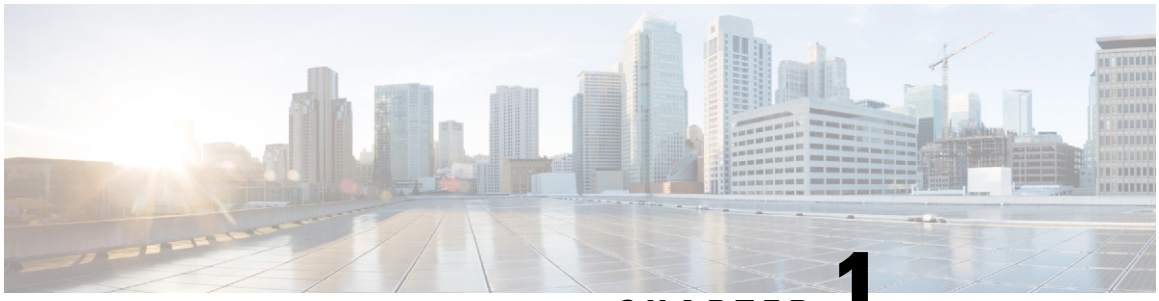
Cisco Firepower 1100 Getting Started Guide

First Published: 2019-06-13

Last Modified: 2020-11-02

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
https://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

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

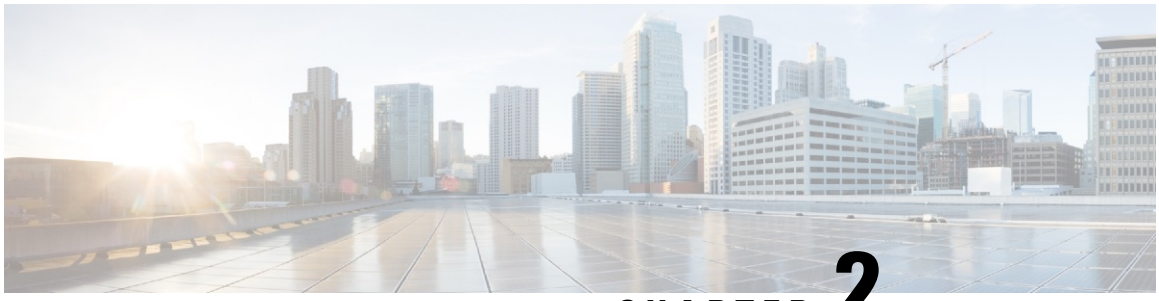
Manager	Description
Firepower Device Manager (FDM)	FDM is a web-based, simplified, on-device manager. Because it is simplified, some FTD features are not supported using FDM. You should use FDM if you are only managing a small number of devices and don't need a multi-device manager. **Note** Both FDM and CDO can discover the configuration on the device, so you can use FDM and CDO to manage the same device. FMC is not compatible with other managers. To get started with FDM, see Firepower Threat Defense Deployment with FDM, on page 43.
Cisco Defense Orchestrator (CDO)	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. In 6.7 and later, CDO offers Low Touch Provisioning that lets branch offices plug in their hardware and leave it alone: the device will automtically register with CDO. **Note** Both FDM and CDO can discover the configuration on the device, so you can use FDM and CDO to manage the same device. FMC is not compatible with other managers. To get started with CDO, see Firepower Threat Defense Deployment with CDO, on page 5.
Firepower Management Center (FMC)	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. **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. To get started with FMC, see Firepower Threat Defense Deployment with FMC, on page 67. For a remote branch setup, we recommend that you use the standalone document specific to that deployment.
FTD REST API	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 device. You cannot use this API if you are managing the FTD using FMC. The FTD REST API is not covered in this guide. For more information, see the FTD REST API guide.

Manager	Description
FMC REST API	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. The FMC REST API is not covered in this guide. For more information, see the FMC REST API guide.

ASA Managers

Table 2: ASA Managers

Manager	Description
Adaptive Security Device Manager (ASDM)	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 device, so you can also use the CLI, CDO, or CSM with ASDM. To get started with ASDM, see ASA Deployment with ASDM, on page 105.
CLI	You should use the ASA CLI if you prefer CLIs over GUIs. The CLI is not covered in this guide. For more information, see the ASA configuration guides.
Cisco Defense Orchestrator (CDO)	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 device, so you can also use the CLI or ASDM. CDO is not covered in this guide. To get started with CDO, see the CDO home page.
Cisco Security Manager (CSM)	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 device, so you can also use the CLI or ASDM. CSM does not support managing FTDs. CSM is not covered in this guide. For more information, see the CSM user guide.
ASA REST API	The ASA REST API lets you automate ASA configuration. However, the API does not include all ASA features, and is no longer being enhanced. The ASA REST API is not covered in this guide. For more information, see the ASA REST API guide.



CHAPTER 2

Firepower Threat Defense Deployment with CDO

Is This Chapter for You?

This chapter explains how to onboard your Firepower Threat Defense (FTD) device to Cisco Defense Orchestrator (CDO) using CDO's onboarding wizard. Before you onboard your FTD device, you need to complete the initial system configuration using the local Firepower Device Manager (FDM), which is hosted directly on the device.

CDO is a cloud-based multi-device manager that facilitates management of security policies in highly distributed environments to achieve consistent policy implementation. CDO helps you optimize your security policies by identifying inconsistencies with them and by giving you tools to fix them. CDO gives you ways to share objects and policies, as well as make configuration templates, to promote policy consistency across devices.

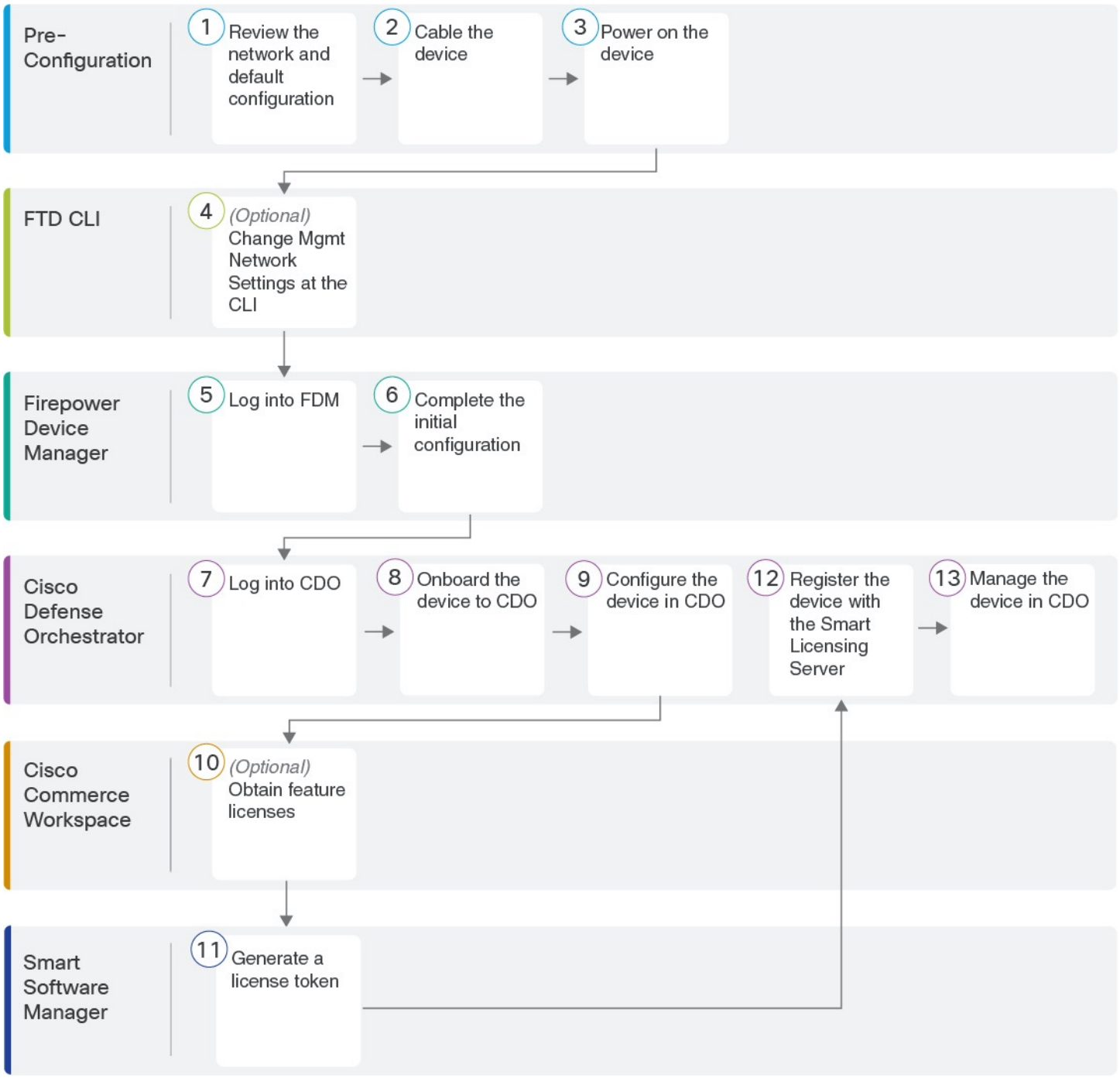
Note This document assumes the Firepower 1100 hardware has a pre-installed FTD image on it. The Firepower 1100 hardware can run either FTD software or ASA software. Switching between FTD and ASA requires you to reimage the device. See Reimage the Cisco ASA or Firepower Threat Defense Device.

Note The Firepower 1100 runs an underlying operating system called the Firepower eXtensible Operating System (FXOS). The Firepower 1100 does not support the FXOS Firepower Chassis Manager; only a limited CLI is supported for troubleshooting purposes. See the FXOS troubleshooting guide for more information.

Note **Privacy Collection Statement**—The Firepower 1100 Series 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

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



1	Pre-Configuration	Review the Network Deployment and Default Configuration, on page 8.
2	Pre-Configuration	Cable the Device, on page 11.

3	Pre-Configuration	Power on the Device, on page 12.
4	FTD CLI	(Optional) Change Management Network Settings at the CLI, on page 12.
5	Firepower Device Manager	Log Into FDM, on page 14.
6	Firepower Device Manager	Complete the Initial Configuration, on page 15.
7	Cisco Defense Orchestrator	Log Into CDO with Cisco Secure Sign-On, on page 19.
8	Cisco Defense Orchestrator	Onboard the Device to CDO, on page 21.
9	Cisco Defense Orchestrator	Configure the Device in CDO, on page 27.
10	Cisco Commerce Workspace	(Optional) Configure Licensing, on page 31: Obtain feature licenses.
11	Smart Software Manager	Configure Licensing, on page 31: Generate a license token.
12	Cisco Defense Orchestrator	Configure Licensing, on page 31: Register the device with the Smart Licensing Server.
13	Cisco Defense Orchestrator	Manage the Device with CDO, on page 37.

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.

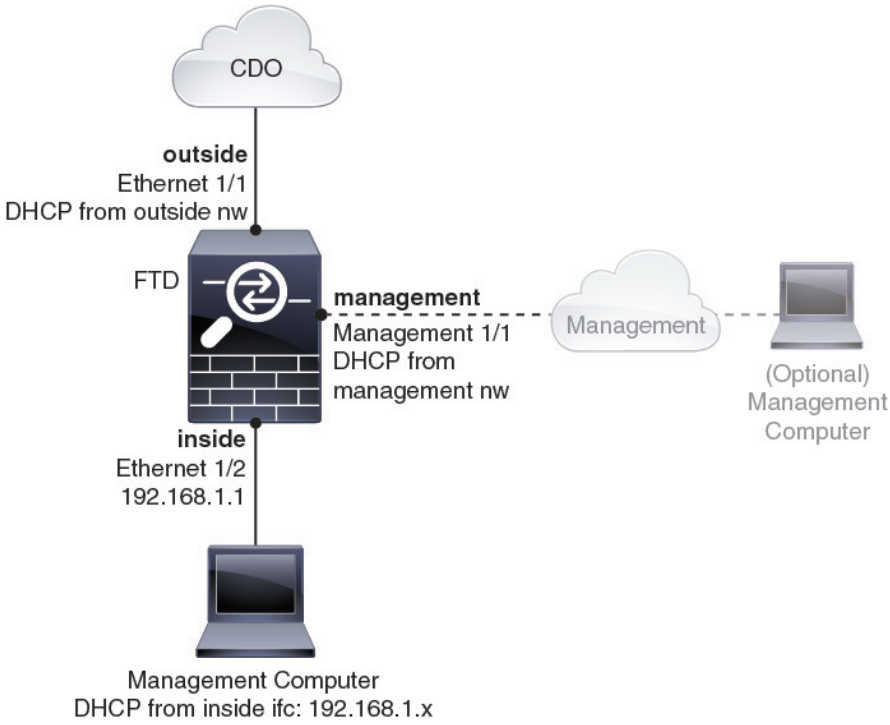
The following figure shows the recommended network deployment for the Firepower 1100. If you connect the outside interface directly to a cable modem or DSL modem, we recommend that you put the modem into bridge mode so the FTD performs all routing and NAT for your inside networks. If you need to configure 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. See Access the FTD and FXOS CLI, on page 38.

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:

- 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.

Figure 1: Suggested Network Deployment



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

Default Configuration

The configuration for the Firepower device after initial setup includes the following:

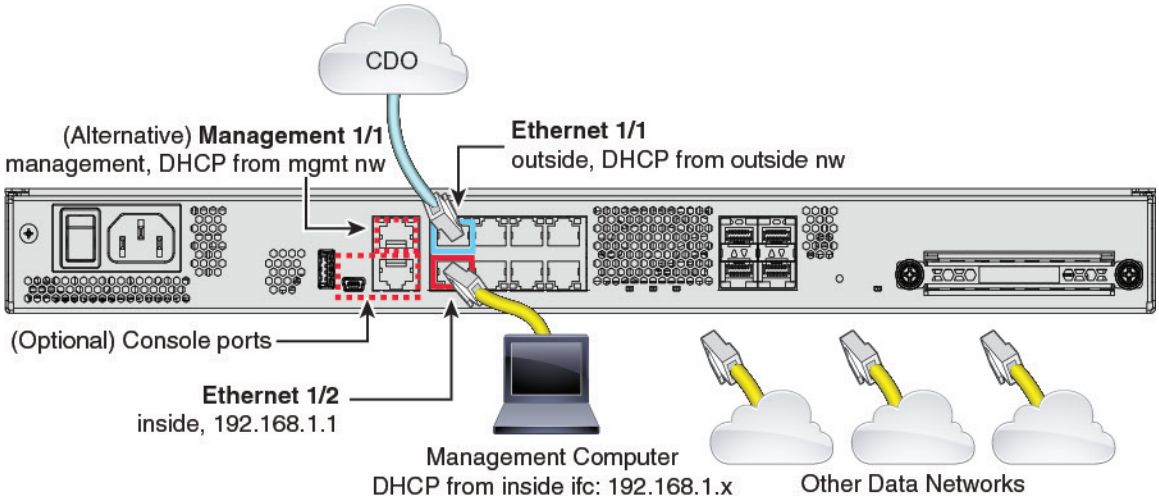
- **inside**—Ethernet 1/2, IP address 192.168.1.1
- **outside**—Ethernet 1/1, IP address from DHCP or an address you specify during setup
- **inside→outside** traffic flow
- **management**—Management 1/1 (management)
  - (6.6 and later) IP address from DHCP
  - (6.5 and earlier) IP address 192.168.45.45

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: 208.67.222.222, 208.67.220.220, 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 FTD requires internet access for licensing and updates.
- **DHCP server**—Enabled on the inside interface and (6.5 and earlier only) management interface
- **FDM access**—Management and inside hosts allowed
- **NAT**—Interface PAT for all traffic from inside to outside

Cable the Device



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

Manage the Firepower 1100 on either Management 1/1 or Ethernet 1/2. The default configuration also configures Ethernet1/1 as outside.

Procedure

Step 1 Connect your management computer to either of the following interfaces:

- Ethernet 1/2—Connect your management computer directly to Ethernet 1/2 for initial configuration, or connect Ethernet 1/2 to your inside network. Ethernet 1/2 has a default IP address (192.168.1.1) 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 (see Default Configuration, on page 9).
- Management 1/1 (labeled MGMT)—Connect Management 1/1 to your management network, and make sure your management computer is on—or has access to—the management network. Management 1/1 obtains an IP address from a DHCP server on your management network; if you use this interface, you must determine the IP address assigned to the FTD so that you can connect to the IP address from your management computer.

  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 computer to the console port. See (Optional) Change Management Network Settings at the CLI, on page 12.

You can later configure FDM management access from other interfaces; see the FDM configuration guide.

Step 2 Connect the outside network to the Ethernet1/1 interface (labeled WAN).

By default, the IP address is obtained using DHCP, 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. The power switch is implemented as a soft notification switch that supports graceful shutdown of the system to reduce the risk of system software and data corruption.

Before you begin

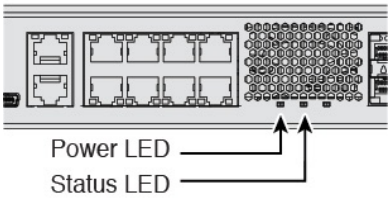
It's important that you provide reliable power for your device (for example, using an uninterruptable power supply (UPS)). Loss of power without first shutting down can cause serious file system damage. There are many processes running in the background all the time, and losing power does not allow the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



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

Note When the switch is toggled from ON to OFF, it may take several seconds for the system to eventually power off. During this time, the Power LED on the front of the chassis blinks green. Do not remove the power until the Power LED is completely off.

(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 CDO or FDM.

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 FTD command reference.

Procedure

Step 1 Connect to the FTD console port. See Access the FTD and FXOS CLI, on page 38 for more information.

Log in with the **admin** user and the default password, **Admin123**.

You connect to the FXOS CLI. The first time you log in, you are prompted to change the password. This password is also used for the FTD login for SSH.

Example:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

Step 2 Connect to the FTD CLI.

connect ftd

Example:

```
firepower# connect ftd
>
```

Step 3 The first time you log in to FTD, you are prompted to accept the End User License Agreement (EULA). 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 outgoing 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 FDM on the Management interface if you are directly-connected to the Management network, but for remote management on Management, you need to enter the IP address

of a gateway router on the Management network. 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 CDO or FDM. 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 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 4 Log into FDM on the new Management IP address.

What to do next

When you choose to use the CLI to change your management network settings, you'll accept the EULA, change the IP addresses, and change the password. You can then complete the initial configuration; see Complete the Initial Configuration, on page 15.

Log Into FDM

Log into FDM to configure your FTD. You use the FDM setup wizard to complete the initial configuration prior to onboarding the device to CDO.

Before you begin

- Use a current version of Firefox or Chrome.

Procedure

Step 1 Enter the following URL in your browser.

- Inside (Ethernet 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 thedefault password **Admin123**.

What to do next

- Run through the FDM setup wizard; see Complete the Initial Configuration, on page 15.

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 (Ethernet1/1) and an inside interface (Ethernet1/2).
- 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.

Attention If you used the CLI to connect to the console port and perform initial setup at the CLI, some of these setup items (accepting the EULA, setting the management interface and gateway address), should have already been completed. You can then complete the remaining configuration items.

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 Select **Start 90 day evaluation period without registration**.

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

Attention Choose to use the 90 day evaluation license even if you have a Smart Software Manager account and available licences. You can Smart License the FTD after you have onboarded it to CDO. Making this choice avoids having to unregister and re-register the license.

Step 5 Click **Finish**.

What to do next

- Continue to to begin the onboarding process.
- You should register and license your device after you onboard to CDO; see Onboard the Device to CDO, on page 21.

Log Into CDO

CDO uses Cisco Secure Sign-On as its identity provider and Duo Security for multi-factor authentication (MFA). CDO requires MFA which provides an added layer of security in protecting your user identity.

Two-factor authentication, a type of MFA, requires two components, or factors, to ensure the identity of the user logging into CDO.

The first factor is a username and password, and the second is a one-time password (OTP), which is generated on demand from Duo Security.

After you establish your Cisco Secure Sign-On credentials, you can log into CDO from your Cisco Secure Sign-On dashboard. From the Cisco Secure Sign-On dashboard, you can also log into any other supported Cisco products.

- If you have a Cisco Secure Sign-On account, skip ahead to Log Into CDO with Cisco Secure Sign-On, on page 19.
- If you don't have a Cisco Secure Sign-On account, see Create a New Cisco Secure Sign-On Account, on page 17.

Create a New Cisco Secure Sign-On Account

The initial sign-on workflow is a four-step process. You need to complete all four steps.

Before you begin

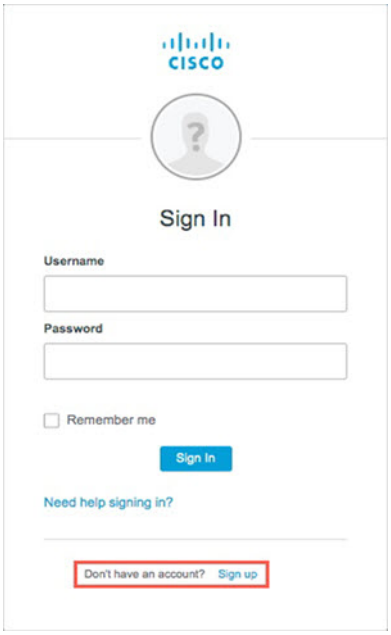
- **Install DUO Security—**We recommend that you install the Duo Security app on a mobile phone. Review Duo Guide to Two Factor Authentication: Enrollment Guide if you have questions about installing Duo.
- **Time Synchronization—**You are going to use your mobile device to generate a one-time password. It is important that your device clock is synchronized with real time as the OTP is time-based. Make sure your device clock is set to the correct time.
- Use a current version of Firefox or Chrome.

Procedure

Step 1 **Sign Up for a New Cisco Secure Sign-On Account.**

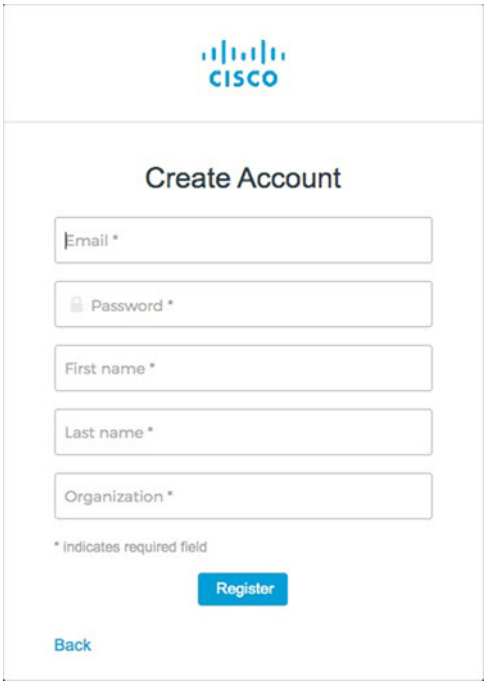
a) Browse to https://sign-on.security.cisco.com.
b) At the bottom of the Sign In screen, click **Sign up**.

Figure 2: Cisco SSO Sign Up



c) Fill in the fields of the **Create Account** dialog and click **Register**.

Figure 3: Create Account



Tip Enter the email address that you plan to use to log in to CDO and add an Organization name to represent your company.

d) After you click **Register**, Cisco sends you a verification email to the address you registered with. Open the email and click **Activate Account**.

Step 2 **Set up Multi-factor Authentication Using Duo.**

a) In the **Set up multi-factor authentication** screen, click **Configure**.

b) Click **Start setup** and follow the prompts to choose a device and verify the pairing of that device with your account.

For more information, see Duo Guide to Two Factor Authentication: Enrollment Guide. If you already have the Duo app on your device, you'll receive an activation code for this account. Duo supports multiple accounts on one device.

c) At the end of the wizard click **Continue to Login**.

d) Log in to Cisco Secure Sign-On with the two-factor authentication.

Step 3 (Optional) **Setup Google Authenticator as a an additional authenticator.**

a) Choose the mobile device you are pairing with Google Authenticator and click **Next**.

b) Follow the prompts in the setup wizard to setup Google Authenticator.

Step 4 **Configure Account Recovery Options for your Cisco Secure Sign-On Account.**

a) Choose a "forgot password" question and answer.

b) Choose a recovery phone number for resetting your account using SMS.

