



Firepower Threat Defense Deployment with CDO

Is This Chapter for You?

To see all available operating systems and managers, see [Which Operating System and Manager is Right for You?](#) This chapter applies to FTD with Cisco Defense Orchestrator (CDO) using CDO's onboarding wizard or low-touch provisioning (LTP). LTP streamlines the deployment of new firewalls by allowing network administrators to deliver the firewalls directly to a branch office, add the firewalls to CDO, and then manage the firewalls after the FTD successfully connects to the Cisco Cloud.

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.

About the Firewall

The hardware can run either FTD software or ASA software. Switching between FTD and ASA requires you to reimage the device. You should also reimage if you need a different software version than is currently installed. See [Reimage the Cisco ASA or Firepower Threat Defense Device](#).

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

Privacy Collection Statement—The firewall 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.

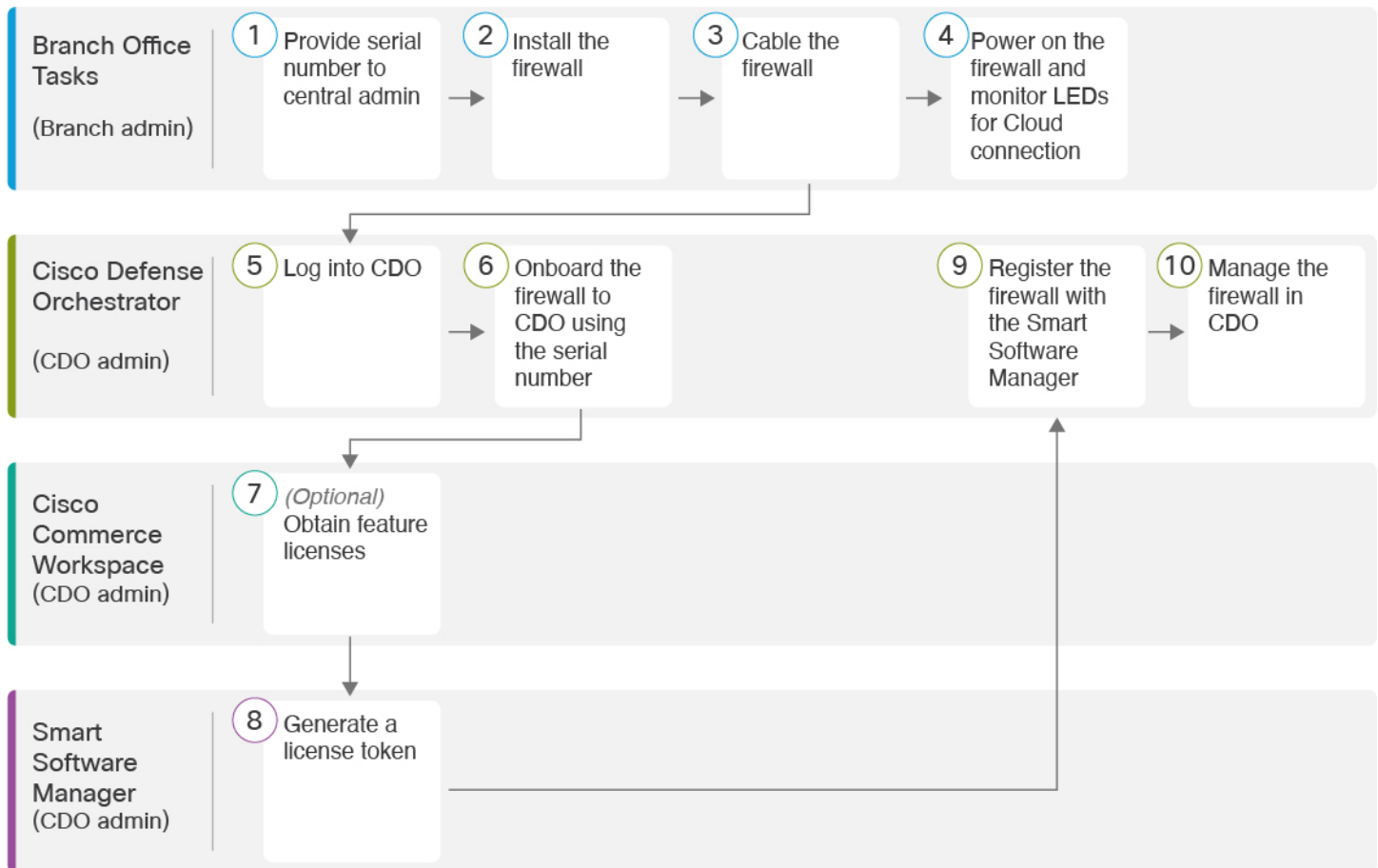
- [Deploy the Firewall for Low-Touch Provisioning, on page 2](#)
- [Deploy the Firewall for CDO's Onboarding Wizard, on page 7](#)
- [Log Into CDO, on page 22](#)
- [Onboard the FTD to CDO, on page 26](#)
- [Configure the Device in CDO, on page 35](#)
- [Configure Licensing, on page 39](#)
- [Access the FTD and FXOS CLI, on page 44](#)
- [Power Off the Firewall Using FDM, on page 45](#)
- [What's Next, on page 45](#)

Deploy the Firewall for Low-Touch Provisioning

This section describes how a branch office can install the firewall without having to perform any configuration. The CDO administrator can then onboard the firewall remotely.

End-to-End Procedure

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



1	Branch Office Tasks (Branch admin)	Provide the Firewall Serial Number to the Central Administrator, on page 3.
2	Branch Office Tasks (Branch admin)	Install the firewall. See the hardware installation guide .
3	Branch Office Tasks (Branch admin)	Cable the Device, on page 4.

4	Branch Office Tasks (Branch admin)	Power On the Device, on page 5.
5	Cisco Defense Orchestrator (CDO admin)	Log Into CDO with Cisco Secure Sign-On, on page 25.
6	Cisco Defense Orchestrator (CDO admin)	Onboard the Device Using Low-Touch Provisioning and the Serial Number, on page 26.
7	Cisco Commerce Workspace (CDO admin)	(Optional) Obtain feature licenses (Configure Licensing, on page 39).
8	Smart Software Manager (CDO admin)	Generate a license token (Configure Licensing, on page 39).
9	Cisco Defense Orchestrator (CDO admin)	Register the device with the Smart Licensing Server (Configure Licensing, on page 39).
10	Cisco Defense Orchestrator (CDO admin)	Configure the Device in CDO, on page 35.

Branch Office Installation

After you receive the FTD from your corporate IT department, you need to record the firewall'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.

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



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

Provide the Firewall Serial Number to the Central Administrator

Before you rack the firewall or discard the shipping box, verify that your firewall can be deployabled using low-touch provisioning, and record the serial number so you can coordinate with the central administrator.



