



Cisco Firepower 1010 Getting Started Guide

First Published: 2019-06-13

Last Modified: 2021-01-29

Americas Headquarters

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



CHAPTER 1

Which Operating System and Manager is Right for You?

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

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

Operating Systems

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

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

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

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

Managers

The FTD and ASA support multiple managers.

FTD Managers

Table 1: FTD Managers

| Manager | Description |
|-----------------------------------|--|
| Firepower Device Manager (FDM) | <p>FDM is a web-based, simplified, on-device manager. Because it is simplified, some FTD features are not supported using FDM. You should use FDM if you are only managing a small number of devices and don't need a multi-device manager.</p> <p>Note Both FDM and CDO can discover the configuration on the device, so you can use FDM and CDO to manage the same device. FMC is not compatible with other managers.</p> <p>To get started with FDM, see Firepower Threat Defense Deployment with FDM, on page 61.</p> |
| Cisco Defense Orchestrator (CDO) | <p>CDO is a simplified, cloud-based multi-device manager. Because it is simplified, some FTD features are not supported using CDO. You should use CDO if you want a multi-device manager that offers a simplified management experience (similar to FDM). And because CDO is cloud-based, there is no overhead of running CDO on your own servers. CDO also manages other security devices, such as ASAs, so you can use a single manager for all of your security devices.</p> <p>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 automatically register with CDO.</p> <p>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.</p> <p>To get started with CDO provisioning, see Firepower Threat Defense Deployment with CDO Provisioning, on page 25.</p> |
| Firepower Management Center (FMC) | <p>FMC is a powerful, web-based, multi-device manager that runs on its own server hardware, or as a virtual device on a hypervisor. You should use FMC if you want a multi-device manager, and you require all features on the FTD. FMC also provides powerful analysis and monitoring of traffic and events.</p> <p>Note FMC is not compatible with other managers because the FMC owns the FTD configuration, and you are not allowed to configure the FTD directly, bypassing the FMC.</p> <p>To get started with FMC, see Firepower Threat Defense Deployment with FMC, on page 89.</p> <p>For a remote branch setup, we recommend that you use the standalone document specific to that deployment.</p> |
| FTD REST API | <p>The FTD REST API lets you automate direct configuration of the FTD. This API is compatible with FDM and CDO use because they can both discover the configuration on the device. You cannot use this API if you are managing the FTD using FMC.</p> <p>The FTD REST API is not covered in this guide. For more information, see the FTD REST API guide.</p> |

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

ASA Managers

Table 2: ASA Managers

| Manager | Description |
|---|--|
| Adaptive Security Device Manager (ASDM) | <p>ASDM is a Java-based, on-device manager that provides full ASA functionality. You should use ASDM if you prefer using a GUI over the CLI, and you only need to manage a small number of ASAs. ASDM can discover the configuration on the device, so you can also use the CLI, CDO, or CSM with ASDM.</p> <p>To get started with ASDM, see ASA Deployment with ASDM, on page 135.</p> |
| CLI | <p>You should use the ASA CLI if you prefer CLIs over GUIs.</p> <p>The CLI is not covered in this guide. For more information, see the ASA configuration guides.</p> |
| Cisco Defense Orchestrator (CDO) | <p>CDO is a simplified, cloud-based multi-device manager. Because it is simplified, some ASA features are not supported using CDO. You should use CDO if you want a multi-device manager that offers a simplified management experience. And because CDO is cloud-based, there is no overhead of running CDO on your own servers. CDO also manages other security devices, such as FTDs, so you can use a single manager for all of your security devices. CDO can discover the configuration on the device, so you can also use the CLI or ASDM.</p> <p>CDO is not covered in this guide. To get started with CDO, see the CDO home page.</p> |
| Cisco Security Manager (CSM) | <p>CSM is a powerful, multi-device manager that runs on its own server hardware. You should use CSM if you need to manage large numbers of ASAs. CSM can discover the configuration on the device, so you can also use the CLI or ASDM. CSM does not support managing FTDs.</p> <p>CSM is not covered in this guide. For more information, see the CSM user guide.</p> |
| ASA REST API | <p>The ASA REST API lets you automate ASA configuration. However, the API does not include all ASA features, and is no longer being enhanced.</p> <p>The ASA REST API is not covered in this guide. For more information, see the ASA REST API guide.</p> |



PART I

Firepower Threat Defense Deployment with CDO

- [Firepower Threat Defense Deployment with CDO and Low-Touch Provisioning, on page 7](#)
- [Firepower Threat Defense Deployment with CDO Provisioning, on page 25](#)



CHAPTER 2

Firepower Threat Defense Deployment with CDO and Low-Touch Provisioning

Is This Chapter for You?

Low-Touch Provisioning (LTP) simplifies and automates the onboarding of new Firepower Threat Defense (FTD) devices to Cisco Defense Orchestrator (CDO). LTP streamlines the deployment of new Firepower devices by allowing network administrators to deliver the devices directly to a branch office, add the devices to the CDO cloud-based device manager, and then manage the devices after the FTD device successfully connects to the Cisco Cloud.

This chapter explains how to onboard your Firepower devices to CDO using low-touch provisioning. 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 feature requires Firepower version 6.7 or later.



Note This document assumes the Firepower 1010 hardware has a pre-installed FTD image on it. The Firepower 1010 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 1010 runs an underlying operating system called the Firepower eXtensible Operating System (FXOS). The Firepower 1010 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 1010 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.

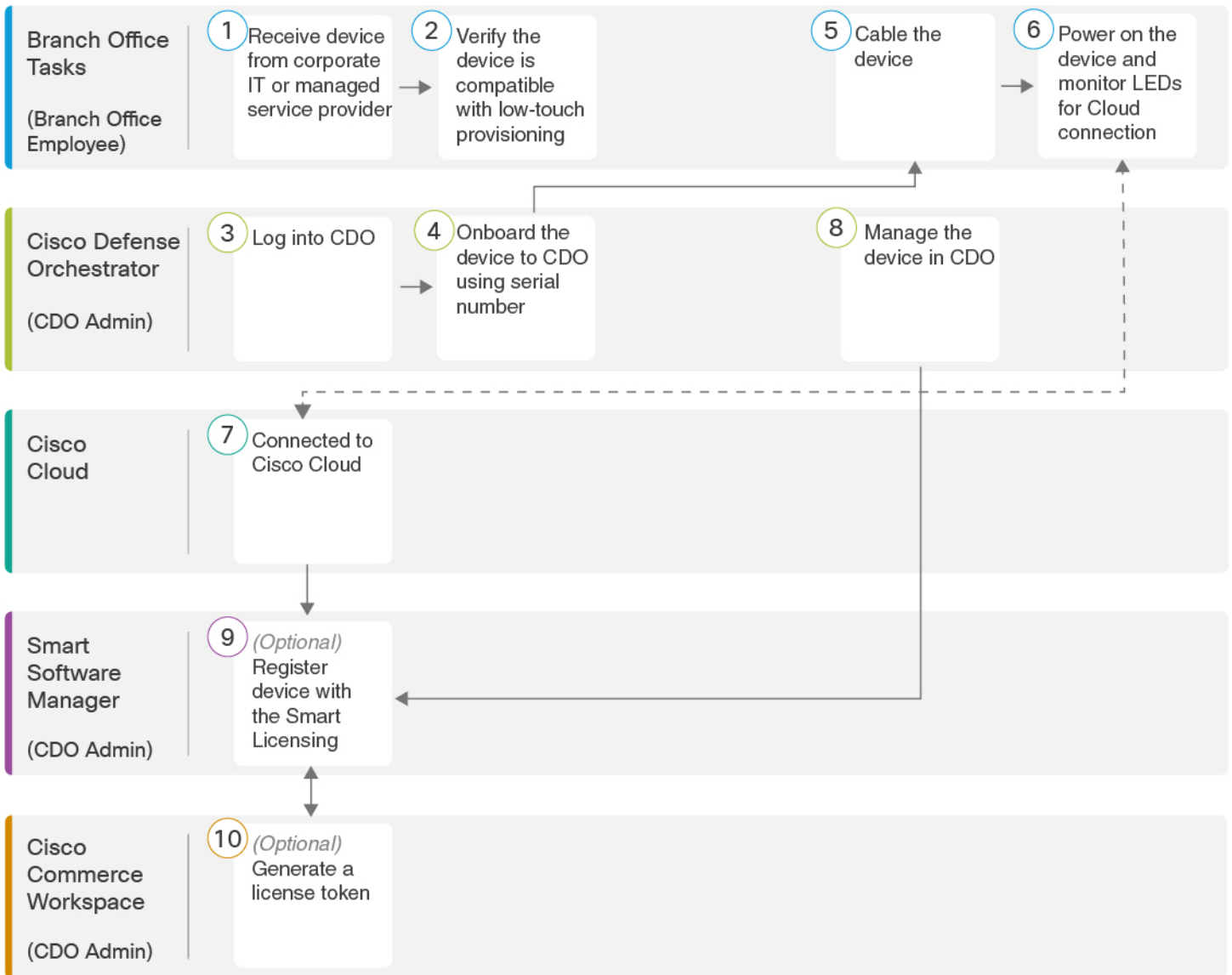
- [End-to-End Procedure, on page 8](#)
- [Branch Office - Receive the Device, on page 10](#)
- [CDO Administrator - Central Headquarters, on page 11](#)
- [Branch Office - Install the Device, on page 17](#)
- [CDO Administrator - Complete the Onboarding, on page 19](#)

End-to-End Procedure

This chapter explains how to deploy a factory-default FTD 1010 device at a remote branch office using the low-touch provisioning feature:

1. Your branch office receives an FTD 6.7+ device that has either been shipped directly from Cisco or one that has been reimaged with FTD 6.7+ software.
2. An administrator at the central headquarters onboards the device to CDO using the device's serial number.
3. The branch office employee cables and powers on the FTD.
4. The administrator at the central headquarters completes onboarding and configuration of the FTD using CDO.

See the following tasks to deploy FTD with CDO using low-touch provisioning on your chassis.



| | | |
|---|---|--|
| 1 | Branch Office Tasks (Branch Office Employee) | Verify the Device Supports Low-Touch Provisioning from a Branch Office, on page 10 : Receive the device from corporate IT or managed service provider. |
| 2 | Branch Office Tasks (Branch Office Employee) | Verify the Device Supports Low-Touch Provisioning from a Branch Office, on page 10 : Take inventory of the device and packaging; record the serial number. |
| 3 | Cisco Defense Orchestrator (CDO Admin) | Log Into CDO with Cisco Secure Sign-On, on page 14 . |

| | | |
|----|---|---|
| 4 | Cisco Defense Orchestrator (CDO Admin) | Onboard the Device Using Low-Touch Provisioning and the Serial Number, on page 15. |
| 5 | Branch Office Tasks (Branch Office Employee) | Cable the Device, on page 17. |
| 6 | Branch Office Tasks (Branch Office Employee) | Power On the Device, on page 18: Attach the power cord to the device, and connect it to an electrical outlet. |
| 7 | Cisco Cloud | Power On the Device, on page 18: Observe the Status LED on the device for connection to the Cisco cloud. |
| 8 | Cisco Defense Orchestrator (CDO Admin) | Manage the Device with CDO, on page 24. |
| 9 | Smart Software Manager (CDO Admin) | Configure Licensing, on page 19: Optionally, register the device with the Smart Licensing Server; or continue to use the 90-day evaluation license. |
| 10 | Cisco Commerce Workspace (CDO Admin) | Configure Licensing, on page 19: Optionally, generate a license token. |

Branch Office - Receive the Device

After you receive the FTD from your corporate IT department, you need to record the device's serial number and send it to the CDO administrator. Outline a communication plan for the onboarding process. Include any key tasks to be completed and provide points of contact for each item.



Tip You can [watch this video](#) to see how a Branch employee onboards a Firepower device using CDO and low-touch provisioning.

Verify the Device Supports Low-Touch Provisioning from a Branch Office

Before you rack the device or discard the shipping box, verify that your Firepower device can be deployed using low-touch provisioning.



Note This procedure assumes you are working with a new Firepower device running FTD Version 6.7 or later.

Before you begin

- Unpack the chassis and chassis components.
- Take inventory of your Firepower device and packaging before you connect any cables or power on the device.
- Your IT department needs your device serial number to connect to the device and manage it remotely.
- You should also familiarize yourself with the chassis layout, components, and LEDs.

Procedure

- Step 1** Verify the product ID (PID) on the shipping box. The cardboard box in which the device was shipped should have a plain white sticker on it that indicates the shipped version of Firepower software (6.7 or later).
The PID should be similar to this example of a Firepower 1010 PID: SF-F1K-TD6.7-K9.
- Step 2** Record the device's serial number. The serial number of the device can be found on the shipping box. It can also be found on a sticker on the bottom of the device chassis.
- Step 3** Send the device serial number to the CDO network administrator at your IT department/central headquarters.
- Note** Your network administrator needs your device serial number to facilitate low-touch provisioning, connect to the device, and configure it remotely.
-

What to do next

Communicate with the CDO administrator at your IT department/central headquarters to develop an onboarding timeline. Your next steps are to cable the device and connect power after your network administrator onboards the device to CDO.

CDO Administrator - Central Headquarters

After the remote branch administrator sends the serial number information to the central headquarters, the CDO administrator onboards the FTD to CDO.

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 14](#).
- If you don't have a Cisco Secure Sign-On account, see [Create a New Cisco Secure Sign-On Account, on page 12](#).

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.

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

Figure 1: Cisco SSO Sign Up

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

Figure 2: Create Account

The screenshot shows the Cisco 'Create Account' registration page. At the top is the Cisco logo. Below it is the title 'Create Account'. The form contains five input fields: 'Email *', 'Password *', 'First name *', 'Last name *', and 'Organization *'. A small asterisk indicates required fields. Below the fields is a blue 'Register' button and a 'Back' link.

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.

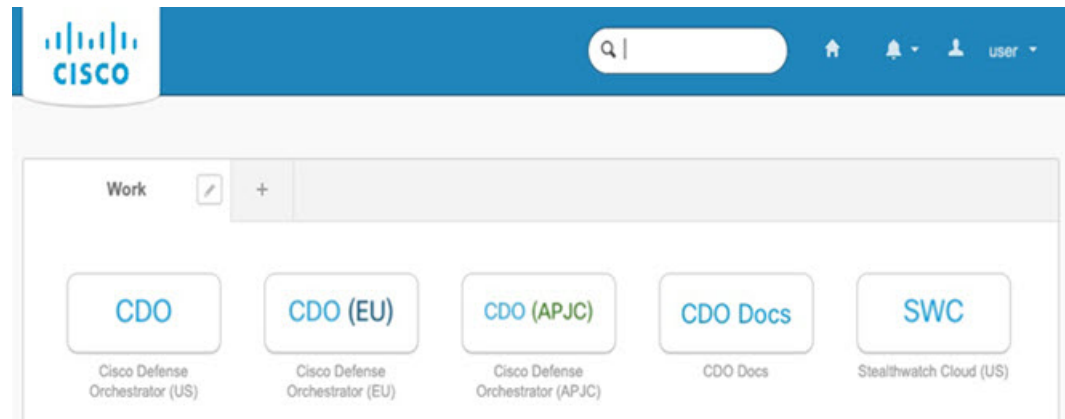
Step 4 Configure Account Recovery Options for your Cisco Secure Sign-On Account.

- 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 3: Cisco SSO Dashboard



Log Into CDO with Cisco Secure Sign-On

Log into CDO to onboard and manage your FTD.

Before you begin

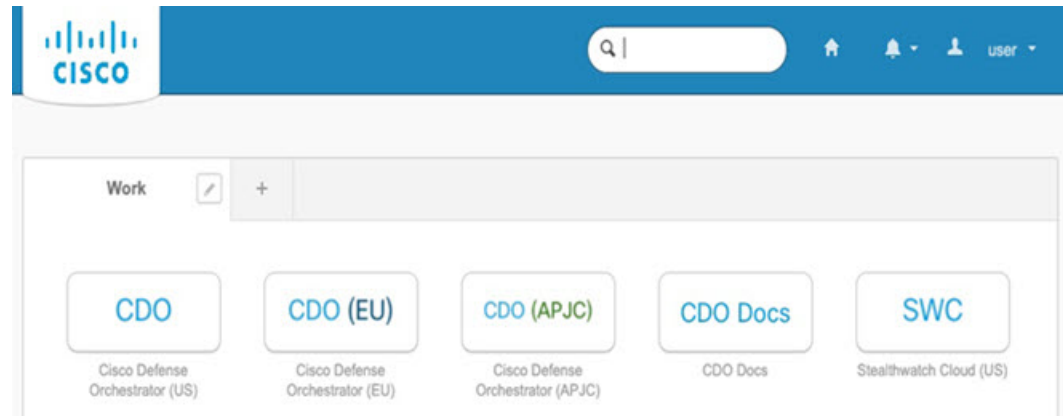
Cisco Defense Orchestrator (CDO) uses Cisco Secure Sign-On as its identity provider and Duo Security for multi-factor authentication (MFA).

- 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 12](#).
- 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 <https://www.apj.cdo.cisco.com>.

Figure 4: 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 Using Low-Touch Provisioning and the Serial Number

To onboard a Firepower device to CDO using LTP, you complete this procedure, connect the device to a network that can reach the internet, and power on the device.

Before you begin

Low-touch provisioning (LTP) is a feature that allows a new factory-shipped Firepower 1010 series device to be provisioned and configured automatically, eliminating many of the manual tasks involved with onboarding the device to CDO.



Note Your device needs to have Version 6.7 or greater installed to use LTP. If you want to use this method to onboard an FTD device running on an older software version (6.4, 6.5, and 6.6), you need to perform a fresh installation of the software on that device, **not** an upgrade.

Procedure

- Step 1** In the navigation pane, click **Devices & Services** and click the blue plus button to **Onboard** a device.
- Step 2** Click on the **FTD** card.

Note When you attempt to onboard an FTD device, CDO prompts 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 doesn't prompt it again in subsequent FTD onboarding. If the EULA agreement changes in the future, you must accept it again when prompted.

Step 3 On the **Onboard FTD Device** screen, click **Use Serial Number**.

Step 4 In the **Connection** area, provide the following:

a) Select the Secure Device Connector (SDC) that this device will communicate with.

The default SDC is displayed, but you can change it by clicking the blue **Change** link.

b) **Device Serial Number**: Enter the serial number or the PCA number of the device you want to onboard.

c) **Device Name**: Provide a name for the device.

