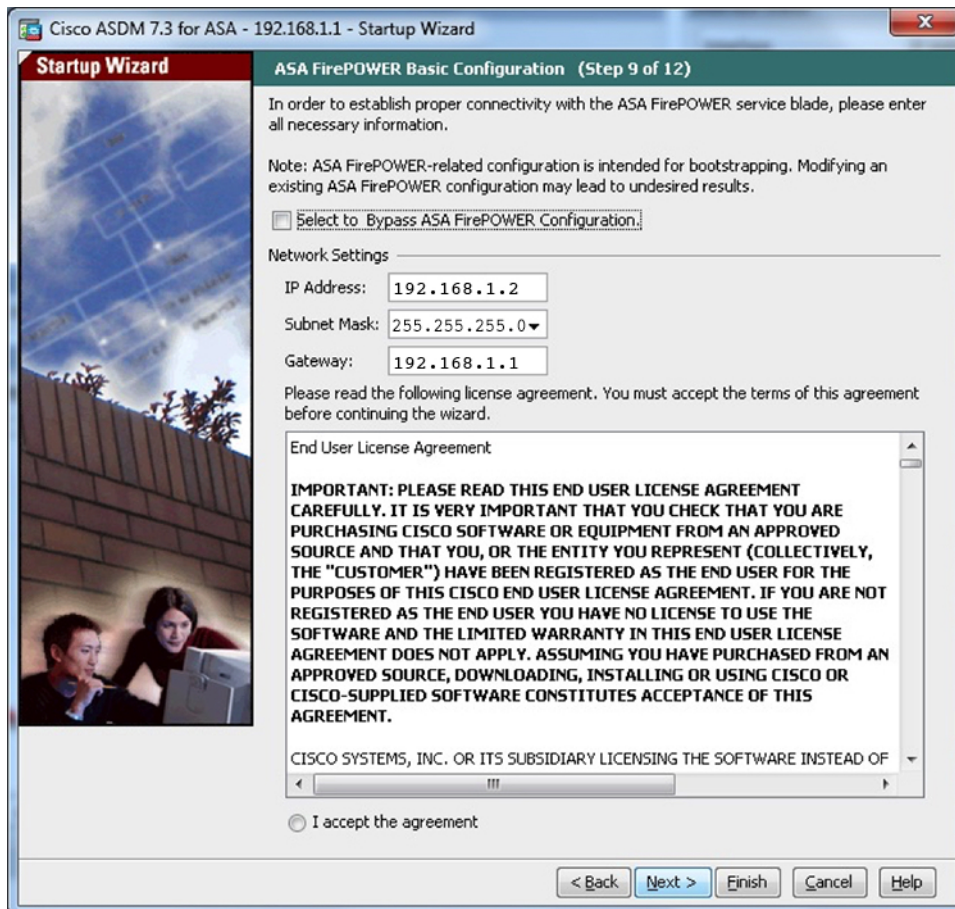
Step 2 The **Startup Wizard** walks you through configuring:

- The enable password
- Interfaces, including setting the inside and outside interface IP addresses and enabling interfaces.
- Static routes
- The DHCP server
- And more...

Step 3 Configure the ASA FirePOWER module management IP address.

Note The ASA FirePOWER module is supported with 9.16 and earlier only.

- a) Configure additional ASA settings as desired, or skip screens until you reach the **ASA FirePOWER Basic Configuration** screen.



b) Set the following values to work with the default configuration:

- **IP Address**—192.168.1.2. If you changed the ASA default IP address according to [\(Optional\) Change the IP Address, on page 70](#), then use an available IP address on the same network. Be sure not to use an IP address in the DHCP server range (if you used the **configure factory-default** command, do not use any address higher than the ASA address you specified).
- **Subnet Mask**—255.255.255.0
- **Gateway**—192.168.1.1

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

d) Quit ASDM, and then relaunch. You should see **ASA FirePOWER** tabs on the **Home** page.

Step 4 (Optional) From the **Wizards** menu, run other wizards.

Step 5 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

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.

1	Configure FirePOWER Licensing, on page 76.
2	Configure the FirePOWER Security Policy, on page 77.
3	Send ASA Traffic to the FirePOWER Module, on page 77.

Configure FirePOWER Licensing

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, which you should receive in your email. See the [Cisco Firepower System Feature Licenses](#) for more information.

To install ASA FirePOWER licenses, perform the following steps.

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 FirePOWER Security Policy

Configure the security policy for traffic that you send from the ASA to the 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 ASA Traffic to the FirePOWER Module

Configure the ASA to send traffic to the FirePOWER module. By default, no traffic is sent to the FirePOWER module. You can send all traffic or a subset of traffic to the module for next-generation firewall services.

Procedure

- Step 1** Choose **Configuration > Firewall > Service Policy Rules**.
- Step 2** Choose **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** (Optional) In the **If ASA FirePOWER Card Fails** area, click one of the following:
- **Permit traffic**—(Default) 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**.
- Repeat this procedure to configure additional traffic flows as desired.

Access the ASA CLI

You can use the ASA CLI to troubleshoot or configure the ASA instead of using ASDM. You can access the CLI by connecting to the console port. You can later configure SSH access to the ASA on any interface; SSH access is disabled by default. See the [ASA general operations configuration guide](#) for more information.

You can also connect to the ASA FirePOWER module internal console port from the ASA CLI. For details about the FirePOWER CLI, see the "Classic Device Command Reference" in the [FMC configuration guide](#).

Procedure

- Step 1** Connect your management computer to the console port. The ASA 5508-X and 5516-X ship with a USB A-to-B serial cable. Be sure to install any necessary USB serial drivers for your operating system (see the [hardware guide](#)). 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#
```

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) Access the ASA FirePOWER module console.

session sfr

Log in with the **admin** username and the password. The default password is **Admin123**. The first time you log in, you are prompted for a new password and for Management interface network settings. You can alternatively set the network settings using ASDM.

Exit the FirePOWER CLI by typing **Ctrl-Shift-6, X**.

Example:

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

```
FP3 login: admin
Password: *****
Last login: Wed Mar 13 05:16:08 UTC 2019 on ttyS1
```

```
Copyright 2004-2017, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.
```

```
Cisco Fire Linux OS v6.2.0 (build 42)
Cisco ASA5555 v6.2.0 (build 362)
```

```
>
```

What's Next?

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

- See the online help or the [ASA FirePOWER module local management configuration guide](#) or the [FMC configuration guide](#) for your version.