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

Procedure

- Step 1** Unpack the chassis and chassis components.
- Take inventory of your firewall and packaging before you connect any cables or power on the firewall. You should also familiarize yourself with the chassis layout, components, and LEDs.
- Step 2** Verify that the software version is 6.7 or later by checking the product ID (PID) on the shipping box.
- The cardboard box in which the firewall was shipped should have a plain white sticker on it that indicates the shipped version of software (6.7 or later).
- The PID should be similar to this example of a Firepower 2100 series PID: SF-F2K-TD6.7-K9.
- Step 3** Record the firewall's serial number.
- The serial number of the firewall can be found on the shipping box. It can also be found on a sticker on a pull-out tab on the front of the firewall.
- Step 4** Send the firewall serial number to the CDO network administrator at your IT department/central headquarters.
- Your network administrator needs your firewall serial number to facilitate low-touch provisioning, connect to the firewall, and configure it remotely.
- Communicate with the CDO administrator to develop an onboarding timeline.
-

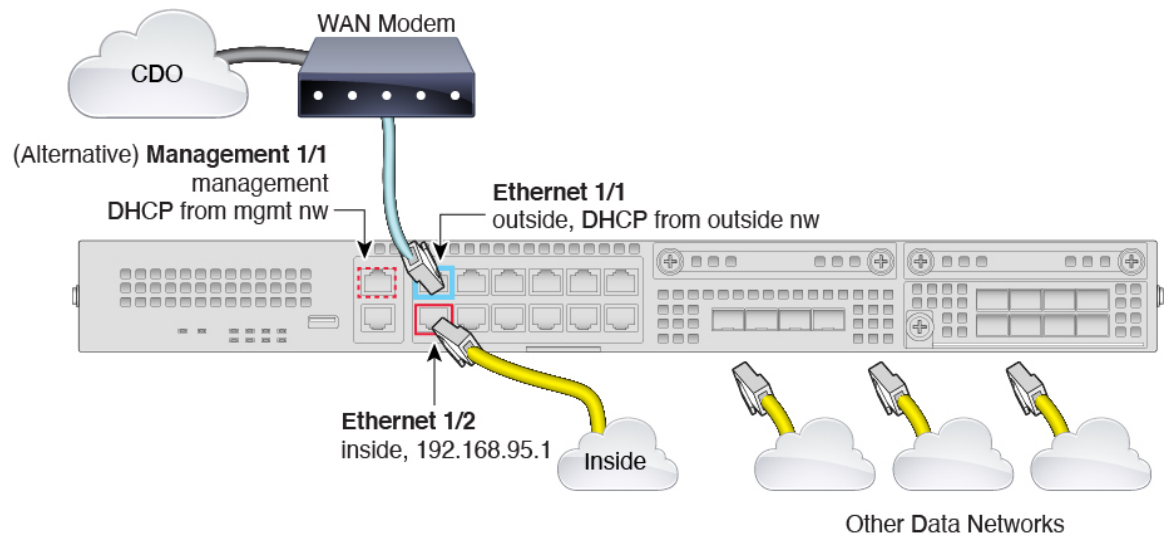
Cable the Device

This topic describes the how to connect the Firepower 2100 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 1: Cabling the Firepower 2100



Note For 6.7, the Ethernet 1/2 inside IP address is 192.168.1.1.

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** Install the chassis. See the [hardware installation guide](#).
- Step 2** 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 device'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 18](#). The outside Ethernet 1/1 interface only supports IPv4 for low-touch provisioning.
- Step 3** Connect the inside network to Ethernet 1/2.
- Step 4** Connect other networks to the remaining interfaces as needed.

Power On the Device

The power switch is located to the left of power supply module 1 on the rear of the chassis. It is a toggle switch that controls power to the system. If the power switch is in standby position, only the 3.3-V standby power is enabled from the power supply module and the 12-V main power is OFF. When the switch is in the ON position, the 12-V main power is turned on and the system boots.



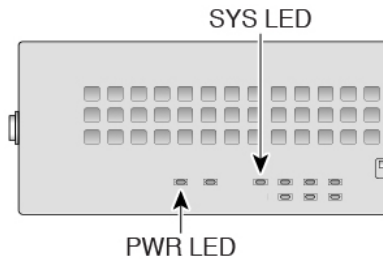
Note The first time you boot up the FTD, initialization can take approximately 15 to 30 minutes.

Before you begin

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

Procedure

- Step 1** Attach the power cord to the device and connect it to an electrical outlet.
- Step 2** Press the power switch on the back of the device.
- Step 3** Check the PWR LED on the front of the device; if it is solid green, the device is powered on.



- Step 4** Observe the SYS LED on the front the device; when the device is booting correctly, the SYS LED flashes fast green.
- If there is a problem, the SYS LED flashes fast amber. If this happens, call your IT department.
- Step 5** Observe the SYS LED on the front; when the device connects to the Cisco cloud, the SYS LED slowly flashes green.
- If there is a problem, the SYS 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

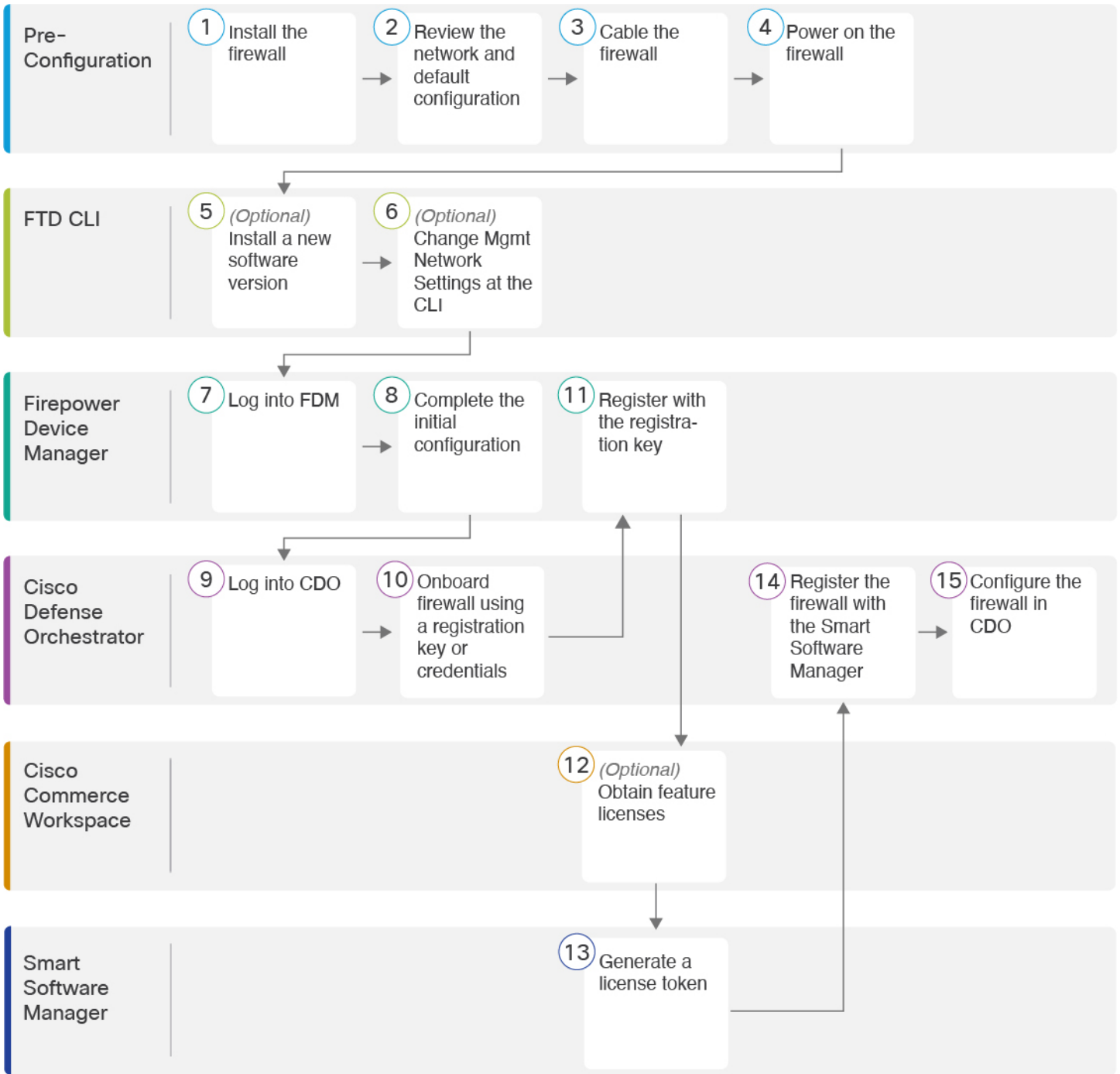
- Communicate with your IT department to confirm your onboarding timeline and activities. You should have a communication plan in place with the CDO administrator at your central headquarters.
- After you complete this task, your CDO administrator will be able to configure and manage the Firepower device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

Deploy the Firewall for CDO's Onboarding Wizard

This section describes how to configure the firewall for onboarding using CDO's onboarding wizard.