Step 5 Click **Next**.

Step 6 In the **Password Reset** area, provide the following:

a) **Default Password Not Changed**: Select this option to change the default password of a new device.

- Enter a **New Password** for the device and **Confirm Password**.
- Ensure that the new password meets the requirements mentioned onscreen.

Note If the device's default password is already changed, the entries made in this field will be ignored.

b) **Default Password Changed**: Select this option only for the device whose default password has already been changed using FDM or on Firepower eXtensible Operating System (FXOS) Console.

Step 7 Click **Next**.

Step 8 In the **Smart License** area, select one of the required options.

- **Apply Smart License**: Select this option if your device is not smart licensed already. You have to generate a token using the Cisco Smart Software Manager and copy in this field.
- **Device Already Licensed**: Select this option if your device has already been licensed.

Note If the default password has already been changed, this radio button will be selected automatically. However, you can choose another option that you want.

- **Use 90-day Evaluation License**: Apply a 90-day evaluation license.

Step 9 Click **Next**.

Step 10 In the **Subscription Licenses** area, perform the following:

- If the smart license is applied, you can enable the additional licenses you want and click **Next**.
- If the evaluation license is enabled, all other licenses are available except for the RA VPN license. Select the licenses that you want and click **Next** to continue.
- You can choose to continue only with the base license.

Note If the **Device Already Licensed** is selected in the **Smart License** step, you cannot perform any selection here. CDO displays **Keep Existing Subscription** and moves to the **Labels** step.

Step 11 (Optional) In the **Labels** area, you can enter a label name if required.

Step 12 Click **Go to Devices and Services**.

What to do next

Communicate with the branch office where the device is being deployed. After the branch office administrator cables and powers on the FTD, your next steps are to complete the onboarding process and configure/manage the device.

Branch Office - Install the Device

After the CDO administrator onboards the FTD to CDO, you need to cable and power on the device so that it has internet access from the outside interface. The CDO administrator can then complete the onboarding process.

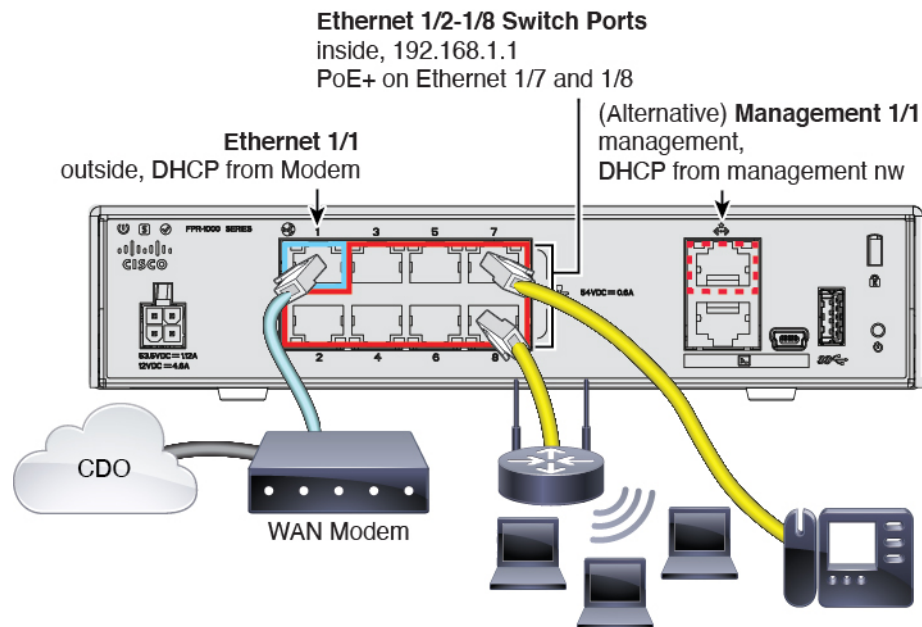
Cable the Device

This topic describes the how to connect the Firepower 1010 to your network so that it can be managed remotely by a CDO administrator.

- If you received a Firepower firewall at your branch office and your job is to plug it in to your network, [watch this video](#).

The video describes your Firepower device and the LED sequences on the device that indicate the device's status. If you need to, you'll be able to confirm the device's status with your IT department just by looking at the LEDs.

Figure 5: Cabling the Firepower 1010



Note Ethernet1/2 through 1/8 are configured as hardware switch ports; PoE+ is also available on Ethernet1/7 and 1/8.

Low-touch provisioning supports connecting to CDO on Ethernet 1/1 (outside). You can alternatively use low-touch provisioning on the Management 1/1 interface.

Procedure

Step 1 Connect the network cable from the Ethernet 1/1 interface to your wide area network (WAN) modem. Your WAN modem is your branch's connection to the internet and will be your Firepower firewall's route to the internet as well.

Note Alternatively, you can connect the network cable from the device's Management 1/1 interface to your WAN. Whichever interface you use must have a route to the internet. The Management interface supports IPv6 if you manually set the IP address at the CLI. See [\(Optional\) Change Management Network Settings at the CLI, on page 33](#). To use IPv6 on Management, make sure you also keep or set an IPv4 address; dual stack is required for IPv6 to work. The outside Ethernet 1/1 interface only supports IPv4 for low-touch provisioning.

Step 2 Connect inside devices to the remaining switch ports, Ethernet 1/2 through 1/8. Ethernet 1/7 and 1/8 are PoE+ ports.

What to do next

Proceed to the next task, [Power On the Device, on page 18](#).

Power On the Device

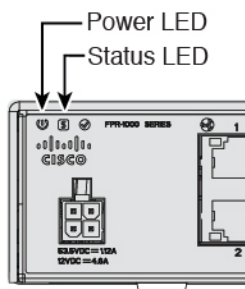
System power is controlled by the power cord; there is no power button.

Procedure

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

The power turns on automatically when you plug in the power cord.

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



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

- Step 4** Observe the Status LED on the back or top of the device; when the device is booting correctly, the Status LED flashes fast green.
- If there is a problem, the Status LED flashes fast amber. If this happens, call your IT department.
- Step 5** Observe the Status LED on the back or top of the device; when the device connects to the Cisco cloud, the Status LED slowly flashes green.
- If there is a problem, the Status LED flashes amber and green, and the device did not reach the Cisco Cloud. If this happens, make sure that your network cable is connected to the Ethernet 1/1 interface and to your WAN modem. If after adjusting the network cable, the device does not reach the Cisco cloud after about 10 more minutes, call your IT department.

What to do next

- Communicate with your IT department to confirm your onboarding timeline and activities. You should have a communication plan in place with the CDO administrator at your central headquarters.
- After you complete this task, your CDO administrator will be able to configure and manage the Firepower device remotely. You're done.

CDO Administrator - Complete the Onboarding

When you onboard the device in CDO using the serial number, the device is associated with your CDO tenant in the Cisco cloud. After the branch office administrator cables and powers on the FTD, the device connects to the Cisco cloud and, because the device is already associated with your tenant, CDO syncs the device's configuration automatically.

You can now configure and manage your device with CDO. Optionally, if you are using the evaluation license, you can obtain feature licenses and complete the steps to license the device.

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.

- **Security Plus**—High Availability.

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 54](#).

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 6: 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-FPR1010T-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-FPR1010T-TMC-1Y
- L-FPR1010T-TMC-3Y
- L-FPR1010T-TMC-5Y

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

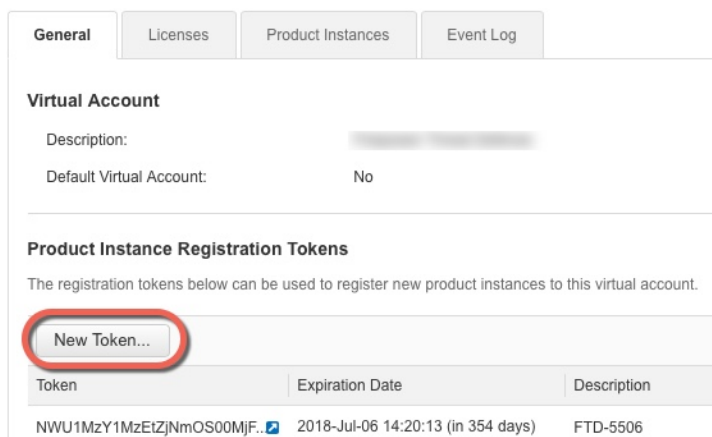
- Security Plus license: L-FPR1010-SEC-PL=. The Security Plus license enables High Availability.

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**:

The 'Create Registration Token' dialog box contains the following fields and options:

- Virtual Account:** [Redacted]
- Description:** [Empty text box]
- Expire After:** 30 Days
- Allow export-controlled functionality on the products registered with this token

Buttons: Create Token, Cancel

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

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 7: View Token

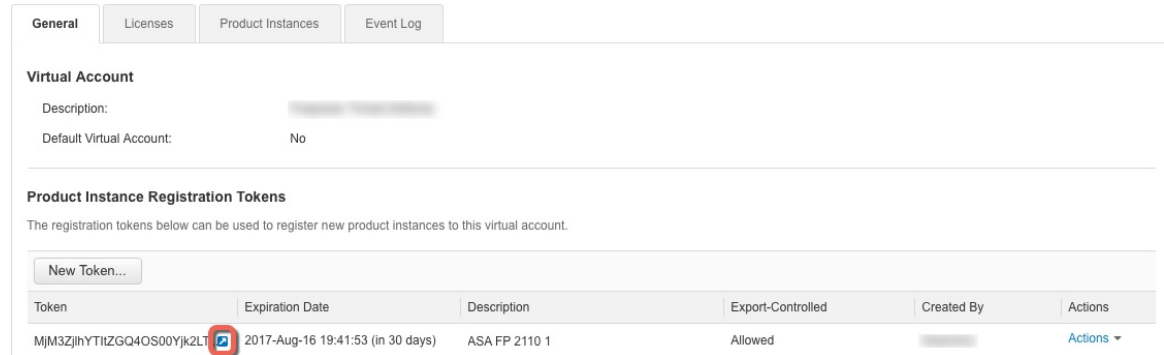
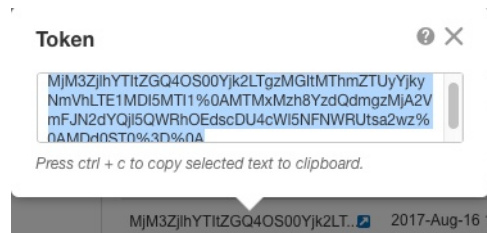


Figure 8: Copy Token



- 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:

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

- 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.

Manage Licenses
ftd-650-115-1543-181
✕

✔ Connected
Sufficient license.

Last Sync: May 26, 2020 4:24:05 PM
Next Sync: May 26, 2020 4:34:05 PM

Refresh Licenses

✔

Base License

STATUS: ENABLED ALWAYS

This perpetual license is included with the purchase of the system. You must have this license to configure and use the device. It covers all features not covered by subscription licenses.

Includes: Base Firewall Capabilities, Application Visibility and Control

✔

Threat

STATUS: ENABLED

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

Includes: Intrusion Policy

✔

Malware

STATUS: ENABLED

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

Includes: File Policy

✔

URL License

STATUS: ENABLED

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

Includes: URL Reputation

⊘

RA VPN Only License

STATUS: DISABLED

AnyConnect VPN Only license includes basic VPN services such as device and per-application VPN (including third-party IKEv2 remote access VPN headend support), trusted network detection, basic device context collection, and Federal Information Processing Standards (FIPS) compliance.

Includes: RA-VPN

✔

RA VPN Plus License

STATUS: ENABLED

AnyConnect Plus license includes basic VPN services and also other non-VPN services such as the AnyConnect Network Access Manager 802.1X supplicant, the Cloud Web Security module, and the Cisco Umbrella Roaming module

Includes: RA-VPN

✔

RA VPN Anex I license

Close

Save

- **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.

Cisco Firepower 1010 Getting Started Guide

23

- **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**:

Device Summary
Smart License

LICENSE ISSUE
OUT OF COMPLIANCE

Last sync: 10 Jul 2019 11:47 AM
Next sync: 10 Jul 2019 11:57 AM

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

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

Step 7 Choose **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 37](#).
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.



CHAPTER 3

Firepower Threat Defense Deployment with CDO Provisioning

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 to CDO, 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 1010 hardware has a pre-installed FTD image on it. The Firepower 1010 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 1010 runs an underlying operating system called the Firepower eXtensible Operating System (FXOS). The Firepower 1010 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.



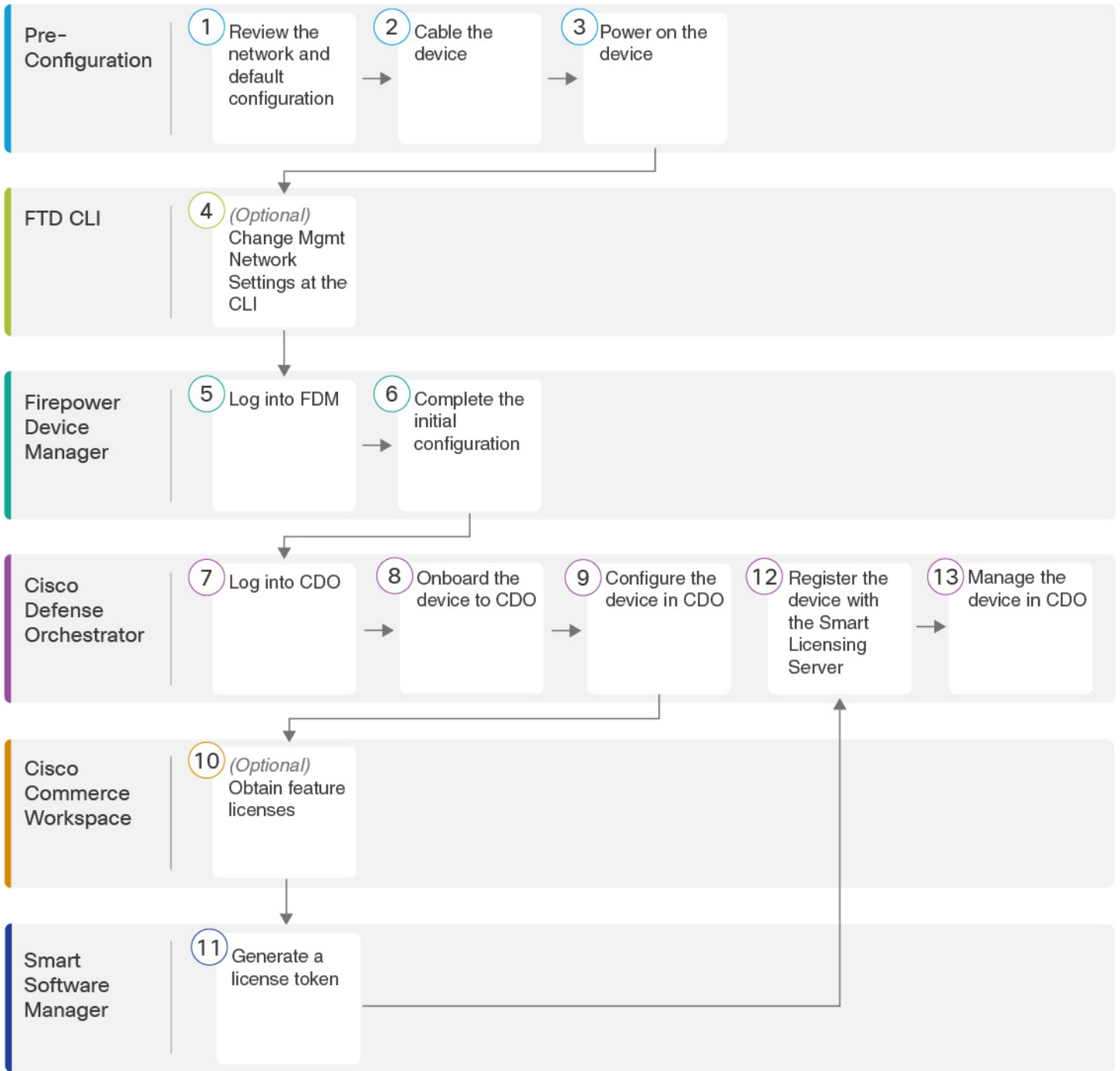
Note **Privacy Collection Statement**—The Firepower 1010 Series does not require or actively collect personally-identifiable information. However, you can use personally-identifiable information in the configuration, for example for usernames. In this case, an administrator might be able to see this information when working with the configuration or when using SNMP.

- [End-to-End Procedure, on page 26](#)
- [Review the Network Deployment and Default Configuration, on page 28](#)
- [Cable the Device, on page 31](#)
- [Power On the Device, on page 32](#)

- [\(Optional\) Change Management Network Settings at the CLI, on page 33](#)
- [Log Into FDM, on page 35](#)
- [Complete the Initial Configuration, on page 35](#)
- [Log Into CDO, on page 37](#)
- [Onboard the Device to CDO, on page 41](#)
- [Configure the Device in CDO, on page 45](#)
- [Configure Licensing, on page 49](#)
- [Manage the Device with CDO, on page 55](#)
- [Access the FTD and FXOS CLI, on page 55](#)
- [Power Off the Device Using FDM, on page 56](#)
- [What's Next, on page 57](#)

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 28. |
| 2 | Pre-Configuration | Cable the Device, on page 31. |

| | | |
|----|----------------------------|---|
| 3 | Pre-Configuration | Power On the Device, on page 32. |
| 4 | FTD CLI | (Optional) Change Management Network Settings at the CLI, on page 33. |
| 5 | Firepower Device Manager | Log Into FDM, on page 35. |
| 6 | Firepower Device Manager | Complete the Initial Configuration, on page 35 |
| 7 | Cisco Defense Orchestrator | Log Into CDO with Cisco Secure Sign-On, on page 39. |
| 8 | Cisco Defense Orchestrator | Onboard the Device to CDO, on page 41. |
| 9 | Cisco Defense Orchestrator | Configure the Device in CDO, on page 45 |
| 10 | Cisco Commerce Workspace | (Optional) Configure Licensing, on page 49: Obtain feature licenses. |
| 11 | Smart Software Manager | Configure Licensing, on page 49: Generate a license token. |
| 12 | Cisco Defense Orchestrator | Configure Licensing, on page 49: Register the device with the Smart Licensing Server. |
| 13 | Cisco Defense Orchestrator | Manage the Device with CDO, on page 55. |

Review the Network Deployment and Default Configuration

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

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

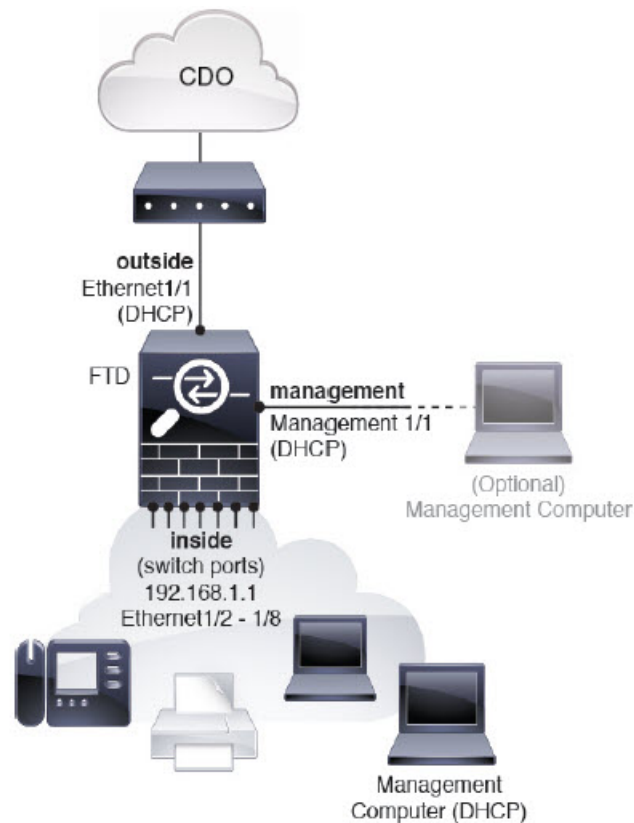


Note If you cannot use the default management IP address (for example, your management network does not include a DHCP server), then you can connect to the console port and perform initial setup at the CLI, including setting the Management IP address, gateway, and other basic networking settings.

