Firepower Threat Defense Deployment with CDO

Is This Chapter for You?

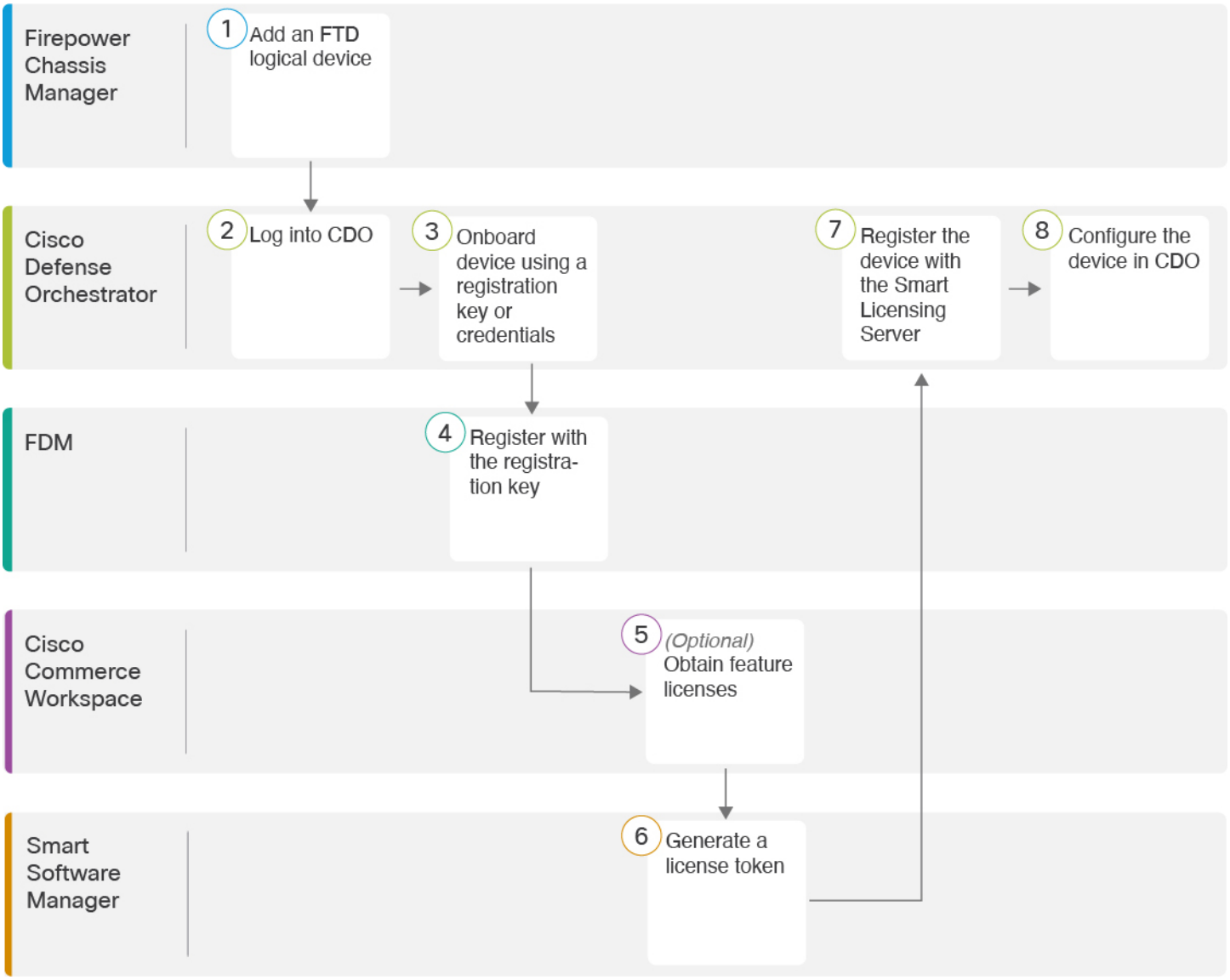
This chapter explains how to onboard a standalone FTD logical device to Cisco Defense Orchestrator (CDO) using CDO's onboarding wizard. To deploy a High Availability pair, see the FDM configuration guide.