End-to-End Procedure

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



1	Pre-Configuration	Install the firewall. See the hardware installation guide .
2	Pre-Configuration	Review the Network Deployment and Default Configuration, on page 10

3	Pre-Configuration	Cable the Device, on page 15.
4	Pre-Configuration	Power on the Device, on page 16.
5	CLI	(Optional) Check the Software and Install a New Version, on page 17
6	CLI	(Optional) Change Management Network Settings at the CLI, on page 18.
7	Firepower Device Manager	Log Into FDM, on page 20.
8	Firepower Device Manager	Complete the Initial Configuration, on page 21.
9	Cisco Defense Orchestrator	Log Into CDO with Cisco Secure Sign-On, on page 25.
10	Cisco Defense Orchestrator	Onboard the device using a registration key or credentials (Onboard the FTD to CDO, on page 26).
11	Firepower Device Manager	Register with the registration key (Onboard the FTD to CDO, on page 26). If you onboard using credentials, you do not need to log into FDM.
12	Cisco Commerce Workspace	(Optional) Obtain feature licenses (Configure Licensing, on page 39).
13	Smart Software Manager	Generate a license token (Configure Licensing, on page 39).
14	Cisco Defense Orchestrator	Register the device with the Smart Licensing Server (Configure Licensing, on page 39).
15	Cisco Defense Orchestrator	Configure the Device in CDO, on page 35.

How Cisco Defense Orchestrator Works with the FTD

CDO and FDM Co-Management

After you complete initial configuration in the FDM to establish internet connectivity and configure a basic network policy, you can onboard the device to CDO. After you onboard the device to CDO, you can continue to use FDM as needed. You can choose whether to accept out-of-band changes in CDO on a case-by-case basis.

Secure Device Connector (SDC)

All communication between CDO and the devices it manages passes through an SDC. CDO and the devices it manages do not communicate directly.

SDCs can be deployed in the cloud or in your network using the following methods:

- **Cloud Secure Device Connector**—The CDO support team deploys a cloud-based SDC for every tenant when the tenant is created.
- **On-Premises Secure Device Connector**—An on-premises SDC is a virtual appliance installed in your network. We recommend that you use an on-premises SDC if you use credentials-based onboarding. If you use the cloud SDC instead, then you need to allow HTTPS access from the cloud SDC to the interface used for CDO management. The typical network deployment would require you to enable HTTPS access on the FTD outside interface, which can be a security risk and also prevents use of the outside interface for VPN client termination.

For more information, including links for installing an on-premises SDC and cloud SDC IP addresses for which you may need to grant access to your network (for credentials-based onboarding), see [Security Device Connector \(SDC\)](#).

CDO Onboarding Methods

You can onboard a device in the following ways:

- **Registration key (recommended)**—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.
- **Credentials (username and password) and an IP address**—You can onboard an FTD using the device admin username and password as well as a static IP address or FQDN. We recommend using an on-premises SDC connected to the inside interface for this method.
- **(6.7+) Serial number**—For Low-Touch Provisioning where you do not need to preconfigure the device using FDM, see the Low-Touch Provisioning section. You can also onboard using a serial number if you already started configuring the device in the FDM, although that method is not covered in this guide. See [Onboard an FTD using the Device's Serial Number](#) for more information.

Review the Network Deployment and Default Configuration

You can perform initial setup of the FTD using FDM from either the Management 1/1 interface or the inside interface. The dedicated Management interface is a special interface that does not allow through traffic and that has its own network settings.

See the following typical network deployments depending on your Secure Device Connector (SDC) type and onboarding method.

Cloud SDC Network, Registration Key Onboarding

The following figure shows the recommended network deployment for registration key onboarding using the cloud SDC. You can use an on-premises SDC with registration key onboarding, but this example shows the more common cloud SDC use case. You can also use credentials-based onboarding with a cloud SDC, but that method requires additional configuration in FDM, which may not be desirable.

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

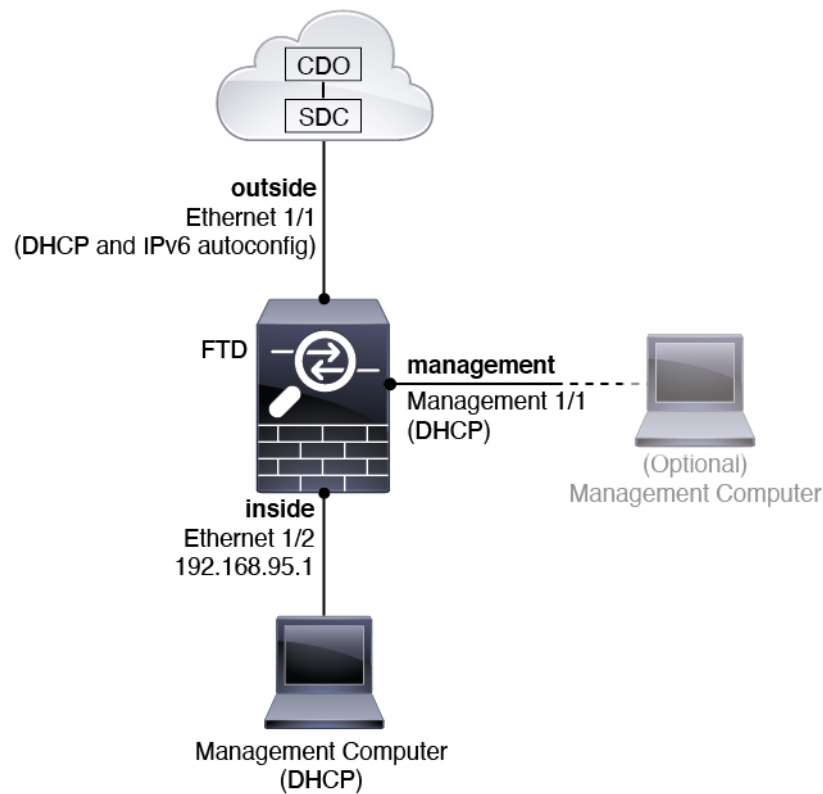


Note If you cannot use the default management IP address (for example, your management network does not include a DHCP server), then you can connect to the console port and perform initial setup at the CLI, including setting the Management IP address, gateway, and other basic networking settings.

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

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

Figure 2: Suggested Network Deployment Cloud SDC



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

On-Premises SDC Network, Credentials Onboarding

The following figure shows the recommended network deployment for credentials onboarding using an on-premises SDC connected to the inside network. You can use a cloud SDC with credentials onboarding, but that method requires additional configuration in FDM, which may not be desirable. This example shows the more common on-premises SDC use case. If you add the SDC to the optional management network, which does not allow through traffic, then the SDC will need a path to the internet (not shown in the diagram).