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

- 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 9: 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**—IP address 192.168.1.1.
 - (6.5 and later) **Hardware switch**—Ethernet 1/2 through 1/8 belong to VLAN 1
 - (6.4) **Software switch** (Integrated Routing and Bridging)—Ethernet 1/2 through 1/8 belong to bridge group interface (BVI) 1
- **outside**—Ethernet 1/1, IP address from IPv4 DHCP
- **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



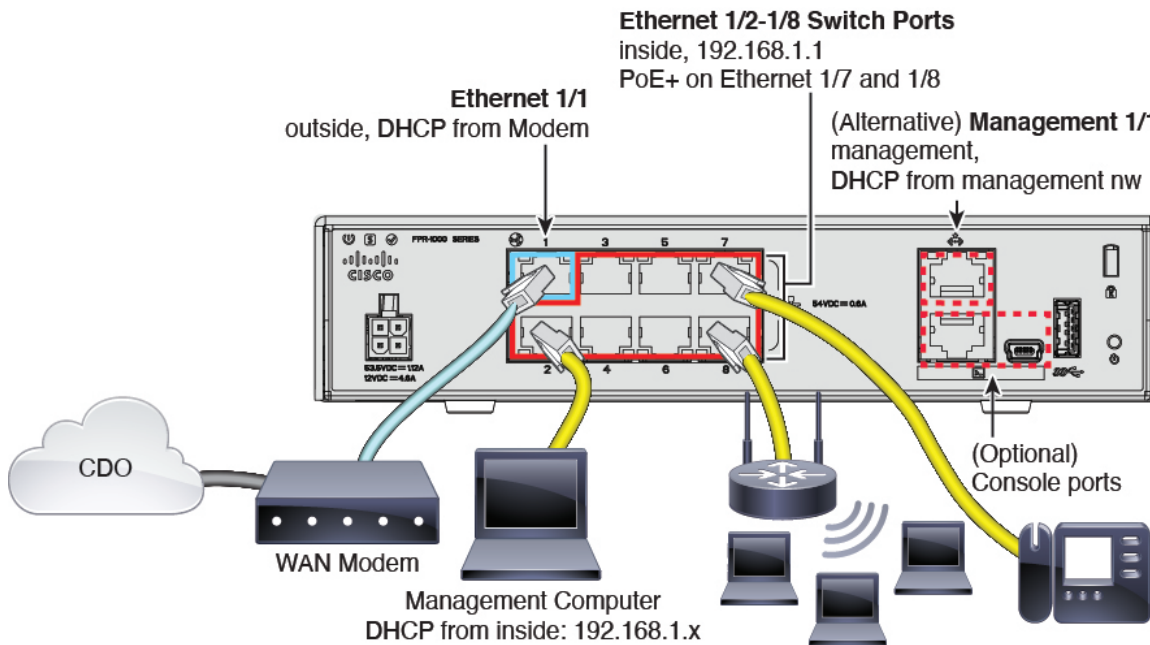
Note The Management 1/1 interface is a special interface separate from data interfaces that is used for management, Smart Licensing, and database updates. The physical interface is shared with a second logical interface, the Diagnostic interface. Diagnostic is a data interface, but is limited to other 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

Figure 10: Cabling the Firepower 1010



Note In version 6.5 and later, Ethernet1/2 through 1/8 are configured as hardware switch ports; PoE+ is also available on Ethernet1/7 and 1/8. In version 6.4, Ethernet1/2 through 1/8 are configured as bridge group members (software switch ports); PoE+ is not available. The initial cabling is the same for both versions.



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

Manage the Firepower 1010 on either Management 1/1 or Ethernet 1/2 through 1/8. The default configuration also configures Ethernet1/1 as outside.

Procedure

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

- Ethernet 1/2 through 1/8—Connect your management computer directly to one of the inside switch ports (Ethernet 1/2 through 1/8). inside 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 30](#)).
- 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 68](#).

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

By default, the IP address is obtained using IPv4 DHCP, but you can set a static address during initial configuration.

Step 3 Connect inside devices to the remaining switch ports, Ethernet 1/2 through 1/8.

Ethernet 1/7 and 1/8 are PoE+ ports.

Power On the Device

System power is controlled by the power cord; there is no power button.

Before you begin

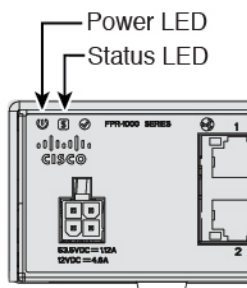
It's important that you provide reliable power for your device (using an uninterruptable power supply (UPS), for example). Loss of power without first shutting down can cause serious file system damage. There are many processes running in the background all the time, and losing power does not allow the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

Procedure

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

The power turns on automatically when you plug in the power cord.

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



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

(Optional) Change Management Network Settings at the CLI

If you cannot use the default management IP address, then you can connect to the console port and perform initial setup at the CLI, including setting the Management IP address, gateway, and other basic networking settings. You can only configure the Management interface settings; you cannot configure inside or outside interfaces, which you can later configure in 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 55](#) 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.

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

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 (Ethernet1/2 through 1/8)—**https://192.168.1.1**. You can connect to the inside address on any inside switch port (Ethernet1/2 through 1/8).
 - (6.6 and later) Management—**https://management_ip**. The Management interface is a DHCP client, so the IP address depends on your DHCP server. If you changed the Management IP address at the CLI setup, then enter that address.
 - (6.5 and earlier) Management—**https://192.168.45.45**. If you changed the Management IP address at the CLI setup, then enter that address.
- Step 2** Log in with the username **admin**, and the default password **Admin123**.
-

What to do next

- Run through the FDM setup wizard; see [Complete the Initial Configuration, on page 70](#).

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 through 1/8 are switch ports on the inside VLAN1 interface (6.5 and later) or inside bridge group members on BVI1 (6.4).
- 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 licenses. 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 [Log Into CDO, on page 37](#) 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 41](#).

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 39](#).
- If you don't have a Cisco Secure Sign-On account, continue to [Create a New Cisco Secure Sign-On Account, on page 37](#).

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.

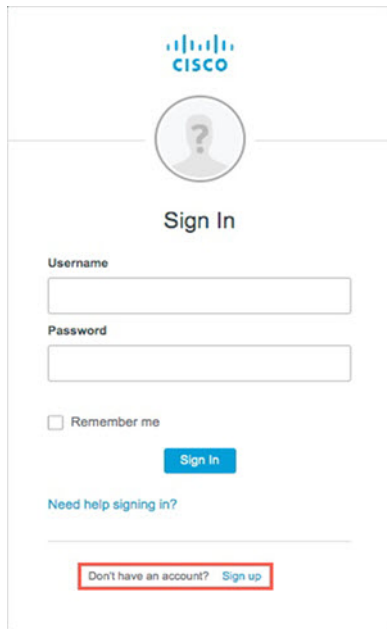
Procedure

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**.

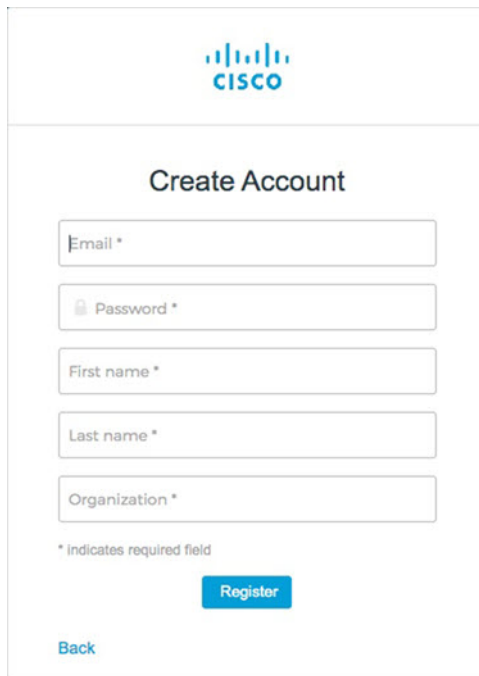
Figure 11: Cisco SSO Sign Up



The screenshot shows the Cisco Sign In interface. At the top is the Cisco logo. Below it is a placeholder for a user profile picture. The main heading is "Sign In". There are two input fields: "Username" and "Password". Below the password field is a checkbox labeled "Remember me". A blue "Sign in" button is positioned below the "Remember me" checkbox. Below the button is a link that says "Need help signing in?". At the bottom of the form, there is a link that says "Don't have an account? Sign up", which is highlighted with a red rectangular box.

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

Figure 12: Create Account



The screenshot shows the Cisco Create Account interface. At the top is the Cisco logo. Below it is the heading "Create Account". There are five input fields, each with an asterisk indicating it is required: "Email *", "Password *", "First name *", "Last name *", and "Organization *". Below the "Organization *" field is a small note: "* indicates required field". A blue "Register" button is located below the note. At the bottom left of the form is a blue "Back" link.

- 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.

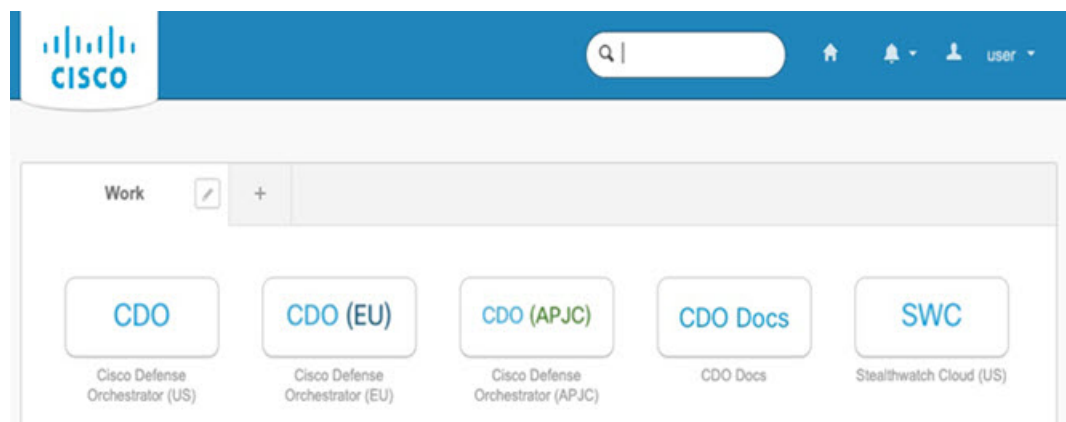
Step 4 Configure Account Recovery Options for your Cisco Secure Sign-On Account.

- 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 13: Cisco SSO Dashboard



Log Into CDO with Cisco Secure Sign-On

Log into CDO to onboard and manage your FTD.

Before you begin

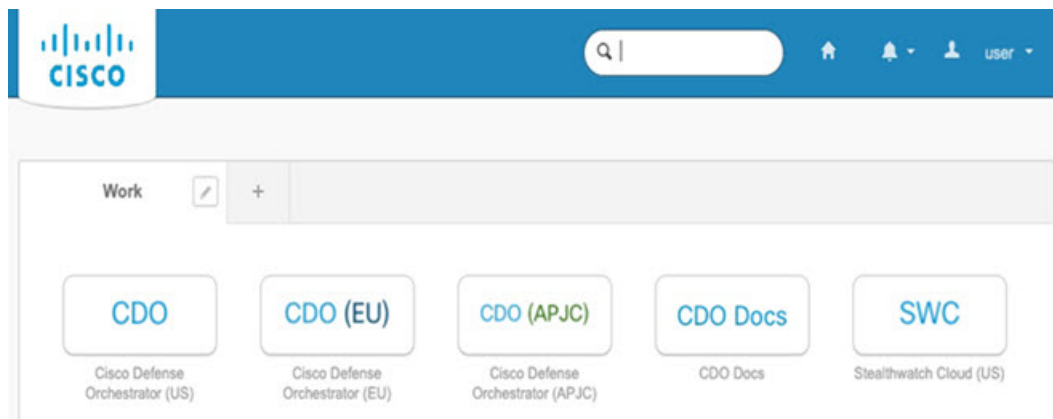
Cisco Defense Orchestrator (CDO) uses Cisco Secure Sign-On as its identity provider and Duo Security for multi-factor authentication (MFA).

- 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 37](#).
- 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 <https://www.apj.cdo.cisco.com>.

Figure 14: 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 72](#).

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 (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 54](#).
- 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 49](#). 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 41](#).



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 49](#). 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 15: Edit Interface

The screenshot shows the 'Editing Physical Interface' configuration page. At the top, there is a title bar with a close button (X). Below the title bar, there are two main sections: 'Logical Name' and 'Description'. The 'Logical Name' field contains 'dmz' and has a 'State' toggle switch to its right. The 'Description' field is empty. Below these fields, there are three tabs: 'IPv4 Address' (selected), 'IPv6 Address', and 'Advanced'. Under the 'IPv4 Address' tab, there are several fields: 'Type' (set to 'Static'), 'IP Address and Subnet Mask' (192.168.6.1 / 24), 'DHCP Address Pool' (Enter DHCP address pool), and 'Standby IP Address' (Enter IP address / 24). There are also 'Cancel' and 'Save' buttons at the bottom right of the form.

- 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 16: Security Zone Object

Adding FTD Security Zone

Object Name
dmz-zone

Description
Object description

Select Interfaces ⓘ

Search for interfaces or devices

| <input checked="" type="checkbox"/> | Name | Devices |
|-------------------------------------|------|------------------|
| <input checked="" type="checkbox"/> | dmz | ftd-650-1543-180 |

Selected Interfaces: 1 [Clear](#)

dmz

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 17: DHCP Server

Edit DHCP Server

Enable DHCP Server

Interface
inside2

Address Pool
192.168.45.46-192.168.45.254

Cancel OK

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 18: Default Route

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

- Name:** isp-gateway
- Description:** isp-gateway
- Protocol:** IPv4 (selected), IPv6
- Gateway:** isp-gateway (dropdown)
- Interface:** outside (dropdown)
- Metric:** 1 (range 1 - 255)
- Destination Networks:** any-ipv4

Buttons for 'Cancel' and 'OK' are located at the bottom right.

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.

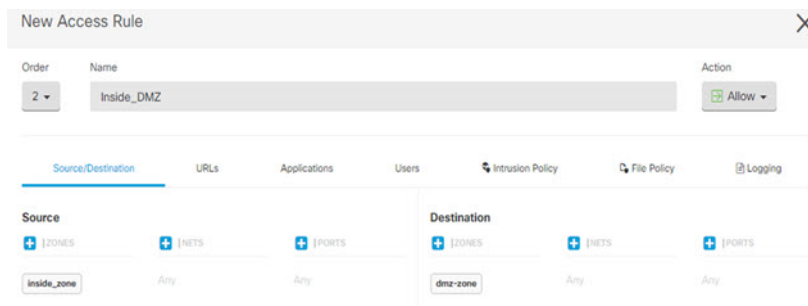
In addition, you can configure other policies to provide additional services, and fine-tune NAT and access rules to get the results that your organization requires. You can configure the following policies:

- **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 19: 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 49](#).

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.
- **Security Plus**—High Availability.

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 54](#).

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 20: 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-FPR1010T-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-FPR1010T-TMC-1Y

- L-FPR1010T-TMC-3Y

- L-FPR1010T-TMC-5Y

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

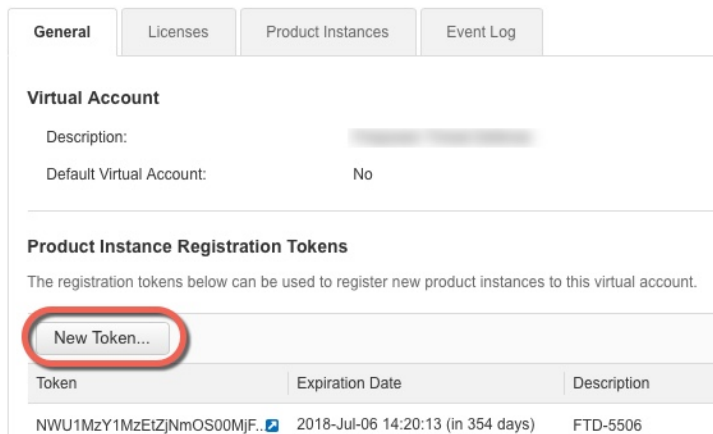
- Security Plus license: L-FPR1010-SEC-PL=. The Security Plus license enables High Availability.

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**:

Create Registration Token

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

Virtual Account: [Redacted]

Description: [Redacted]

* Expire After: 30 Days

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

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

Create Token **Cancel**

- **Description**

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

- **Allow export-controlled functionality on the products registered with this token**—Enables the export-compliance flag if you are in a country that allows for strong encryption.