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.

Privacy Collection Statement—The Firepower 9300 does not require or actively collect personally-identifiable information. However, you can use personally-identifiable information in the configuration, for example for usernames. In this case, an administrator might be able to see this information when working with the configuration or when using SNMP.

End-to-End Procedure

See the following tasks to deploy an FTD logical device and onboard the device to CDO.



	Workspace	Steps
1	Firepower Chassis Manager	Firepower Chassis Manager: Add a Firepower Threat Defense Logical Device, on page 4.
2	Cisco Defense Orchestrator	Log Into CDO with Cisco Secure Sign-On, on page 11.
3	Cisco Defense Orchestrator	Onboard the device using a registration key or credentials (Onboard the FTD to CDO, on page 12).
4	Firepower Device Manager	Register with the registration key (Onboard the FTD to CDO, on page 12). If you onboard using credentials, you do not need to log into FDM.

	Workspace	Steps
5	Cisco Commerce Workspace	(Optional) Obtain feature licenses (Configure Licensing, on page 19).
6	Smart Software Manager	Generate a license token for the FTD (Configure Licensing, on page 19).
7	Cisco Defense Orchestrator	Register the FTD with the Smart Licensing server, and enable feature licenses (Configure Licensing, on page 19).
8	Cisco Defense Orchestrator	Configure the Device in CDO, on page 24.

How Cisco Defense Orchestrator Works with Firepower Threat Defense

CDO and FDM Co-Management

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 recommended 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 Management interface, which can be a security risk.

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 Management interface for this method.

Firepower Chassis Manager: Add a Firepower Threat Defense Logical Device

You can deploy an FTD from the Firepower 9300 as a native instance. Container instances are not supported.

To add a High Availability pair, see the FDM configuration guide.

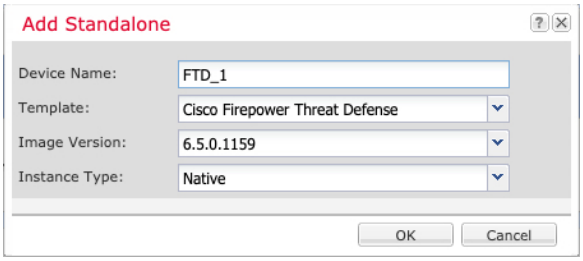
Before you begin

- Configure a Management interface to use with the FTD; see Configure Interfaces. The Management interface is required. Note that this Management interface is not the same as the chassis management port that is used only for chassis management (and that appears at the top of the **Interfaces** tab as **MGMT**).
- You must also configure at least one Data interface.
- Gather the following information:
  - Interface IDs for this device
  - Management interface IP address and network mask
  - Gateway IP address
  - DNS server IP address
  - FTD hostname and domain name

Procedure

Step 1 In Firepower Chassis Manager, choose **Logical Devices**.

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



a) Provide a **Device Name**.

This name is used by the chassis supervisor to configure management settings and to assign interfaces; it is not the device name used in the application configuration.

b) For the **Template**, choose **Cisco Firepower Threat Defense**.

c) Choose the **Image Version**.