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

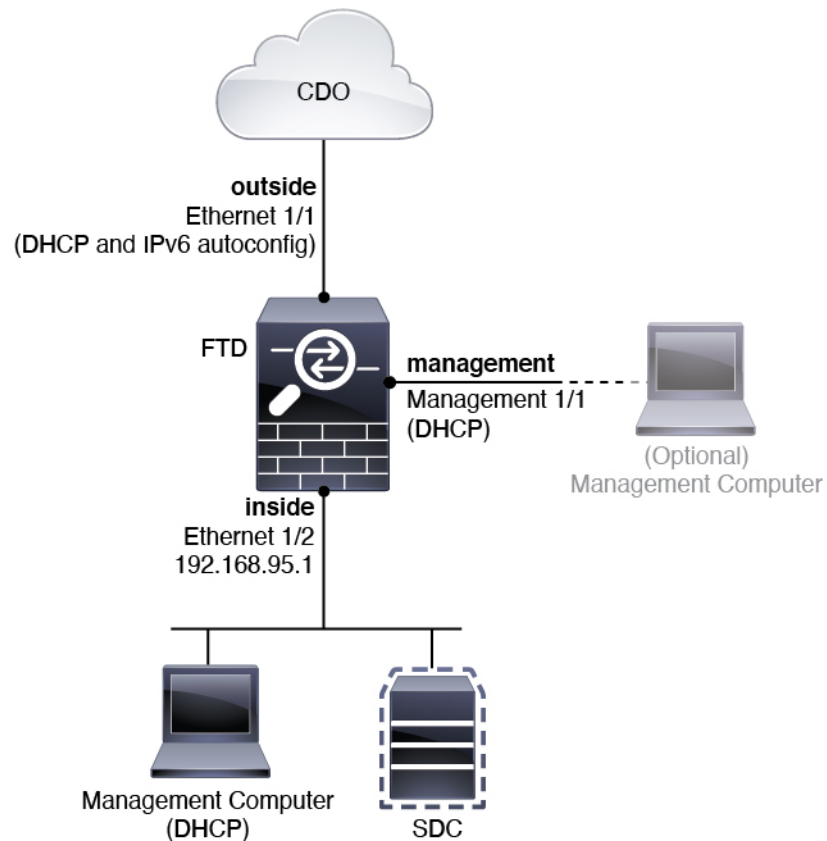


Note If you cannot use the default management IP address (for example, your management network does not include a DHCP server), then you can connect to the console port and perform initial setup at the CLI, including setting the Management IP address, gateway, and other basic networking settings.

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

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

Figure 3: Suggested Network Deployment On-Premises SDC



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

Default Configuration

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

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

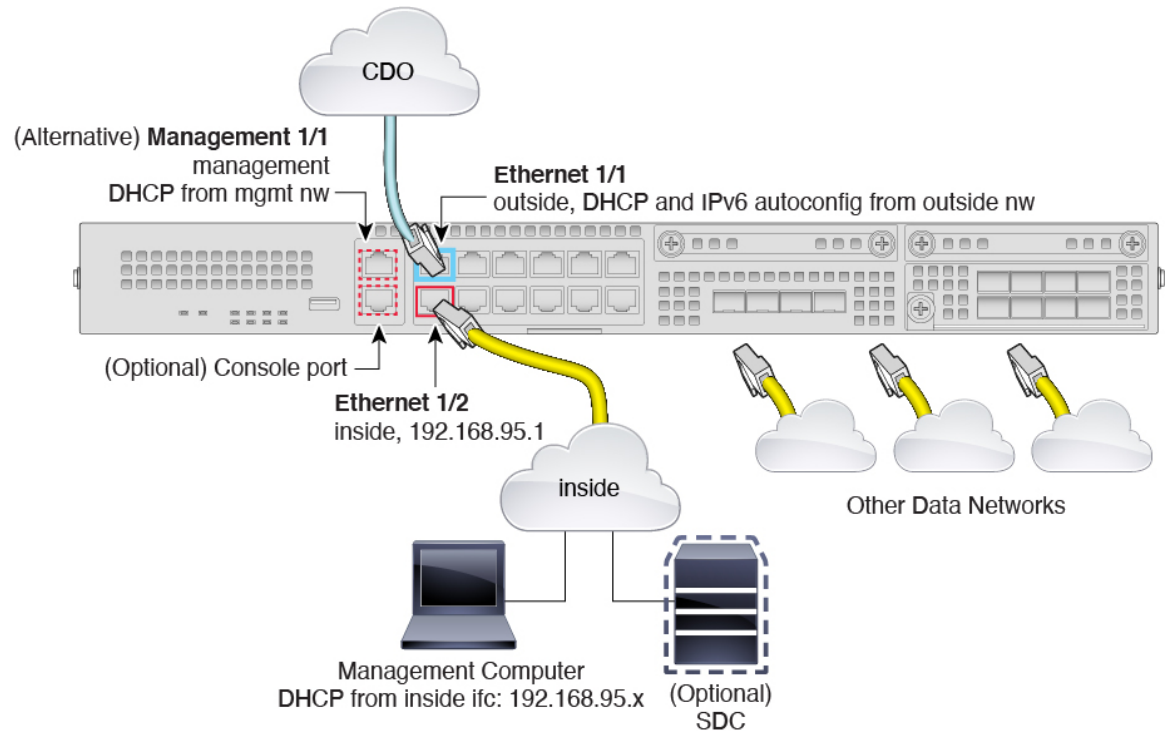


Note The Management 1/1 interface is a special interface separate from data interfaces that is used for management, Smart Licensing, and database updates. The physical interface is shared with a second logical interface, the Diagnostic interface. Diagnostic is a data interface, but is limited to other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

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

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

Cable the Device



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

Manage the Firepower 2100 on either Management 1/1 or Ethernet 1/2. The default configuration also configures Ethernet1/1 as outside.

Procedure

- Step 1** Install the chassis. See the [hardware installation guide](#).
- Step 2** Connect your management computer to either of the following interfaces:
- Ethernet 1/2—Connect your management computer directly to Ethernet 1/2 for initial configuration, or connect Ethernet 1/2 to your inside network. Ethernet 1/2 has a default IP address (192.168.95.1) and also runs a DHCP server to provide IP addresses to clients (including the management computer), so make sure these settings do not conflict with any existing inside network settings (see [Default Configuration](#)).
 - 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 18](#).

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

Step 3 Connect the optional on-premises Secure Device Connector (SDC) to the inside network.

Step 4 Connect the outside network to the Ethernet1/1 interface (labeled WAN).

By default, the IP address is obtained using IPv4 DHCP and IPv6 autoconfiguration, but you can set a static address during initial configuration.

Step 5 Connect other networks to the remaining interfaces.

Power on the Device

The power switch is located to the left of power supply module 1 on the rear of the chassis. It is a toggle switch that controls power to the system. If the power switch is in standby position, only the 3.3-V standby power is enabled from the power supply module and the 12-V main power is OFF. When the switch is in the ON position, the 12-V main power is turned on and the system boots.



Note The first time you boot up the FTD, initialization can take approximately 15 to 30 minutes.

Before you begin

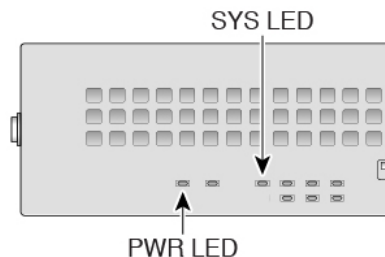
It's important that you provide reliable power for your device (for example, using an uninterruptable power supply (UPS)). Loss of power without first shutting down can cause serious file system damage. There are many processes running in the background all the time, and losing power does not allow the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

Procedure

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

Step 2 Press the power switch on the back of the device.

Step 3 Check the PWR LED on the front of the device; if it is solid green, the device is powered on.



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

Note Before you move the power switch to the OFF position, use the shutdown commands so that the system can perform a graceful shutdown. This may take several minutes to complete. After the graceful shutdown is complete, the console displays `It is safe to power off now`. The front panel blue locator beacon LED lights up indicating the system is ready to be powered off. You can now move the switch to the OFF position. The front panel PWR LED flashes momentarily and turns off. Do not remove the power until the PWR LED is completely off.

See the [FXOS Configuration Guide](#) for more information on using the shutdown commands.

(Optional) Check the Software and Install a New Version

To check the software version and, if necessary, install a different version, perform these steps. We recommend that you install your target version before you configure the firewall. Alternatively, you can perform an upgrade after you are up and running, but upgrading, which preserves your configuration, may take longer than using this procedure.

What Version Should I Run?

Cisco recommends running a Gold Star release indicated by a gold star next to the release number on the software download page. You can also refer to the release strategy described in <https://www.cisco.com/c/en/us/products/collateral/security/firewalls/bulletin-c25-743178.html>; for example, this bulletin describes short-term release numbering (with the latest features), long-term release numbering (maintenance releases and patches for a longer period of time), or extra long-term release numbering (maintenance releases and patches for the longest period of time, for government certification).

Procedure

Step 1 Connect to the CLI. See [Access the FTD and FXOS CLI, on page 44](#) for more information. This procedure shows using the console port, but you can use SSH instead.