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 21: View Token

| Token | Expiration Date | Description | Export-Controlled | Created By | Actions |
|-------------------------------|-----------------------------------|---------------|-------------------|------------|---------|
| MjM3ZjJhYTIzZGQ4OS00Yjk2LT... | 2017-Aug-16 19:41:53 (in 30 days) | ASA FP 2110 1 | Allowed | [Redacted] | Actions |

Figure 22: Copy Token

Token

MjM3ZjJhYTIzZGQ4OS00Yjk2LTgzMGltMTMhZTUyYjkyNmVhLTE1MDI5MTI1%0AMTMxMzh8YzdQdmgzMjA2VmFjN2dYQjJ5QWRhOEpscDU4cWI5NFNWRTUtsa2wz%0AMTdnSTn%3D%0A

Press ctrl + c to copy selected text to clipboard.

MjM3ZjJhYTIzZGQ4OS00Yjk2LT... 2017-Aug-16 19:41:53

- 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:

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

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.

Manage Licenses
ftd-650-115-1543-181
✕

✓ Connected
 Sufficient license.

Last Sync: May 26, 2020 4:24:05 PM
 Next Sync: May 26, 2020 4:34:05 PM

Refresh Licenses

✓

Base License

STATUS: ENABLED ALWAYS

This perpetual license is included with the purchase of the system. You must have this license to configure and use the device. It covers all features not covered by subscription licenses.

Includes: Base Firewall Capabilities, Application Visibility and Control

✓

Threat

STATUS: ENABLED

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

Includes: Intrusion Policy

✓

Malware

STATUS: ENABLED

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

Includes: File Policy

✓

URL License

STATUS: ENABLED

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

Includes: URL Reputation

⊘

RA VPN Only License

STATUS: DISABLED

AnyConnect VPN Only license includes basic VPN services such as device and per-application VPN (including third-party IKEv2 remote access VPN headend support), trusted network detection, basic device context collection, and Federal Information Processing Standards (FIPS) compliance.

Includes: RA-VPN

✓

RA VPN Plus License

STATUS: ENABLED

AnyConnect Plus license includes basic VPN services and also other non-VPN services such as the AnyConnect Network Access Manager 802.1X supplicant, the Cloud Web Security module, and the Cisco Umbrella Roaming module

Includes: RA-VPN

⬆

RA VPN Anex I license

Close

Save

- **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.

Cisco Firepower 1010 Getting Started Guide

53

- **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**:

Device Summary
Smart License

LICENSE ISSUE
OUT OF COMPLIANCE

Last sync: 10 Jul 2019 11:47 AM
Next sync: 10 Jul 2019 11:57 AM

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

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

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

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 41.

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 37](#).
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.

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. The Firepower 1000 ships with a USB A-to-B serial cable. Be sure to install any necessary USB serial drivers for your operating system (see the Firepower 1010 [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 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.



PART II

Firepower Threat Defense Deployment with FDM

- [Firepower Threat Defense Deployment with FDM, on page 61](#)



CHAPTER 4

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 1010 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 1010 runs an underlying operating system called the Firepower eXtensible Operating System (FXOS). The Firepower 1010 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.



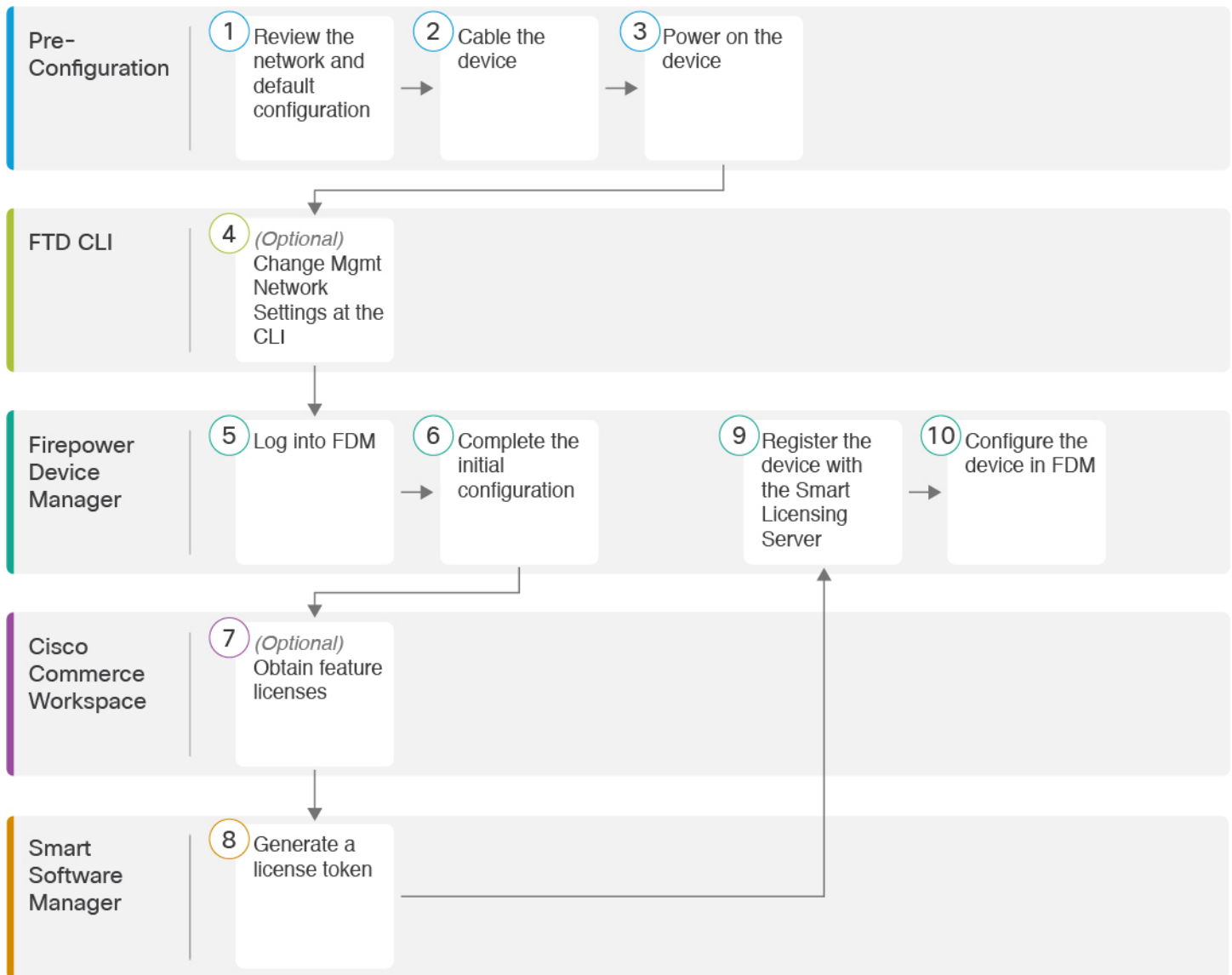
Note **Privacy Collection Statement**—The Firepower 1010 Series does not require or actively collect personally-identifiable information. However, you can use personally-identifiable information in the configuration, for example for usernames. In this case, an administrator might be able to see this information when working with the configuration or when using SNMP.

- [End-to-End Procedure, on page 62](#)
- [Review the Network Deployment and Default Configuration, on page 63](#)
- [Cable the Device, on page 66](#)
- [Power On the Device, on page 67](#)
- [\(Optional\) Change Management Network Settings at the CLI, on page 68](#)
- [Log Into FDM, on page 70](#)
- [Complete the Initial Configuration, on page 70](#)

- [Configure Licensing, on page 72](#)
- [Configure the Device in Firepower Device Manager, on page 78](#)
- [Access the FTD and FXOS CLI, on page 81](#)
- [View Hardware Information, on page 83](#)
- [Power Off the Device, on page 84](#)
- [What's Next?, on page 85](#)

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 63. |
|---|-------------------|--|

| | | |
|----|--------------------------|---|
| 2 | Pre-Configuration | Cable the Device, on page 66. |
| 3 | Pre-Configuration | Power On the Device, on page 32. |
| 4 | FTD CLI | (Optional) Change Management Network Settings at the CLI, on page 68. |
| 5 | Firepower Device Manager | Log Into FDM, on page 35. |
| 6 | Firepower Device Manager | Complete the Initial Configuration, on page 70. |
| 7 | Cisco Commerce Workspace | (Optional) Configure Licensing, on page 72: Obtain feature licenses. |
| 8 | Smart Software Manager | Configure Licensing, on page 72: Generate a license token. |
| 9 | Firepower Device Manager | Configure Licensing, on page 72: Register the device with the Smart Licensing Server. |
| 10 | Firepower Device Manager | Configure the Device in Firepower Device Manager, on page 78. |

Review the Network Deployment and Default Configuration

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

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



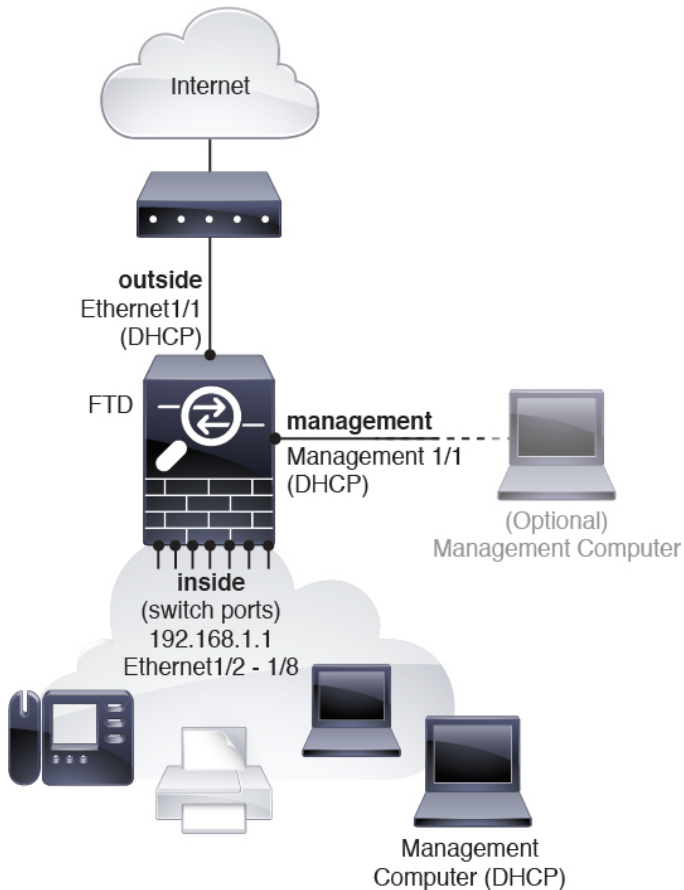
Note If you cannot use the default management IP address (for example, your management network does not include a DHCP server), then you can connect to the console port and perform initial setup at the CLI, including setting the Management IP address, gateway, and other basic networking settings.

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

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

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

Figure 23: 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**—IP address 192.168.1.1.
 - (6.5 and later) **Hardware switch**—Ethernet 1/2 through 1/8 belong to VLAN 1
 - (6.4) **Software switch** (Integrated Routing and Bridging)—Ethernet 1/2 through 1/8 belong to bridge group interface (BVI) 1
- **outside**—Ethernet 1/1, IP address from IPv4 DHCP
- **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



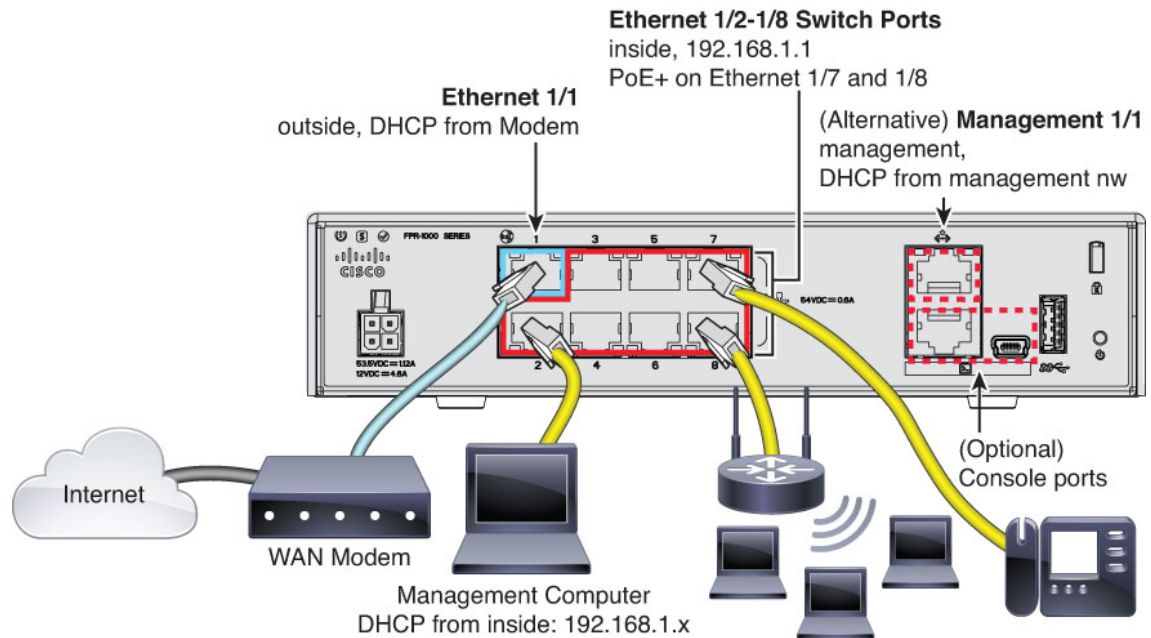
Note The Management 1/1 interface is a special interface separate from data interfaces that is used for management, Smart Licensing, and database updates. The physical interface is shared with a second logical interface, the Diagnostic interface. Diagnostic is a data interface, but is limited to other 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

Figure 24: Cabling the Firepower 1010



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



Note In version 6.5 and later, Ethernet1/2 through 1/8 are configured as hardware switch ports; PoE+ is also available on Ethernet1/7 and 1/8. In version 6.4, Ethernet1/2 through 1/8 are configured as bridge group members (software switch ports); PoE+ is not available. The initial cabling is the same for both versions.

Manage the Firepower 1010 on either Management 1/1 or Ethernet 1/2 through 1/8. The default configuration also configures Ethernet1/1 as outside.

Procedure

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

- Ethernet 1/2 through 1/8—Connect your management computer directly to one of the inside switch ports (Ethernet 1/2 through 1/8). inside 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 30).
- 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 68.

- Step 2** Connect the outside network to the Ethernet 1/1 interface.
- By default, the IP address is obtained using IPv4 DHCP, but you can set a static address during initial configuration.
- Step 3** Connect inside devices to the remaining switch ports, Ethernet 1/2 through 1/8.
- Ethernet 1/7 and 1/8 are PoE+ ports.
-

Power On the Device

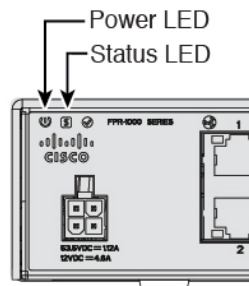
System power is controlled by the power cord; there is no power button.

Before you begin

It's important that you provide reliable power for your device (using an uninterruptible power supply (UPS), for example). 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.
- The power turns on automatically when you plug in the power cord.
- Step 2** Check the Power LED on the back or top of the device; if it is solid green, the device is powered on.



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

(Optional) Change Management Network Settings at the CLI

If you cannot use the default management IP address, then you can connect to the console port and perform initial setup at the CLI, including setting the Management IP address, gateway, and other basic networking settings. You can only configure the Management interface settings; you cannot configure inside or outside interfaces, which you can later configure in 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 81](#) 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.

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

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 (Ethernet1/2 through 1/8)—**https://192.168.1.1**. You can connect to the inside address on any inside switch port (Ethernet1/2 through 1/8).
- (6.6 and later) Management—**https://management_ip**. The Management interface is a DHCP client, so the IP address depends on your DHCP server. If you changed the Management IP address at the CLI setup, then enter that address.
- (6.5 and earlier) Management—**https://192.168.45.45**. If you changed the Management IP address at the CLI setup, then enter that address.

Step 2

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

What to do next

- Run through the FDM setup wizard; see [Complete the Initial Configuration, on page 70](#).

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 through 1/8 are switch ports on the inside VLAN1 interface (6.5 and later) or inside bridge group members on BV11 (6.4).
- 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 68](#) 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 72](#).

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 54](#).

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 72](#).
- 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 41](#).
- You can also choose to configure the device using FDM; see [Configure the Device in Firepower Device Manager, on page 78](#).

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.

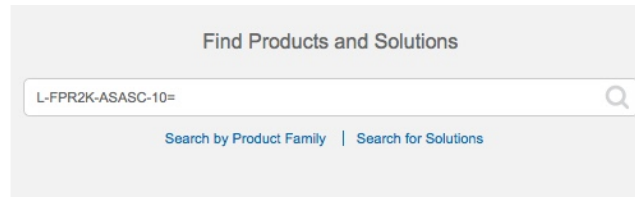
- Your Cisco Smart Software Licensing account must qualify for the Strong Encryption (3DES/AES) license to use some features (enabled using the export-compliance flag).

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 25: 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:

- L-FPR1010T-TMC=

Firepower 1100:

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:

- L-FPR1010T-TMC-1Y
- L-FPR1010T-TMC-3Y
- L-FPR1010T-TMC-5Y

Firepower 1100:

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**.

Cisco Software Central > Smart Software Licensing

Smart Software Licensing

Alerts **Inventory** License Conversion Reports Email Notification Satellites Activity

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

General Licenses Product Instances Event Log

Virtual Account

Description: [blurred]

Default Virtual Account: No

Product Instance Registration Tokens

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

New Token...

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

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

Create Registration Token

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

Virtual Account: [blurred]

Description: [text input field]

* Expire After: 30 Days

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

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

Create Token Cancel

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

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 26: View Token

General Licenses Product Instances Event Log

Virtual Account

Description: [REDACTED]

Default Virtual Account: No

Product Instance Registration Tokens

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

New Token...

| Token | Expiration Date | Description | Export-Controlled | Created By | Actions |
|-------------------------------|-----------------------------------|---------------|-------------------|------------|---------|
| MjM3ZjJhYTItZGQ4OS00Yjk2LT... | 2017-Aug-16 19:41:53 (in 30 days) | ASA FP 2110 1 | Allowed | [REDACTED] | Actions |

Figure 27: Copy Token

Token [?] [X]

MjM3ZjJhYTItZGQ4OS00Yjk2LTgzMGItMThmZTUyYjkyNmVhLTE1MDI5MTI1%0AMTMzMzh8YzdQdmgzMjA2VmFjN2dYQjI5QWRhOEdscDU4cWI5NFNWRUtsa2wz%0AMTdnST0%3D%0A

Press ctrl + c to copy selected text to clipboard.