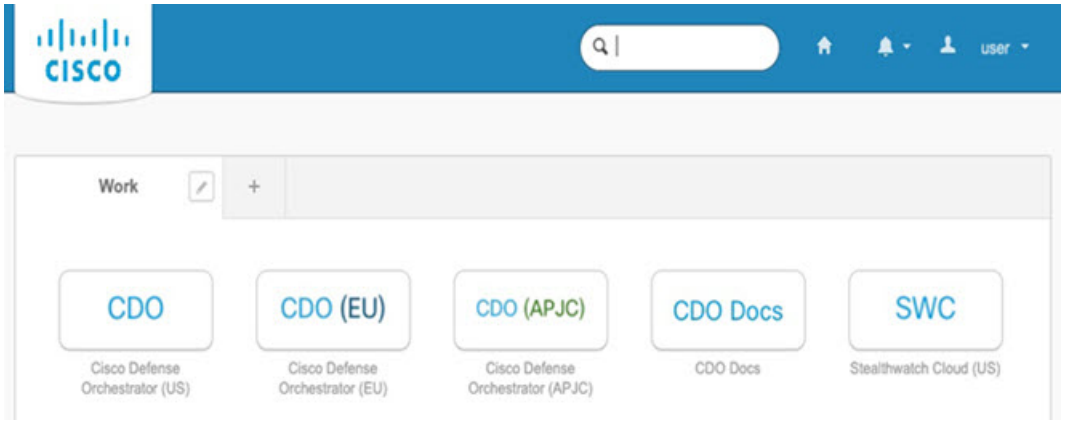
c) Choose a security image.

d) Click **Create My Account**.

You now see the Cisco Security Sign-On dashboard with the CDO app tiles. You may also see other app tiles.

Tip You can drag the tiles around on the dashboard to order them as you like, create tabs to group tiles, and rename tabs.

Figure 4: Cisco SSO Dashboard



Log Into CDO with Cisco Secure Sign-On

Log into CDO to onboard and manage your FTD.

Before you begin

Cisco Defense Orchestrator (CDO) uses Cisco Secure Sign-On as its identity provider and Duo Security for multi-factor authentication (MFA).

- To log into CDO, you must first create your account in Cisco Secure Sign-On and configure MFA using Duo; see Create a New Cisco Secure Sign-On Account, on page 17.
- Use a current version of Firefox or Chrome.

Procedure

Step 1 In a web browser, navigate to https://sign-on.security.cisco.com/.

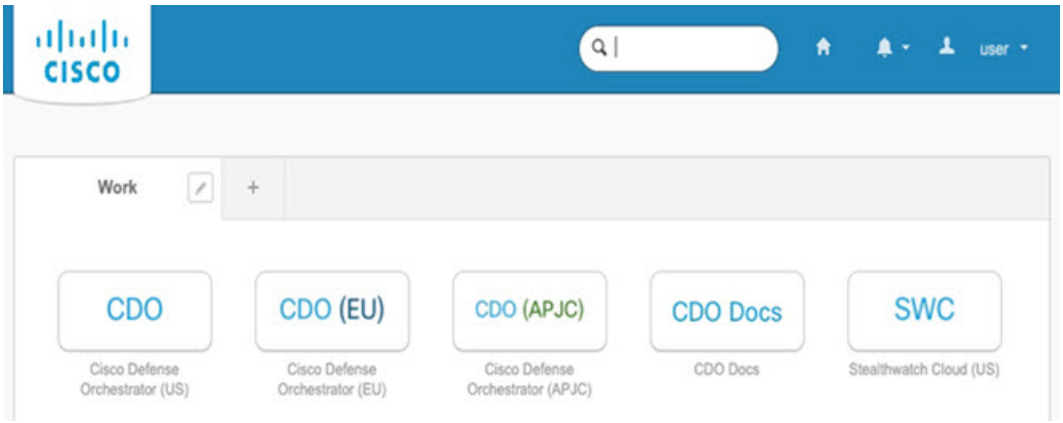
Step 2 Enter your **Username** and **Password**.

Step 3 Click **Log in**.

Step 4 Receive another authentication factor using Duo Security, and confirm your login. The system confirms your login and displays the Cisco Secure Sign-On dashboard.

Step 5 Click the appropriate CDO tile on the Cisco Secure Sign-on dashboard. The **CDO** tile directs you to https://defenseorchestrator.com, the **CDO (EU)** tile directs you to https://defenseorchestrator.eu, and the **CDO (APJC)** tile directs you to to https://www.apj.cdo.cisco.com.

Figure 5: Cisco SSO Dashboard



Step 6 Click the authenticator logo to choose **Duo Security** or **Google Authenticator**, if you have set up both authenticators.

- If you already have a user record on an existing tenant, you are logged into that tenant.
- If you already have a user record on several tenants, you will be able to choose which CDO tenant to connect to.
- If you do not already have a user record on an existing tenant, you will be able to learn more about CDO or request a trial account.

Onboard the Device to CDO

Before you onboard a device, make sure that you complete the FDM installation wizard. Then use CDO's onboarding wizard to onboard your device and license the device.

You can onboard a device in one of two ways:

- With a registration key (recommended).
- With device credentials (username and password) and an IP address.

Attention We recommend using the evaluation license until you onboard the device. Any additional licenses you register with the Smart Software Manager will have to be unregistered before you can onboard to CDO, and then registered again; see Configure Licensing, on page 54.

Onboard With a Registration Key (Recommended)

You can onboard your devices with a registration key. We recommend this method especially if your device uses DHCP to obtain its IP address. If that IP address changes your device remains connected to CDO.

Onboard With Credentials and IP Address

You can onboard an FTD using the device's administrator username and password, and the IP address of the device's outside, inside, or management interface depending on how the device is configured in your network; see the network configuration and deployment details for your device.

CDO needs HTTPS access to the device in order to manage it. How you allow HTTPS access to the device depends on how your FTD is configured in your network, and whether your Secure Device Connector (SDC) is installed on-premise or in the cloud.

Important If you connect to https://www.defenseorchestrator.eu you must onboard your device using username, password, and IP address. You cannot use a registration key to onboard the FTD device.

Using a cloud SDC allows management access to the device's outside interface. Using an on-premise SDC allows management access to the device using the inside or management interface. Note that when using the FTD as the head-end for VPN connections, you will not be able to use the outside interface to manage the device.

See Connect Cisco Defense Orchestrator to the Secure Device Connector for more information about how to connect CDO to your SDC and what network access needs to be allowed.

Onboard an FTD with a Registration Key (Recommended)

We recommend that you onboard an FTD device using a registration key. If your FTD is assigned an IP address using DHCP and the address changes for some reason, your FTD remains connected to CDO. Additionally, your FTD can have an address on your local area network, and as long as the device can access the outside network, you can onboard it to CDO using this method.

Attention If you have a SecureX or Cisco Threat Response (CTR) account, you will need to merge your CDO account and SecureX/CTR account in order for your devices to be registered with SecureX. Until your accounts are merged, you cannot see your device's events in SecureX or benefit from other SecureX features. We strongly recommend merging your accounts before you create a CDO module in SecureX. Your accounts can be merged through the SecureX portal. See Merge Accounts for instructions.

Guidelines for Devices Running Version 6.6+

See Onboard an FTD with a Registration Key (Version 6.6+), on page 22 to onboard a device running Firepower Version 6.6+.

- Your device can be using a 90-day evaluation license or it can be smart-licensed. You will not need to unregister licenses installed on the device from the Cisco Smart Software Manager.
- Your device cannot already be registered with Cisco Cloud Services; see Unregister an FTD from Cisco Cloud Services, on page 39 before you attempt to onboard the device.
- You can use this method to onboard your device to the US, EU, or APJ regions.

Guidelines for Devices Running Versions 6.4 or 6.5

See Onboard an FTD with a Registration Key (Version 6.4 or 6.5), on page 24 to onboard a device running Firepower Version 6.4 or 6.5.

- Make sure the licenses installed on the device are not registered with Cisco Smart Software Manager. You will need to unregister the FTD if it is already smart-licensed; see Unregister a Smart-Licensed FTD, on page 39.
- Your device should be configured to use the 90-day evaluation license.
- You can use this method to onboard your device to the US (Version 6.4 or 6.5), EU (Version 6.5), or APJ (Version 6.5) regions.

Onboard an FTD with a Registration Key (Version 6.6+)

Follow this procedure to onboard an FTD device using a registration key.

Before you begin

- This method is supported for the US, EU, and APJ regions.
- Your device MUST be managed by Firepower Device Manager (FDM).
- Your device can be using a 90-day evaluation license or it can be smart-licensed. You will not need to unregister licenses installed on the device from the Cisco Smart Software Manager.
- Your device cannot already be registered with Cisco Cloud Services; see Unregister an FTD from Cisco Cloud Services, on page 39 before you attempt to onboard the device.
- Log into FDM and make sure that there are no pending changes waiting on the device.
- Make sure DNS is configured properly on your FTD device.

- Make sure the time services are configured properly on the FTD device. Make sure the FTD device shows the correct date and time, otherwise the onboarding will fail.
- Review Connect Cisco Defense Orchestrator to the Secure Device Connector.

Procedure

Step 1 In the navigation pane, click **Devices & Services**, then click the blue plus button to **Onboard** a device.

Step 2 Click the **FTD** card.

Step 3 On the Onboard FTD Device screen, click **Use Registration Key**.

Step 4 In the Device Name area, enter the device name in the **Device Name** field. This could be the hostname of the device or any other name you choose, then click **Next**.

Step 5 In the **Database Updates** area, the **Immediately perform security updates, and enable recurring updates** is enabled by default.

This option immediately triggers a security update as well as automatically schedules the device to check for additional updates every Monday at 2AM. See Update FTD Security Databases and Schedule a Security Database Update for more information.

Note Disabling this option does not affect any previously scheduled updates you may have configured through FDM.

Step 6 Click **Next**.

Step 7 In the **Create Registration Key** area, CDO generates a registration key.

Attention If you navigate away from the onboarding screen after the key is generated and before the device is fully onboarded, you will not be able to return to the onboarding screen. However, CDO creates a placeholder for that device on the **Device & Services** page. Select the device placeholder to see the key for that device.

Step 8 Click the **Copy** icon to copy the registration key.

Note You can skip copying the registration key and click **Next** to complete the place holder entry for the device and later, register the device. This option is useful when you're attempting to create the device first and later register it, or if you're a Cisco partner installing a Proof of Value (POV) device in a customer network.

The device is now in the connectivity state, "Unprovisioned". Copy the registration key that appears under **Unprovisioned** to Firepower Defense Manager to complete the onboarding process.

Step 9 Log into FDM on the device you want to onboard to CDO.

Step 10 In the Cisco Defense Orchestrator tile, click **Get Started**.

Step 11 In the **Registration Key** field, paste the registration key that you generated in CDO.

Step 12 In the **Region** field, select the Cisco cloud region to which your tenant is assigned:

- Choose **US** if you log in to *defenseorchestrator.com*.
- Choose **EU** if you log in to *defenseorchestrator.eu*.
- Choose **APJ** if you log in to *apj.cdo.cisco.com*.

Step 13 Click **Register** and then **Accept** the Cisco Disclosure. FDM sends the registration request to CDO.

Step 14 Return to CDO. In the **Smart License** area, apply your Smart License to the FTD device and click **Next**.

For more information, see Configure Licensing, on page 31. Click **Skip** to continue the onboarding with a 90-day evaluation license.

Step 15 From **Devices & Services**, observe that the device status progresses from *"Unprovisioned"* to *"Locating"* to *"Syncing"* to *"Synced."*

Step 16 In the **Done** area, click **Go to devices** page to view the onboarded device.

Onboard an FTD with a Registration Key (Version 6.4 or 6.5)

Follow this procedure to onboard an FTD device using a registration key.

Before you begin

- (Version 6.4) This method is only supported for the US region (defenseorchestrator.com).

Note For the EU region (defenseorchestrator.eu), this method is available from Version 6.5+. For devices running Version 6.4, you can only onboard your FTD device using username, password, and IP address. You cannot use a registration key.

- (Version 6.5) This method is supported for the US, EU, and APJ (apj.cdo.cisco.com) regions.
- Your device MUST be managed by Firepower Device Manager (FDM).
- Make sure the licenses installed on the device are not registered with Cisco Smart Software Manager. You will need to unregister the FTD if it is already smart-licensed; see Unregister a Smart-Licensed FTD, on page 39.
- Your device should be configured to use the 90-day evaluation license.
- Log into FDM and make sure that there are no pending changes waiting on the device.
- Make sure DNS is configured properly on your FTD device.
- Make sure the time services are configured properly on the FTD device. Make sure the FTD device shows the correct date and time, otherwise the onboarding will fail.
- Review Connect Cisco Defense Orchestrator to the Secure Device Connector.

Procedure

Step 1 In the navigation pane, click **Devices & Services**, then click the blue plus button to **Onboard** a device.

Step 2 Click the **FTD** card.

Step 3 On the Onboard FTD Device screen, click **Use Registration Key**.

Step 4 In the Device Name area, enter the device name in the **Device Name** field. This could be the hostname of the device or any other name you choose, then click **Next**.

Step 5 In the **Database Updates** area, the **Immediately perform security updates, and enable recurring updates** is enabled by default.

This option immediately triggers a security update as well as automatically schedules the device to check for additional updates every Monday at 2AM. See Update FTD Security Databases and Schedule a Security Database Update for more information.

Note Disabling this option does not affect any previously scheduled updates you may have configured through FDM.

Step 6 Click **Next**.

Step 7 In the **Create Registration Key** area, CDO generates a registration key.

Attention If you navigate away from the onboarding screen after the key is generated and before the device is fully onboarded, you will not be able to return to the onboarding screen. However, CDO creates a placeholder for that device on the **Device & Services** page. Select the device placeholder to see the key for that device.

Step 8 Click the **Copy** icon to copy the registration key.

Note You can skip copying the registration key and click **Next** to complete the place holder entry for the device and later, register the device. This option is useful when you're attempting to create the device first and later register it, or if you're a Cisco partner installing a Proof of Value (POV) device in a customer network.

The device is now in the connectivity state, "Unprovisioned". Copy the registration key that appears under **Unprovisioned** to Firepower Defense Manager to complete the onboarding process.

Step 9 Log into FDM on the device you want to onboard to CDO.

Step 10 In the Cisco Defense Orchestrator tile, click **Get Started**.

Step 11 In the **Registration Key** field, paste the registration key that you generated in CDO.

Step 12 In the **Region** field, select the Cisco cloud region to which your tenant is assigned:

- Choose **US** if you log in to *defenseorchestrator.com*.
- Choose **EU** if you log in to *defenseorchestrator.eu* (Version 6.5).
- Choose **APJ** if you log in to *apj.cdo.cisco.com* (Version 6.5).

Step 13 Click **Register** and then **Accept** the Cisco Disclosure. FDM sends the registration request to CDO.

Step 14 Return to CDO. In the **Smart License** area, apply your Smart License to the FTD device and click **Next**.

For more information, see Configure Licensing, on page 31. Click **Skip** to continue the onboarding with a 90-day evaluation license.

Step 15 From **Devices & Services**, observe that the device status progresses from *"Unprovisioned"* to *"Locating"* to *"Syncing"* to *"Synced."*

Step 16 In the **Done** area, click **Go to devices** page to view the onboarded device.

Onboard an FTD Using Credentials and IP Address

Use this procedure to onboard an FTD device using only the administrator username and password and the device's Management IP address.

Before you begin

The simplest way to onboard an FTD device is to use login credentials (user name and password) and the IP address. However, we recommend that you onboard your device with a registration key; see Onboard With a Registration Key (Recommended), on page 21.

Important Before you onboard a device to CDO, read Onboard an FTD. It lists the general device requirements and prerequisites to onboard your FTD device.

You need the following information to onboard using this method:

- The administrator username and password.
- The IP address of the interface you are using to manage the device. This may be the MGMT interface, an inside interface, or the outside interface depending on how you have configured your network.
- The device must be managed by Firepower Device Manager (FDM) and configured for local management in order for you to onboard it to CDO. It cannot be managed by the Firepower Management Center (FMC).

Procedure

Step 1 Navigate to the **Devices & Services** page.

Step 2 Click **Onboard**.

Step 3 Click the **FTD** card.

Note CDO may prompt you to read and accept the Firepower Threat Defense End User License Agreement (EULA), which is a one-time activity in your tenant. Once you accept this agreement, CDO does not prompt it again in subsequent FTD onboarding. If the EULA agreement changes in the future, you must accept it again when prompted.

Step 4 At the Onboard FTD Device screen, click **Use Credentials** and give the device a name.

Step 5 In the **Device Location** field, enter the Management interface IP address, hostname, or fully qualified device name of the device. The default port is 443. You can change the port number to reflect your device's configuration.

Step 6 Click **Go**.

Once the location of the device is verified, you're prompted to enter the device administrator's username and password.

Step 7 In the **Database Updates** area, the **Immediately perform security updates, and enable recurring updates** is enabled by default.

This option immediately triggers a security update as well as automatically schedules the device to check for additional updates every Monday at 2AM. See Update FTD Security Databases and Schedule a Security Database Update for more information.

Note Disabling this option does not affect any previously scheduled updates you may have configured through FDM.

Step 8 Click **Connect**.

Step 9 (Optional) Label your device.

Once the credentials are verified, you're prompted to label the device or service. See Labels and Label Groups for more information.

Step 10 When onboarding is complete, CDO shows the device on the **Devices & Services** page with a "Synced" status.

Step 11 In the **Smart License** area, you can apply a smart-license to the FTD device and click **Next**.

For more information, see Configure Licensing, on page 31. Click **Skip** to continue the onboarding with a 90-day evaluation license.

Configure the Device in CDO

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 Log in to the CDO portal, choose **Devices & Services** from the CDO menu, and then select the device you just onboarded.

Step 2 Choose **Management** > **Interfaces** and select the physical interface you want to configure.

Step 3 Click the edit icon () for each interface you want to configure and give the interface a **Logical Name** and, optionally, a **Description**.

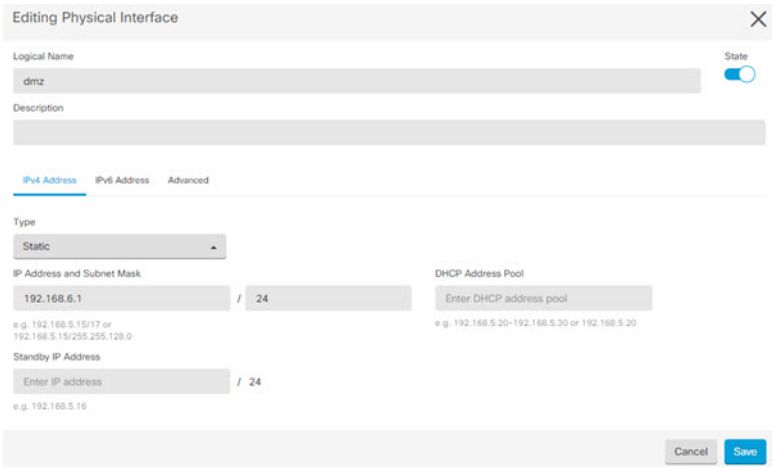
Unless you configure subinterfaces, the interface should have a name.

Note If you change the name, the change is automatically reflected everywhere you used the old name, including security zones, syslog server objects, and DHCP server definitions. However, you cannot remove the name until you first remove all configurations that use the name, because you typically cannot use an unnamed interface for any policy or setting.

Step 4 Set the **Type** 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 6: Edit Interface

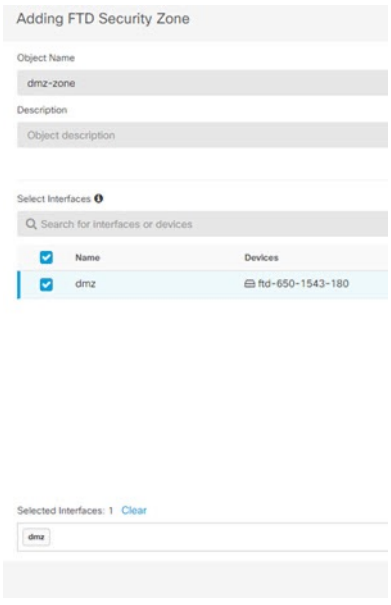


Step 5 If you configured new interfaces, choose **Management** > **Objects**.

Edit or create a new **Security Zone** 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 7: Security Zone Object



Step 6 If you want internal clients to use DHCP to obtain an IP address from the device, choose **Management** > **Settings** > **DHCP Server**, then review the **DHCP Servers** section.

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 review the DNS settings supplied to clients on the **DNS Server** tab. The following example shows how to set up a DHCP server on the inside2 interface with the address pool 192.168.45.46-192.168.45.254.

Figure 8: DHCP Server

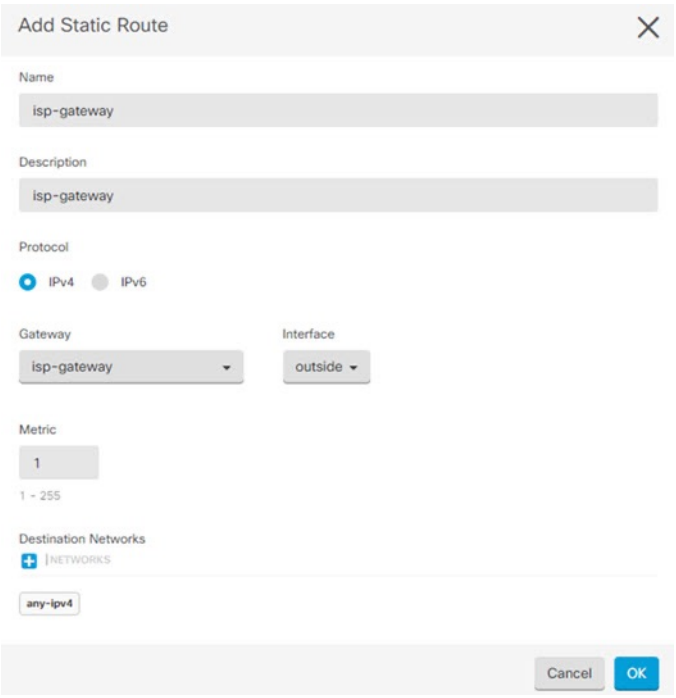
Step 7 Choose **Management** > **Routing**, then click the Add icon to configure a default route.

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 **Management** > **Settings** > **Management Access**.

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 Object** at the bottom of the **Gateway** drop-down list.

Figure 9: Default Route



Step 8 Choose **Management** > **Policy** and configure the security policies for the network.

The initial setup 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.

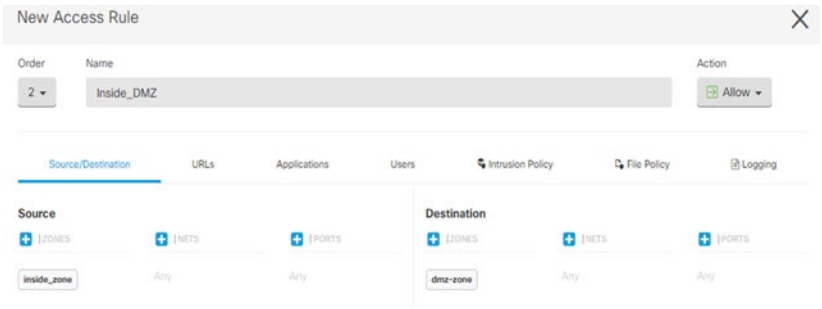
In addition, you can configure other policies to provide additional services, and fine-tune NAT and access rules to get the results that your organization requires. You can configure the following policies:

- **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.
- **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.

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 10: Access Control Policy



Step 9 Locate the **Security Database Updates** section to create a scheduled task to check and update the security databases for an FTD device.

When you onboard an FTD device to CDO, part of the onboarding process allows you to **Enable scheduled recurring updates for databases**. This option is checked by default. When enabled, CDO immediately checks for and applies any security updates as well as automatically schedules the device to check for additional updates. You are able to modify the date and time of the scheduled task after the device is onboarded.

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 10 Click the **Preview and 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.

What to do next

- You should register and license your device after you onboard; see Configure Licensing, on page 31.

Configure Licensing

Configure Licensing

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

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

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 Cisco Smart Software Manager, and purchase the license later. This allows you to deploy and use a feature, and avoid delays due to purchase order approval. See the following licenses:

- **Threat**—Security Intelligence and Cisco Firepower Next-Generation IPS
- **Malware**—Advanced Malware Protection for Networks (AMP)
- **URL**—URL Filtering
- **RA VPN**—AnyConnect Plus, AnyConnect Apex, or AnyConnect VPN Only.

For complete information on licensing your system, see the FDM configuration guide.

Attention Use the evaluation license until you onboard the device to CDO. Any additional licenses you register with the Smart Software Manager will have to be unregistered before you can onboard to CDO, and then registered again; see Unregister a Smart-Licensed FTD, on page 39.

Before you begin

- Have a master account on the Cisco 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.

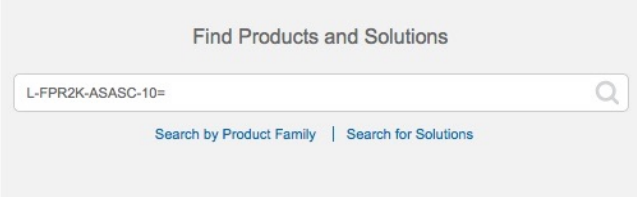
- Your Cisco Smart Software Licensing account must qualify for the Strong Encryption (3DES/AES) license to use some features (enabled using the export-compliance flag).