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 At the FXOS CLI, show the running version.

```
scope ssa
```

```
show app-instance
```

Example:

```
Firepower# scope ssa
Firepower /ssa # show app-instance
```

Application Name	Slot ID	Admin State	Operational State	Running Version	Startup Version
ftd	1	Enabled	Online	7.1.0.65	7.1.0.65
	Not Applicable				

Step 3 If you want to install a new version, perform these steps.

a) If you need to set a static IP address for the Management interface, see [\(Optional\) Change Management Network Settings at the CLI, on page 18](#). By default, the Management interface uses DHCP.

You will need to download the new image from a server accessible from the Management interface.

b) Perform the [reimage procedure](#) in the [FXOS troubleshooting guide](#).

(Optional) Change Management Network Settings at the CLI

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



Note

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

Procedure

Step 1 Connect to the FTD console port. See [Access the FTD and FXOS CLI, on page 44](#) 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 outbound management traffic over the backplane to exit a data interface. This setting is useful if you do not have a separate Management network that can access the internet. Traffic originating on the Management interface includes license registration and database updates that require internet access. If you use **data-interfaces**, you can still use the FDM (or SSH) on the Management interface if you are directly-connected to the Management network, but for remote management for specific networks or hosts, you should add a static route using the **configure network static-routes** command. Note that FDM management on data interfaces is not affected by this setting. If you use DHCP, the system uses the gateway provided by DHCP and uses the **data-interfaces** as a fallback method if DHCP doesn't provide a gateway.
- **If your networking information has changed, you will need to reconnect**—If you are connected with SSH to the default IP address but you change the IP address at initial setup, you will be disconnected. Reconnect with the new IP address and password. Console connections are not affected.
- **Manage the device locally?**—Enter **yes** to use the FDM or the CDO. A **no** answer means you intend to use the FMC to manage the device.