MjM3ZjJhYTItZGQ4OS00Yjk2LT... 2017-Aug-16 19:41:53

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**.

Device Summary

Smart License

LICENSE ISSUE
EVALUATION PERIOD
You are in Evaluation mode now.

69/90 days left. REGISTER DEVICE

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

Smart License Registration
✕

- 1 Create or log in into your [Cisco Smart Software Manager](#) account.

↓
- 2 On your assigned virtual account, under “General tab”, click on “**New Token**” to create token.

↓
- 3 Copy the token and paste it here:


```
MGY2NzMwOGIiODJiZi00NzFiLWJiNjltYWwNzU0ODY2ZGVlTE1NlUz
Nzlv%0AODQ5Mzh8SUQ5Vm5XbzZiSmN5M3l6K3owZ3oyVmpmc3Vtal
JLQ2FFeGhFWmlW%0AWC9WTT0%3D%0A
```
- 4 Select Region

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

Region

SSE US Region
▼
i
- 5 Cisco Success Network

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

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

Enable Cisco Success Network

CANCEL

REGISTER DEVICE

Step 5 Click **Register Device**.

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

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

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

Device Summary

Smart License

✓

CONNECTED
SUFFICIENT LICENSE

Last sync: 10 Jul 2019 11:39 AM

Next sync: 10 Jul 2019 11:49 AM

i

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

SUBSCRIPTION LICENSES INCLUDED

Threat ENABLE

Disabled by user

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

Includes: Intrusion Policy

Malware ENABLE

Disabled by user

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

Includes: File Policy

URL License ENABLE

Disabled by user

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

Includes: URL Reputation

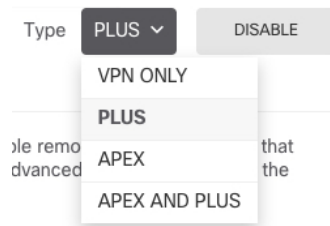
RA VPN License Type: PLUS ▾ ENABLE

Disabled by user

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

Includes: RA-VPN

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



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

Device Summary

Smart License

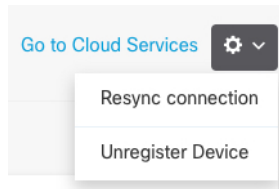
LICENSE ISSUE Last sync: 10 Jul 2019 11:47 AM

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

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

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

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



Configure the 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 want to convert a bridge group interface (6.4) or want to convert a switch port to a firewall interface (6.5 and later), 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 28: Edit Interface

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

- Interface Name:** A text input field containing "dmz".
- Status:** A toggle switch that is currently turned on (blue).
- Description:** A large, empty text area.
- IPv4 Address:** A tab that is selected and underlined.
- IPv6 Address:** A tab that is not selected.
- Advanced Options:** A tab that is not selected.
- Type:** A dropdown menu with "Static" selected.
- IP Address and Subnet Mask:** Two input fields. The first contains "192.168.6.1" and the second contains "24".

 At the bottom, there is a small note: "e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0".

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

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

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

Figure 29: 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 30: 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 31: Default Route

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

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

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

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

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

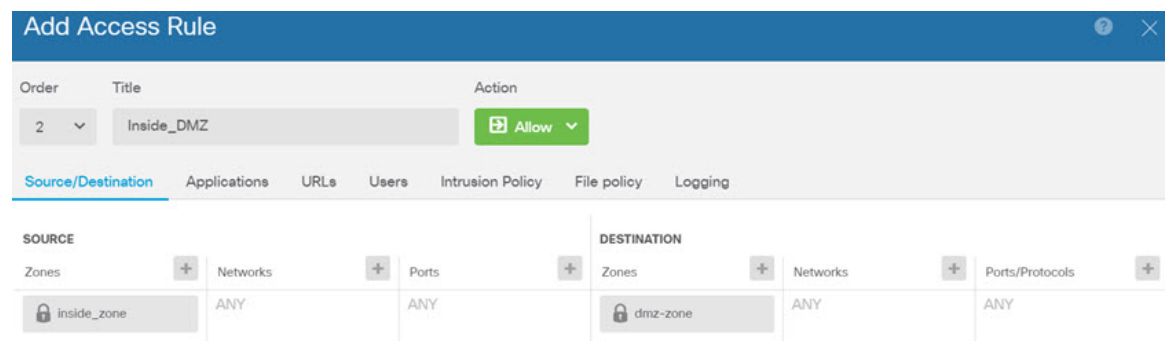
In addition, you can configure other policies to provide additional services, and fine-tune NAT and access rules to get the results that your organization requires. You can configure the following policies:

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

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


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

Figure 32: 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 41](#).

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. The Firepower 1000 ships with a USB A-to-B serial cable. Be sure to install any necessary USB serial drivers for your operating system (see the Firepower 1010 [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#
```

View Hardware Information

Use the command-line interface (CLI) to view information about your hardware, including the device model, hardware version, serial number, and chassis components including power supplies and network modules. You can access the CLI by connecting to the console port; see [Access the FTD and FXOS CLI, on page 81](#).

Procedure

Step 1 To display the hardware model of the device, use the **show model** command.

```
> show model
```

Example:

```
> show model
Cisco Firepower 1010 Threat Defense
```

Step 2 To display the chassis serial number, use the **show serial-number** command.

```
> show serial-number
```

Example:

```
> show serial-number
JMX1943408S
```

This information is also shown in **show version system**, **show running-config**, and **show inventory** output.

Step 3 To display information about all of the Cisco products installed in the networking device that are assigned a product identifier (PID), version identifier (VID), and serial number (SN), use the **show inventory** command.

```
> show inventory
```

a) From the FTD CLI:

Example:

```
> show inventory
Name: "module 0", DESCR: "Firepower 1010 Appliance, Desktop, 8 GE, 1 MGMT"
PID: FPR-1010          , VID: V00          , SN: JMX1943408S
```

b) From the FXOS CLI:

Example:

```
firepower /chassis # show inventory
Chassis  PID          Vendor          Serial (SN) HW Revision
```