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 11: 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-FPR1120T-TMC=

- L-FPR1140T-TMC=
- L-FPR1150T-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:

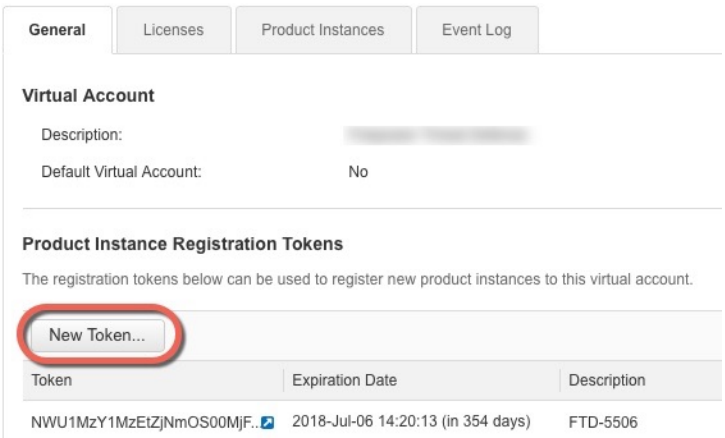
- L-FPR1120T-TMC-1Y
- L-FPR1120T-TMC-3Y
- L-FPR1120T-TMC-5Y
- L-FPR1140T-TMC-1Y
- L-FPR1140T-TMC-3Y
- L-FPR1140T-TMC-5Y
- L-FPR1150T-TMC-1Y
- L-FPR1150T-TMC-3Y
- L-FPR1150T-TMC-5Y

- RA VPN—See the Cisco AnyConnect Ordering Guide.

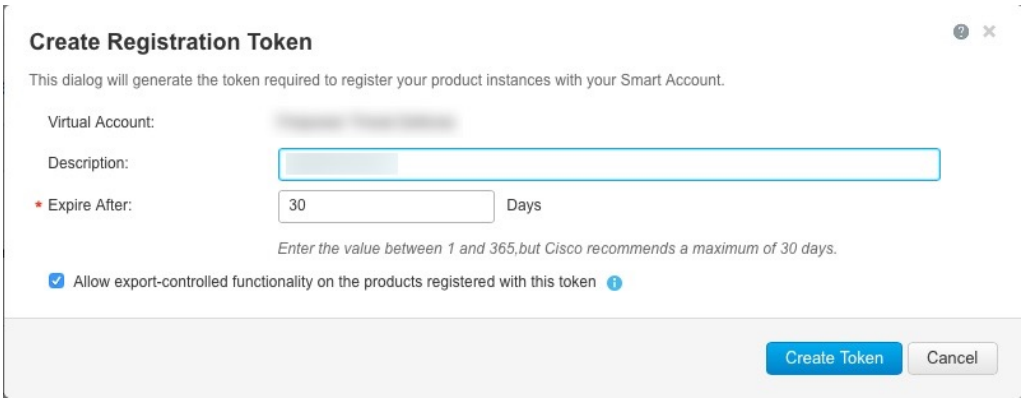
Step 2 In the Cisco Smart Software Manager, request and copy a registration token for the virtual account to which you want to add this device.

a) Click **Inventory**.

b) On the **General** tab, click **New Token**.



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



- **Description**
- **Expire After**—Cisco recommends 30 days.
- **Allow export-controlled functionaility on the products registered with this token**—Enables the export-compliance flag if you are in a country that allows for strong encryption.

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 12: View Token

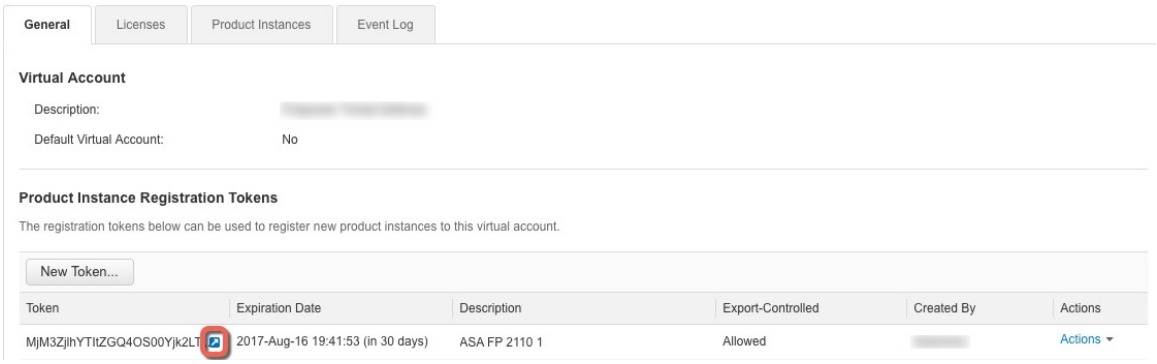
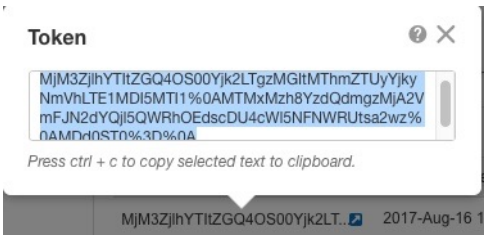


Figure 13: Copy Token

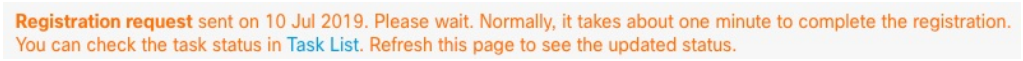


Step 3 In CDO, click **Devices & Services**, and then select the FTD device that you want to license.

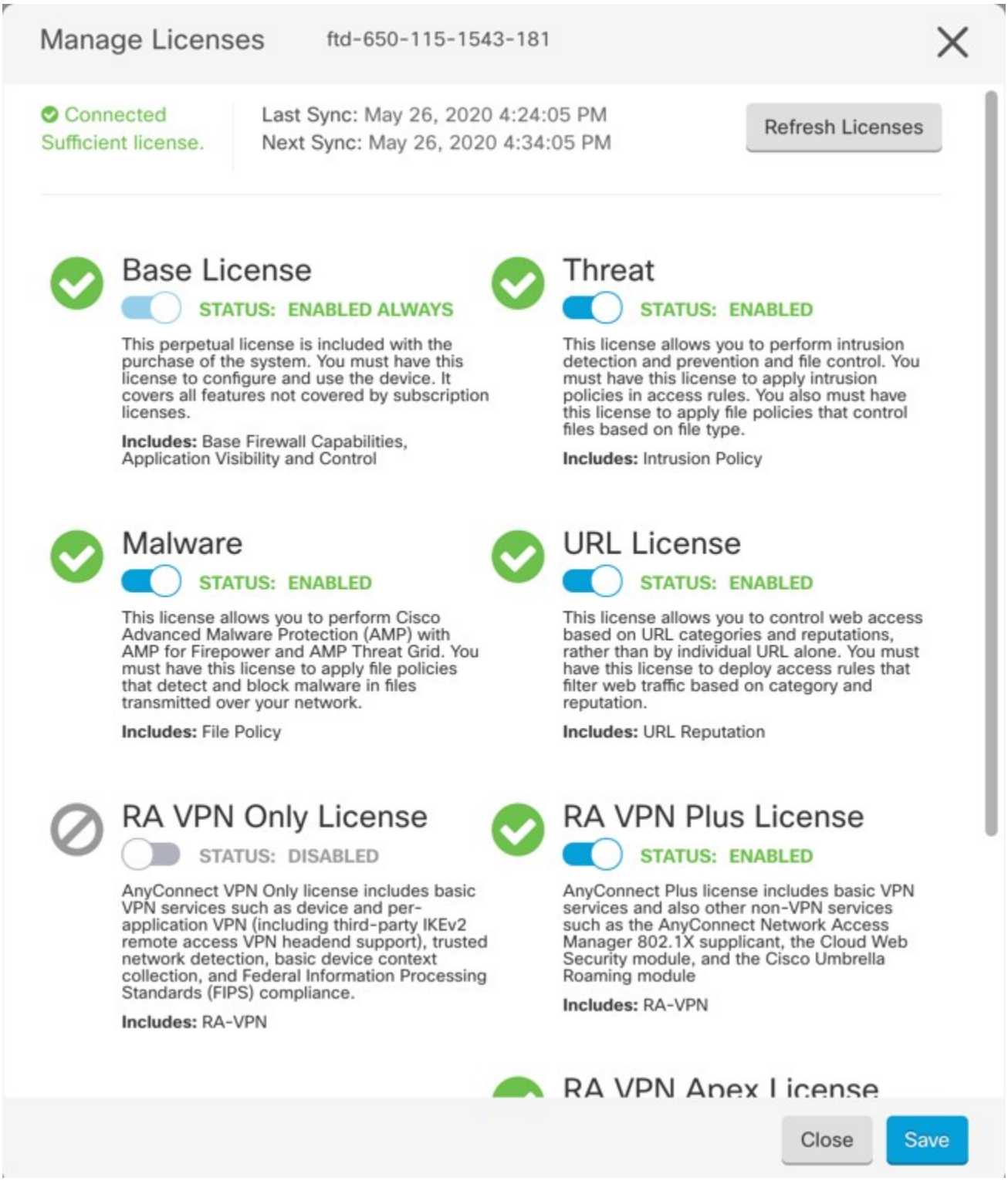
Step 4 In the **Device Actions** pane, click **Manage Licenses**, and follow the on-screen instructions to enter the smart-license generated from Smart Software Manager.

Step 5 Click **Register Device**. After synchronizing with the device, the connectivity state changes to 'Online'.

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



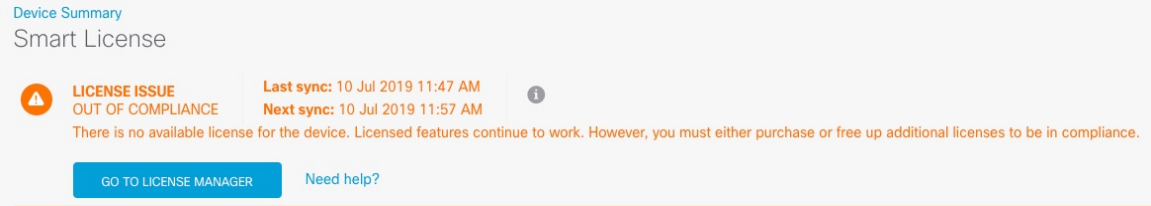
Step 6 After applying the smart license successfully to the FTD device, the device status shows **Connected, Sufficient License**. Click the **Enable/Disable** slider control for each optional license as desired.



- **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 **License Issue, Out of Compliance**:



Step 7 Choose **Refresh Licenses** to synchronize license information with Cisco Smart Software Manager.

Manage the Device with CDO

After having onboarded the device to CDO, you can manage the device with CDO. To manage the FTD with CDO:

1. Browse to https://sign-on.security.cisco.com.
2. Log in as the user you created in Create a New Cisco Secure Sign-On Account, on page 17.
3. Review Managing FTD with Cisco Defense Orchestrator for links to common management tasks.

What to do Next

You have now configured an FTD device and onboarded it to CDO, which provides a simplified management interface and cloud-access to your FTD devices. Use CDO to upgrade software, configure high availability, and configure device settings and network resources for your FTD devices.

Additional FTD Management Procedures

The following topics provide you with some additional information about managing the FTD device:

- Access the FTD and FXOS CLI, on page 38—Use the command-line interface (CLI) to do basic system troubleshooting. Use the FXOS CLI for chassis-level troubleshooting only. Use the FTD CLI for basic configuration, monitoring, and normal system troubleshooting.
- Unregister an FTD from Cisco Cloud Services, on page 39—If your device is running Firepower Version 6.6+ and is already registered with the Cisco cloud, you must unregister the device from Cisco Cloud Services before you onboard it to CDO with a registration key.

- Unregister a Smart-Licensed FTD, on page 39—We highly recommend that you use the evaluation license until you onboard the device to CDO. Any additional licenses you register with the Smart Software Manager will have to be unregistered before you can onboard to CDO, and then registered again.
- Power Off the Device Using FDM, on page 40—If you need to shut down your system for any reason, such as relocating your device, it's important that you follow the recommended procedure to power off the device gracefully.
- What's Next, on page 40—Provides helpful links to CDO resources.

Access the FTD and FXOS 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 also access the FXOS CLI for troubleshooting purposes.

Note You can alternatively SSH to the Management interface of the FTD device. Unlike a console session, the SSH session defaults to the FTD CLI, from which you can connect to the FXOS CLI using the **connect fxos** command. You can later 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. This procedure describes console port access, which defaults to the FXOS CLI.

Procedure

Step 1 To log into the CLI, connect your management computer to the console port. Be sure to install any necessary USB serial drivers for your operating system (see the Firepower 1100 hardware guide). The console port defaults to the FXOS CLI. Use the following serial settings:

- 9600 baud
- 8 data bits
- No parity
- 1 stop bit

You connect to the FXOS CLI. Log in to the CLI using the **admin** username and the password you set at initial setup (the default is **Admin123**).

Example:

```
firepower login: admin
Password:
Last login: Thu May 16 14:01:03 UTC 2019 on ttyS0
Successful login attempts for user 'admin' : 1

firepower#
```

Step 2 Access the FTD CLI.

connect ftd

Example:

```
firepower# connect ftd
>
```

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*.

Step 3 To exit the FTD CLI, enter the **exit** or **logout** command.

This command returns you to the FXOS CLI prompt. For information on the commands available in the FXOS CLI, enter **?**.

Example:

```
> exit
firepower#
```

Unregister an FTD from Cisco Cloud Services

If your device is running Firepower Version 6.6+ and is already registered with the Cisco cloud, you must unregister the device from Cisco Cloud Services before you onboard it to CDO with a registration key.

You can use the following procedure to verify whether or not your device is registered to Cisco Cloud Services, and if so, you can unregistered the device.

Procedure

Step 1 Log on to the FTD using FDM.

Step 2 Click the device icon in the FDM menu.

Step 3 Expand the **System Settings** menu and select **Cloud Services**.

Step 4 On the **Cloud Services** page, click the gear menu and select **Unregister Cloud Services**.

Step 5 Read the warning and click **Unregister** to unregister the device.

What to do next

- After you unregister the device from Cisco Cloud Services, you can then onboard the device to CDO using a registration key; see Onboard an FTD with a Registration Key (Recommended), on page 21.

Unregister a Smart-Licensed FTD

If the FTD is already smart-licensed, the device is likely to be registered with the Smart Software Manager. You must unregister the device from Smart Software Manager before you onboard it to CDO with a registration

key. When you unregister, the base license and all optional licenses associated with the device, are freed in your virtual account.

Note After you unregister the device, the current configuration and policies on the device continue to work as-is, but you cannot make or deploy any changes.

Procedure

Step 1 Log on to the FTD using FDM.

Step 2 Click the name of the device in the FDM menu, then click **View Configuration** in the Smart License summary area.

Step 3 From the gear drop-down menu, choose **Unregister Device**.

Step 4 Read the warning and click **Unregister** to unregister the device.

What to do next

- After you unregister the device with the Smart Software Manager, you can then onboard the device to CDO using a registration token; see Onboard an FTD with a Registration Key (Version 6.4 or 6.5), on page 24.

Power Off the Device Using FDM

You can shut down your system properly using FDM.

Procedure

Step 1 (6.5 and later) Use FDM to shut down the device.

Note For 6.4 and earlier, enter the **shutdown** command at the FDM CLI.

a) Click **Device**, then click the **System Settings** > **Reboot/Shutdown** link.
b) Click **Shut Down**.

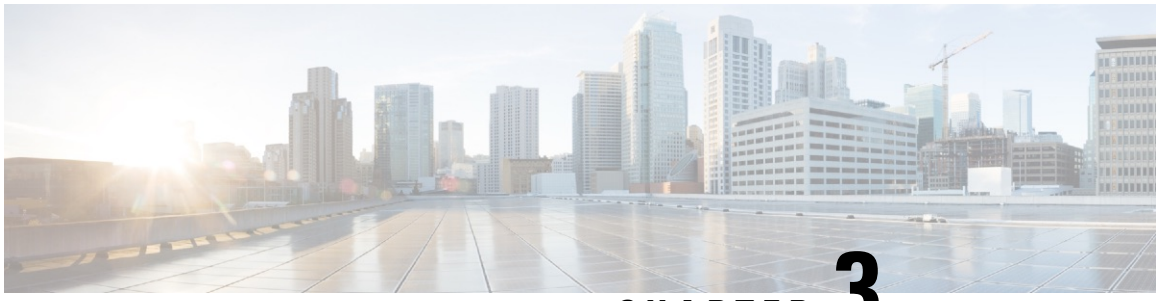
Step 2 Observe the Power LED and Status LED to verify that the chassis is powered off (appear unlit).

Step 3 After the chassis has successfully powered off, you can then unplug the power to physically remove power from the chassis if necessary.

What's Next

To continue configuring your FTD device using CDO, see the CDO Configuration Guides.

For additional information related to using CDO, see the Cisco Defense Orchestrator home page.



CHAPTER 3

Firepower Threat Defense Deployment with FDM

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.

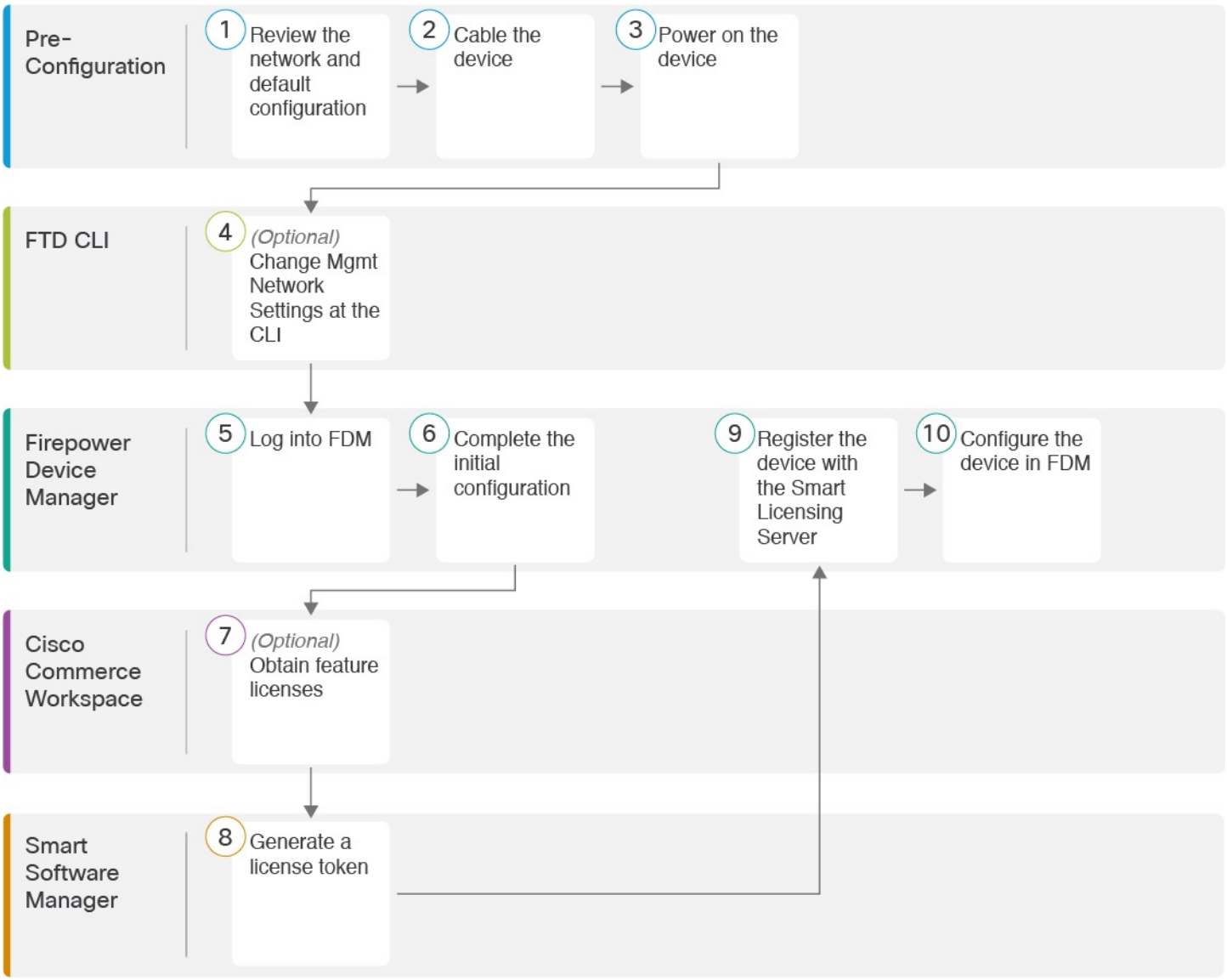
Note The Firepower 1100 Series hardware can run either FTD software or ASA software. Switching between FTD and ASA requires you to reimage the device. See Reimage the Cisco ASA or Firepower Threat Defense Device.

Note The Firepower 1100 runs an underlying operating system called the Firepower eXtensible Operating System (FXOS). The Firepower 1100 does not support the FXOS Firepower Chassis Manager; only a limited CLI is supported for troubleshooting purposes. See the FXOS troubleshooting guide for more information.

Note **Privacy Collection Statement**—The Firepower 1100 Series 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

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



1	Pre-Configuration	Review the Network Deployment and Default Configuration, on page 45.

2	Pre-Configuration	Cable the Device, on page 48.
3	Pre-Configuration	Power on the Device, on page 49.
4	FTD CLI	(Optional) Change Management Network Settings at the CLI, on page 49.
5	Firepower Device Manager	Log Into FDM, on page 51.
6	Firepower Device Manager	Complete the Initial Configuration, on page 52.
7	Cisco Commerce Workspace	(Optional) Configure Licensing, on page 54: Obtain feature licenses.
8	Smart Software Manager	Configure Licensing, on page 54: Generate a license token.
9	Firepower Device Manager	Configure Licensing, on page 54: Register the device with the Smart Licensing Server.
10	Firepower Device Manager	Configure the Device in Firepower Device Manager, on page 60.

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.

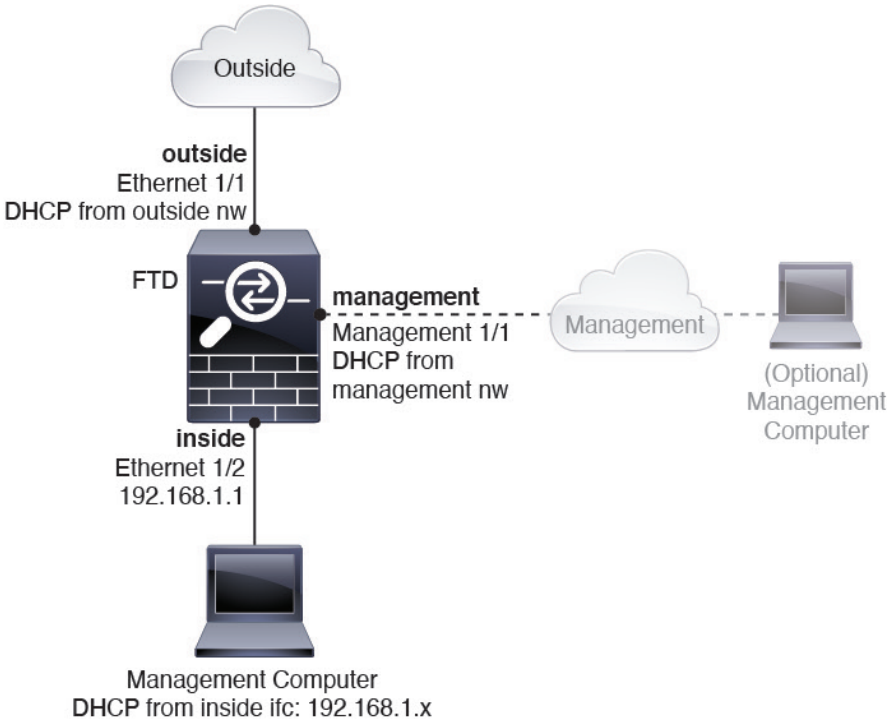
The following figure shows the recommended network deployment for the Firepower 1100. If you connect the outside interface directly to a cable modem or DSL modem, we recommend that you put the modem into bridge mode so the FTD performs all routing and NAT for your inside networks. If you need to configure 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. See (Optional) Change Management Network Settings at the CLI, on page 49.

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:

- 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.