Example:

```

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

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

System initialization in progress. Please stand by.
You must 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 the FDM on the new Management IP address.

What to do next

When you choose to use the CLI to change your management network settings, you'll accept the EULA, change the IP addresses, and change the password. You can then complete the initial configuration; see [Complete the Initial Configuration, on page 21](#).

Log Into FDM

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

Before you begin

- Use a current version of Firefox or Chrome.

Procedure

Step 1 Enter the following URL in your browser.

- (7.0 and later) Inside (Ethernet 1/2)—**<https://192.168.95.1>**.
- (6.7 and earlier) Inside (Ethernet 1/2)—**<https://192.168.1.1>**.
- (6.6 and later) Management—**https://management_ip**. The Management interface is a DHCP client, so the IP address depends on your DHCP server. If you changed the Management IP address at the CLI setup, then enter that address.

- (6.5 and earlier) Management—<https://192.168.45.45>. If you changed the Management IP address at the CLI setup, then enter that address.

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

What to do next

- Run through the FDM setup wizard; see [Complete the Initial Configuration, on page 21](#).

Complete the Initial Configuration

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

- An outside (Ethernet1/1) and an inside interface (Ethernet1/2).
- Security zones for the inside and outside interfaces.
- An access rule trusting all inside to outside traffic.
- An interface NAT rule that translates all inside to outside traffic to unique ports on the IP address of the outside interface.
- A DHCP server running on the inside interface.



Note If you performed the [\(Optional\) Change Management Network Settings at the CLI](#) 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 Select **Start 90 day evaluation period without registration**.

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

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

Step 5 Click **Finish**.

What to do next

- Continue to [Log Into CDO, on page 22](#) to begin the onboarding process.

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 25](#).
- If you don't have a Cisco Secure Sign-On account, continue to [Create a New Cisco Secure Sign-On Account, on page 23](#).

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

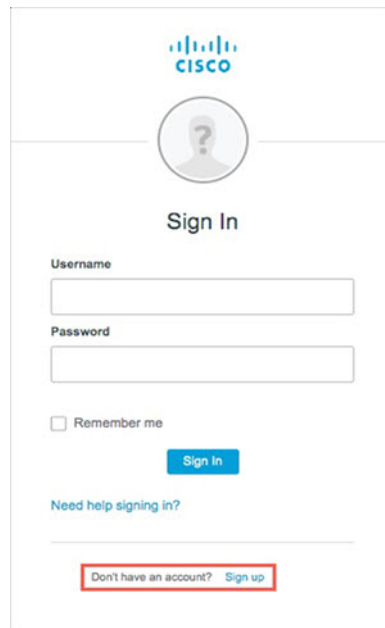
- **Install DUO Security**—We recommend that you install the Duo Security app on a mobile phone. Review [Duo Guide to Two Factor Authentication: Enrollment Guide](#) if you have questions about installing Duo.
- **Time Synchronization**—You are going to use your mobile device to generate a one-time password. 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 4: Cisco SSO Sign Up



The screenshot shows the Cisco Sign In page. At the top is the Cisco logo. Below it is a circular placeholder for a profile picture. The text "Sign In" is centered. 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. At the bottom of the page, there is a link "Need help signing in?". A red-bordered box highlights the text "Don't have an account? Sign up" at the bottom center.

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

Figure 5: 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 that these fields are required. 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.

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

- At the end of the wizard click **Continue to Login**.
- Log in to Cisco Secure Sign-On with the two-factor authentication.

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

- Choose the mobile device you are pairing with Google Authenticator and click **Next**.
- Follow the prompts in the setup wizard to setup Google Authenticator.

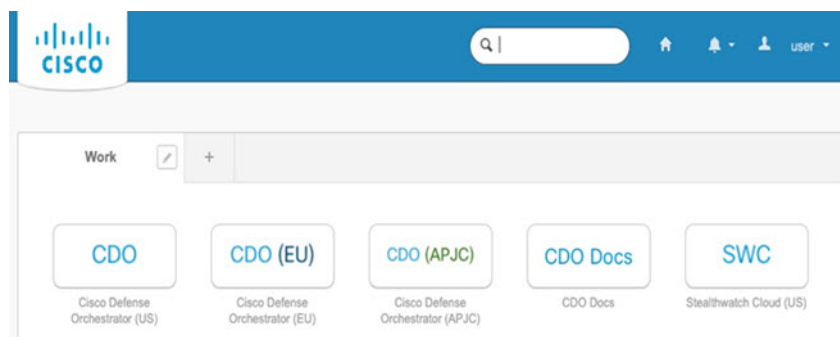
Step 4 Configure Account Recovery Options for your Cisco Secure Sign-On Account.

- Choose a "forgot password" question and answer.
- Choose a recovery phone number for resetting your account using SMS.
- Choose a security image.
- 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 6: Cisco SSO Dashboard



Log Into CDO with Cisco Secure Sign-On

Log into CDO to onboard and manage your FTD.

Before you begin

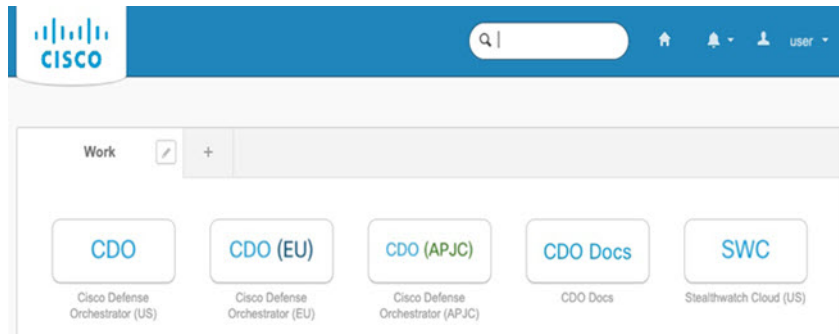
Cisco Defense Orchestrator (CDO) uses Cisco Secure Sign-On as its identity provider and Duo Security for multi-factor authentication (MFA).

- 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 23](#).
- 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 7: 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 FTD to CDO

Onboard the firewall to CDO.

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 2100 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:
- 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.
 - Device Serial Number:** Enter the serial number or the PCA number of the device you want to onboard.
 - Device Name:** Provide a name for the device.
- Step 5** Click **Next**.
- Step 6** In the **Password Reset** area, provide the following:
- 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.
- 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.

Onboard the FTD with a Registration Key (Recommended)

We recommend that you onboard an FTD device using a registration key. If your FTD is assigned an IP address using DHCP and the address changes for some reason, your FTD remains connected to CDO. Additionally, your FTD does not need to have a public IP address, and as long as the device can access the outside network, you can onboard it to CDO using this method.



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

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

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

Before you begin

- You can use this method to onboard your device to the US, EU, or APJ regions.
- Your device **MUST** be managed by Firepower Device Manager (FDM). Make sure that there are no pending changes waiting on the device.
- Your device can use either a 90-day evaluation license or it can be smart-licensed. You will not need to unregister licenses installed on the device from the Cisco Smart Software Manager.
- 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.

Procedure


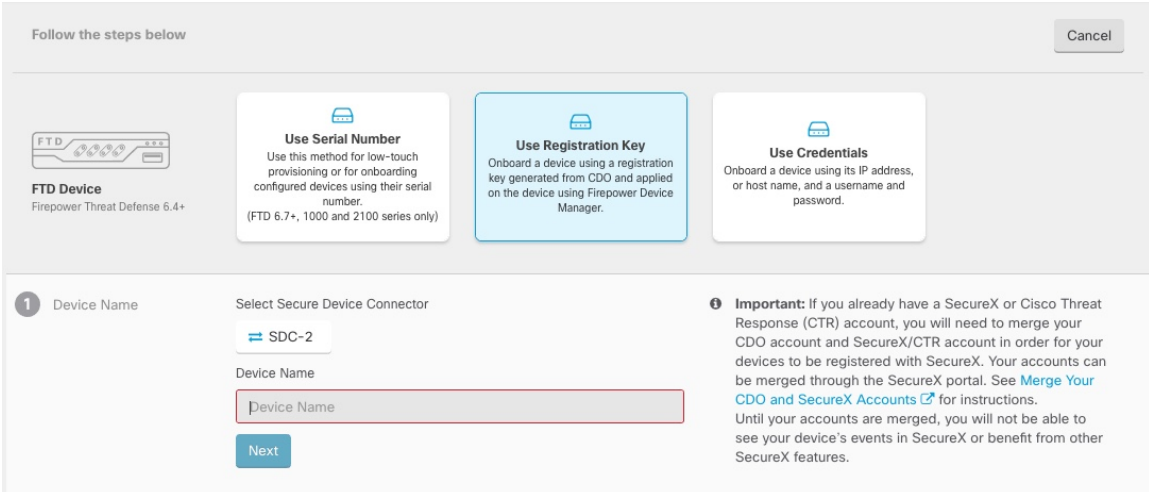
- Step 1** In the CDO navigation pane, click **Devices & Services**, then click the blue plus button () to **Onboard** a device.
- Step 2** Click the **FTD** card.
- Step 3** Click **Use Registration Key**.
- Step 4** Complete the **Device Name** area fields.

Figure 8: Device Name



Follow the steps below Cancel

FTD Device
Firepower Threat Defense 6.4+

Use Serial Number
Use this method for low-touch provisioning or for onboarding configured devices using their serial number.
(FTD 6.7+, 1000 and 2100 series only)

Use Registration Key
Onboard a device using a registration key generated from CDO and applied on the device using Firepower Device Manager.

Use Credentials
Onboard a device using its IP address, or host name, and a username and password.

1 Device Name

Select Secure Device Connector
SDC-2

Device Name

Next

Important: If you already have a SecureX or Cisco Threat Response (CTR) account, you will need to merge your CDO account and SecureX/CTR account in order for your devices to be registered with SecureX. Your accounts can be merged through the SecureX portal. See [Merge Your CDO and SecureX Accounts](#) for instructions. Until your accounts are merged, you will not be able to see your device's events in SecureX or benefit from other SecureX features.

- a) Choose the **Secure Device Connector** that this device will communicate with. The default SDC is displayed but you can change it by clicking the SDC name.
- b) Enter the device name in the **Device Name** field. This could be the hostname of the device or any other name you choose.
- c) Click **Next**.


- Step 5** In the **Database Updates** area, check or uncheck the **Immediately perform security updates, and enable recurring updates**, and click **Next**.

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

Note 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 7 Click the **Copy** icon () to copy the registration key, and click **Next**.