```
1 FPR-1010 Cisco Systems, In JMX1943408S 0.3
```

Power Off the Device

It's important that you shut down your system properly. Simply unplugging the power 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.

The Firepower 1010 chassis does not have an external power switch. 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 81](#).

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 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](#).



PART **III**

Firepower Threat Defense Deployment with FMC

- [Firepower Threat Defense Deployment with FMC](#), on page 89



CHAPTER 5

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 1010 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 1010 runs an underlying operating system called the Firepower eXtensible Operating System (FXOS). The Firepower 1010 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 1010 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.

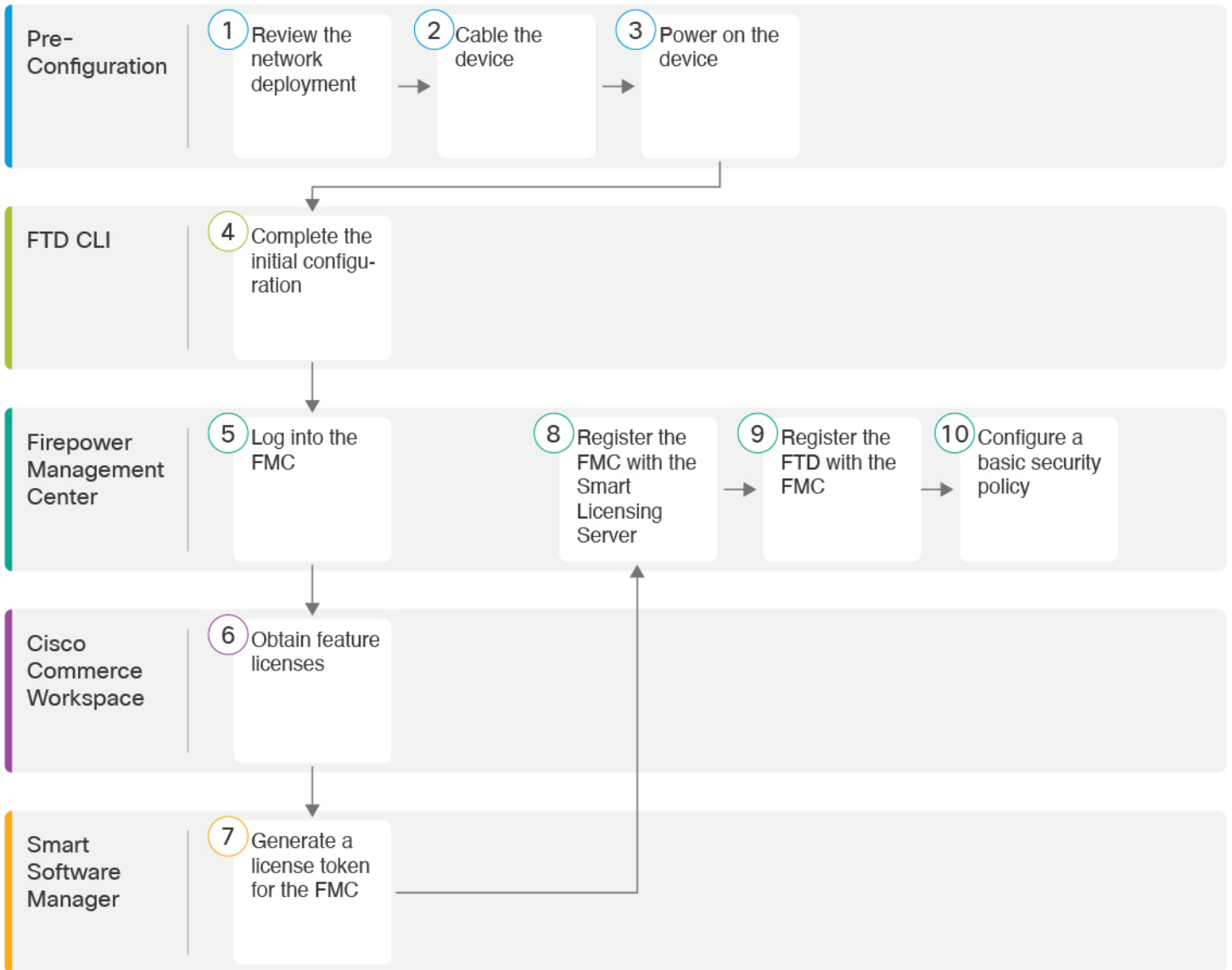
- [Before You Start](#), on page 90
- [End-to-End Procedure](#), on page 90
- [Review the Network Deployment](#), on page 92
- [Cable the Device \(6.7 and Later\)](#), on page 97
- [Cable the Device \(6.5 and 6.6\)](#), on page 99
- [Cable the Device \(6.4\)](#), on page 101
- [Power On the Device](#), on page 102
- [Complete the FTD Initial Configuration](#), on page 102
- [Log Into the Firepower Management Center](#), on page 108
- [Obtain Licenses for the Firepower Management Center](#), on page 108
- [Register the FTD with the FMC](#), on page 110
- [Configure a Basic Security Policy](#), on page 112
- [Access the FTD and FXOS CLI](#), on page 128
- [Power Off the Device](#), on page 130
- [What's Next?](#), on page 131

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 92. |
| ② | Pre-Configuration | Cable the Device (6.7 and Later), on page 97 Cable the Device (6.5 and 6.6), on page 99 Cable the Device (6.4), on page 101. |
| ③ | Pre-Configuration | Power On the Device, on page 32. |
| ④ | FTD CLI | Complete the FTD Initial Configuration, on page 102. |

| | | |
|----|-----------------------------|---|
| 5 | Firepower Management Center | Log Into the Firepower Management Center, on page 108. |
| 6 | Cisco Commerce Workspace | Obtain Licenses for the Firepower Management Center, on page 108: Buy feature licenses. |
| 7 | Smart Software Manager | Obtain Licenses for the Firepower Management Center, on page 108: Generate a license token for the FMC. |
| 8 | Firepower Management Center | Obtain Licenses for the Firepower Management Center, on page 108: Register the FMC with the Smart Licensing server. |
| 9 | Firepower Management Center | Register the FTD with the FMC, on page 110 |
| 10 | Firepower Management Center | Configure a Basic Security Policy, on page 112 |

Review the Network Deployment

6.7 and Later Deployment

You can manage the FTD using FMC from either a data interface or from the Management 1/1 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.

This guide shows you how to manage the FTD using the inside interface or the outside interface, which you can configure during initial setup at the console port. You can configure other data interfaces after you connect the FTD to the FMC. Note that Ethernet1/2 through 1/8 are enabled as switch ports by default.



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

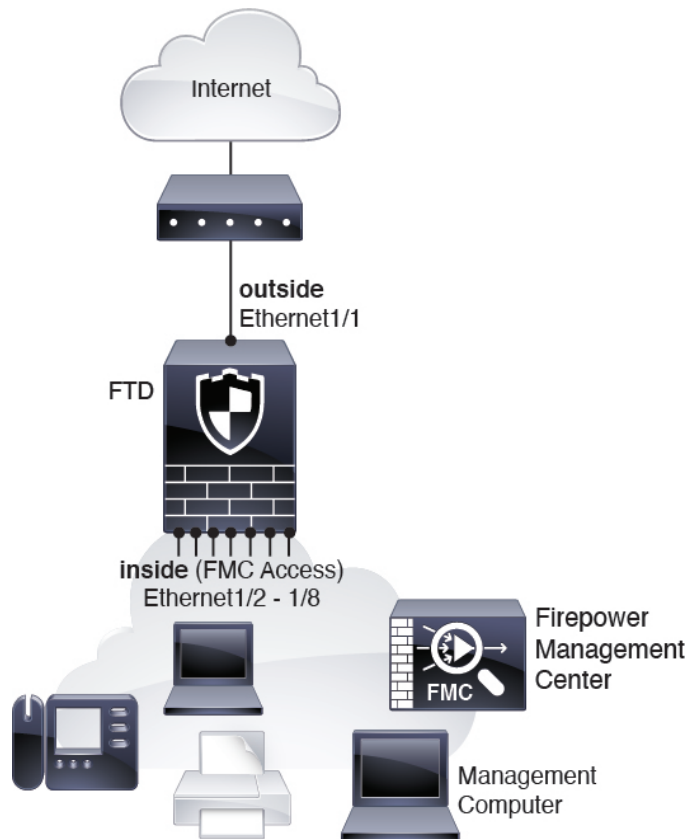
- You can only enable FMC access on one physical, data interface. You cannot use a subinterface or EtherChannel.
- This interface cannot be management-only.
- Routed firewall mode only, using a routed interface.
- High Availability is not supported. You must use the Management interface in this case.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

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

Inside Management Deployment

The following figure shows the recommended network deployment for the Firepower 1010 using the inside interface for management.

Figure 33: Suggested Inside Management Deployment



Remote Management Deployment

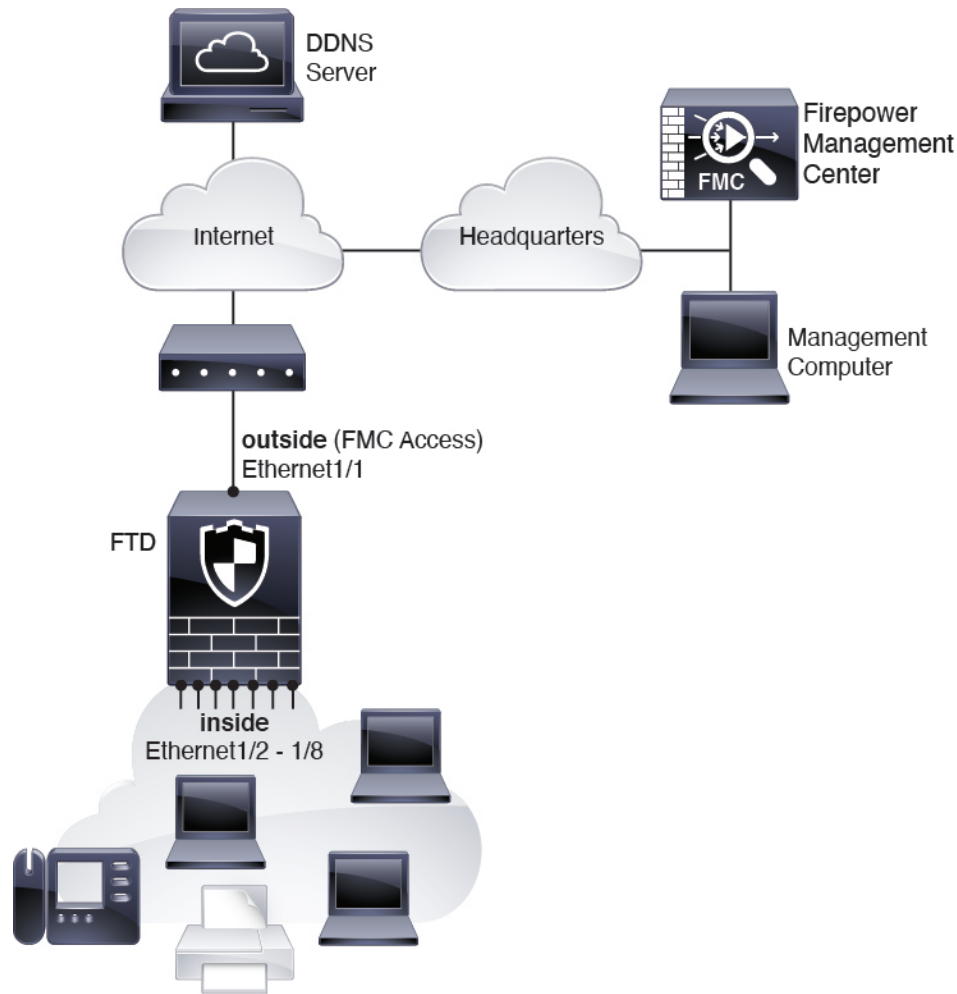


Note For a remote branch setup, we recommend that you use the [standalone document](#) specific to that deployment.

The following figure shows the recommended network deployment for the Firepower 1010 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 34: Suggested Remote Management Deployment



6.5 and 6.6 Deployment

The dedicated Management 1/1 interface is a special interface with its own network settings. By default, the Management 1/1 interface is enabled and configured as a DHCP client. If your network does not include a DHCP server, you can set the Management interface to use a static IP address during initial setup at the console port. You can configure other interfaces after you connect the FTD to FMC. Note that Ethernet1/2 through 1/8 are enabled as switch ports by default.



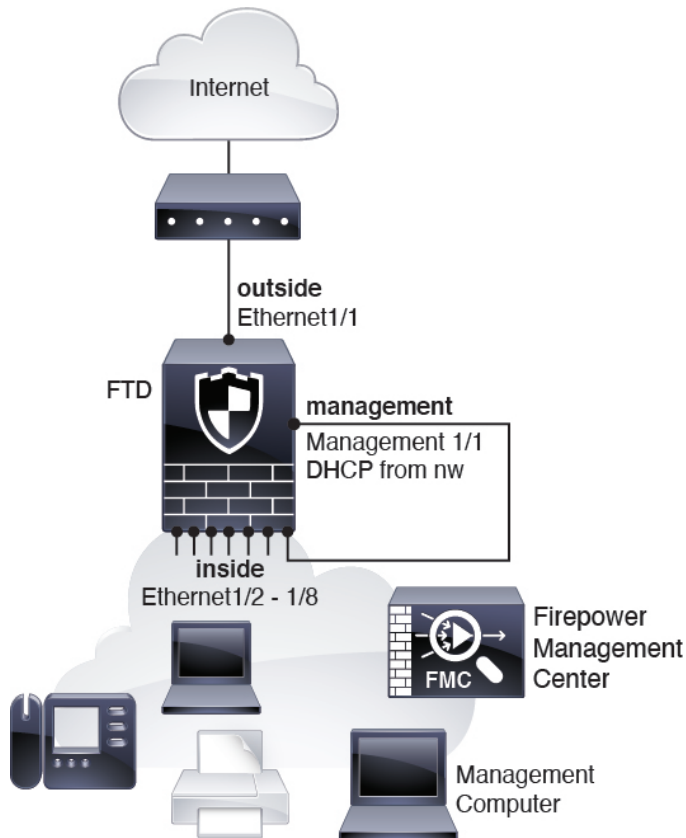
Note In 6.5 and earlier, the Management interface is configured with an IP address (192.168.45.45).

The following figure shows the recommended network deployment for the Firepower 1010. You can also use this scenario in 6.7 and later for a High Availability deployment, for example.

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

In the following diagram, the Firepower 1010 acts as the internet gateway for the Management interface and the FMC by connecting Management 1/1 directly to an inside switch port, and by connecting the FMC and management computer to other inside switch ports. (This direct connection is allowed because the Management interface is separate from the other interfaces on the FTD.)

Figure 35: Suggested Network Deployment



6.4 Deployment

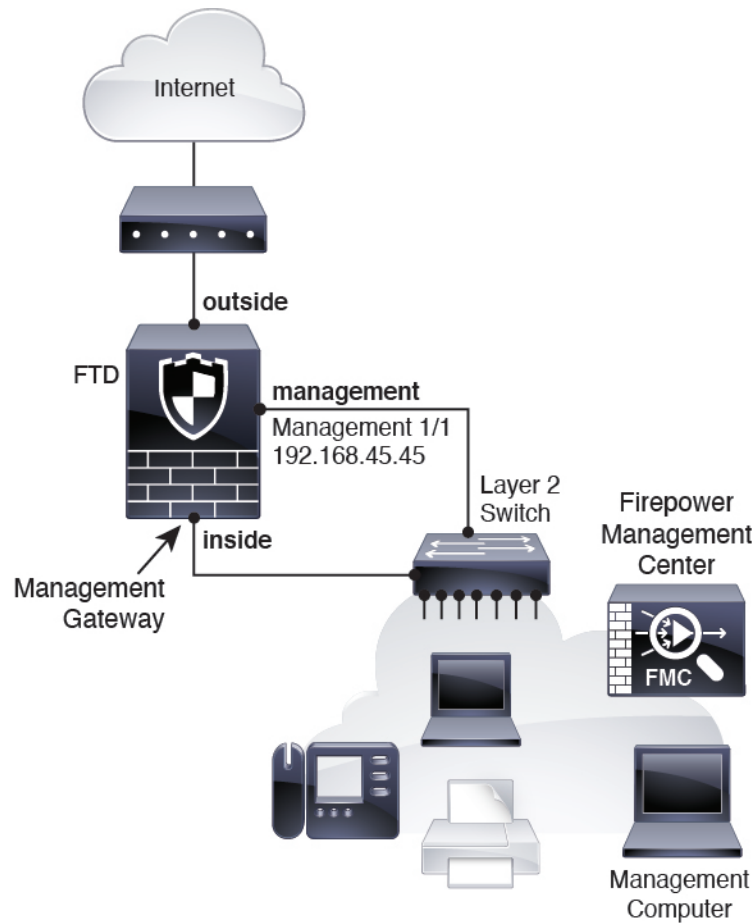
The dedicated Management 1/1 interface is a special interface with its own network settings. By default, only the Management 1/1 interface is enabled and configured with an IP address (192.168.45.45). This interface also runs a DHCP server initially; after you select FMC as the manager during initial setup, the DHCP server is disabled. You can configure other interfaces after you connect the FTD to FMC.

The following figure shows the recommended network deployment for the Firepower 1010.

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

In the following diagram, the Firepower 1010 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 36: Suggested Network Deployment



Cable the Device (6.7 and Later)

To cable one of the recommended scenarios on the Firepower 1010, see the following steps.

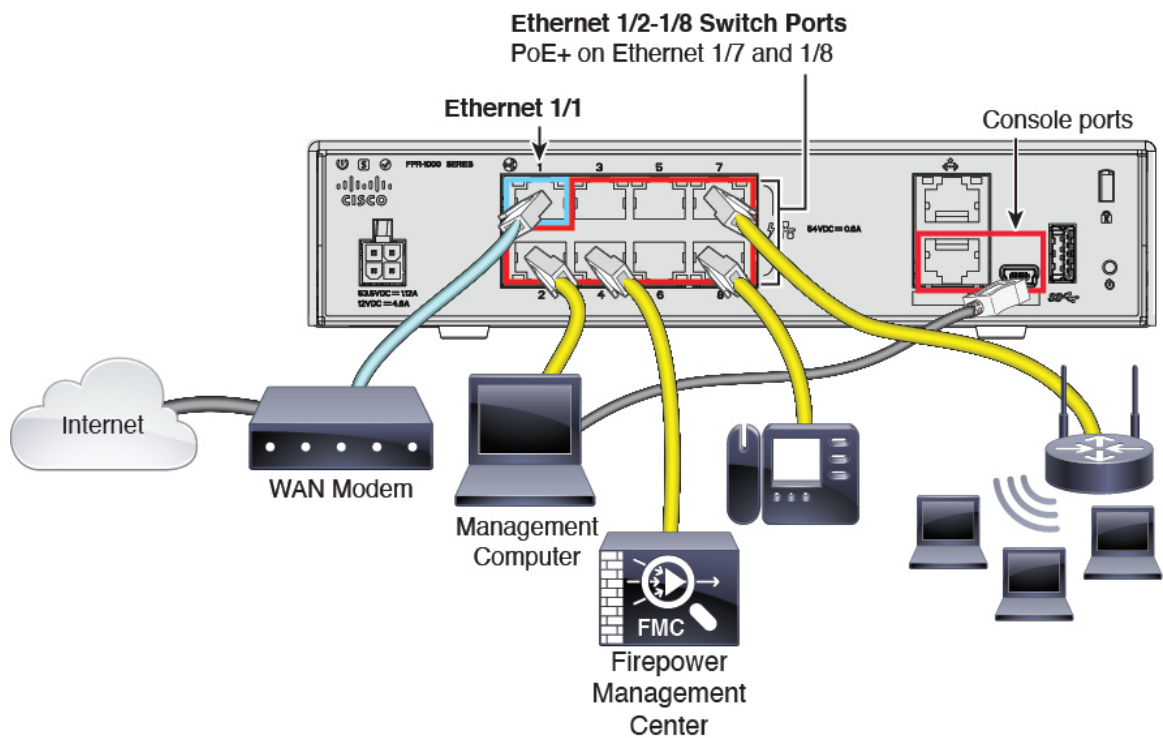


Note Other topologies can be used, and your deployment will vary depending on your requirements. For example, you can convert the switch ports to firewall interfaces.

Procedure

Step 1 Cable for FMC access on the inside network.

Figure 37: Cabling the Firepower 1010 for Inside FMC Access

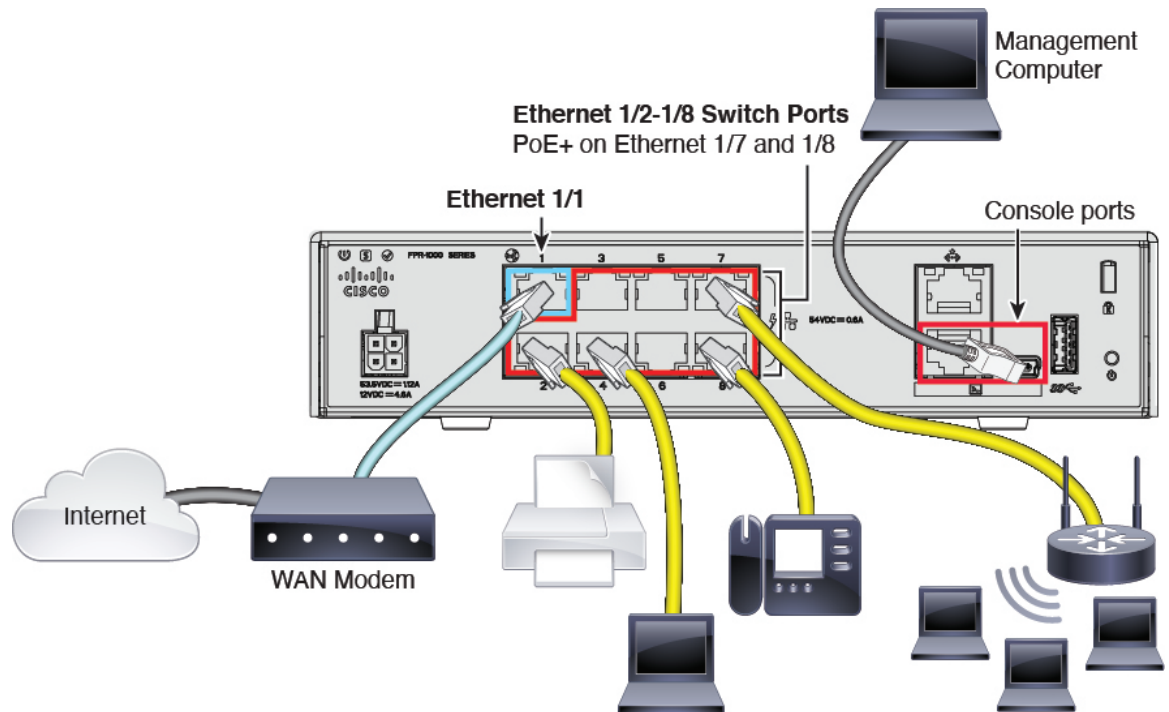


The FMC and your management computer reside on the inside network with your other inside end points.

- Connect the management computer to the console port. You need to use the console port to access the CLI for initial setup.
- Cable the following to the switch ports, Ethernet1/2 through 1/8:
 - Firepower Management Center
 - Management computer
 - Additional end points
- Connect Ethernet 1/1 to your outside router.

Step 2 Cable for FMC access on the outside network.

Figure 38: Cabling the Firepower 1010 for Outside FMC Access



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 end points to the switch ports, Ethernet1/2 through 1/8.
- c) Connect Ethernet 1/1 to your outside router.

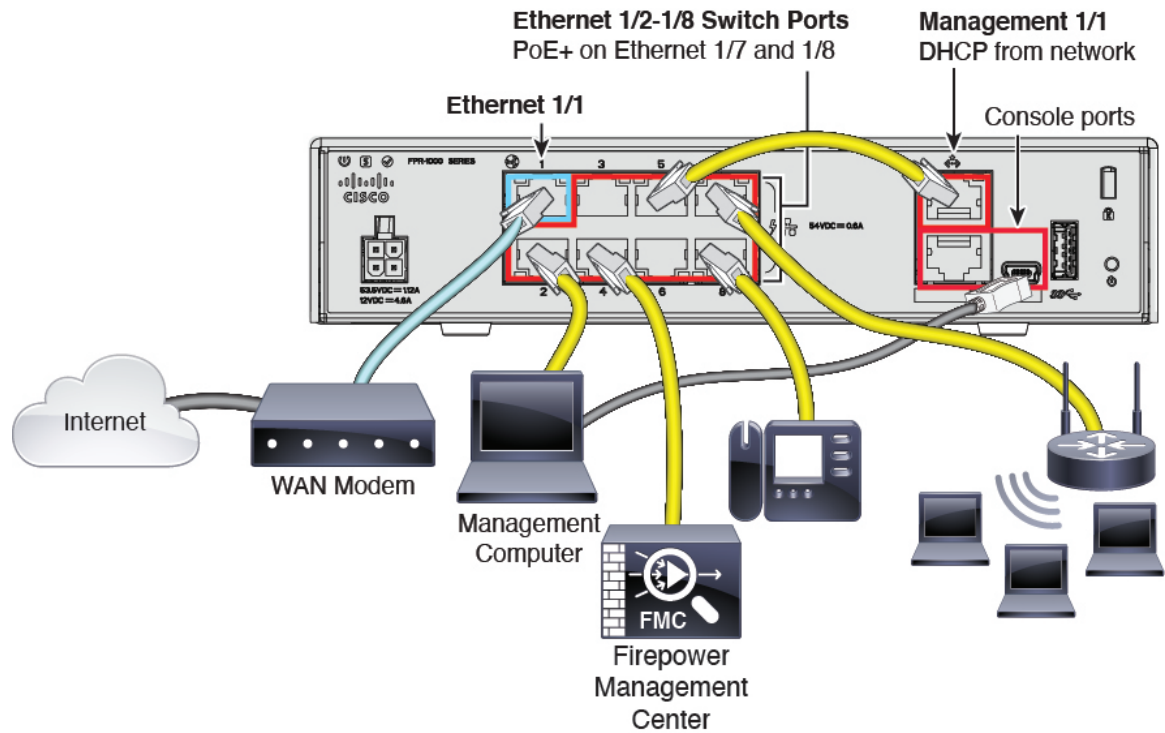
Cable the Device (6.5 and 6.6)

To cable the recommended scenario on the Firepower 1010, see the following illustration, which shows a sample topology using Ethernet1/1 as the outside interface and the remaining interfaces as switch ports on the inside network.



Note Other topologies can be used, and your deployment will vary depending on your requirements. For example, you can convert the switch ports to firewall interfaces.

Figure 39: Cabling the Firepower 1010



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

Procedure

- Step 1** Connect Management1/1 directly to one of the switch ports, Ethernet1/2 through 1/8.
- Step 2** Cable the following to the switch ports, Ethernet1/2 through 1/8:
- Firepower Management Center
 - Management computer
 - Additional end points
- Step 3** 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.
- Step 4** Connect Ethernet 1/1 to your outside router.

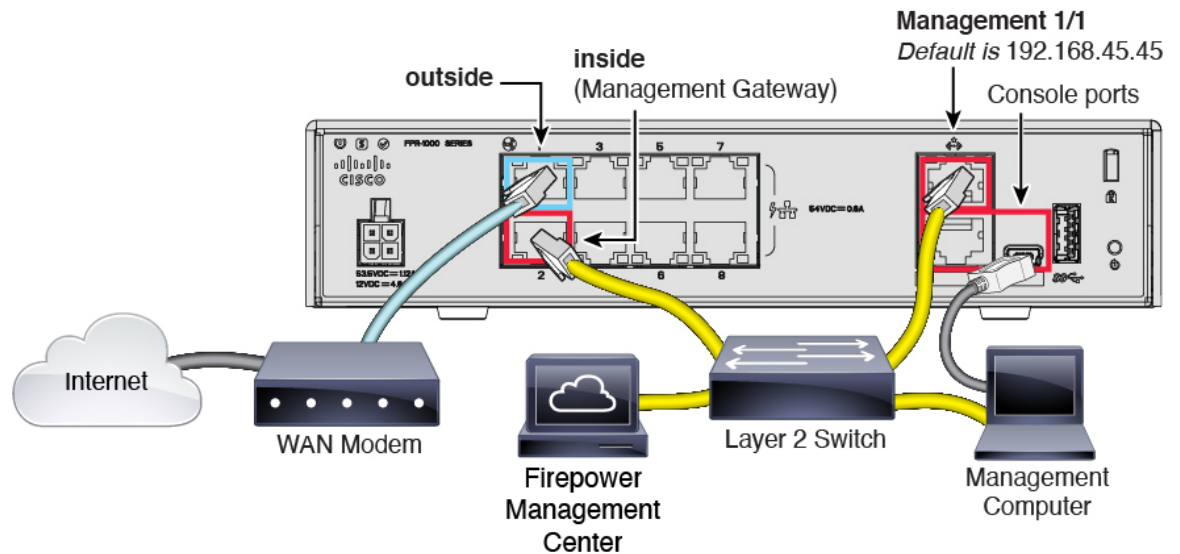
Cable the Device (6.4)

To cable the recommended scenario on the Firepower 1010, see the following illustration, which shows a sample topology using a Layer 2 switch.



Note Other topologies can be used, and your deployment will vary depending on your requirements.

Figure 40: Cabling the Firepower 1010



Procedure

Step 1 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

Note The Firepower 1010 and the FMC both have the same default management IP address: 192.168.45.45. This guide assumes that you will set different IP addresses for your devices during initial setup. Note that the FMC on 6.5 and later defaults to a DHCP client for the management interface; however, if there is no DHCP server, it will default to 192.168.45.45.

Step 2 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.

Step 3 Connect the outside interface (for example, Ethernet 1/1) to your outside router.

- Step 4** Connect other networks to the remaining interfaces.
-

Power On the Device

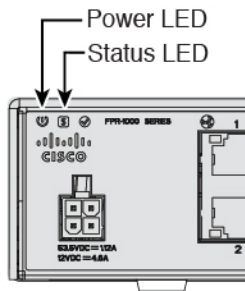
System power is controlled by the power cord; there is no power button.

Before you begin

It's important that you provide reliable power for your device (using an uninterruptable power supply (UPS), for example). 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.
The power turns on automatically when you plug in the power cord.
- Step 2** Check the Power LED on the back or top of the device; if it is solid green, the device is powered on.



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

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.

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

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 alphanumeric characters (A–Z, a–z, 0–9) and the hyphen (-).
- *nat_id*—Specifies a unique, one-time string of your choice that you will also specify on the FMC when you register the FTD when one side does not specify a reachable IP address or hostname. It is required if you set the FMC to **DONTRESOLVE**. The NAT ID must not exceed 37 characters. Valid characters include alphanumeric characters (A–Z, a–z, 0–9) and the hyphen (-). This ID cannot be used for any other devices registering to the FMC.

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

Example:

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

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

Example:

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

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

Example:

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

Step 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 physical, data interface. You cannot use a subinterface or EtherChannel.
 - This interface cannot be management-only.
 - Routed firewall mode only, using a routed interface.
 - High Availability is not supported. You must use the Management interface in this case.
 - PPPoE is not supported. If your ISP requires PPPoE, you will have to put a router with PPPoE support between the FTD and the WAN modem.
 - The interface must be in the global VRF only.
 - You cannot use separate management and event-only interfaces.
 - SSH is not enabled by default for data interfaces, so you will have to enable SSH later using FMC. Because the Management interface gateway will be changed to be the data interfaces, you also cannot SSH to the Management interface from a remote network unless you add a static route for the Management interface using the **configure network static-routes** command.
- When you add the FTD to the FMC, the FMC discovers and maintains the interface configuration, including the following settings: interface name and IP address, static route to the gateway, DNS servers, and DDNS server. For more information about the DNS server configuration, see below. In FMC, you can later make changes to the FMC access interface configuration, but make sure you don't make changes that can prevent the FTD or FMC from re-establishing the management connection. If the management connection is disrupted, the FTD includes the **configure policy rollback** command to restore the previous deployment.
- If you configure a DDNS server update URL, the FTD automatically adds certificates for all of the major CAs from the Cisco Trusted Root CA bundle so that the FTD can validate the DDNS server certificate

for the HTTPS connection. The FTD supports any DDNS server that uses the DynDNS Remote API specification (<https://help.dyn.com/remote-access-api/>).

- This command sets the *data* interface DNS server. The Management DNS server that you set with the setup script (or using the **configure network dns servers** command) is used for management traffic. The data DNS server is used for DDNS (if configured) or for security policies applied to this interface.

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

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

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

Example:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]:
IP address (manual / dhcp) [dhcp]:
DDNS server update URL [none]:
https://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).

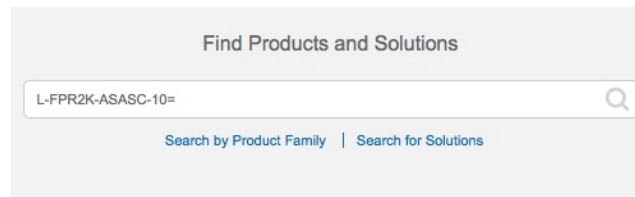
Procedure

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 41: 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:

- L-FPR1010T-TMC=

Firepower 1100:

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:

- L-FPR1010T-TMC-1Y
- L-FPR1010T-TMC-3Y
- L-FPR1010T-TMC-5Y

Firepower 1100:

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.

Add Device ?

Host:†

Display Name:

Registration Key:†

Group:

Access Control Policy:†

Smart Licensing

Malware

Threat

URL Filtering

Advanced

Unique NAT ID:†

Transfer Packets

- **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 125](#).

The screenshot shows a 'New Policy' configuration window. The 'Name' field is filled with 'ftd_ac_policy'. The 'Default Action' section has three radio buttons: 'Block all traffic' (selected and circled in red), 'Intrusion Prevention', and 'Network Discovery'. The 'Save' and 'Cancel' buttons are at the bottom right.

- **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 | (Firepower 1010) Configure Interfaces, on page 113 (All Other Models) Configure Interfaces, on page 117. |
| 2 | Configure the DHCP Server, on page 120. |
| 3 | Add the Default Route, on page 121. |
| 4 | Configure NAT, on page 123. |
| 5 | Allow Traffic from Inside to Outside, on page 125. |
| 6 | Deploy the Configuration, on page 128. |

(Firepower 1010) Configure Interfaces

Add the VLAN1 interface for the switch ports or convert switch ports to firewall interfaces, assign interfaces 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. By default, Ethernet1/1 is a regular firewall interface that you can use for outside, and the remaining interfaces are switch ports on VLAN 1; after you add the VLAN1 interface, you can make it your inside interface. You can alternatively assign switch ports to other VLANs, or convert switch ports to firewall interfaces.