Figure 14: Suggested Network Deployment



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

Default Configuration

The configuration for the Firepower device after initial setup includes the following:

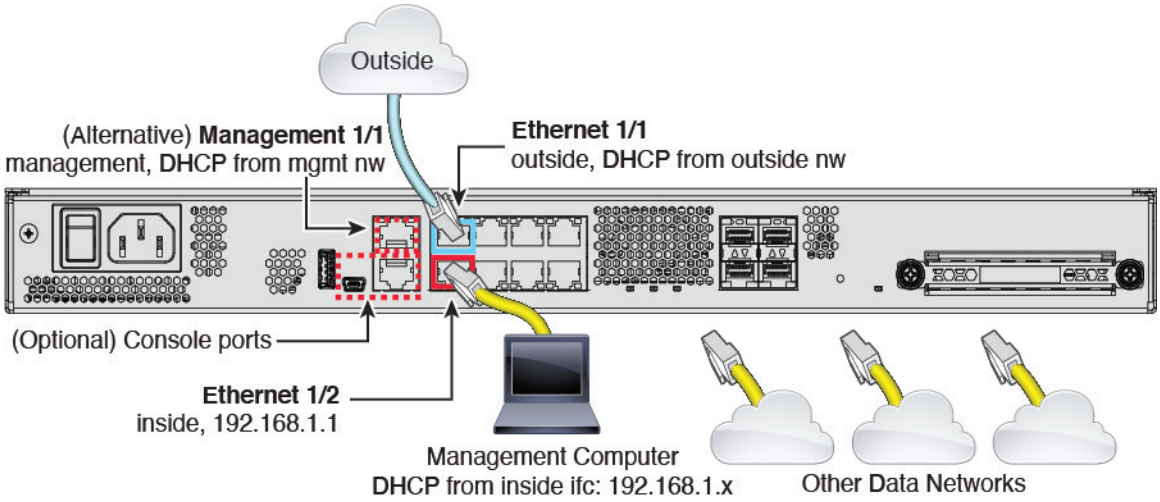
- **inside**—Ethernet 1/2, IP address 192.168.1.1
- **outside**—Ethernet 1/1, IP address from DHCP or an address you specify during setup
- **inside→outside** traffic flow
- **management**—Management 1/1 (management)
  - (6.6 and later) IP address from DHCP
  - (6.5 and earlier) IP address 192.168.45.45

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: 208.67.222.222, 208.67.220.220, 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 FTD requires internet access for licensing and updates.
- **DHCP server**—Enabled on the inside interface and (6.5 and earlier only) management interface
- **FDM access**—Management and inside hosts allowed
- **NAT**—Interface PAT for all traffic from inside to outside

Cable the Device



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

Manage the Firepower 1100 on either Management 1/1 or Ethernet 1/2. The default configuration also configures Ethernet1/1 as outside.

Procedure

Step 1 Connect your management computer to either of the following interfaces:

- Ethernet 1/2—Connect your management computer directly to Ethernet 1/2 for initial configuration, or connect Ethernet 1/2 to your inside network. Ethernet 1/2 has a default IP address (192.168.1.1) 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 (see Default Configuration, on page 9).
- Management 1/1 (labeled MGMT)—Connect Management 1/1 to your management network, and make sure your management computer is on—or has access to—the management network. Management 1/1 obtains an IP address from a DHCP server on your management network; if you use this interface, you must determine the IP address assigned to the FTD so that you can connect to the IP address from your management computer.

  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 computer to the console port. See (Optional) Change Management Network Settings at the CLI, on page 49.

You can later configure FDM management access from other interfaces; see the FDM configuration guide.

Step 2 Connect the outside network to the Ethernet1/1 interface (labeled WAN).

By default, the IP address is obtained using DHCP, 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. The power switch is implemented as a soft notification switch that supports graceful shutdown of the system to reduce the risk of system software and data corruption.

Before you begin

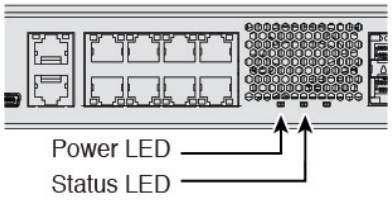
It's important that you provide reliable power for your device (for example, using an uninterruptable power supply (UPS)). Loss of power without first shutting down can cause serious file system damage. There are many processes running in the background all the time, and losing power does not allow the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



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

Note When the switch is toggled from ON to OFF, it may take several seconds for the system to eventually power off. During this time, the Power LED on the front of the chassis blinks green. Do not remove the power until the Power LED is completely off.

(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 CDO or FDM.

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 FTD command reference.

Procedure

Step 1 Connect to the FTD console port. See Access the FTD and FXOS CLI, on page 63 for more information.

Log in with the **admin** user and the default password, **Admin123**.

You connect to the FXOS CLI. The first time you log in, you are prompted to change the password. This password is also used for the FTD login for SSH.

Example:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

Step 2 Connect to the FTD CLI.

connect ftd

Example:

```
firepower# connect ftd
>
```

Step 3 The first time you log in to FTD, you are prompted to accept the End User License Agreement (EULA). 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 outgoing 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 FDM on the Management interface if you are directly-connected to the Management network, but for remote management on Management, you need to enter the IP address

of a gateway router on the Management network. 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 CDO or FDM. 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 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 4 Log into 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.

- Inside (Ethernet 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 thedefault password **Admin123**.

What to do next

- Run through the FDM setup wizard; see Complete the Initial Configuration, on page 52.

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 (Ethernet1/1) and an inside interface (Ethernet1/2).
- 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 49 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 54.

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

Attention If you plan to onboard the device to CDO, we recommend using the evaluation license until you onboard the device. Any additional licenses you register with the Smart Software Manager will have to be unregistered before you can onboard to CDO, and then registered again; see Unregister a Smart-Licensed FTD, on page 39.

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 if using FDM; see Configure Licensing, on page 54.
- You can also choose to onboard the device to CDO. If so, you should register and license your device after you onboard; see Onboard the Device to CDO, on page 21.

- You can also choose to configure the device using FDM; see Configure the Device in Firepower Device Manager, on page 60.

Configure Licensing

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

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

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 Cisco Smart Software Manager, and purchase the license later. This allows you to deploy and use a feature, and avoid delays due to purchase order approval. See the following licenses:

- **Threat**—Security Intelligence and Cisco Firepower Next-Generation IPS
- **Malware**—Advanced Malware Protection for Networks (AMP)
- **URL**—URL Filtering
- **RA VPN**—AnyConnect Plus, AnyConnect Apex, or AnyConnect VPN Only.

For complete information on licensing your system, see the FDM configuration guide.

Before you begin

- Have a master account on the Cisco 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.

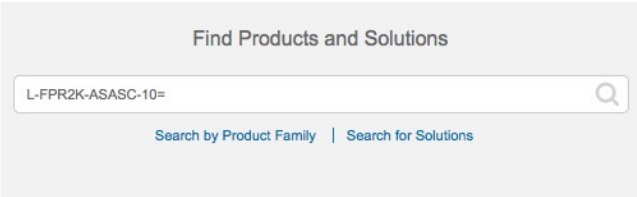
- Your Cisco Smart Software Licensing account must qualify for the Strong Encryption (3DES/AES) license to use some features (enabled using the export-compliance flag).

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 15: License Search



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

- Threat, Malware, and URL license combination:

  Firepower 1010:

  Firepower 1100:

  - L-FPR1120T-TMC=
  - L-FPR1140T-TMC=
  - L-FPR1150T-TMC=

  Firepower 2100:

  ASA 5508-X and 5516-X:

  ISA 3000:

  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:

  Firepower 1010:

  Firepower 1100:

  - L-FPR1120T-TMC-1Y
  - L-FPR1120T-TMC-3Y
  - L-FPR1120T-TMC-5Y
  - L-FPR1140T-TMC-1Y
  - L-FPR1140T-TMC-3Y
  - L-FPR1140T-TMC-5Y
  - L-FPR1150T-TMC-1Y
  - L-FPR1150T-TMC-3Y
  - L-FPR1150T-TMC-5Y

  Firepower 2100:

  ASA 5508-X and 5516-X:

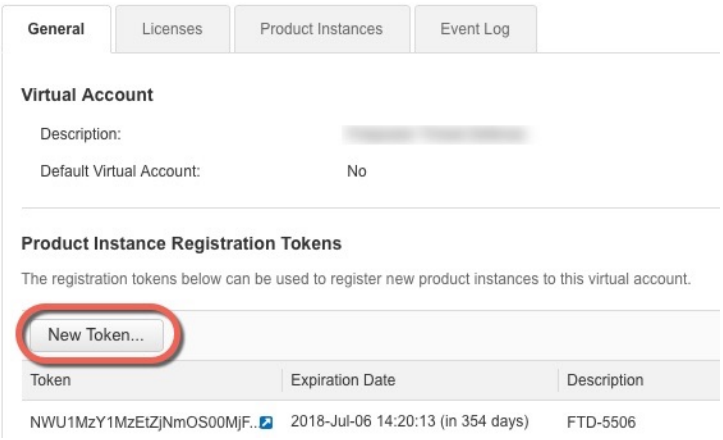
  ISA 3000:

- RA VPN—See the Cisco AnyConnect Ordering Guide.

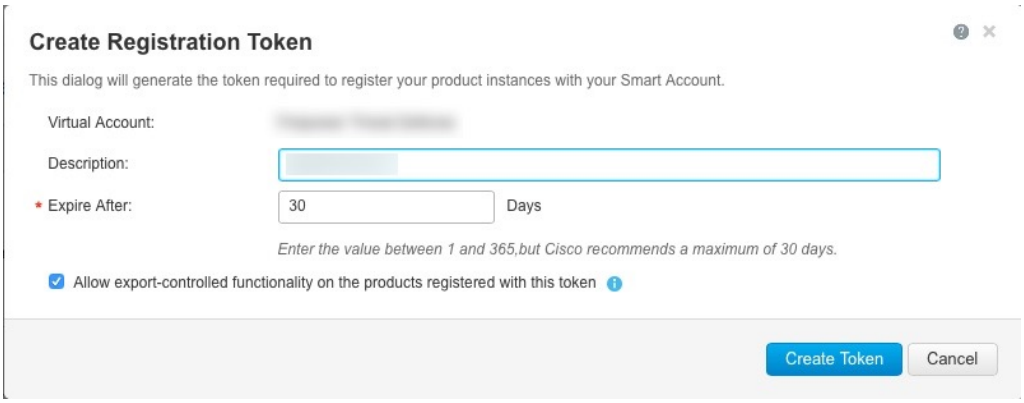
Step 2 In the Cisco Smart Software Manager, request and copy a registration token for the virtual account to which you want to add this device.

a) Click **Inventory**.

b) On the **General** tab, click **New Token**.



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



- **Description**
- **Expire After**—Cisco recommends 30 days.
- **Allow export-controlled functionaility on the products registered with this token**—Enables the export-compliance flag if you are in a country that allows for strong encryption.

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 16: View Token

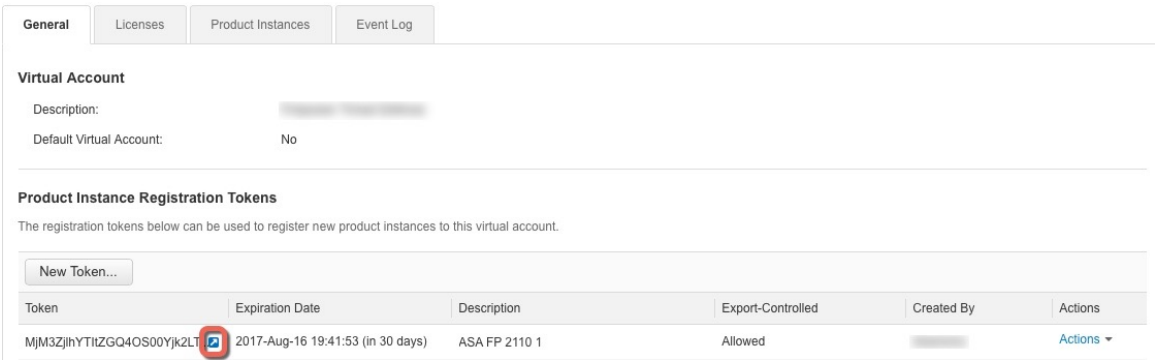
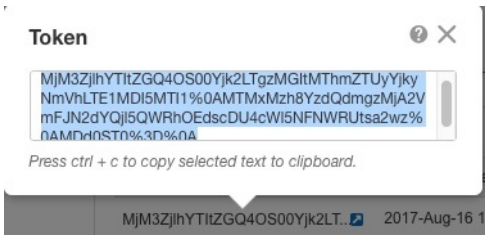


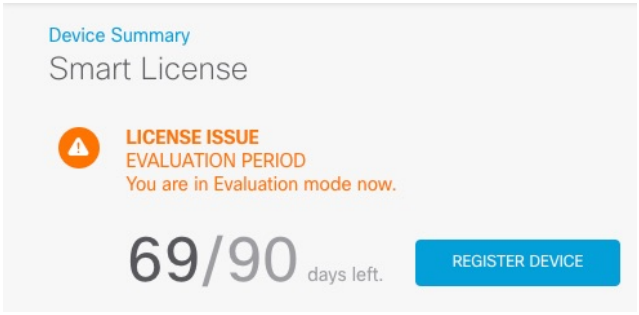
Figure 17: Copy Token



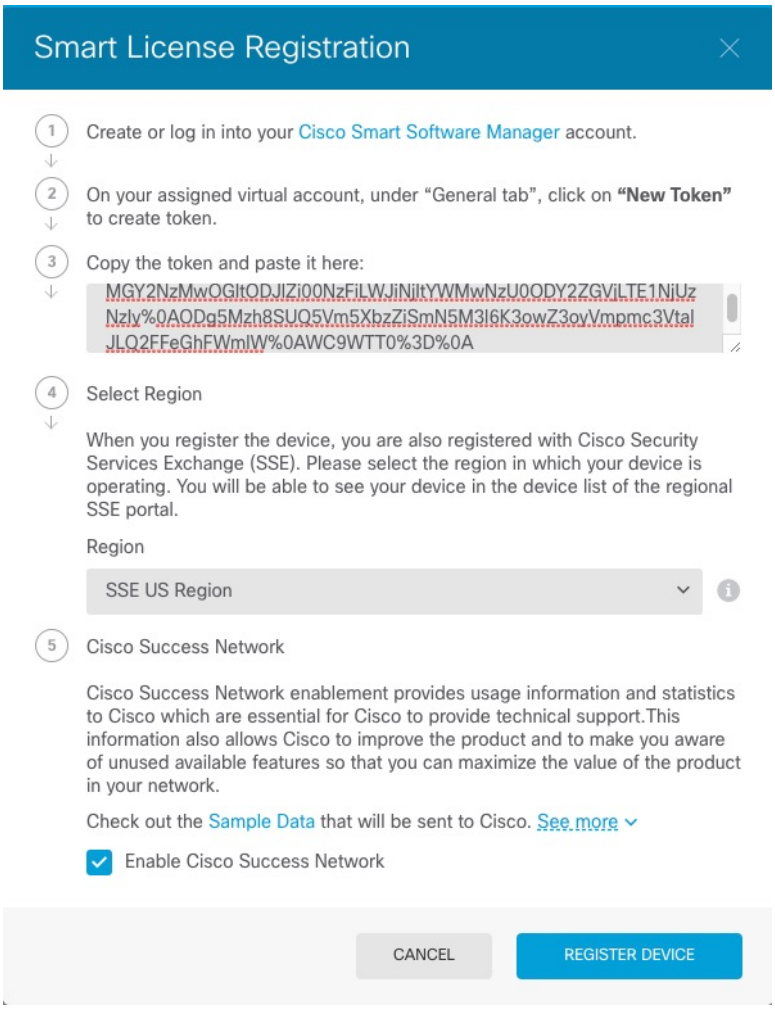
Step 3 In FDM, click **Device**, and then in the **Smart License** summary, click **View Configuration**.

You see the **Smart License** page.

Step 4 Click **Register Device**.

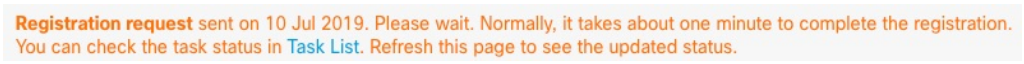


Then follow the instructions on the **Smart License Registration** dialog box to paste in your token:

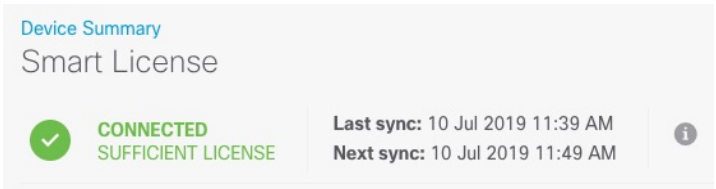


Step 5 Click **Register Device**.

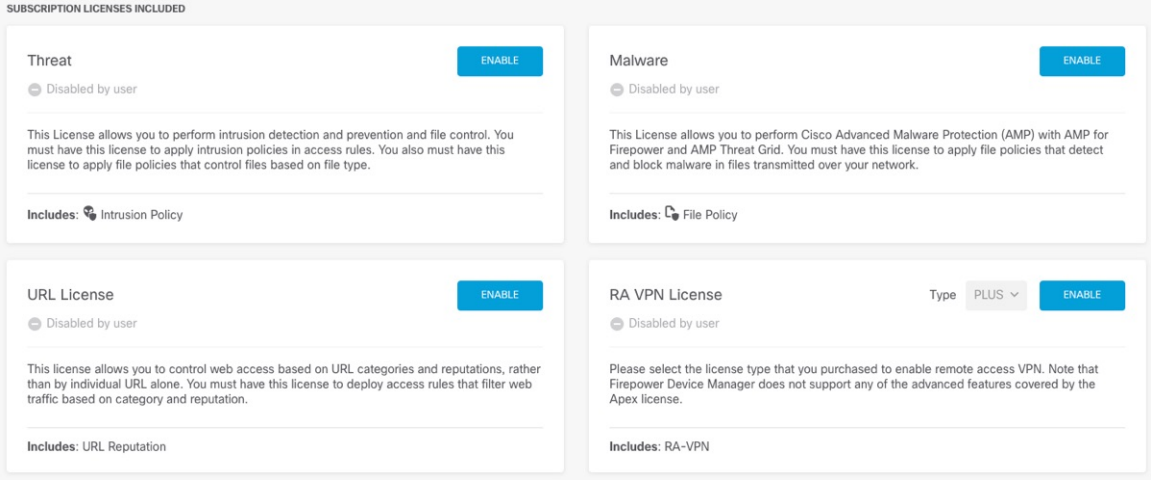
You return to the **Smart License** page. While the device registers, you see the following message:



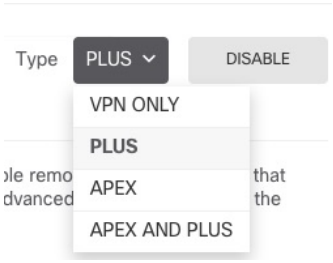
After the device successfully registers and you refresh the page, you see the following:



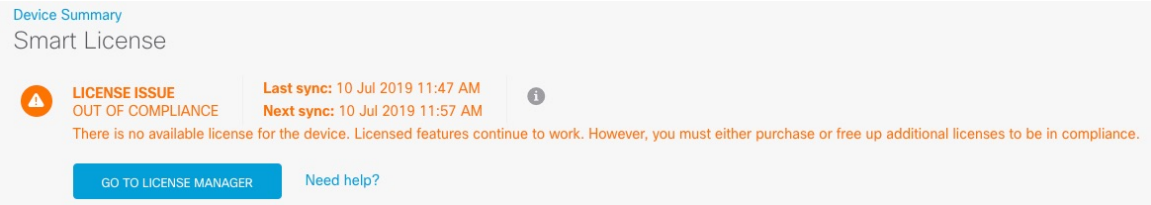
Step 6 Click the **Enable/Disable** control for each optional license as desired.



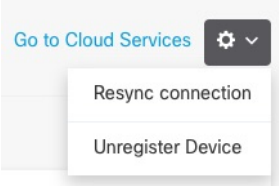
- **Enable**—Registers the license with your Cisco Smart Software Manager account and enables the controlled features. You can now configure and deploy policies controlled by the license.
- **Disable**—Unregisters the license with your Cisco Smart Software Manager account and disables the controlled 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:



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



Configure the Device 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.

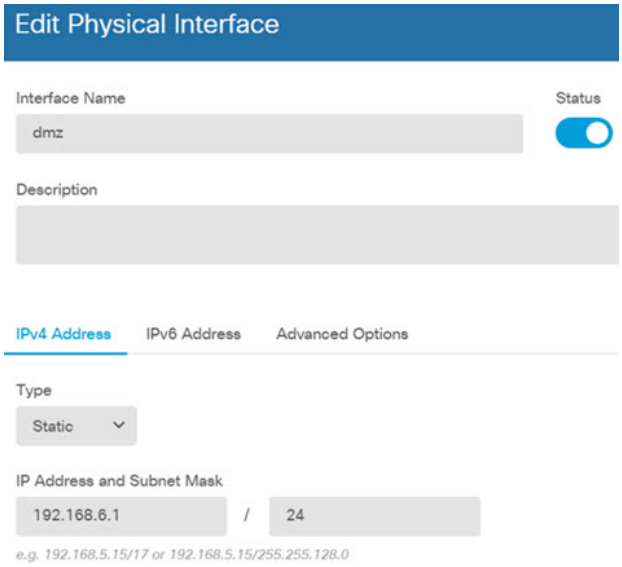
Procedure

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 18: Edit Interface



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.

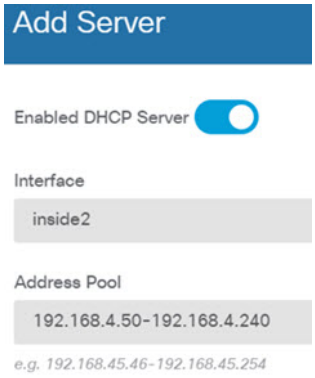
Figure 19: Security Zone Object

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 20: 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 21: Default Route

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.

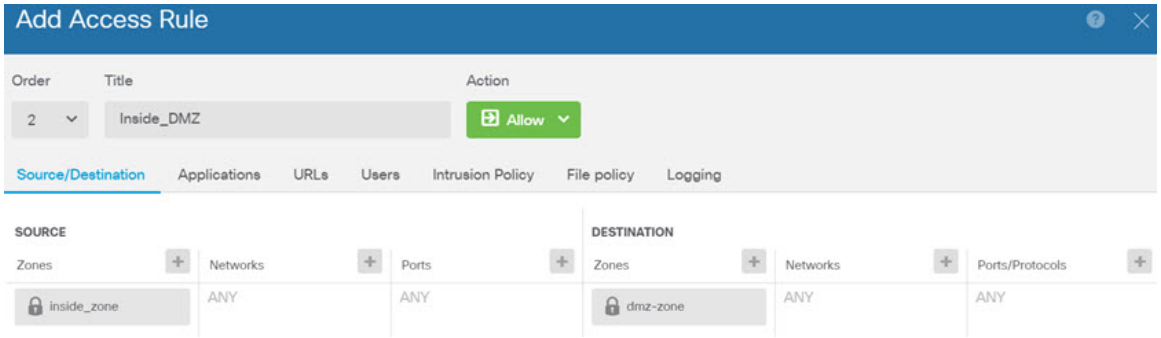
In addition, you can configure other policies to provide additional services, and fine-tune NAT and access rules to get the results that your organization requires. You can configure the following policies:

- **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 22: 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.

What to do next

- You can choose to onboard the device to CDO. If so, you should register and license your device after you onboard; see Onboard the Device to CDO, on page 21.

Access the FTD and FXOS 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 also access the FXOS CLI for troubleshooting purposes.

Note You can alternatively SSH to the Management interface of the FTD device. Unlike a console session, the SSH session defaults to the FTD CLI, from which you can connect to the FXOS CLI using the **connect fxos** command. You can later 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. This procedure describes console port access, which defaults to the FXOS CLI.

Procedure

Step 1 To log into the CLI, connect your management computer to the console port. Be sure to install any necessary USB serial drivers for your operating system (see the Firepower 1100 hardware guide). The console port defaults to the FXOS CLI. Use the following serial settings:

- 9600 baud
- 8 data bits
- No parity
- 1 stop bit

You connect to the FXOS CLI. Log in to the CLI using the **admin** username and the password you set at initial setup (the default is **Admin123**).

Example:

```
firepower login: admin
Password:
Last login: Thu May 16 14:01:03 UTC 2019 on ttyS0
Successful login attempts for user 'admin' : 1

firepower#
```

Step 2 Access the FTD CLI.

connect ftd

Example:

```
firepower# connect ftd
>
```

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*.

Step 3 To exit the FTD CLI, enter the **exit** or **logout** command.

This command returns you to the FXOS CLI prompt. For information on the commands available in the FXOS CLI, enter **?**.

Example:

```
> exit
```

```
firepower#
```

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.

You can power off the device using FDM, or you can use the FXOS CLI.

Power Off the Device Using FDM

You can shut down your system properly using FDM.

Procedure

Step 1 (6.5 and later) Use FDM to shut down the device.

Note For 6.4 and earlier, enter the **shutdown** command at the FDM CLI.

a) Click **Device**, then click the **System Settings** > **Reboot/Shutdown** link.
b) Click **Shut Down**.