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

- a) Under **System Settings**, click **Cloud Services**.
- b) If you already registered the device with Cisco Smart Licensing and this page shows you are already registered with the cloud, then click the gear menu and choose **Unregister Cloud Services**. Reload the page to see the unregistered options.
- c) In the **Enrollment Type** area, click **Security/CDO Account**.
For 6.6, this tab is called **Security Account**.
- d) (6.7+) Do NOT check **Auto-enroll with Tenancy from Cisco Defense Orchestrator**.
See the [FDM configuration guide](#) for more information about auto-enrollment using the serial number.
- e) In the **Region** field, choose the Cisco cloud region to which your tenant is assigned:
 - Choose **US** if you log in to *defenseorchestrator.com*.
 - Choose **EU** if you log in to *defenseorchestrator.eu*.
 - Choose **APJ** if you log in to *apj.cdo.cisco.com*.
- f) In the **Registration Key** field, paste the registration key that you generated in CDO.
- g) (6.7+) In the **Service Enrollment** area, check **Enable Cisco Defense Orchestrator**.
For 6.6, you have to complete cloud registration before you can enable CDO (see Step 8.j, on page 30).
- h) (6.7+) Review the information about the Cisco Success Network. If you do not want to participate, uncheck **Enroll Cisco Success Network**.
For 6.6, you have to complete cloud registration before you can enable Cisco Success Network.
- i) Click **Register** and then **Accept** the Cisco Disclosure. FDM sends the registration request to CDO.
- j) (6.6) Refresh the **Cloud Services** page. If the device successfully registered with the Cisco cloud, on the **Cisco Defense Orchestrator** tile, click **Enable**.

For 6.7+, you can enable CDO at the time of registration.

Step 9 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 39](#). Click **Skip** to continue the onboarding with a 90-day evaluation license.

Step 10 In the **Done** area, click **Go to devices** to view the onboarded device.

- Step 11** On **Devices & Services**, observe that the device status progresses from *"Unprovisioned"* to *"Locating"* to *"Syncing"* to *"Synced"*.
-

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 6.5) This method is supported for the US, EU, and APJ (apj.cdo.cisco.com) regions.
(Version 6.4) This method is only supported for the US region (defenseorchestrator.com). For version 6.4 for the EU region (defenseorchestrator.eu), you can only onboard your FTD device using username, password, and IP address. You cannot use a registration key.
- Your device **MUST** be managed by Firepower Device Manager (FDM). Make sure that there are no pending changes waiting on the device.
- Your device should be configured to use the 90-day evaluation license. You will need to unregister the FTD if it is already smart-licensed. On the FDM **Device** > > **Smart License** page, from the gear drop-down menu choose **Unregister 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.

Procedure


- Step 1** In the CDO navigation pane, click **Devices & Services**, then click the blue plus button () to **Onboard** a device.
- Step 2** Click the **FTD** card.
- Step 3** Click **Use Registration Key**.
- Step 4** Complete the **Device Name** area fields.

Figure 9: Device Name

The screenshot shows the onboarding interface for a Firepower Threat Defense (FTD) device. At the top, it says "Follow the steps below" with a "Cancel" button. Below this are four options for onboarding: "Use Serial Number", "Use Registration Key" (highlighted in blue), and "Use Credentials". The "Use Registration Key" option is selected, and the "Device Name" step is active. The "Device Name" step includes a "Select Secure Device Connector" dropdown menu with "SDC-2" selected, a "Device Name" input field containing "Device Name", and a "Next" button. An "Important" note is displayed on the right side of the form.

- Choose the **Secure Device Connector** that this device will communicate with. The default SDC is displayed but you can change it by clicking the SDC name.
- Enter the device name in the **Device Name** field. This could be the hostname of the device or any other name you choose.
- Click **Next**.

Step 5

In the **Database Updates** area, check or uncheck the **Immediately perform security updates, and enable recurring updates**, and click **Next**.

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

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

Note 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 7

Click the **Copy** icon () to copy the registration key, and click **Next**.

Note You can skip copying the registration key and click **Next** to complete the placeholder 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 8

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

- a) Under **System Settings**, click **Cloud Services**.
- b) Click **Get Started** in the **Cisco Defense Orchestrator** group.
- c) In the **Region** field, choose 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).
- d) In the **Registration Key** field, paste the registration key that you generated in CDO.
- e) Click **Register** and then **Accept** the Cisco Disclosure. FDM sends the registration request to CDO.

Step 9 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 39](#). Click **Skip** to continue the onboarding with a 90-day evaluation license.

Step 10 In the **Done** area, click **Go to devices** to view the onboarded device.

Step 11 On **Devices & Services**, observe that the device status progresses from *"Unprovisioned"* to *"Locating"* to *"Syncing"* to *"Synced"*.

Onboard an FTD Using Credentials and IP Address

You can onboard an FTD using login credentials (username and password) and the IP address or FQDN. However, we recommend that you onboard your device with a registration key because it is not dependent on a static IP address and does not require an on-premises SDC; see [Onboard an FTD with a Registration Key \(Version 6.6+\), on page 28](#).

Before you begin

- You can use this method to onboard your device to the US, EU, or APJ regions.
- Your device **MUST** be managed by Firepower Device Manager (FDM). Make sure that there are no pending changes waiting on the device.
- Your device can use either a 90-day evaluation license or it can be smart-licensed. You will not need to unregister licenses installed on the device from the Cisco Smart Software Manager.
- We recommend that you deploy an on-premises Secure Device Connector (SDC) connected to the inside interface. Alternatively, if you want to use a cloud SDC through the outside interface, you need to allow HTTPS access on outside (FDM **System Settings** > **Management Access**), which is not recommended for security reasons. For more information about the SDC, see [How Cisco Defense Orchestrator Works with the FTD, on page 9](#).
- Configure the interface used for CDO management/SDC communication with a static IP address, or use Dynamic DNS (DDNS) to maintain a consistent FQDN. You can configure DDNS in FDM.

Procedure


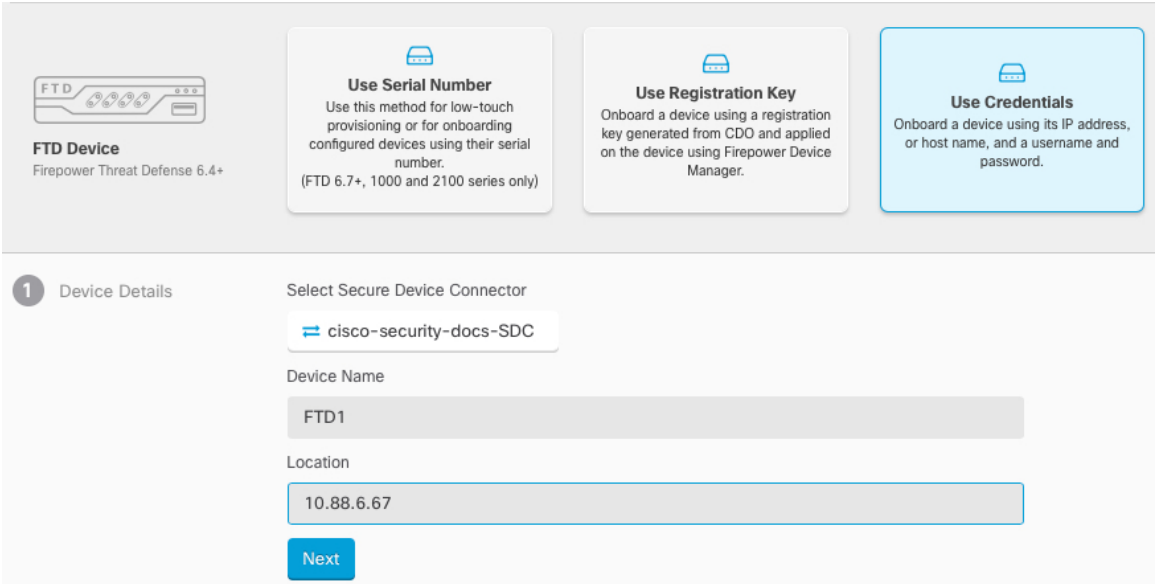
- Step 1** In the CDO navigation pane, click **Devices & Services**, then click the blue plus button () to **Onboard** a device.
- Step 2** Click the **FTD** card.
- Step 3** Click **Use Credentials**.
- Step 4** Complete the **Device Name** area fields.

Figure 10: Device Name



The screenshot shows the 'Device Details' form in the CDO interface. At the top, there are four cards for different onboarding methods: 'FTD Device', 'Use Serial Number', 'Use Registration Key', and 'Use Credentials'. The 'Use Credentials' card is highlighted in blue. Below the cards, the 'Device Details' form is shown with the following fields:

- Select Secure Device Connector:** A dropdown menu with 'cisco-security-docs-SDC' selected.
- Device Name:** A text input field containing 'FTD1'.
- Location:** A text input field containing '10.88.6.67'.
- Next:** A blue button at the bottom of the form.

- Choose the **Secure Device Connector** that this device will communicate with. The default SDC is displayed but you can change it by clicking the SDC name.
- Enter the device name in the **Device Name** field. This could be the hostname of the device or any other name you choose.
- For the **Location**, enter the IP address, hostname, or FQDN.