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 (VLAN1) with a static address and a routed mode outside interface using DHCP (Ethernet1/1).

Procedure

-
- Step 1** Choose **Devices > Device Management**, and click the **Edit** (✎) for the device.
- Step 2** Click **Interfaces**.

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

Step 3 (Optional) Disable switch port mode for any of the switch ports (Ethernet1/2 through 1/8) by clicking the slider in the **SwitchPort** column so it shows as disabled ().

Step 4 Enable the switch ports.

a) Click the **Edit** () for the switch port.

Edit Physical Interface

General | Hardware Configuration

Interface ID: Enabled

Description:

Port Mode: ▼

VLAN ID: (1 - 4070)

Protected:

OK Cancel

b) Enable the interface by checking the **Enabled** check box.

c) (Optional) Change the VLAN ID; the default is 1. You will next add a VLAN interface to match this ID.

d) Click **OK**.

Step 5 Add the *inside* VLAN interface.

a) Click **Add Interfaces > VLAN Interface**.

The **General** tab appears.

- b) Enter a **Name** up to 48 characters in length.
For example, name the interface **inside**.
- c) Check the **Enabled** check box.
- d) Leave the **Mode** set to **None**.
- e) 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.

- f) Set the **VLAN ID** to **1**.

By default, all of the switchports are set to VLAN 1; if you choose a different VLAN ID here, you need to also edit each switchport to be on the new VLAN ID.

You cannot change the VLAN ID after you save the interface; the VLAN ID is both the VLAN tag used, and the interface ID in your configuration.

- g) 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**

Edit Physical Interface

General **IPv4** IPv6 Advanced Hardware Configuration

IP Type: Use Static IP

IP Address: 192.168.1.1/24 eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25

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

h) Click **OK**.

Step 6 Click the **Edit** (✎) for Ethernet1/1 that you want to use for *outside*.

The **General** tab appears.

Edit Physical Interface ? X

General **IPv4** IPv6 Advanced Hardware Configuration

Name: outside Enabled Management Only

Description:

Mode: None

Security Zone: outside_zone

Interface ID: GigabitEthernet0/0

MTU: 1500 (64 - 9000)

OK Cancel

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.

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

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

- e) Click the **IPv4** and/or **IPv6** tab.
- **IPv4**—Choose **Use DHCP**, and configure the following optional parameters:
 - **Obtain default route using DHCP**—Obtains the default route from the DHCP server.
 - **DHCP route metric**—Assigns an administrative distance to the learned route, between 1 and 255. The default administrative distance for the learned routes is 1.

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

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

- f) Click **OK**.

Step 7 Click **Save**.

(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**.

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

- Step 3** Click the **Edit** (✎) for the interface that you want to use for *inside*.
The **General** tab appears.

Edit Physical Interface

General | IPv4 | IPv6 | Advanced | Hardware Configuration

Name: Enabled Management Only

Description:

Mode: ▼

Security Zone: ▼

Interface ID:

MTU: (64 - 9000)

OK Cancel

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

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

policies only support security zones; you can use zones or interface groups in NAT policies, prefilter policies, and QoS policies.

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

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

For example, enter **192.168.1.1/24**

Edit Physical Interface

General **IPv4** IPv6 Advanced Hardware Configuration

IP Type: Use Static IP

IP Address: 192.168.1.1/24 eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25

- **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.

Edit Physical Interface ? x

General **IPv4** IPv6 Advanced Hardware Configuration

Name: outside Enabled Management Only

Description:

Mode: None

Security Zone: outside_zone

Interface ID: GigabitEthernet0/0

MTU: 1500 (64 - 9000)

OK Cancel

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

- a) Enter a **Name** up to 48 characters in length.
For example, name the interface **outside**.
- b) Check the **Enabled** check box.
- c) Leave the **Mode** set to **None**.
- d) From the **Security Zone** drop-down list, choose an existing outside security zone or add a new one by clicking **New**.
For example, add a zone called **outside_zone**.
- e) Click the **IPv4** and/or **IPv6** tab.

- **IPv4**—Choose **Use DHCP**, and configure the following optional parameters:
 - **Obtain default route using DHCP**—Obtains the default route from the DHCP server.
 - **DHCP route metric**—Assigns an administrative distance to the learned route, between 1 and 255. The default administrative distance for the learned routes is 1.

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

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

- f) Click **OK**.

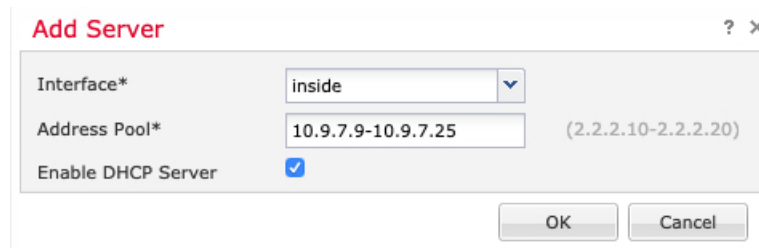
Step 5 Click **Save**.

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:



Add Server ? ×

Interface*

Address Pool* (2.2.2.10-2.2.2.20)

Enable DHCP Server

OK Cancel

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

Step 4 Click **OK**.

Step 5 Click **Save**.

Add the Default Route

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

Procedure

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

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

Add the Default Route

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

Step 3 Click **OK**.

The route is added to the static route table.

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

Step 4 Click **Save**.

Configure NAT

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

Procedure

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

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

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

Step 3 Click **Add Rule**.

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

Step 4 Configure the basic rule options:

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

- **Type**—Choose **Dynamic**.

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

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

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

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

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

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

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

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

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

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

Allow Traffic from Inside to Outside

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

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

Procedure

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

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

The screenshot shows the 'Add Rule' configuration page. The rule name is 'inside_to_outside', it is enabled, and the action is 'Allow'. The rule is set to be inserted 'into Mandatory'. The 'Zones' tab is selected, showing the following configuration:

| Available Zones | Source Zones (1) | Destination Zones (1) |
|-----------------------------|------------------|-----------------------|
| inside_zone outside_zone | inside_zone | outside_zone |

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

Leave the other settings as is.

Step 3 Click Add.

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

The screenshot shows the FMC interface with the 'Policies' tab selected. The rule 'ftd_ac_policy' is being configured. The 'Rules' table below shows the following entries:

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

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 interface; however, this screen does not affect Management SSH access.

The Management 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**.

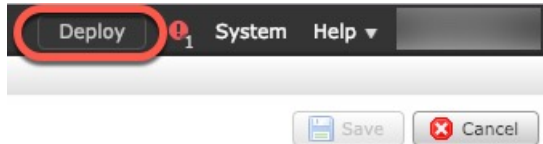
You can now go to **Deploy > Deployment** and deploy the policy to assigned devices. The changes are not active until you deploy them.

Deploy the Configuration

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

Procedure

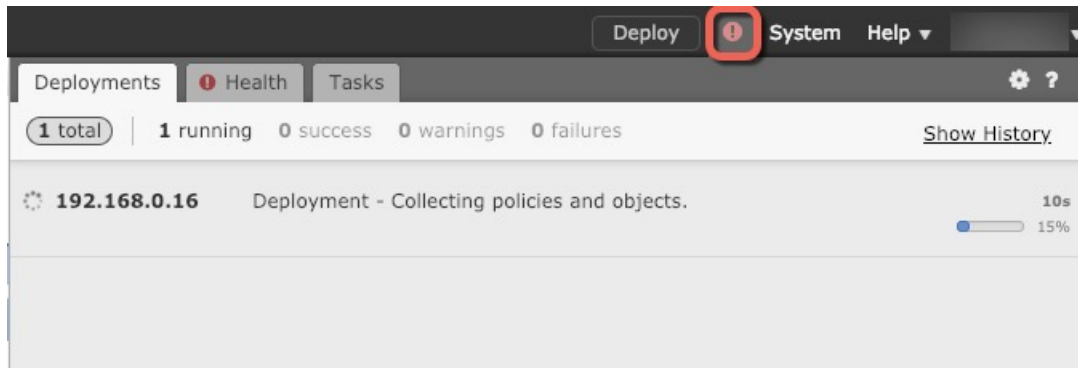
Step 1 Click **Deploy** in the upper right.



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. The Firepower 1000 ships with a USB A-to-B serial cable. Be sure to install any necessary USB serial drivers for your operating system (see the Firepower 1010 [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 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.

The Firepower 1010 chassis does not have an external power switch. 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 128](#).

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 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](#).



PART **IV**

ASA Deployment with ASDM

- [ASA Deployment with ASDM, on page 135](#)



CHAPTER 6

ASA Deployment with ASDM

Is This Chapter for You?

This chapter describes how to set up the Firepower 1010 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 1010 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 1010 runs an underlying operating system called the Firepower eXtensible Operating System (FXOS). The Firepower 1010 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 1010 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, on page 136](#)
- [End-to-End Procedure, on page 138](#)
- [Review the Network Deployment and Default Configuration, on page 140](#)
- [Cable the Device, on page 143](#)
- [Power On the Device, on page 144](#)
- [\(Optional\) Change the IP Address, on page 145](#)
- [Log Into ASDM, on page 146](#)

- [Configure Licensing, on page 147](#)
- [Configure the ASA, on page 151](#)
- [Access the ASA and FXOS CLI, on page 153](#)
- [What's Next?, on page 154](#)

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

General ASA Unsupported Features

The following ASA features are not supported on the Firepower 1010:

- Multiple context mode
- Active/Active failover
- 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

VLAN Interface and Switch Port Unsupported Features

VLAN interfaces and switch ports do not support:

- Dynamic routing
- Multicast routing
- Policy based routing

- Equal-Cost Multi-Path routing (ECMP)
- Inline sets or Passive interfaces
- VXLAN
- EtherChannels
- Redundant Interfaces; the Firepower 1010 does not support redundant interfaces for any interface type.
- Failover and state link
- Traffic zones
- Security group tagging (SGT)

Migrating an ASA 5500-X Configuration

You can copy and paste an ASA 5500-X configuration into the Firepower 1010. 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 1010, 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.

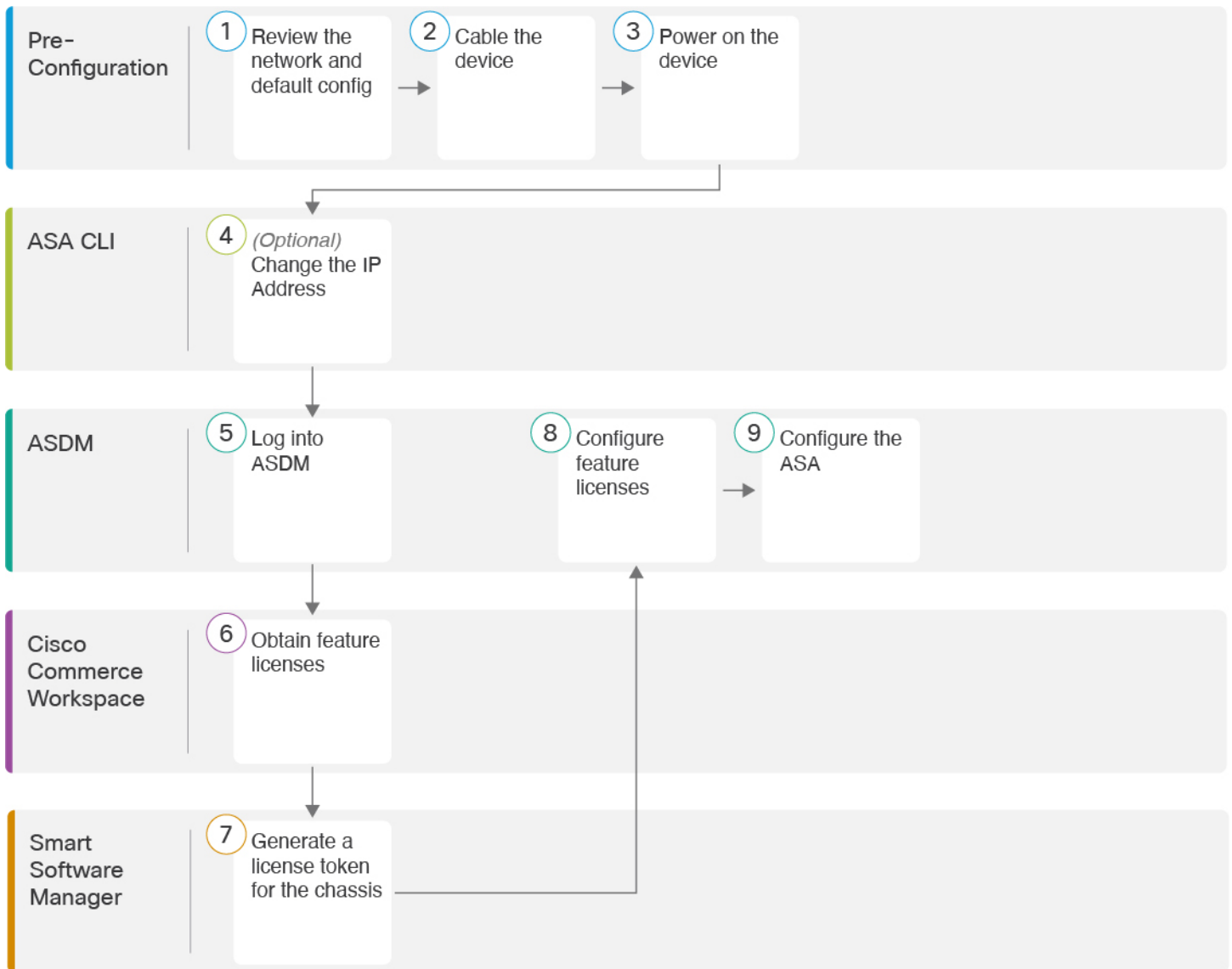
This guide assumes a factory default configuration, so if you paste in an existing configuration, some of the procedures in this guide will not apply to your ASA.

| ASA 5500-X Configuration | Firepower 1010 Configuration |
|--|---|
| Ethernet 1/2 through 1/8 firewall interfaces | <p>Ethernet 1/2 through 1/8 switch ports</p> <p>These Ethernet ports are configured as switch ports by default. For each interface in your configuration, add the no switchport command to make them regular firewall interfaces. For example:</p> <pre>interface ethernet 1/2 no switchport ip address 10.8.7.2 255.255.255.0 nameif inside</pre> |

| ASA 5500-X Configuration | Firepower 1010 Configuration |
|---|---|
| PAK License | <p>Smart License</p> <p>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).</p> |
| Initial ASDM access | <p>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.</p> <p>You can reenab these features after you obtain the Strong Encryption (3DES) license.</p> <p>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.</p> |
| Interface IDs | <p>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.</p> |
| <p>boot system commands</p> <p>The ASA 5500-X allows up to four boot system commands to specify the booting image to use.</p> | <p>The Firepower 1010 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 <i>any</i> 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.</p> <p>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.</p> |

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 140. |
| 2 | Pre-Configuration | Cable the Device, on page 143. |
| 3 | Pre-Configuration | Power On the Device, on page 32 |
| 4 | ASA CLI | (Optional) Change the IP Address, on page 145. |
| 5 | ASDM | Log Into ASDM, on page 146. |

| | | |
|---|--------------------------|--|
| 6 | Cisco Commerce Workspace | Configure Licensing, on page 147 : Obtain feature licenses. |
| 7 | Smart Software Manager | Configure Licensing, on page 147 : Generate a license token for the chassis. |
| 8 | ASDM | Configure Licensing, on page 147 : Configure feature licenses. |
| 9 | ASDM | Configure the ASA, on page 151 . |

Review the Network Deployment and Default Configuration

The following figure shows the default network deployment for the Firepower 1010 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.

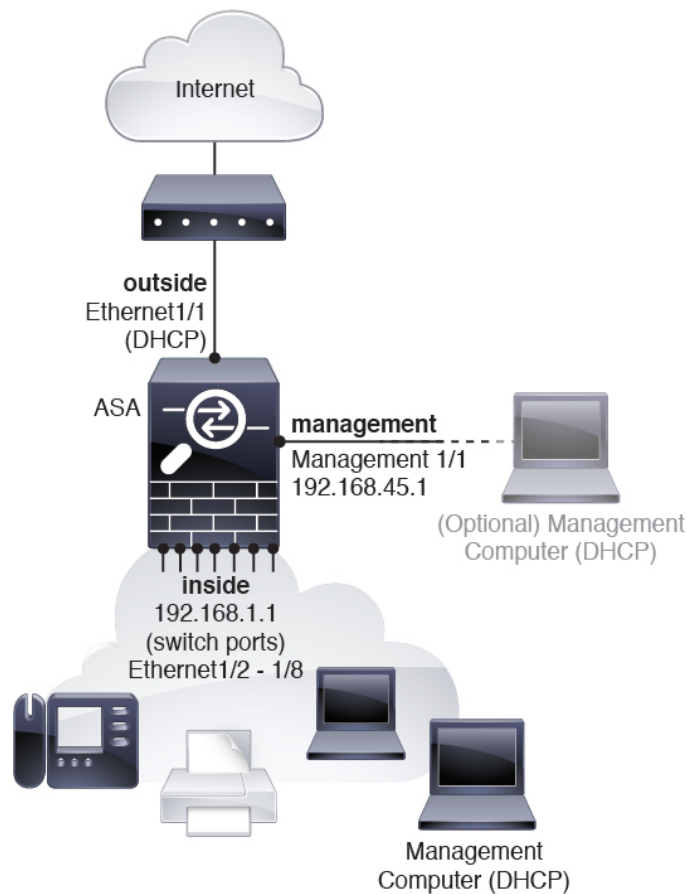


Note

If you cannot use the default Management IP address for ASDM access, you can set the Management IP address at the ASA CLI. See [\(Optional\) Change the IP Address, on page 145](#).

If you need to change the inside IP address, you can do so using the ASDM Startup Wizard. 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 1010 Default Configuration

The default factory configuration for the Firepower 1010 configures the following:

- **Hardware switch**—Ethernet 1/2 through 1/8 belong to VLAN 1
- **inside→outside** traffic flow—Ethernet 1/1 (outside), VLAN1 (inside)
- **management**—Management 1/1 (management), IP address 192.168.45.1
- **outside IP address** from DHCP, inside IP address—192.168.1.1
- **DHCP server** on inside interface, management interface
- **Default route** from outside DHCP
- **ASDM access**—Management and inside hosts allowed. Management hosts are limited to the 192.168.45.0/24 network, and 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 Vlan1
nameif inside
security-level 100
ip address 192.168.1.1 255.255.255.0
no shutdown
!
interface Management1/1
management-only
nameif management
no shutdown
security-level 100
ip address 192.168.45.1 255.255.255.0
!
interface Ethernet1/1
nameif outside
ip address dhcp setroute
no shutdown
!
interface Ethernet1/2
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/3
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/4
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/5
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/6
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/7
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/8
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
object network obj_any
subnet 0.0.0.0 0.0.0.0
nat (any,outside) dynamic interface