Step 2 Observe the Power LED and Status LED to verify that the chassis is powered off (appear unlit).

Step 3 After the chassis has successfully powered off, you can then unplug the power to physically remove power from the chassis if necessary.

Power Off the Device at the CLI

You can use the FXOS CLI to safely shut down the system and power off the device. You access the CLI by connecting to the console port; see Access the FTD and FXOS CLI, on page 63.

Procedure

Step 1 In the FXOS CLI, connect to local-mgmt:

firepower # **connect local-mgmt**

Step 2 Issue the shutdown command:

firepower(local-mgmt) # **shutdown**

Example:

```
firepower(local-mgmt)# shutdown
This command will shutdown the system.  Continue?
Please enter 'YES' or 'NO': yes
INIT: Stopping Cisco Threat Defense......ok
```

Step 3 Monitor the system prompts as the device shuts down.

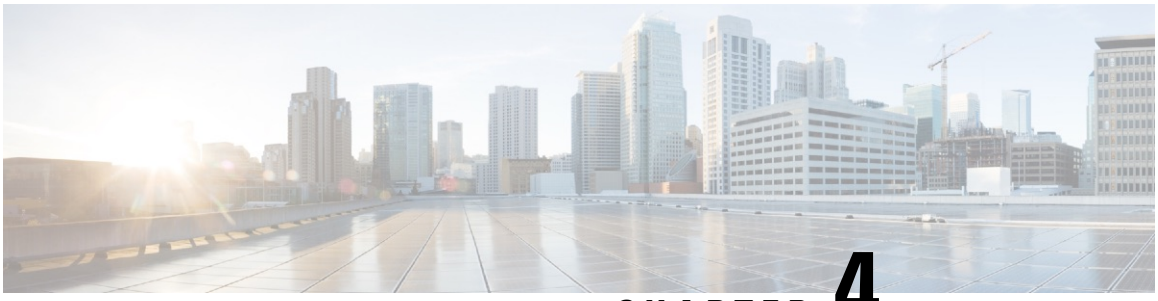
Step 4 Observe the Power LED and Status LED to verify that the chassis is powered off (appear unlit).

Step 5 After the chassis has successfully powered off, you can then turn off the power switch and unplug the power to physically remove power from the chassis if necessary.

What's Next?

To continue configuring your FTD device, 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 4

Firepower Threat Defense Deployment with FMC

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 For a remote branch setup, we recommend that you use the standalone document specific to that deployment.

Note The Cisco Firepower 1100 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.

Note The Firepower 1100 runs an underlying operating system called the Firepower eXtensible Operating System (FXOS). The Firepower 1100 does not support the FXOS Firepower Chassis Manager; only a limited CLI is supported for troubleshooting purposes. See the FXOS troubleshooting guide for more information.

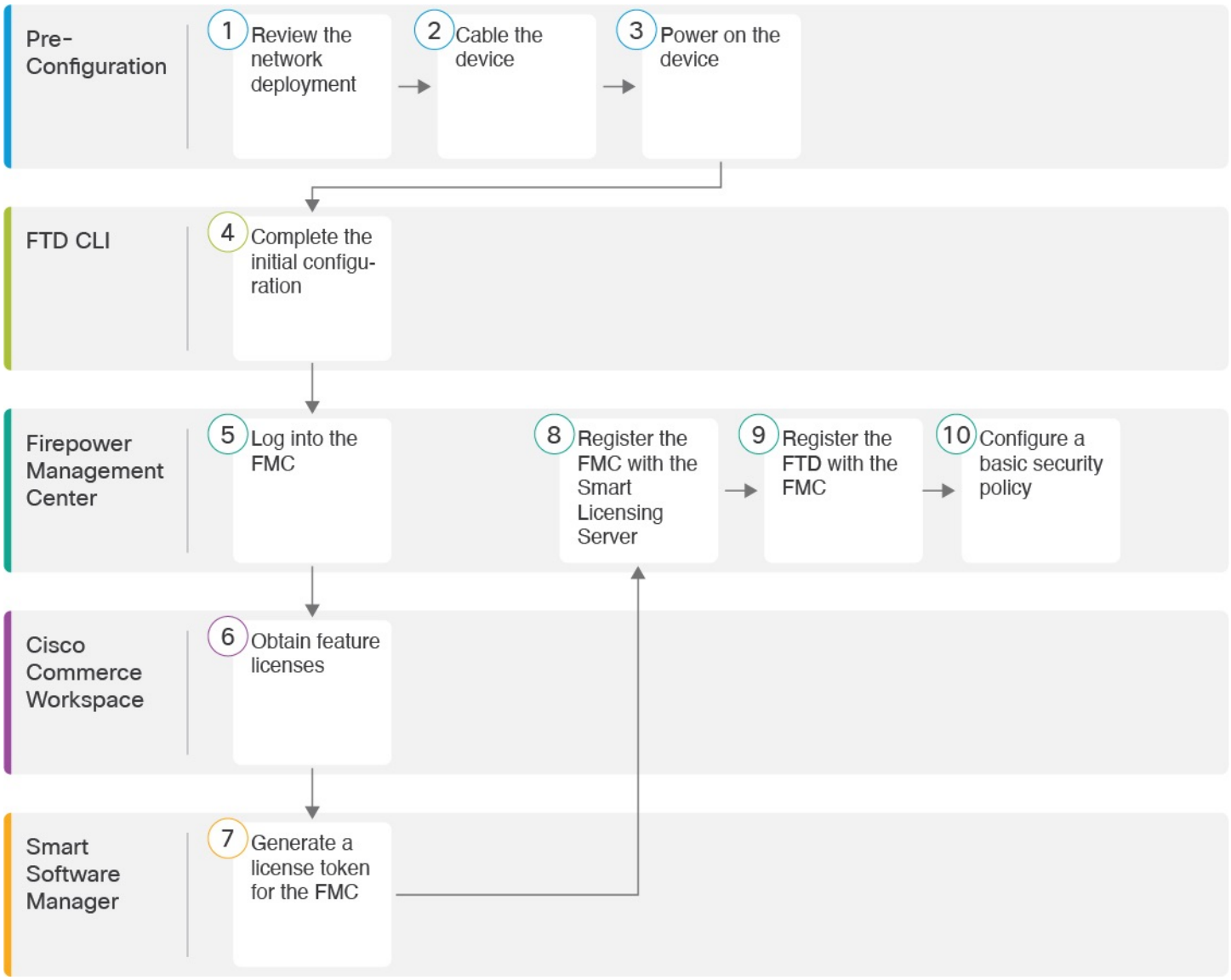
Note **Privacy Collection Statement**—The Firepower 1100 does not require or actively collect personally-identifiable information. However, you can use personally-identifiable information in the configuration, for example for usernames. In this case, an administrator might be able to see this information when working with the configuration or when using SNMP.

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.



1	Pre-Configuration	Review the Network Deployment, on page 70.
2	Pre-Configuration	Cable the Device, on page 74.
3	Pre-Configuration	Power on the Device, on page 78.
4	FTD CLI	Complete the FTD Initial Configuration, on page 79.
5	Firepower Management Center	Log Into the Firepower Management Center, on page 85.

6	Cisco Commerce Workspace	Obtain Licenses for the Firepower Management Center, on page 85: Buy feature licenses.
7	Smart Software Manager	Obtain Licenses for the Firepower Management Center, on page 85: Generate a license token for the FMC.
8	Firepower Management Center	Obtain Licenses for the Firepower Management Center, on page 85: Register the FMC with the Smart Licensing server.
9	Firepower Management Center	Register the FTD with the FMC, on page 87.
10	Firepower Management Center	Configure a Basic Security Policy, on page 89.

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. The dedicated Management interface is a special interface with its own network settings. When you enable FMC access from a data interface, the FTD forwards management traffic over the backplane so it can be routed through the 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 data interface.
- 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).

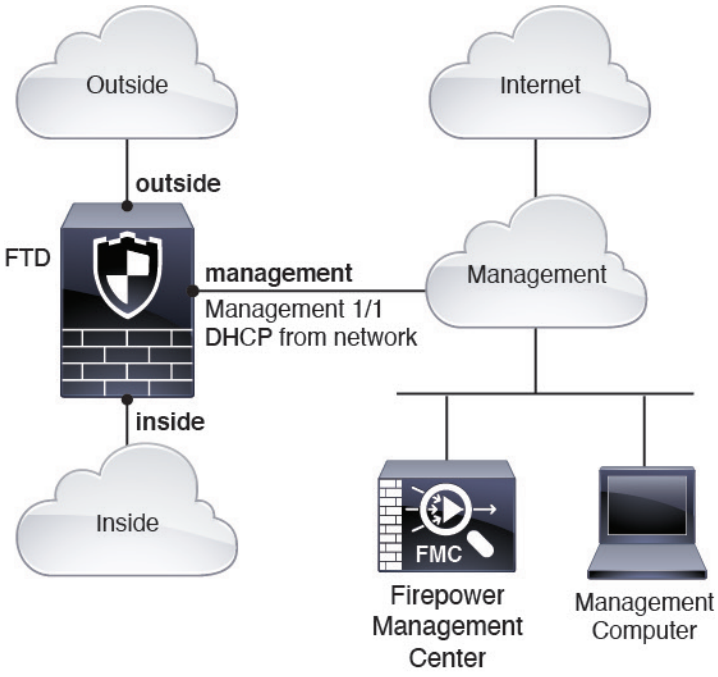
See the following sample network deployments for ideas on how to place your FTD device in your network.

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 Firepower 1100 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 23: Separate Management Network



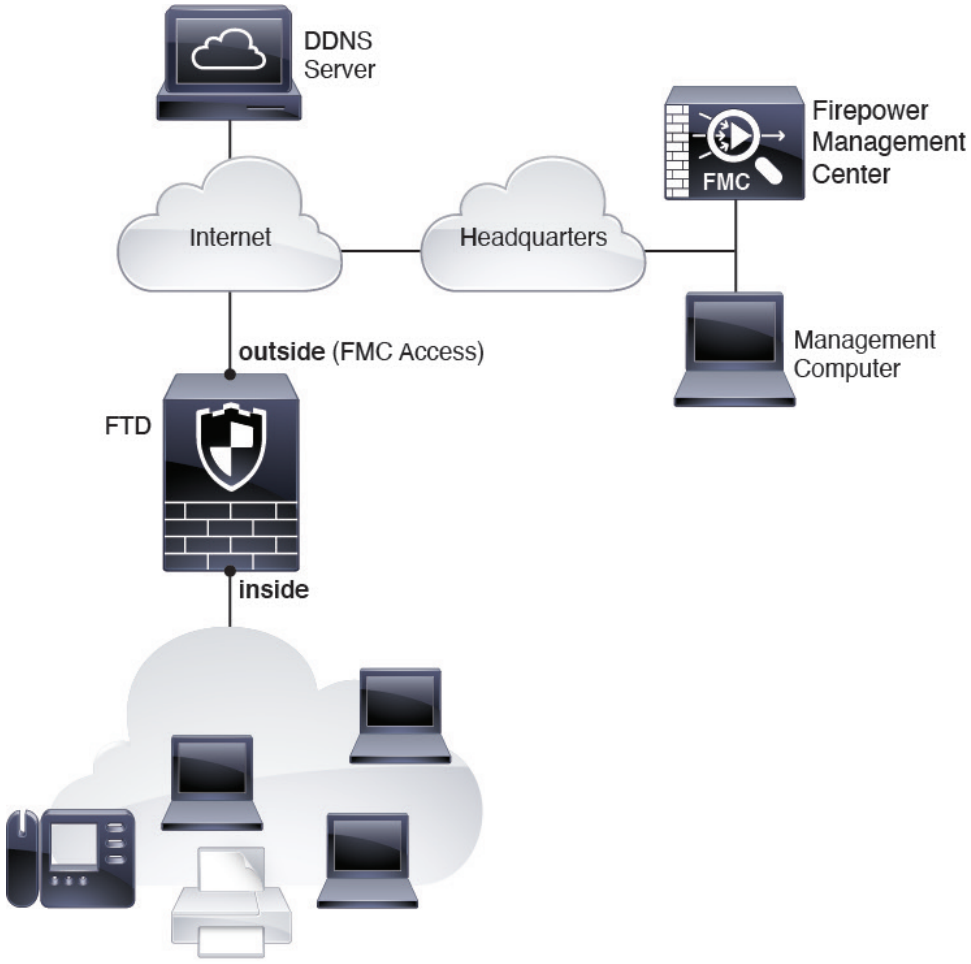
6.7 and Later Remote Management Deployment

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 Firepower 1100 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.

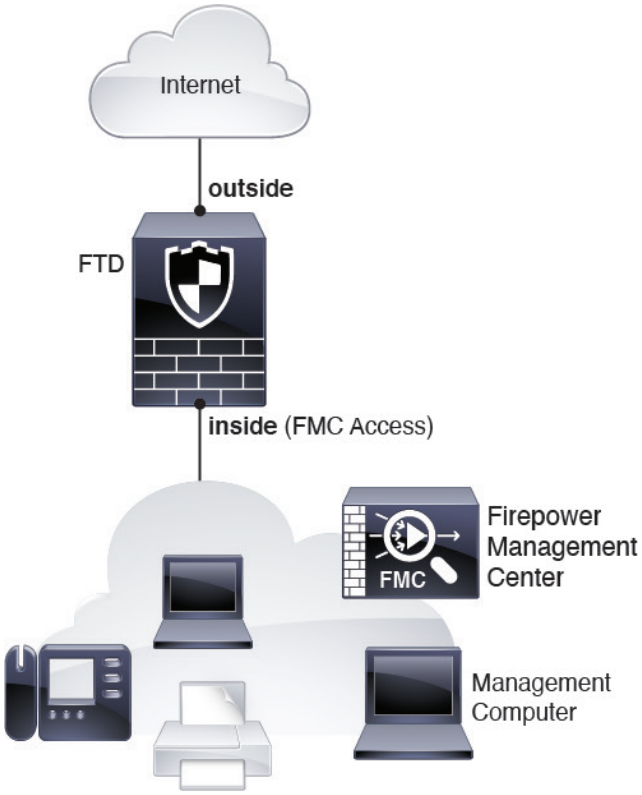
Figure 24: Remote Management Deployment



6.7 and Later Inside Management Deployment

The following figure shows the recommended network deployment for the Firepower 1100 using the inside interface for management.

Figure 25: Inside Management Deployment



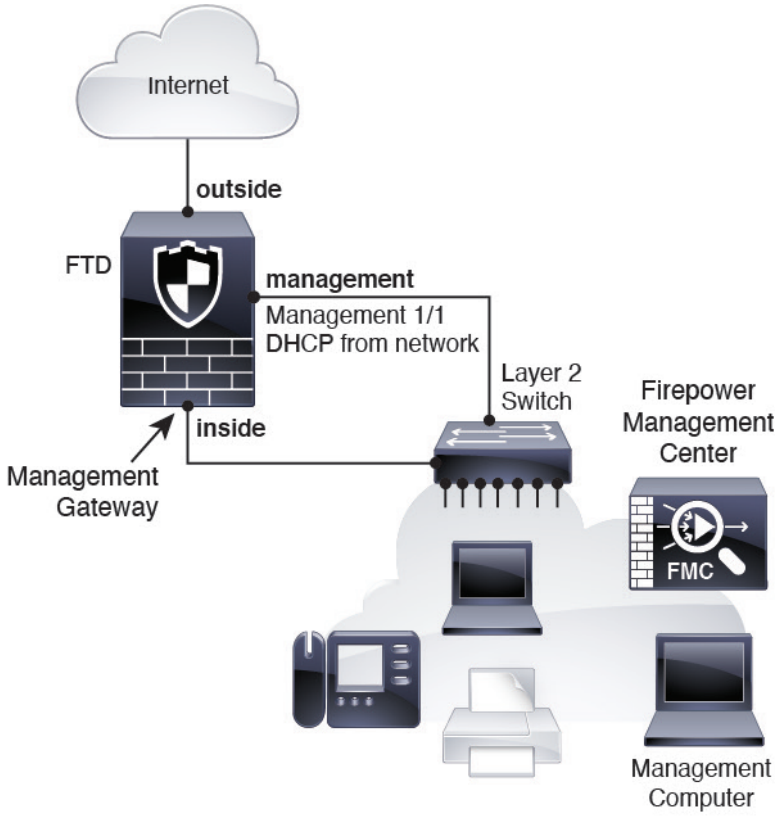
6.6 and Earlier Edge Network Deployment

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 Firepower 1100 where the Firepower 1100 acts as the internet gateway for the FMC and FTD managamement. You can also use this scenario in 6.7 and later for a High Availability deployment, for example.

In the following diagram, the Firepower 1100 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 26: Edge Network Deployment



Cable the Device

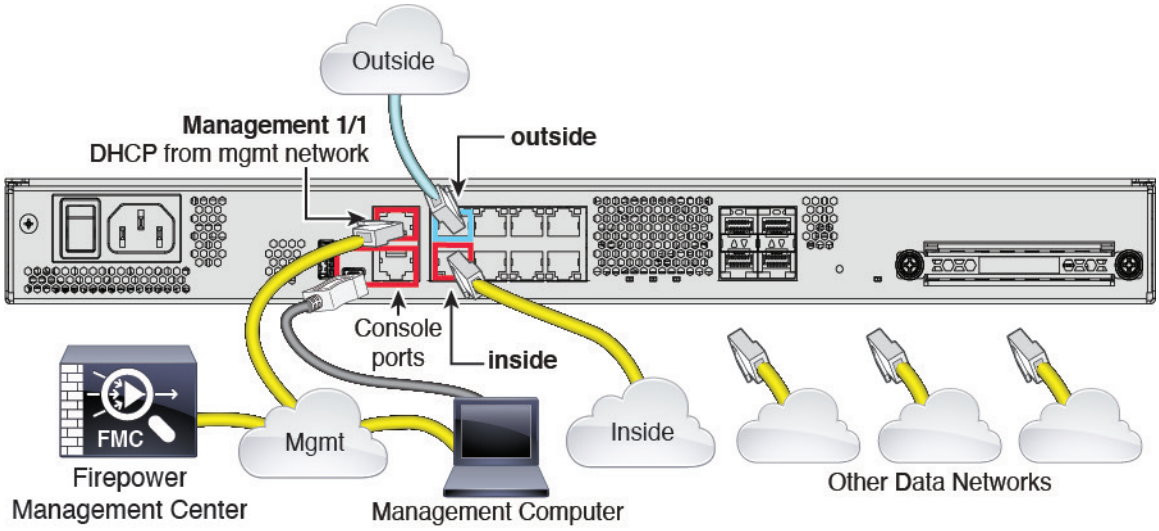
To cable one of the recommended scenarios on the Firepower 1100, see the following steps.

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 27: Cabling a Separate Management Network



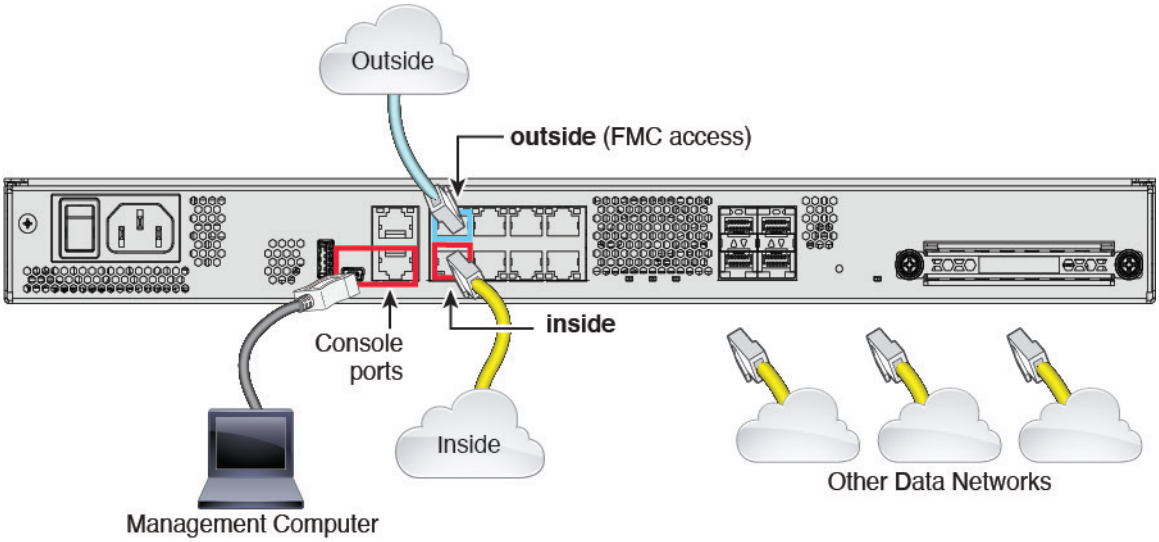
Note For version 6.5 and earlier, the Management 1/1 default IP address is 192.168.45.45.

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, Ethernet 1/2) to your inside router.
d) Connect the outside interface (for example, Ethernet 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 28: Cabling a Remote Management Deployment



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

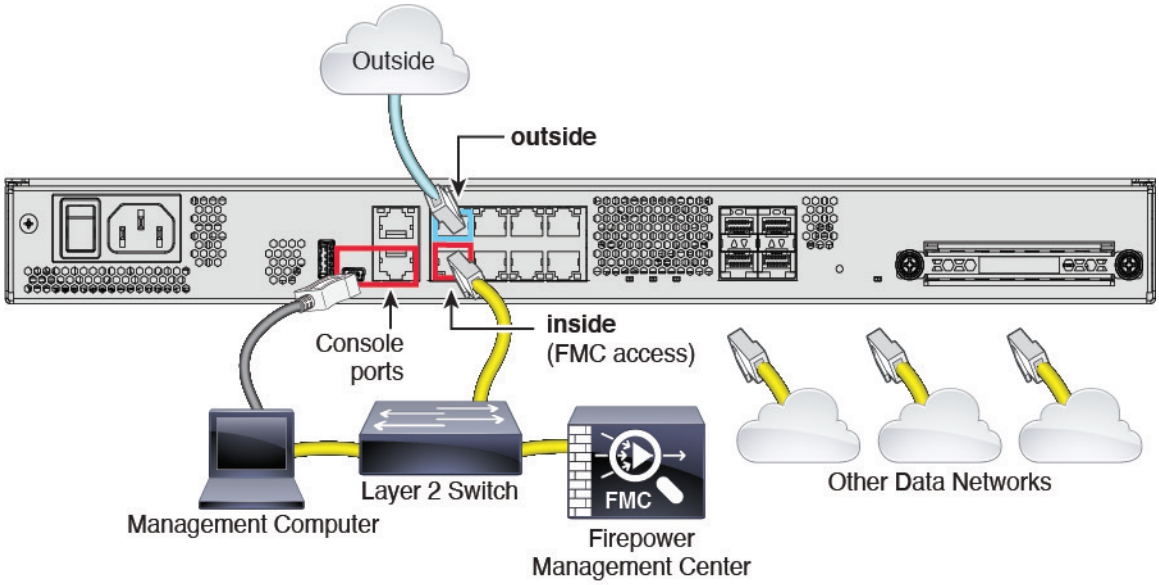
a) Connect the management computer to the console port. You need to use the console port to access the CLI for initial setup.

   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, Ethernet 1/2).
c) Connect the outside interface (for example, Ethernet 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 29: Cabling an Inside Management Deployment

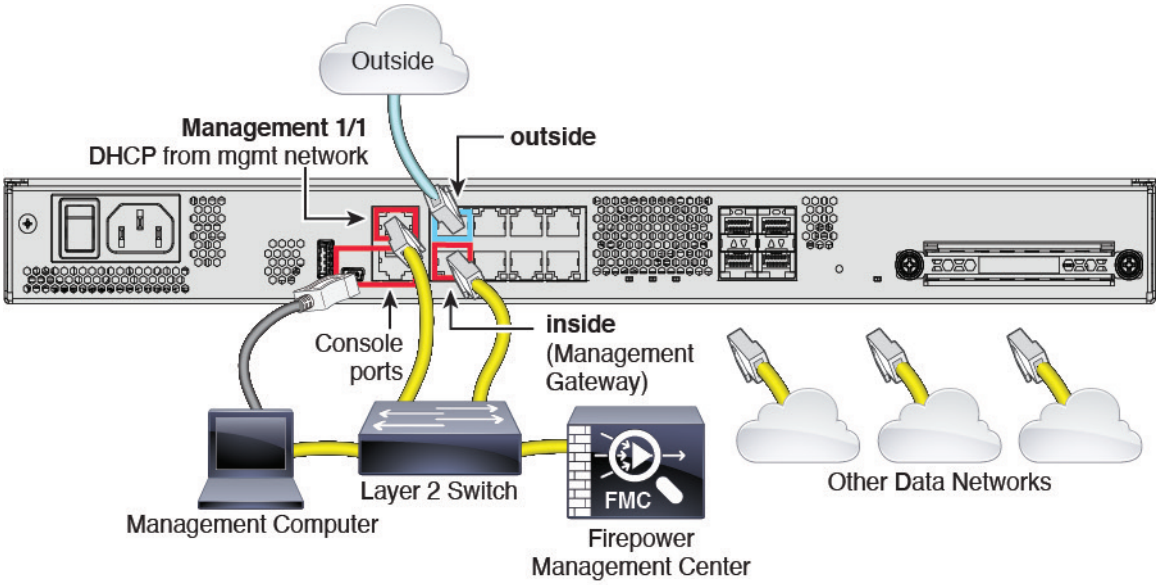


The FMC and your management computer reside on the inside network with your other inside end points.