The default port is 443. You can change the port number to reflect your device's configuration.
- Click **Next**.

- Step 5** In the **Database Updates** area, check or uncheck the **Immediately perform security updates, and enable recurring updates**, and click **Next**.

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** In the **Credentials** area, enter the username as **admin** and enter the password that you set during initial setup. Then click **Next**.

CDO will test the connection, and ensure that it can reach the device. If successful, you will see **Connected** in the **Credentials** area, and **Done** in the **Onboarding Checks** area.

Step 7 In the **Done** area, click **Go to devices** to view the onboarded device.

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 11: Edit Interface

The screenshot shows the 'Editing Physical Interface' configuration window. At the top, there is a title bar with a close button (X). Below the title bar, there are two main sections. The first section contains 'Logical Name' with a text input field containing 'dmz' and a 'State' toggle switch that is turned on. Below this is a 'Description' field with a text input area. The second section is titled 'IPv4 Address' and contains a 'Type' dropdown menu set to 'Static'. Below the dropdown is the 'IP Address and Subnet Mask' field, which has a text input '192.168.6.1' followed by a slash and a dropdown menu set to '24'. Below this is the 'Standby IP Address' field with a text input 'Enter IP address' and a slash and a dropdown menu. To the right of these fields is the 'DHCP Address Pool' section with a text input 'Enter DHCP address pool'. At the bottom right of the form are 'Cancel' and 'Save' buttons.

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 12: Security Zone Object

Adding FTD Security Zone

Object Name
dmz-zone

Description
Object description

Select Interfaces 0

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 13: 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 14: 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 of the window.

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.

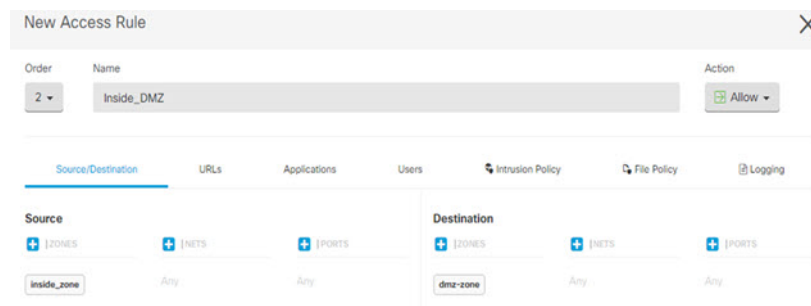
In addition, you can configure other policies to provide additional services, and fine-tune NAT and access rules to get the results that your organization requires. You can configure the following policies:

- **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 15: 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.

Configure Licensing

Configure Licensing

The FTD uses Smart Software Licensing, which lets you purchase and manage a pool of licenses centrally. When you register the chassis, the Smart Software Manager issues an ID certificate for communication between the chassis and the Smart Software Manager. It also assigns the chassis to the appropriate virtual account.

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

The Base license is included automatically. Smart Licensing does not prevent you from using product features that you have not yet purchased. You can start using a license immediately, as long as you are registered with the Smart Software Manager, and purchase the license later. This allows you to deploy and use a feature, and avoid delays due to purchase order approval. See the following licenses:

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

Before you begin

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

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

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

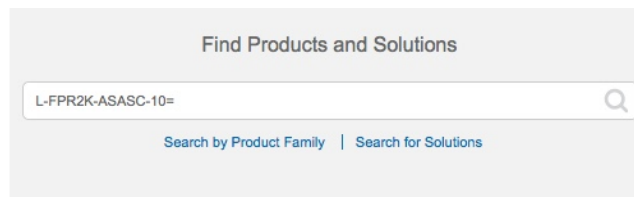
Procedure

Step 1

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

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

Figure 16: License Search



Find Products and Solutions

L-FPR2K-ASASC-10=

Search by Product Family | Search for Solutions

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

- Threat, Malware, and URL license combination:

- L-FPR2110T-TMC=
- L-FPR2120T-TMC=
- L-FPR2130T-TMC=
- L-FPR2140T-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-FPR2110T-TMC-1Y
- L-FPR2110T-TMC-3Y
- L-FPR2110T-TMC-5Y
- L-FPR2120T-TMC-1Y
- L-FPR2120T-TMC-3Y
- L-FPR2120T-TMC-5Y
- L-FPR2130T-TMC-1Y
- L-FPR2130T-TMC-3Y
- L-FPR2130T-TMC-5Y
- L-FPR2140T-TMC-1Y
- L-FPR2140T-TMC-3Y
- L-FPR2140T-TMC-5Y

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

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

- 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**.

The screenshot shows a configuration page with tabs for 'General', 'Licenses', 'Product Instances', and 'Event Log'. The 'Product Instances' tab is active. Under the 'Virtual Account' section, the 'Description' is blurred and 'Default Virtual Account' is set to 'No'. The 'Product Instance Registration Tokens' section contains a text box with the instruction: 'The registration tokens below can be used to register new product instances to this virtual account.' Below this is a table with columns 'Token', 'Expiration Date', and 'Description'. A 'New Token...' button is circled in red. The table contains one entry: 'NWU1MzY1MzEtZjNmOS00MjF.' with an expiration date of '2018-Jul-06 14:20:13 (in 354 days)' and a description of '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. It includes a title bar with a help icon and a close button. The main text reads: 'This dialog will generate the token required to register your product instances with your Smart Account.' Below this are fields for 'Virtual Account' (blurred), 'Description' (with a red box around the input field), and 'Expire After' (set to 30 Days). A note below the 'Expire After' field states: 'Enter the value between 1 and 365, but Cisco recommends a maximum of 30 days.' At the bottom, there is a checked checkbox for 'Allow export-controlled functionality on the products registered with this token' and two buttons: 'Create Token' and 'Cancel'.

- **Description**

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

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

The token is added to your inventory.

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

Figure 17: View Token

General Licenses Product Instances Event Log

Virtual Account

Description: [Redacted]

Default Virtual Account: No

Product Instance Registration Tokens

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

New Token...

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

Figure 18: Copy Token

Token ? X

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

Press ctrl + c to copy selected text to clipboard.

MJM3ZjYhYtIiZGQ4OS00Yjk2LT... 2017-Aug-16 1

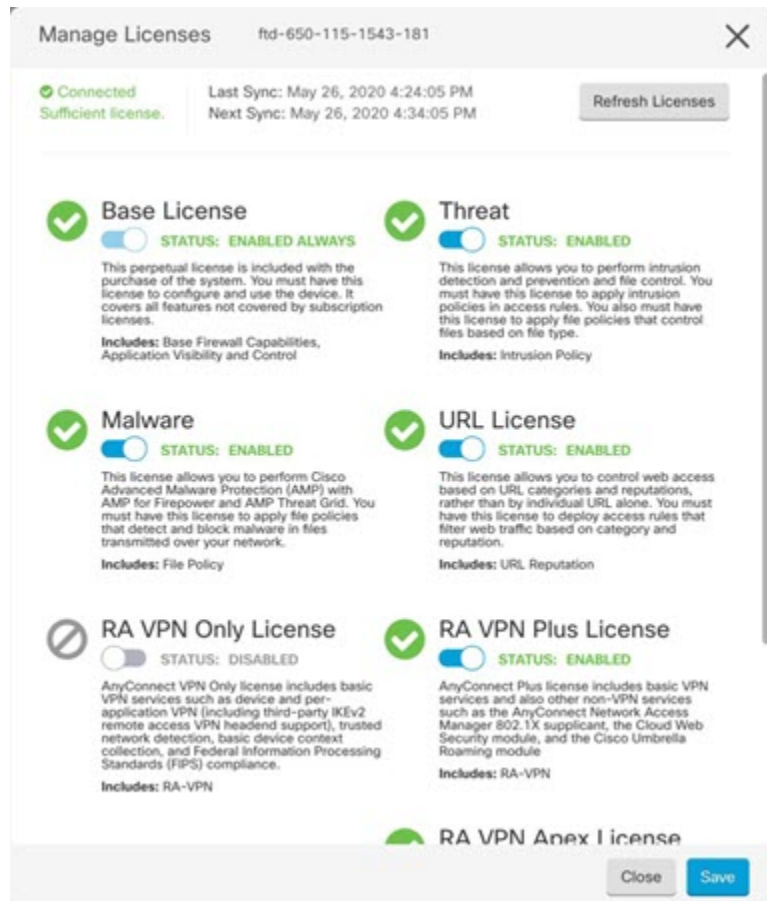
Step 3 In CDO, click **Devices & Services**, and then select the FTD device that you want to license.

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:

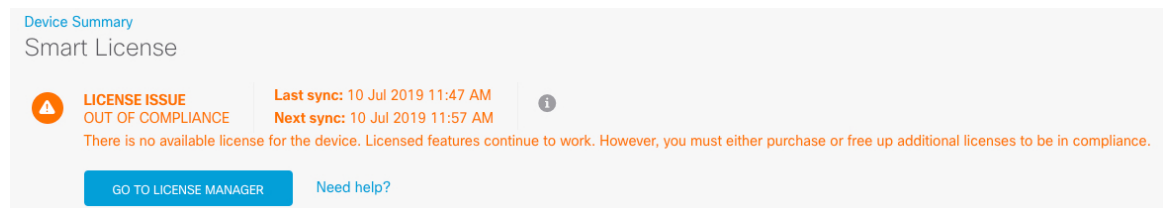
Registration request sent on 10 Jul 2019. Please wait. Normally, it takes about one minute to complete the registration. You can check the task status in [Task List](#). Refresh this page to see the updated status.

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.



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

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



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

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 2100 ships with a DB-9 to RJ-45 serial cable, so you will need a third party serial-to-USB cable to make the connection. Be sure to install any necessary USB serial drivers for your operating system. 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 Firewall Using FDM

You can shut down your system properly using FDM.

Procedure

Step 1 Use FDM to shut down the firewall.

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 If you have a console connection to the firewall, monitor the system prompts as the firewall shuts down. You will see the following prompt:

```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

If you do not have a console connection, wait approximately 3 minutes to ensure the system has shut down.

Step 3 You can now turn off the power switch and unplug the power to physically remove power from the chassis if necessary.

What's Next

To continue configuring your FTD using CDO, see the CDO [Configuration Guides](#).

For additional information related to using CDO, see the [Cisco Defense Orchestrator](#) home page.