```

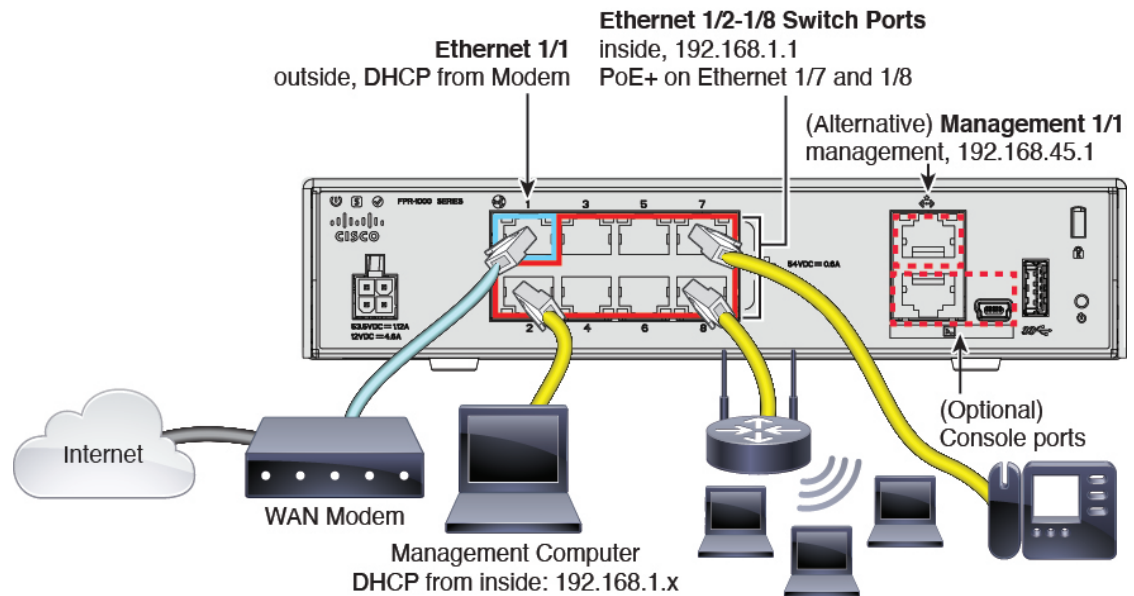


```

!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd address 192.168.45.10-192.168.45.12 management
dhcpd enable inside
dhcpd enable management
!
http server enable
http 192.168.45.0 255.255.255.0 management
http 192.168.1.0 255.255.255.0 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 1010 on either Management 1/1, or on Ethernet 1/2 through 1/8 (inside switch ports). The default configuration also configures Ethernet 1/1 as outside.

Procedure

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

- Ethernet 1/2 through 1/8—Connect your management computer directly to one of the inside switch ports (Ethernet 1/2 through 1/8). The inside interface 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 1010 Default Configuration](#), on page 141).

- Management 1/1—Connect your management computer directly to Management 1/1. Or connect Management 1/1 to your management network; make sure your management computer is on the management network, because only clients on that network can access the ASA. Management 1/1 has a default IP address (192.168.45.1) 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 management network settings (see [Firepower 1010 Default Configuration, on page 141](#)).

If you need to change the Management 1/1 IP address from the default, you must also cable your management computer to the console port. See [\(Optional\) Change the IP Address, on page 145](#).

- Step 2** Connect the outside network to the Ethernet 1/1 interface.
For Smart Software Licensing, the ASA needs internet access so that it can access the License Authority.
- Step 3** Connect inside devices to the remaining inside switch ports, Ethernet 1/2 through 1/8.
Ethernet 1/7 and 1/8 are PoE+ ports.

Power On the Device

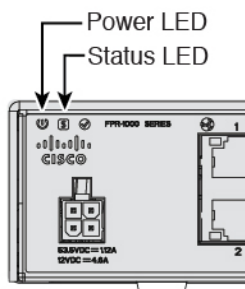
System power is controlled by the power cord; there is no power button.

Before you begin

It's important that you provide reliable power for your device (using an uninterruptable power supply (UPS), for example). 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.
The power turns on automatically when you plug in the power cord.
- Step 2** Check the Power LED on the back or top of the device; if it is solid green, the device is powered on.



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

(Optional) Change the IP Address

If you cannot use the default IP address for ASDM access, you can set the IP address of the management 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 153](#) 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 management1/1
Executing command: nameif management
INFO: Security level for "management" set to 0 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 interface IP address. You can connect to the inside address on any inside switch port (Ethernet1/2 through 1/8).
- **https://192.168.45.1**—Management interface IP address.

Note Be sure to specify **https://**, and not **http://** or just the IP address (which defaults to HTTP); the ASA does not automatically forward an HTTP request to HTTPS.

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

Step 2

Click one of these available options: **Install ASDM Launcher** or **Run ASDM**.

Step 3

Follow the onscreen instructions to launch ASDM according to the option you chose.

The **Cisco ASDM-IDM Launcher** appears.

Step 4

Leave the username and password fields empty, and click **OK**.

The main ASDM window appears.

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 Plus—For Active/Standby failover
- 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).

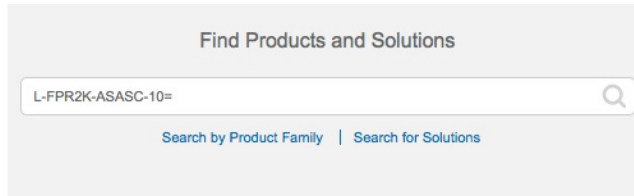
Procedure

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 42: 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.
- Security Plus license—L-FPR1010-SEC-PL=. The Security Plus license enables failover.
- Strong Encryption (3DES/AES) license—L-FPR1K-ENC-K9=. This license is free. Although this license is not generally required (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.

- Click **Inventory**.

Cisco Software Central > Smart Software Licensing

Smart Software Licensing

Alerts **Inventory** License Conversion | Reports | Email Notification | Satellites | Activity

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

The screenshot shows the 'Product Instance Registration Tokens' section in the ASA configuration interface. The 'New Token...' button is highlighted with a red circle. Below it is a table with the following data:

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

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

The 'Create Registration Token' dialog box is shown with the following settings:

- Virtual Account:** [Redacted]
- Description:** [Empty text box]
- Expire After:** 30 Days
- Allow export-controlled functionality on the products registered with this token

Buttons: **Create Token** (blue), **Cancel** (grey)

- **Description**

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

- **Allow export-controlled functionality 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 43: View Token

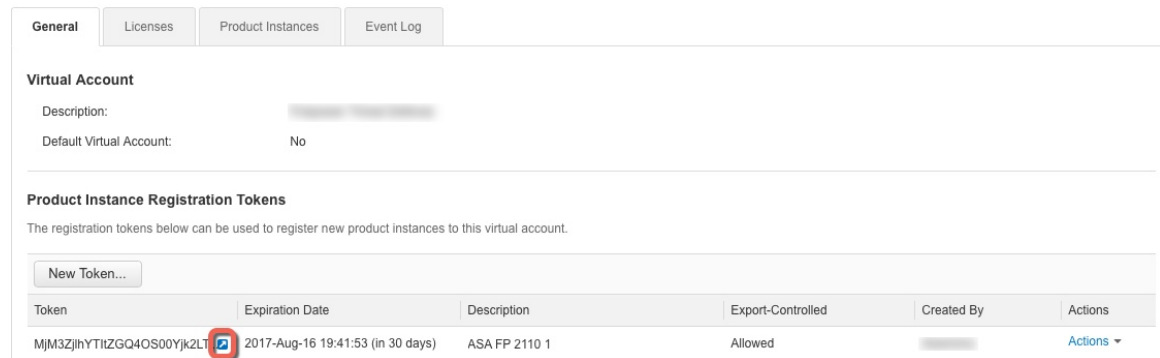
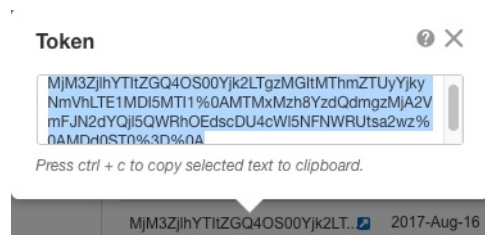


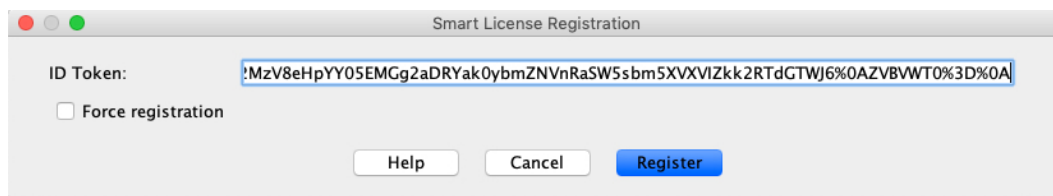
Figure 44: Copy Token



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

Step 4 Click **Register**.

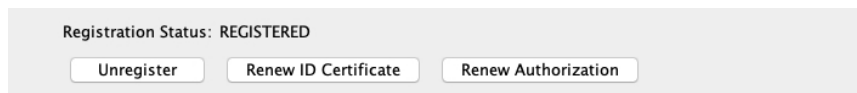
Step 5 Enter the registration token in the **ID Token** field.



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) Check **Enable Security Plus**.

The Security Plus tier enables Active/Standby failover.

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.

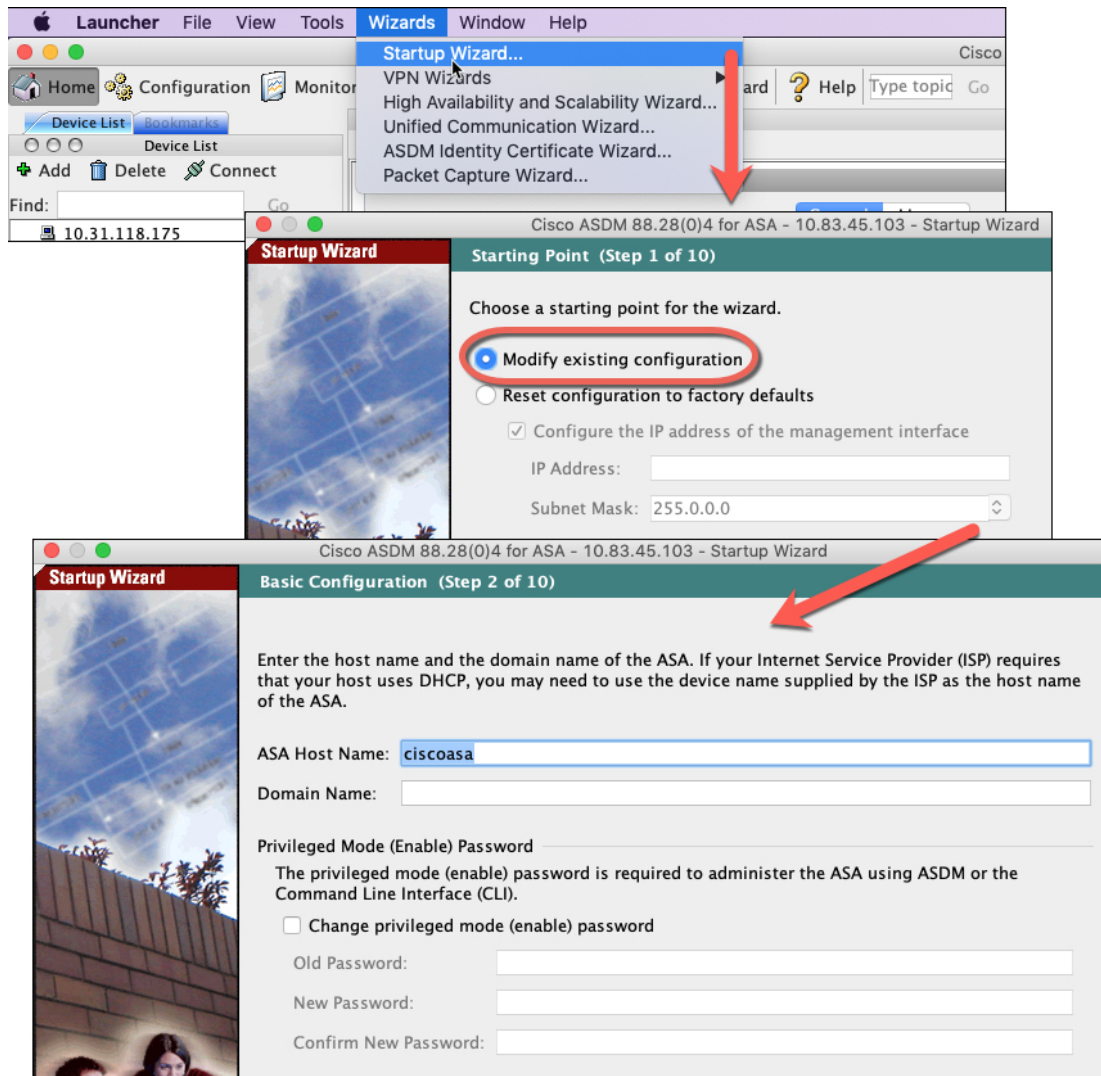
When you change licenses, you need to relaunch ASDM to show updated screens.

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. The Firepower 1000 ships with a USB A-to-B serial cable. Be sure to install any necessary USB serial drivers for your operating system (see the [Firepower 1010 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](#).