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, Ethernet 1/2):
   - Firepower Management Center
   - Management computer
c) Connect the outside interface (for example, Ethernet 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 30: 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, Ethernet 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, Ethernet 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. The power switch is implemented as a soft notification switch that supports graceful shutdown of the system to reduce the risk of system software and data corruption.

Before you begin

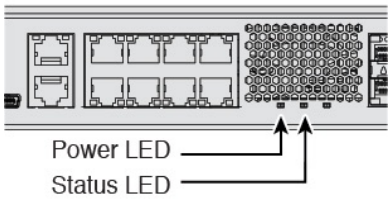
It's important that you provide reliable power for your device (for example, using an uninterruptable power supply (UPS)). Loss of power without first shutting down can cause serious file system damage. There are many processes running in the background all the time, and losing power does not allow the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



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

Note When the switch is toggled from ON to OFF, it may take several seconds for the system to eventually power off. During this time, the Power LED on the front of the chassis blinks green. Do not remove the power until the Power LED is completely off.

Complete the FTD Initial Configuration

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.

The console port connects to the FXOS CLI. The SSH session connects directly to the FTD CLI.

Step 2 Log in with the username **admin** and the password **Admin123**.

At the console port, you connect to the FXOS CLI. The first time you log in to FXOS, you are prompted to change the password. This password is also used for the FTD login for SSH.

Example:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1
```

```
[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

Step 3 If you connected to FXOS on the console port, connect to the FTD CLI.

connect ftd

Example:

```
firepower# connect ftd
>
```

Step 4 The first time you log in to FTD, you are prompted to accept the End User License Agreement (EULA) and, if using an SSH connection, 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. This IP address is NATted when the traffic is forwarded to the data interface. 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 5 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 alphanumerical 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 6 (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 data interface.
  - 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 managemement, 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://jcrichton: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 7 (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 Firepower Management Center

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

- **Threat**—Security Intelligence and Cisco Firepower Next-Generation IPS
- **Malware**—Advanced Malware Protection for Networks (AMP)
- **URL**—URL Filtering
- **RA VPN**—AnyConnect Plus, AnyConnect Apex, or AnyConnect VPN Only.

Before you begin

- Have a master account on the Cisco 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.

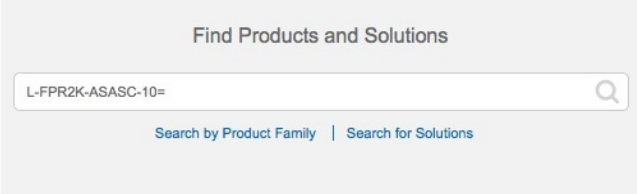
- Your Cisco Smart Software Licensing account must qualify for the Strong Encryption (3DES/AES) license to use some features (enabled using the export-compliance flag).

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 31: License Search



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

- Threat, Malware, and URL license combination:

  Firepower 1010:

  Firepower 1100:

  - L-FPR1120T-TMC=
  - L-FPR1140T-TMC=
  - L-FPR1150T-TMC=

  Firepower 2100:

  ASA 5508-X and 5516-X:

  ISA 3000:

  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:

  Firepower 1010:

  Firepower 1100:

  - L-FPR1120T-TMC-1Y
  - L-FPR1120T-TMC-3Y
  - L-FPR1120T-TMC-5Y
  - L-FPR1140T-TMC-1Y
  - L-FPR1140T-TMC-3Y
  - L-FPR1140T-TMC-5Y
  - L-FPR1150T-TMC-1Y
  - L-FPR1150T-TMC-3Y
  - L-FPR1150T-TMC-5Y

  Firepower 2100:

  ASA 5508-X and 5516-X:

  ISA 3000:

- 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.

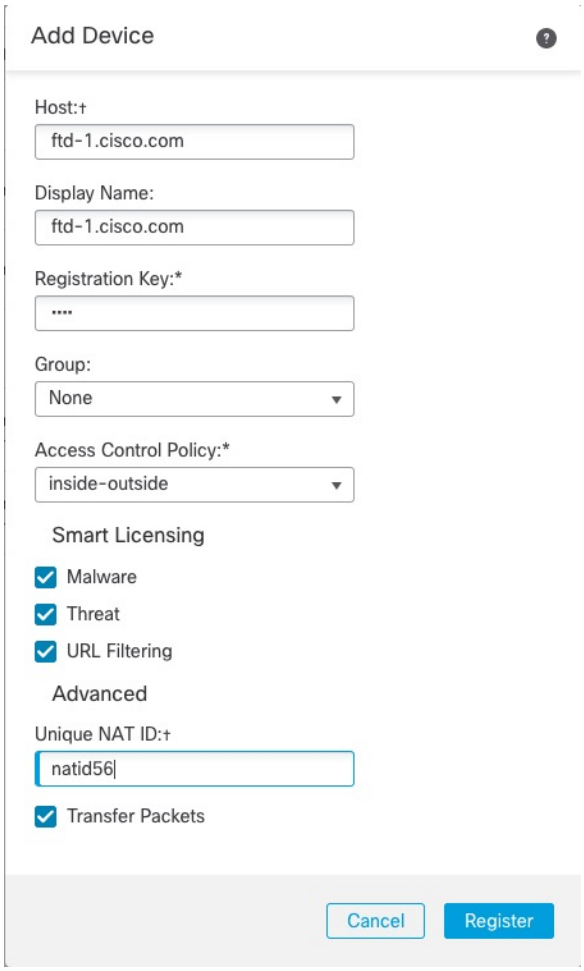
Before you begin

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

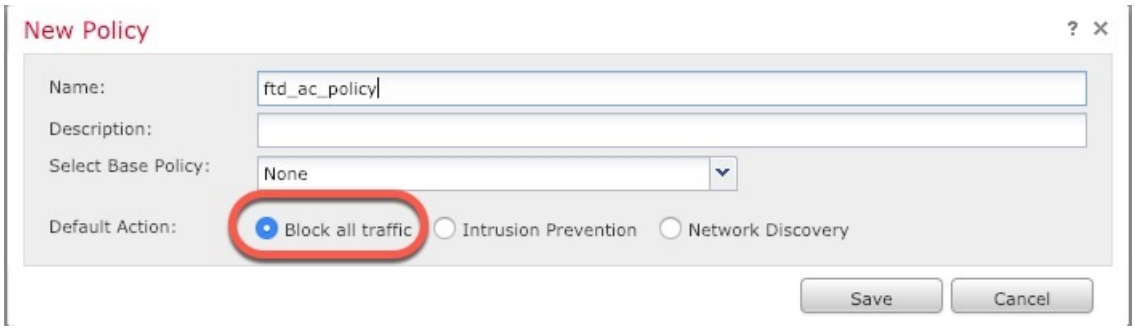
Procedure

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

Step 2 From the **Add** drop-down list, choose **Add Device**, and enter 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 98.



- **Smart Licensing**—Assign the Smart Licenses you need for the features you want to deploy: **Malware** (if you intend to use AMP 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 management, 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 FTD 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	(All Other Models) Configure Interfaces, on page 90.
2	Configure the DHCP Server, on page 93.
3	Add the Default Route, on page 94.
4	Configure NAT, on page 96.
5	Allow Traffic from Inside to Outside, on page 98.
6	Deploy the Configuration, on page 101.

(All Other Models) 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.

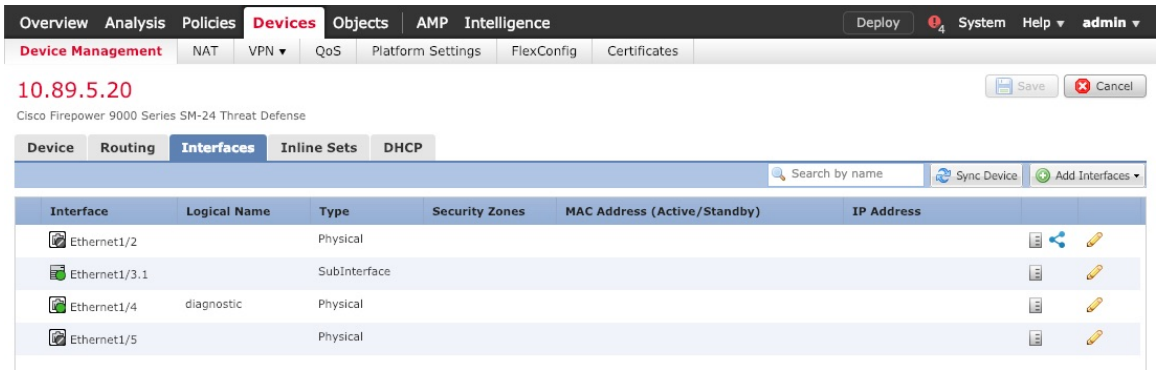
A typical edge-routing situation is to obtain the outside interface address through DHCP from your ISP, while you define static addresses on the inside interfaces.

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

Procedure

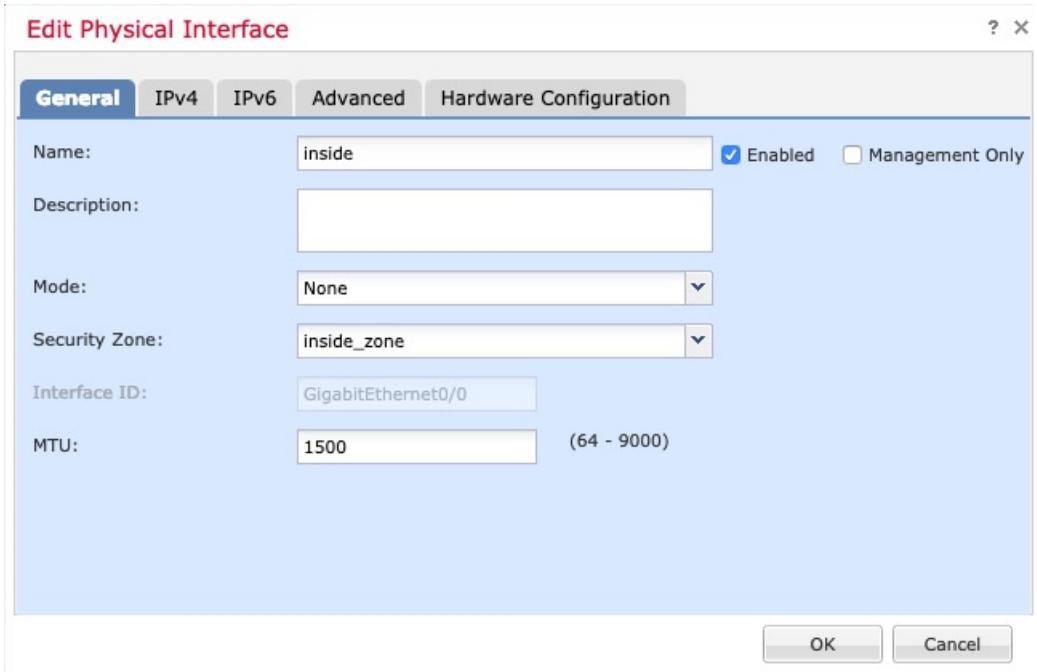
Step 1 Choose **Devices** > **Device Management**, and click the **Edit** (✎) for the device.

Step 2 Click **Interfaces**.



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

The **General** tab appears.



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

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

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

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

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

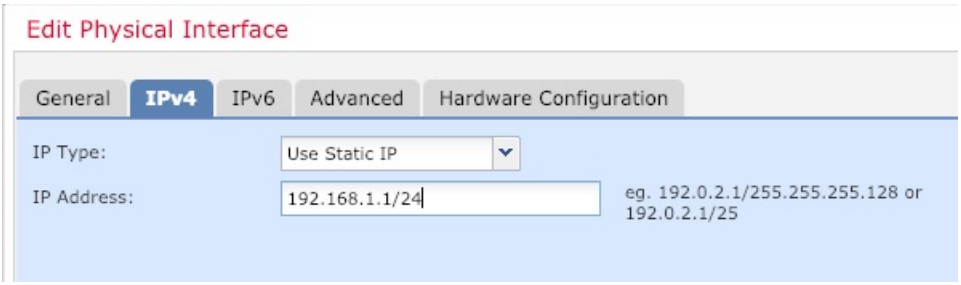
For example, add a zone called **inside_zone**. Each interface must be assigned to a security zone and/or interface group. An interface can belong to only one security zone, but can also belong to multiple interface groups. You apply your security policy based on zones or groups. For example, you can 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**

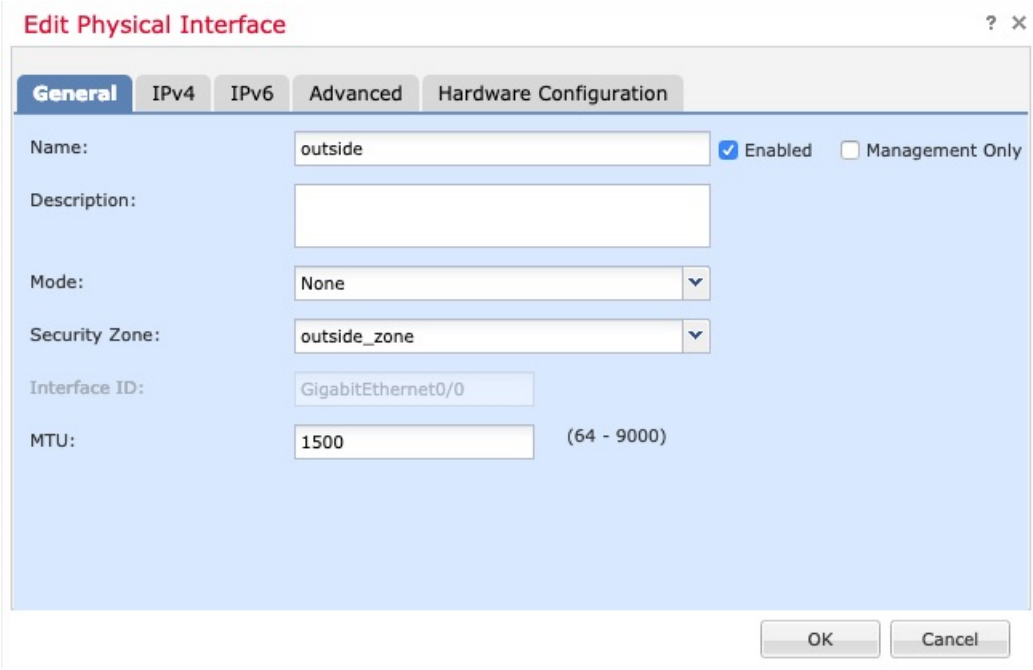


- **IPv6**—Check the **Autoconfiguration** check box for stateless autoconfiguration.

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.

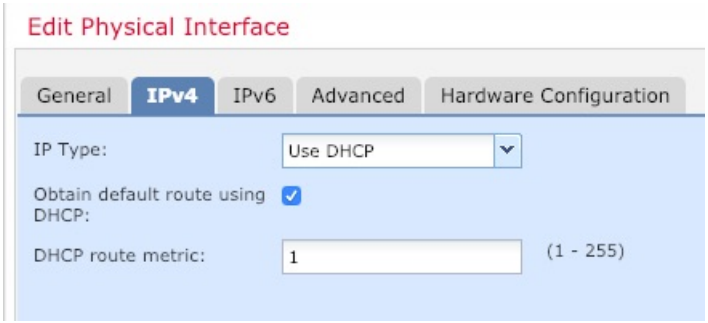
c) Leave the **Mode** set to **None**.

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.



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

f) Click **OK**.

Step 5 Click **Save**.

Configure the DHCP Server

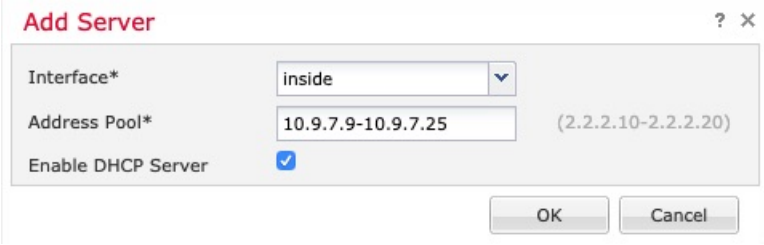
Enable the DHCP server if you want clients to use DHCP to obtain IP addresses from the FTD.

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**.

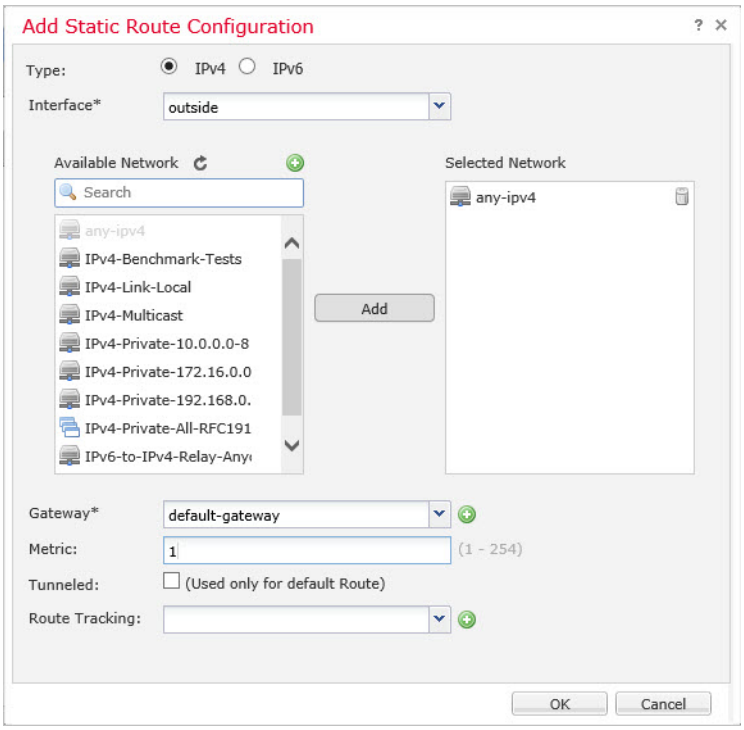
Add the Default Route

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.

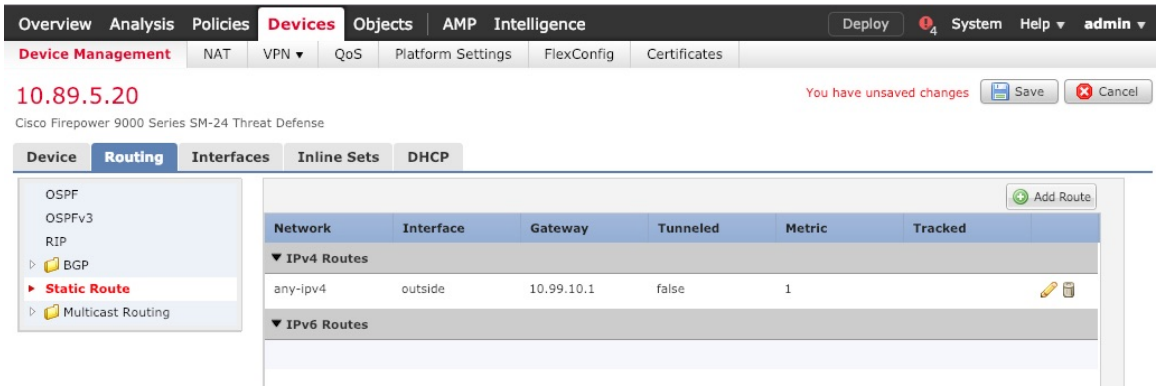
Step 2 Choose **Routing** > **Static Route**, click **Add Route**, and set the following:



- **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.



Step 4 Click **Save**.

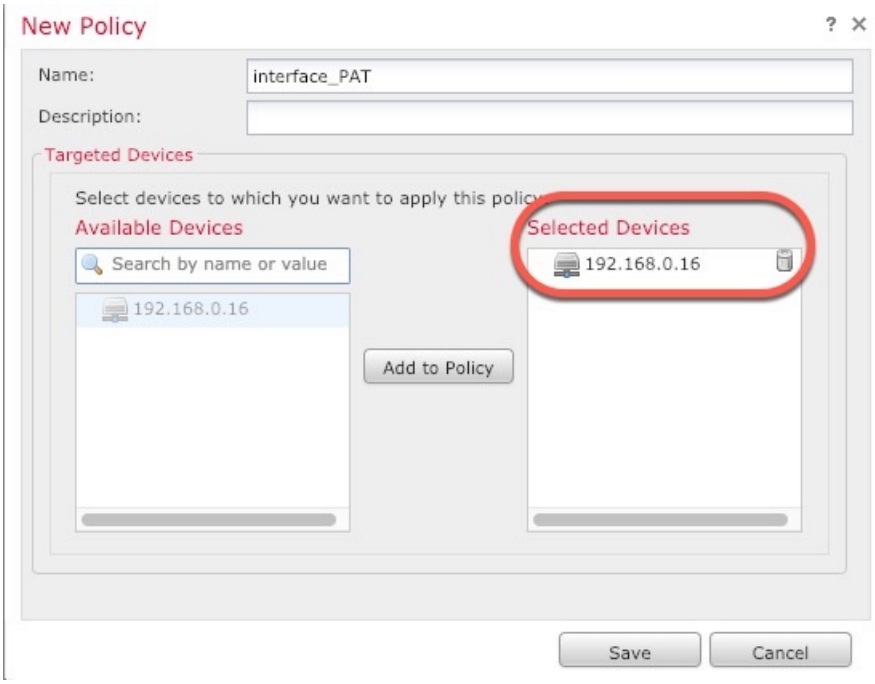
Configure NAT

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

Step 3 Click **Add Rule**.

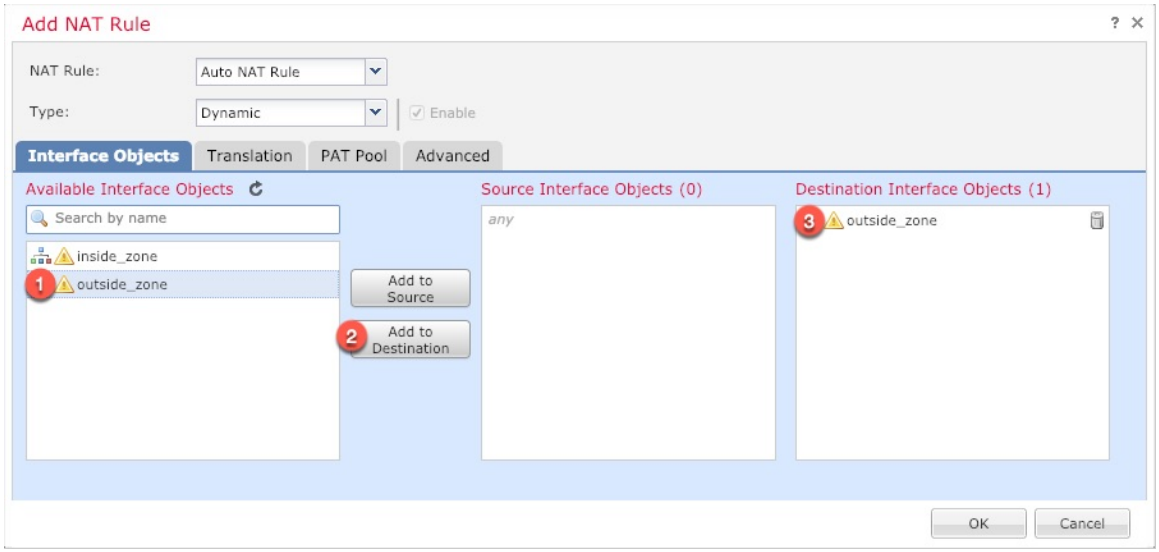
The **Add NAT Rule** dialog box appears.

Step 4 Configure the basic rule options:

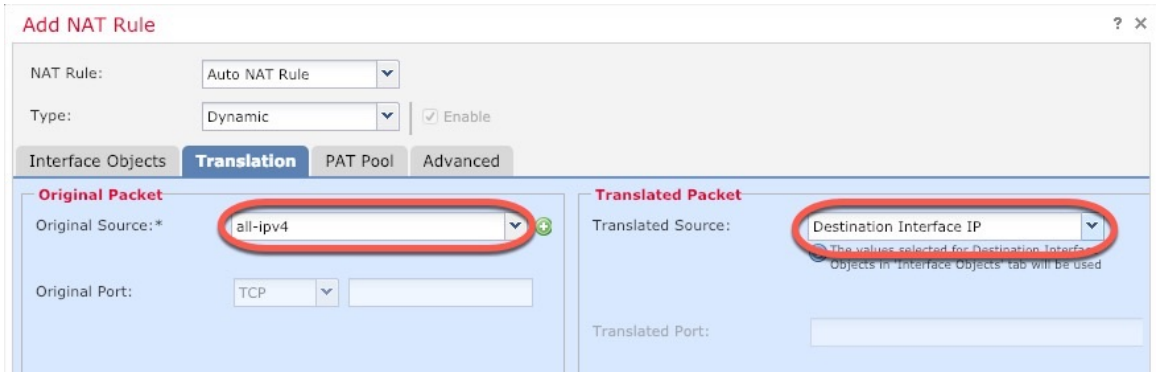
- **NAT Rule**—Choose **Auto NAT Rule**.

- **Type**—Choose **Dynamic**.

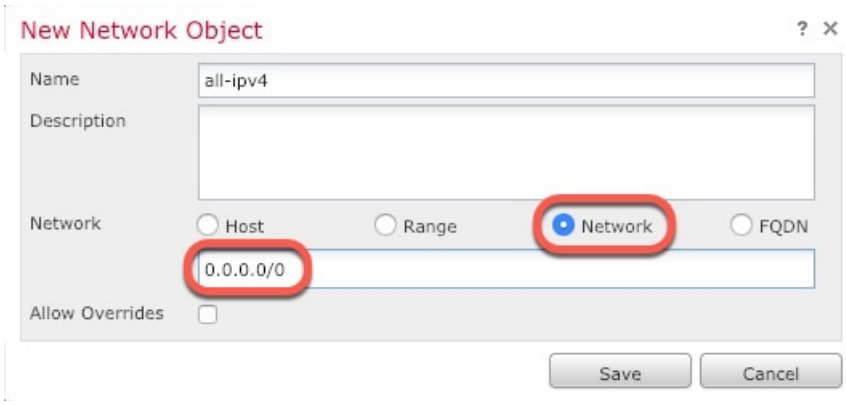
Step 5 On the **Interface Objects** page, add the outside zone from the **Available Interface Objects** area to the **Destination Interface Objects** area.



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).

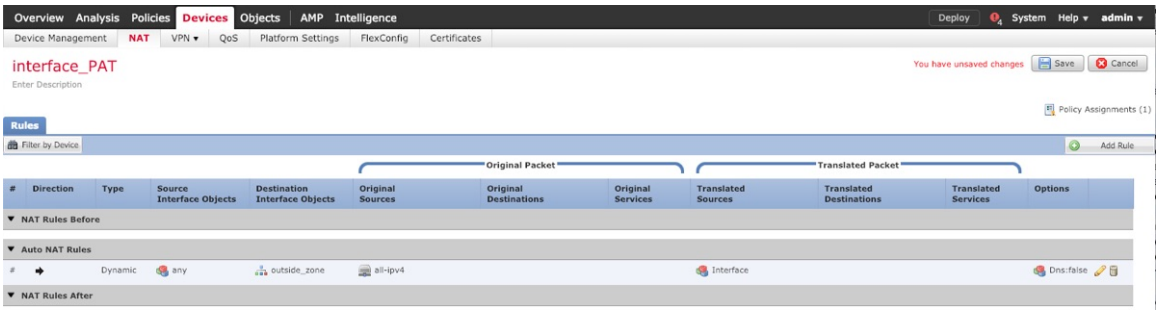


Note You cannot use the system-defined **any-ipv4** object, because Auto NAT rules add NAT as part of the object definition, and you cannot edit system-defined objects.

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

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

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



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

Allow Traffic from Inside to Outside

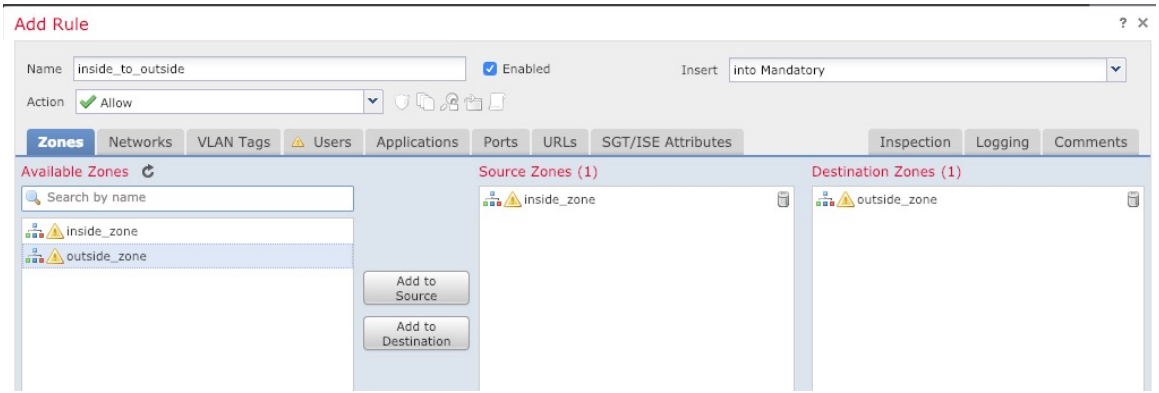
If you created a basic **Block all traffic** access control policy when you registered the FTD with the FMC, then you need to add rules to the policy to allow traffic through the device. The following procedure adds a rule to allow traffic from the inside zone to the outside zone. If you have other zones,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

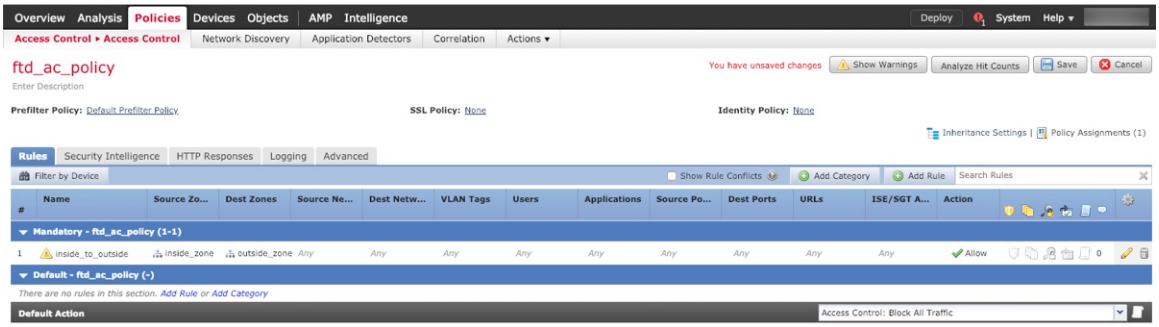


- **Name**—Name this rule, for example, **inside_to_outside**.
- **Source Zones**—Select the inside zone from **Available Zones**, and click **Add to Source**.
- **Destination Zones**—Select the outside zone from **Available Zones**, and click **Add to Destination**.

Leave the other settings as is.

Step 3 Click **Add**.

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



Step 4 Click **Save**.

Configure SSH on the FMC Access Data Interface

If you enabled FMC access on a data interface, such as outside, you should enable SSH on that interface using this procedure. This section describes how to enable SSH connections to one or more *data* interfaces on the FTD. SSH is not supported to the Diagnostic logical interface.

Note SSH is enabled by default on the *Management* logical interface; however, this screen does not affect Management SSH access.

The Management logical interface is separate from the other interfaces on the device. It is used to set up and register the device to the Firepower Management Center. SSH for data interfaces shares the internal and external user list with SSH for the Management interface. Other settings are configured separately: for data interfaces, enable SSH and access lists using this screen; SSH traffic for data interfaces uses the regular routing configuration, and not any static routes configured at setup or at the CLI.

For the Management interface, to configure an SSH access list, see the **configure ssh-access-list** command in the Firepower Threat Defense Command Reference. To configure a static route, see the **configure network static-routes** command. By default, you configure the default route through the Management interface at initial setup.

To use SSH, you do not also need an access rule allowing the host IP address. You only need to configure SSH access according to this section.

You can only SSH to a reachable interface; if your SSH host is located on the outside interface, you can only initiate a management connection directly to the outside interface.

The device allows a maximum of 5 concurrent SSH connections.

Note On all appliances, after a user makes three consecutive failed attempts to log into the CLI via SSH, the system terminates the SSH connection.

Before you begin

- You can configure SSH internal users at the CLI using the **configure user add** command. By default, there is an **admin** user for which you configured the password during initial setup. You can also configure external users on LDAP or RADIUS by configuring **External Authentication** in platform settings.
- You need network objects that define the hosts or networks you will allow to make SSH connections to the device. You can add objects as part of the procedure, but if you want to use object groups to identify a group of IP addresses, ensure that the groups needed in the rules already exist. Select **Objects** > **Object Management** to configure objects.

Note You cannot use the system-provided **any** network object. Instead, use **any-ipv4** or **any-ipv6**.

Procedure

Step 1 Select **Devices** > **Platform Settings** and create or edit an FTD policy.

Step 2 Select **Secure Shell**.

Step 3 Identify the interfaces and IP addresses that allow SSH connections.

Use this table to limit which interfaces will accept SSH connections, and the IP addresses of the clients who are allowed to make those connections. You can use network addresses rather than individual IP addresses.

a) Click **Add** to add a new rule, or click **Edit** to edit an existing rule.

b) Configure the rule properties:

- **IP Address**—The network object that identifies the hosts or networks you are allowing to make SSH connections. Choose an object from the drop-down menu, or add a new network object by clicking +.
- **Security Zones**—Add the zones that contain the interfaces to which you will allow SSH connections. For interfaces not in a zone, you can type the interface name into the field below the Selected Security Zone list and click **Add**. These rules will be applied to a device only if the device includes the selected interfaces or zones.

c) Click **OK**.

Step 4 Click **Save**.

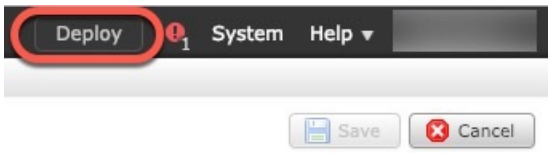
You can now go to **Deploy** > **Deployment** and deploy the policy to assigned devices. The changes are not active until you deploy them.

Deploy the Configuration

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

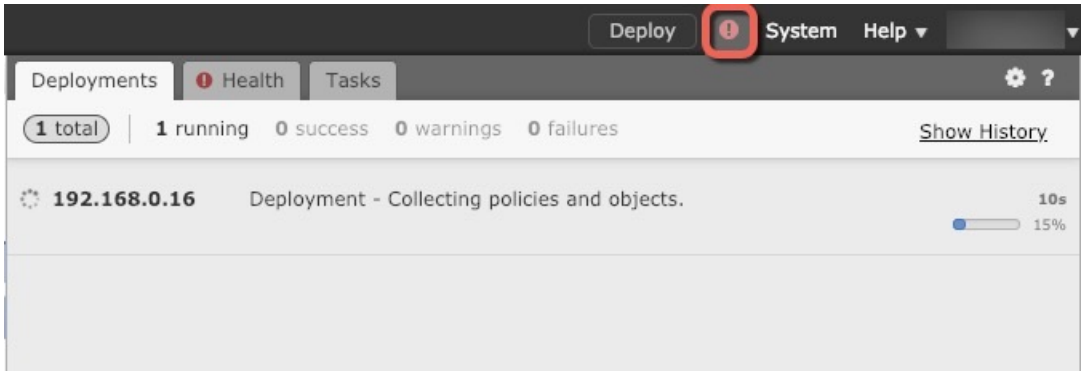
Procedure

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



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

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 FTD and FXOS 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 also access the FXOS CLI for troubleshooting purposes.

Note You can alternatively SSH to the Management interface of the FTD device. Unlike a console session, the SSH session defaults to the FTD CLI, from which you can connect to the FXOS CLI using the **connect fxos** command. You can later 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. This procedure describes console port access, which defaults to the FXOS CLI.

Procedure

Step 1 To log into the CLI, connect your management computer to the console port. Be sure to install any necessary USB serial drivers for your operating system (see the Firepower 1100 hardware guide). The console port defaults to the FXOS CLI. Use the following serial settings:

- 9600 baud
- 8 data bits
- No parity
- 1 stop bit

You connect to the FXOS CLI. Log in to the CLI using the **admin** username and the password you set at initial setup (the default is **Admin123**).

Example:

```
firepower login: admin
Password:
Last login: Thu May 16 14:01:03 UTC 2019 on ttyS0
Successful login attempts for user 'admin' : 1

firepower#
```

Step 2 Access the FTD CLI.

connect ftd

Example:

```
firepower# connect ftd
>
```

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*.

Step 3 To exit the FTD CLI, enter the **exit** or **logout** command.

This command returns you to the FXOS CLI prompt. For information on the commands available in the FXOS CLI, enter **?**.

Example:

```
> exit
```

```
firepower#
```

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.

You can power off the device using the FMC device management page, or you can use the FXOS CLI.

Power Off the Device Using FMC

You shut down your system properly using FMC.

Procedure

Step 1 Choose **Devices** > **Device Management**.

Step 2 Next to the device that you want to restart, click the edit icon ( ).

Step 3 Click the **Device** tab.

Step 4 Click the shut down device icon ( ) in the **System** section.

Step 5 When prompted, confirm that you want to shut down the device.

Step 6 Observe the Power LED and Status LED to verify that the chassis is powered off (appear unlit).

Step 7 After the chassis has successfully powered off, you can then unplug the power to physically remove power from the chassis if necessary.

Power Off the Device at the CLI

You can use the FXOS CLI to safely shut down the system and power off the device. You access the CLI by connecting to the console port; see Access the FTD and FXOS CLI, on page 101.

Procedure

Step 1 In the FXOS CLI, connect to local-mgmt:

firepower # **connect local-mgmt**

Step 2 Issue the shutdown command:

firepower(local-mgmt) # **shutdown**

Example:

```
firepower(local-mgmt)# shutdown
This command will shutdown the system.  Continue?
Please enter 'YES' or 'NO': yes
INIT: Stopping Cisco Threat Defense......ok
```

Step 3 Monitor the system prompts as the device shuts down.

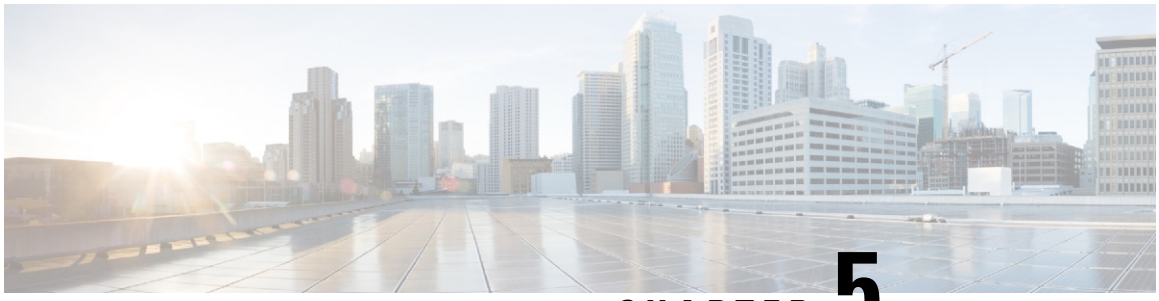
Step 4 Observe the Power LED and Status LED to verify that the chassis is powered off (appear unlit).

Step 5 After the chassis has successfully powered off, you can then turn off the power switch and unplug the power to physically remove power from the chassis if necessary.

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 5

ASA Deployment with ASDM

Is This Chapter for You?

This chapter describes how to set up the Firepower 1100 for use with the ASA. This chapter does not cover the following deployments, for which you should refer to the ASA configuration guide:

- Failover
- CLI configuration

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

Note The Firepower 1100 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.

Note The Firepower 1100 runs an underlying operating system called the Firepower eXtensible Operating System (FXOS). The Firepower 1100 does not support the FXOS Firepower Chassis Manager; only a limited CLI is supported for troubleshooting purposes. See the FXOS troubleshooting guide for more information.

Note **Privacy Collection Statement**—The Firepower 1100 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.

About the ASA

The ASA provides advanced stateful firewall and VPN concentrator functionality in one device.

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 Security Manager—A multi-device manager on a separate server.

You can also access the FXOS CLI for troubleshooting purposes.

Unsupported Features

The following ASA features are not supported on the Firepower 1100:

- Redundant interfaces
- Clustering
- ASA REST API
- ASA FirePOWER module
- Botnet Traffic Filter
- The following inspections:
  - SCTP inspection maps (SCTP stateful inspection using ACLs is supported)
  - Diameter
  - GTP/GPRS

Migrating an ASA 5500-X Configuration

You can copy and paste an ASA 5500-X configuration into the Firepower 1100. However, you will need to modify your configuration. Also note some behavioral differences between the platforms.

1. To copy the configuration, enter the **more system:running-config** command on the ASA 5500-X.
2. Edit the configuration as necessary (see below).
3. Connect to the console port of the Firepower 1100, and enter global configuration mode:

```
ciscoasa> enable
Password:
```

```
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
ciscoasa# configure terminal
ciscoasa(config)#
```

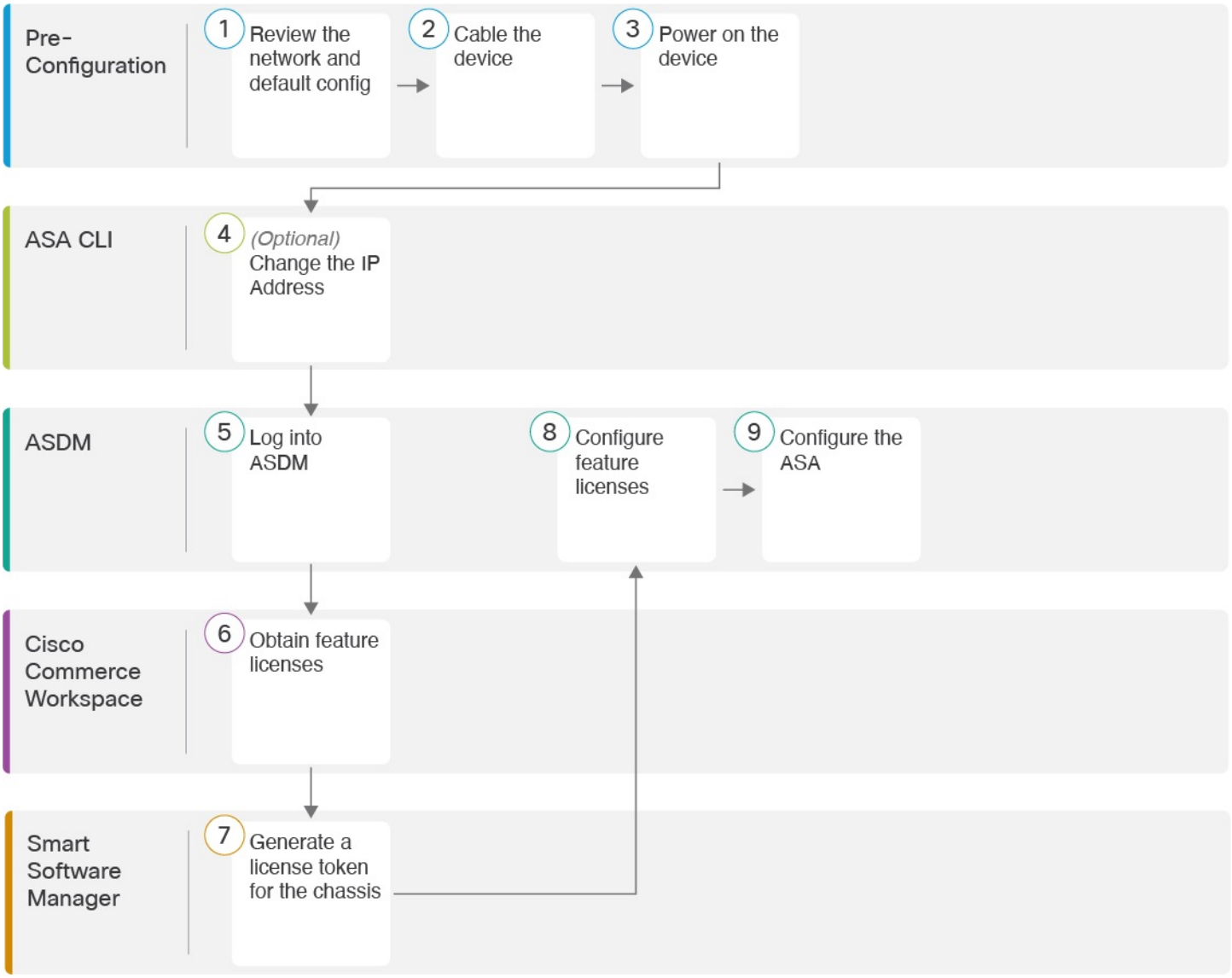
4. Clear the current configuration using the **clear configure all** command.
5. Paste the modified configuration at the ASA CLI.

This guide assumes a factory default configuration, so if you paste in an existing configuration, some of the procedures in this guide will not apply to your ASA.

ASA 5500-X Configuration	Firepower 1100 Configuration
PAK License	Smart License PAK licensing is not applied when you copy and paste your configuration. There are no licenses installed by default. Smart Licensing requires that you connect to the Smart Licensing server to obtain your licenses. Smart Licensing also affects ASDM or SSH access (see below).
Initial ASDM access	Remove any VPN or other strong encryption feature configuration—even if you only configured weak encryption—if you cannot connect to ASDM or register with the Smart Licensing server. You can reenable these features after you obtain the Strong Encryption (3DES) license. The reason for this issue is that the ASA includes 3DES capability by default for management access only. If you enable a strong encryption feature, then ASDM and HTTPS traffic (like that to and from the Smart Licensing server) are blocked. The exception to this rule is if you are connected to a management-only interface, such as Management 1/1. SSH is not affected.
Interface IDs	Make sure you change the interface IDs to match the new hardware IDs. For example, the ASA 5525-X includes Management 0/0, and GigabitEthernet 0/0 through 0/5. The Firepower 1120 includes Management 1/1 and Ethernet 1/1 through 1/8.
boot system commands The ASA 5500-X allows up to four **boot system** commands to specify the booting image to use.	The Firepower 1100 only allows a single **boot system** command, so you should remove all but one command before you paste. You actually do not need to have *any* **boot system** commands present in your configuration, as it is not read at startup to determine the booting image. The last-loaded boot image will always run upon reload. The **boot system** command performs an action when you enter it: the system validates and unpacks the image and copies it to the boot location (an internal location on disk0 managed by FXOS). The new image will load when you reload the ASA.

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 109.
2	Pre-Configuration	Cable the Device, on page 111.
3	Pre-Configuration	Power on the Device, on page 112.

4	ASA CLI	(Optional) Change the IP Address, on page 113.
5	ASDM	Log Into ASDM, on page 114.
6	Cisco Commerce Workspace	Configure Licensing, on page 115: Obtain feature licenses.
7	Smart Software Manager	Configure Licensing, on page 115: Generate a license token for the chassis.
8	ASDM	Configure Licensing, on page 115: Configure feature licenses.
9	ASDM	Configure the ASA, on page 120.

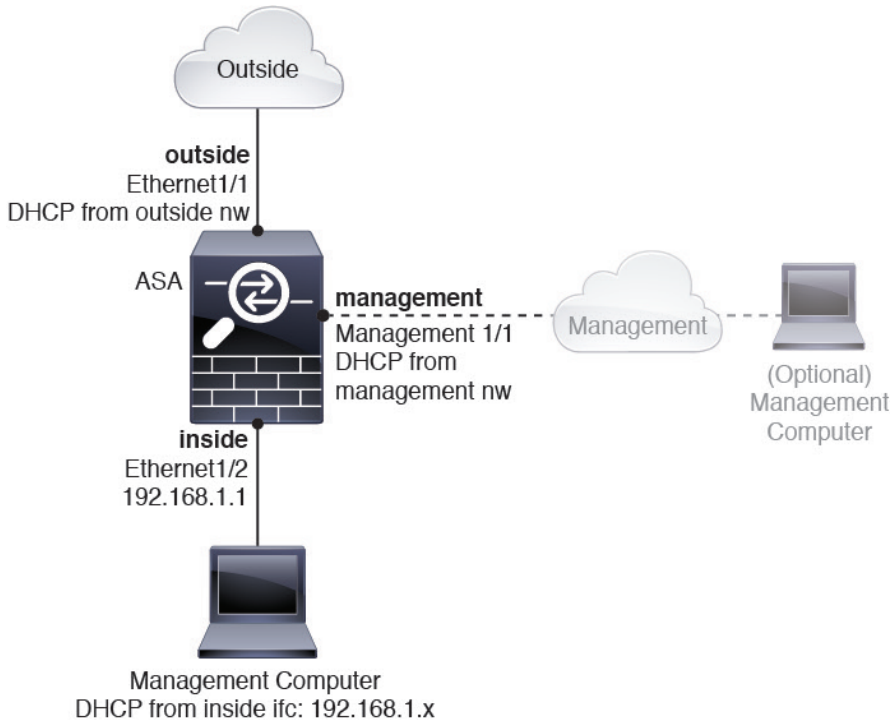
Review the Network Deployment and Default Configuration

The following figure shows the default network deployment for the Firepower 1100 using the default configuration.

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 113. 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 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 to be on the existing network.



Firepower 1100 Default Configuration

The default factory configuration for the Firepower 1100 configures the following:

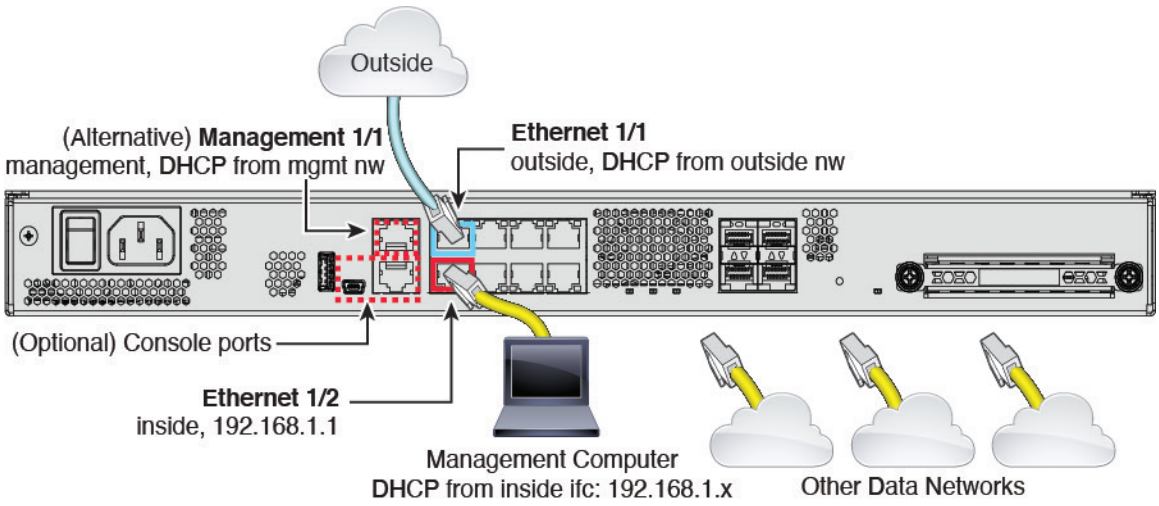
- **inside→outside traffic flow**—Ethernet 1/1 (outside), Ethernet 1/2 (inside)
- **outside IP address** from DHCP, **inside IP address**—192.168.1.1
- **management**—Management 1/1 (management), IP address from DHCP
- **DHCP server** on inside interface
- **Default routes** from outside DHCP, management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

The configuration consists of the following commands:

```
interface Management1/1
  management-only
  nameif management
  security-level 100
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/1
```

```
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/2
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
  no shutdown
!
object network obj_any
  subnet 0.0.0.0 0.0.0.0
  nat (any,outside) dynamic interface
!
http server enable
http 0.0.0.0 0.0.0.0 management
http 192.168.1.0 255.255.255.0 inside
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd enable inside
!
dns domain-lookup outside
dns server-group DefaultDNS
   name-server 208.67.222.222 outside
   name-server 208.67.220.220 outside
!
```

Cable the Device



Manage the Firepower 1100 on either Management 1/1 or Ethernet 1/2. The default configuration also configures Ethernet1/1 as outside.

Procedure

Step 1 Connect your management computer to either of the following interfaces:

- Management 1/1—Connect Management 1/1 to your management network, and make sure your management computer is on—or has access to—the management network. Management 1/1 obtains an IP address from a DHCP server on your management network; if you use this interface, you must determine the IP address assigned to the ASA so that you can connect to the IP address from your management computer.
- Ethernet 1/2—Connect your management computer directly to Ethernet 1/2 for initial configuration. Or connect Ethernet 1/2 to your inside network; make sure your management computer is on the inside network, because only clients on that network can access the ASA. Ethernet 1/2 has a default IP address (192.168.1.1) 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 (see Firepower 1100 Default Configuration, on page 110).

  If you need to change the Ethernet 1/2 IP address from the default, you must also cable your management computer to the console port. See (Optional) Change the IP Address, on page 113.

You can later configure ASA management access from other interfaces; see the ASA general operations configuration guide.

Step 2 Connect the outside network to the Ethernet1/1 interface.

For Smart Software Licensing, the ASA needs internet access so that it can access the License Authority.

Step 3 Connect other networks to the remaining interfaces.

Power on the Device

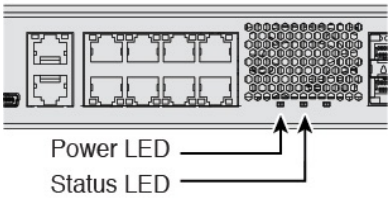
System power is controlled by a rocker power switch located on the rear of the device. The power switch is implemented as a soft notification switch that supports graceful shutdown of the system to reduce the risk of system software and data corruption.

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 back of the device; if it is solid green, the device is powered on.



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

Note When the switch is toggled from ON to OFF, it may take several seconds for the system to eventually power off. During this time, the Power LED on the front of the chassis blinks green. Do not remove the power until the Power LED is completely off.

(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 and FXOS CLI, on page 122 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 ethernet1/2
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.

The ASA includes 3DES capability by default for management access only, so you can connect to the License Authority and also use ASDM immediately. You can also use SSH and SCP if you later configure SSH access on the ASA. Other features that require strong encryption (such as VPN) must have the Strong Encryption license enabled, which requires you to first register to the License Authority.

Note If you attempt to configure any features that can use strong encryption before you have the license—even if you only configure weak encryption—then your HTTPS connection will be dropped on that interface, and you cannot reconnect. The exception to this rule is if you are connected to a management-only interface, such as Management 1/1. SSH is not affected. If you lose your HTTPS connection, you can connect to the console port to reconfigure the ASA, connect to a management-only interface, or connect to an interface not configured for a strong encryption feature.

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 (Ethernet 1/2) interface IP address.
- **https://***management_ip*—Management interface IP address assigned from DHCP.

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.

Configure Licensing

The ASA uses Cisco Smart Software Licensing. You can use regular Smart Software Licensing, which requires internet access; or for offline management, you can configure Permanent License Reservation or a Satellite server. For more information about these offline licensing methods, see Cisco ASA Series Feature Licenses; this guide applies to regular Smart Software Licensing.

When you register the chassis, the License Authority issues an ID certificate for communication between the chassis and the License Authority. It also assigns the chassis to the appropriate virtual account. Until you register with the License Authority, you will not be able to make configuration changes to features requiring special licenses, but operation is otherwise unaffected. Licensed features include:

- Standard
- Security Contexts
- Strong Encryption (3DES/AES)
- AnyConnect—AnyConnect Plus, AnyConnect Apex, or AnyConnect VPN Only.

The ASA includes 3DES capability by default for management access only, so you can connect to the License Authority and also use ASDM immediately. You can also use SSH and SCP if you later configure SSH access on the ASA. Other features that require strong encryption (such as VPN) must have the Strong Encryption license enabled, which requires you to first register to the License Authority.

Note If you attempt to configure any features that can use strong encryption before you have the license—even if you only configure weak encryption—then your HTTPS connection will be dropped on that interface, and you cannot reconnect. The exception to this rule is if you are connected to a management-only interface, such as Management 1/1. SSH is not affected. If you lose your HTTPS connection, you can connect to the console port to reconfigure the ASA, connect to a management-only interface, or connect to an interface not configured for a strong encryption feature.

When you request the registration token for the ASA from your Smart Software Licensing account, check the **Allow export-controlled functionality on the products registered with this token** check box so that the full Strong Encryption license is applied (your account must be qualified for its use). The Strong Encryption license is automatically enabled for qualified customers when you apply the registration token on the chassis, so no additional action is required.

Before you begin

- Have a master account on the Cisco 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.

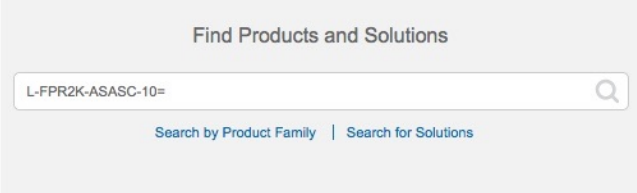
- Your Cisco Smart Software Licensing account must qualify for the Strong Encryption (3DES/AES) license to use some features (enabled using the export-compliance flag).

Procedure

Step 1 Make sure your Smart Licensing account contains the available licenses you need, including at a minimum the Standard license.

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 32: License Search

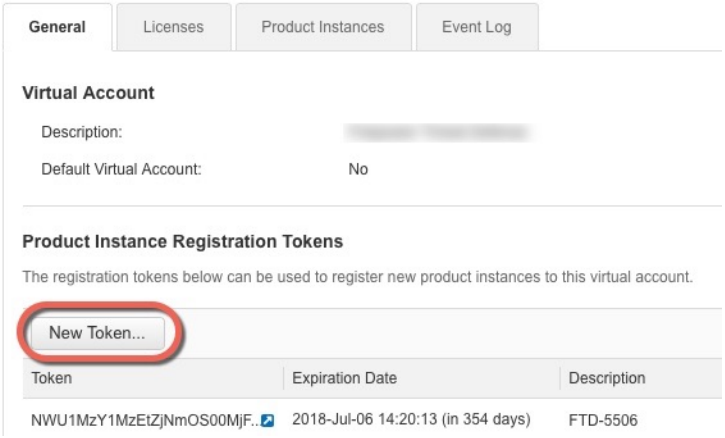


- Standard license—L-FPR1000-ASA=. The Standard license is free, but you still need to add it to your Smart Software Licensing account.
- 5 context license—L-FPR1K-ASASC-5=. Context licenses are additive; buy multiple licenses to meet your needs.
- 10 context license—L-FPR1K-ASASC-10=. Context licenses are additive; buy multiple licenses to meet your needs.
- Strong Encryption (3DES/AES) license—L-FPR1K-ENC-K9=. This license is free. Although this license is not generally rquired (for example, ASAs that use older Satellite Server versions (pre-2.3.0) require this license), you should still add it to your account for tracking purposes.
- Anyconnect—See the Cisco AnyConnect Ordering Guide. You do not enable this license directly in the ASA.

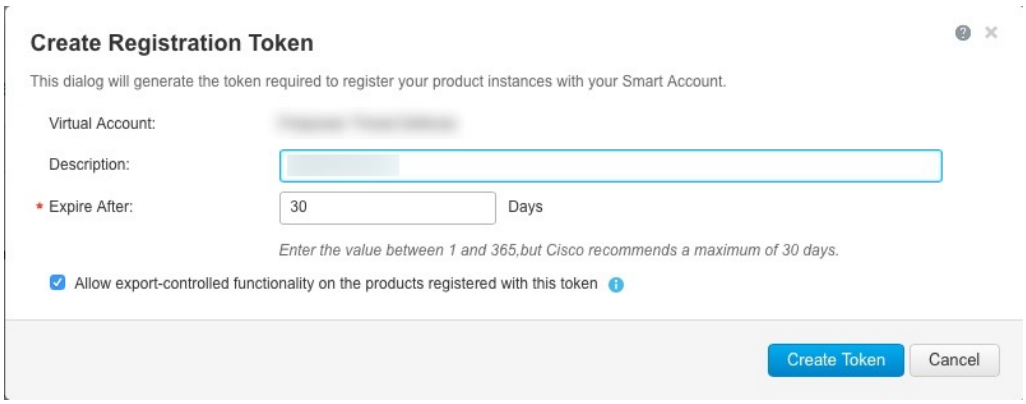
Step 2 In the Cisco Smart Software Manager, request and copy a registration token for the virtual account to which you want to add this device.

a) Click **Inventory**.

b) On the **General** tab, click **New Token**.



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



- **Description**
- **Expire After**—Cisco recommends 30 days.
- **Allow export-controlled functionaility on the products registered with this token**—Enables the export-compliance flag.

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 ASA.

Figure 33: View Token

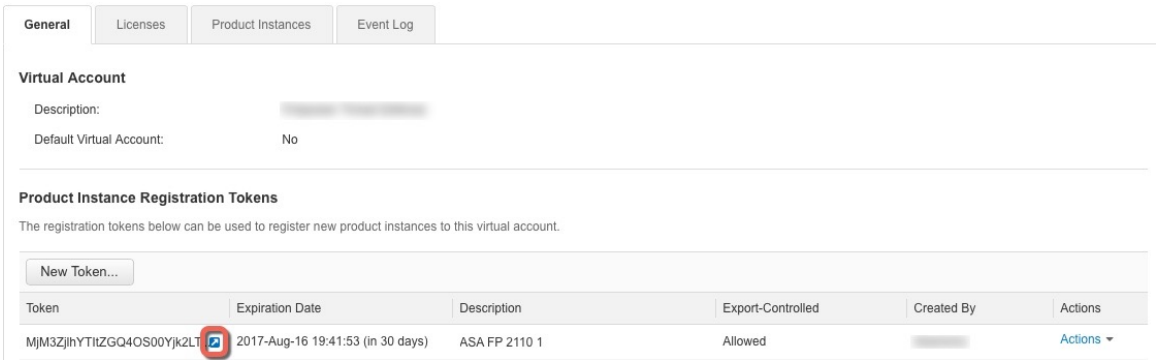
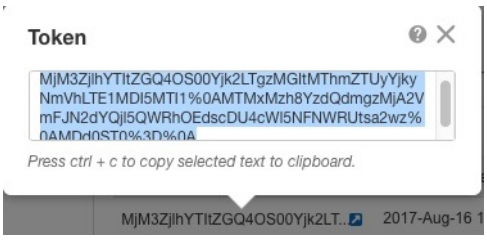
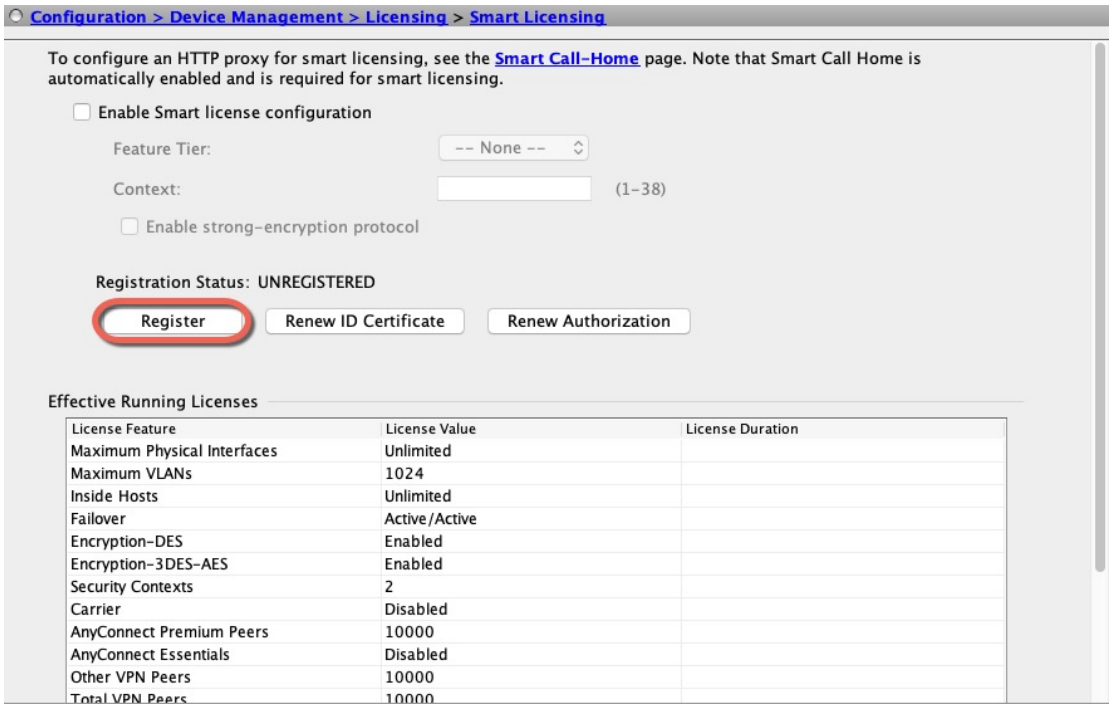


Figure 34: Copy Token

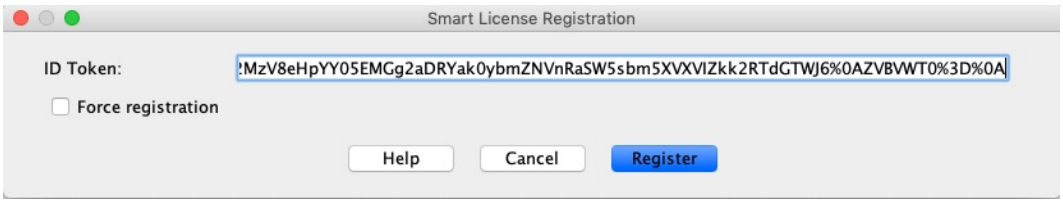


Step 3 In ASDM, choose **Configuration** > **Device Management** > **Licensing** > **Smart Licensing**.

Step 4 Click **Register**.



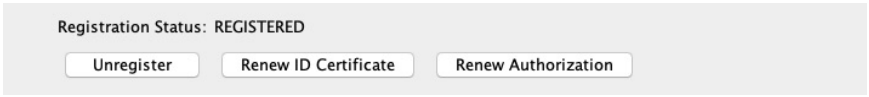
Step 5 Enter the registration token in the **ID Token** field.



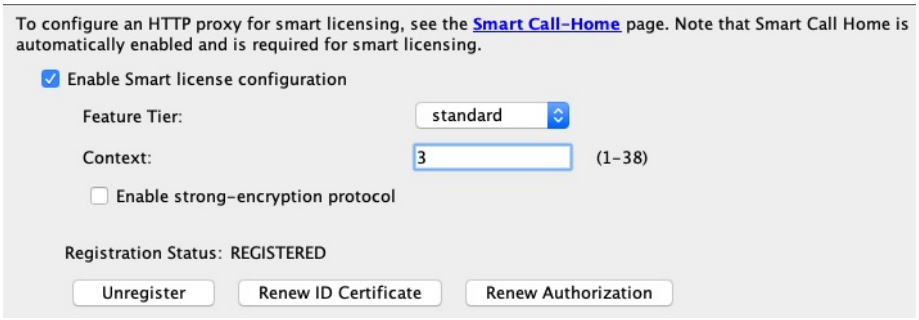
You can optionally check the **Force registration** check box to register an ASA that is already registered, but that might be out of sync with the License Authority. For example, use **Force registration** if the ASA was accidentally removed from the Smart Software Manager.

Step 6 Click **Register**.

The ASA registers with the License Authority using the pre-configured outside interface, and requests authorization for the configured license entitlements. The License Authority also applies the Strong Encryption (3DES/AES) license if your account allows. ASDM refreshes the page when the license status is updated. You can also choose **Monitoring** > **Properties** > **Smart License** to check the license status, particularly if the registration fails.



Step 7 Set the following parameters:



a) Check **Enable Smart license configuration**.

b) From the **Feature Tier** drop-down list, choose **Standard**.

Only the Standard tier is available.

c) (Optional) For the **Context** license, enter the number of contexts.

You can use 2 contexts without a license. The maximum number of contexts depends on your model:

- Firepower 1120—5 contexts
- Firepower 1140—10 contexts
- Firepower 1150—15 contexts

For example, to use the maximum of 5 contexts on the Firepower 1120, enter 3 for the number of contexts; this value is added to the default of 2.

Step 8 (Optional) The **Enable strong-encryption protocol** is generally not required; for example, ASAs that use older Satellite Server versions (pre-2.3.0) require this license, but you can check this box if you know you need to, or if you want to track usage of this license in your account.

Step 9 Click **Apply**.

Step 10 Click the **Save** icon in the toolbar.

Step 11 Quit ASDM and relaunch it.

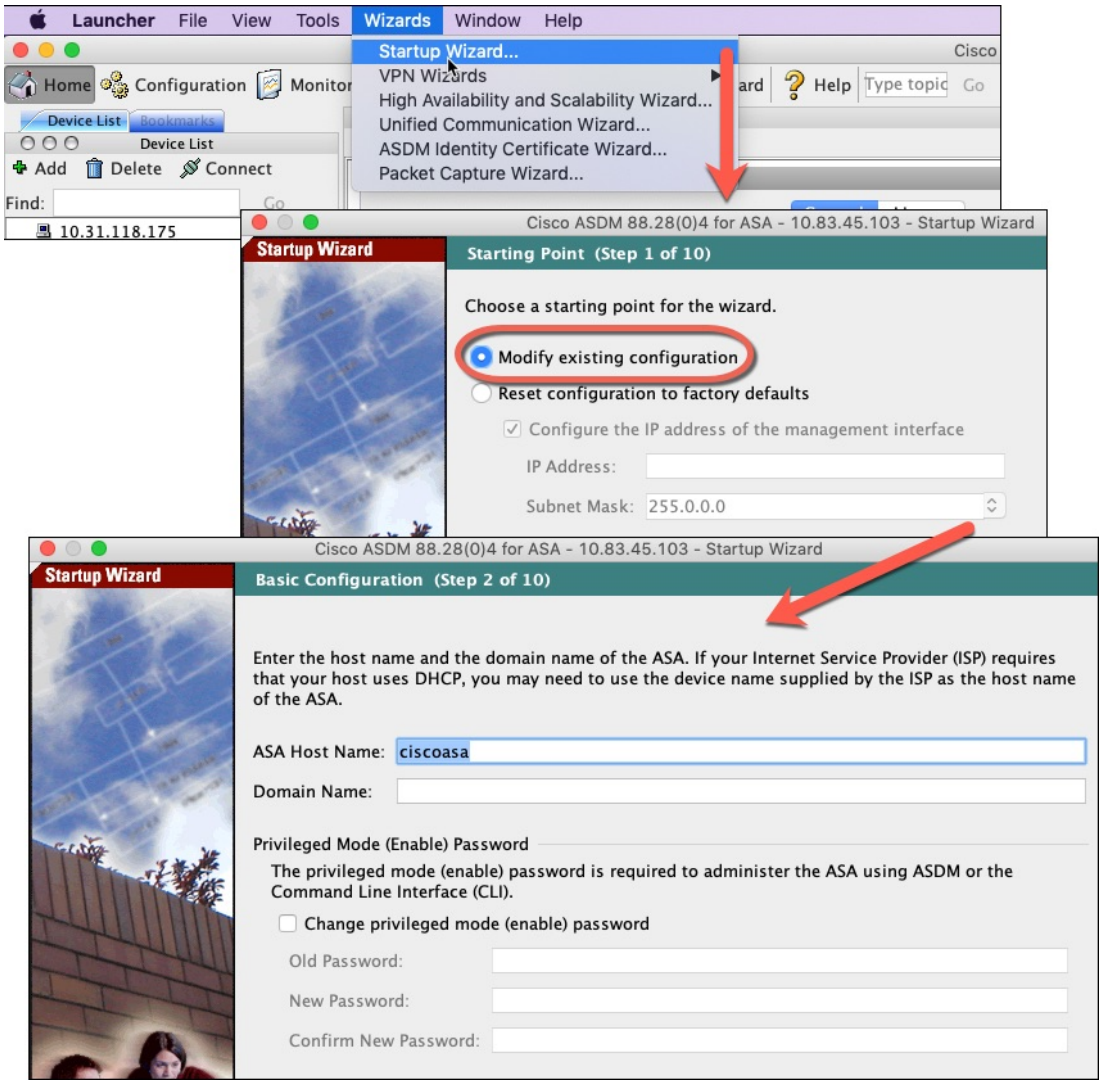
When you change licenses, you need to relaunch ASDM to show updated screens.

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

Step 4 To continue configuring your ASA, see the documents available for your software version at Navigating the Cisco ASA Series Documentation.

Access the ASA and FXOS 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 access the FXOS CLI from the ASA CLI for troubleshooting purposes.

Procedure

Step 1 Connect your management computer to the console port. Be sure to install any necessary USB serial drivers for your operating system (see the Firepower 1100 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#
```

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

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

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

Step 3 Access global configuration mode.

configure terminal

Example:

```
ciscoasa# configure terminal
ciscoasa(config)#
```

You can begin to configure the ASA from global configuration mode. To exit global configuration mode, enter the **exit**, **quit**, or **end** command.

Step 4 (Optional) Connect to the FXOS CLI.

connect fxos [**admin**]

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

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

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

Example:

```
ciscoasa# connect fxos admin
Connecting to fxos.
Connected to fxos. Escape character sequence is 'CTRL-^X'.
firepower#
firepower# exit
Connection with FXOS terminated.
Type help or '?' for a list of available commands.
ciscoasa#
```

What's Next?

- To continue configuring your ASA, see the documents available for your software version at Navigating the Cisco ASA Series Documentation.
- For troubleshooting, see the FXOS troubleshooting guide.