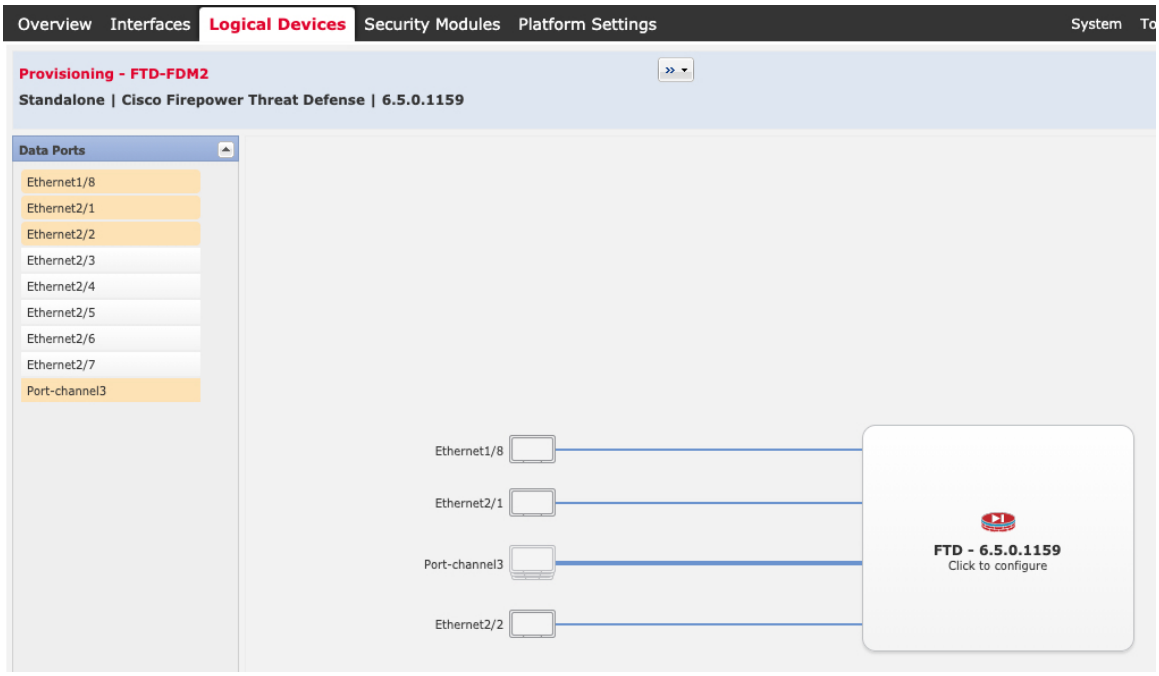
d) Choose the **Instance Type**: **Native**.

Container instances are not supported with FDM.

e) Click **OK**.

You see the Provisioning - *device name* window.

Step 3 Expand the **Data Ports** area, and click each interface that you want to assign to the device.

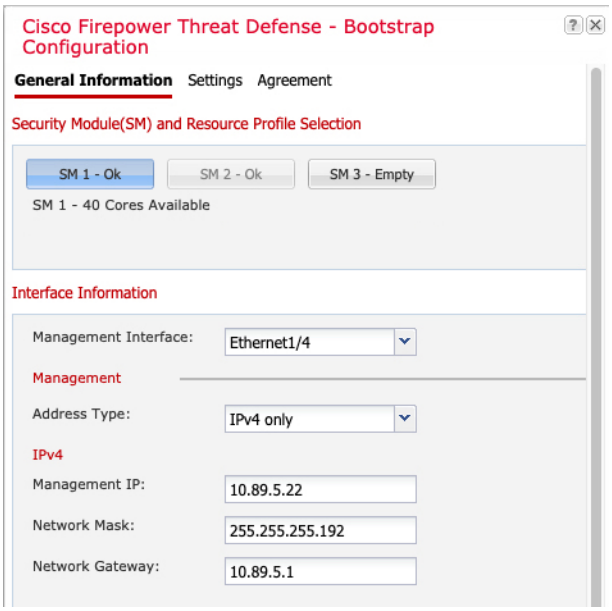


You can only assign data interfaces that you previously enabled on the **Interfaces** page. You will later enable and configure these interfaces in FDM, including setting the IP addresses.

Step 4 Click the device icon in the center of the screen.

A dialog box appears where you can configure initial bootstrap settings. These settings are meant for initial deployment only, or for disaster recovery. For normal operation, you can later change most values in the application CLI configuration.

Step 5 On the **General Information** page, complete the following:



a) (For the Firepower 9300) Under **Security Module Selection** click the security module that you want to use for this logical device.
b) Choose the **Management Interface**.

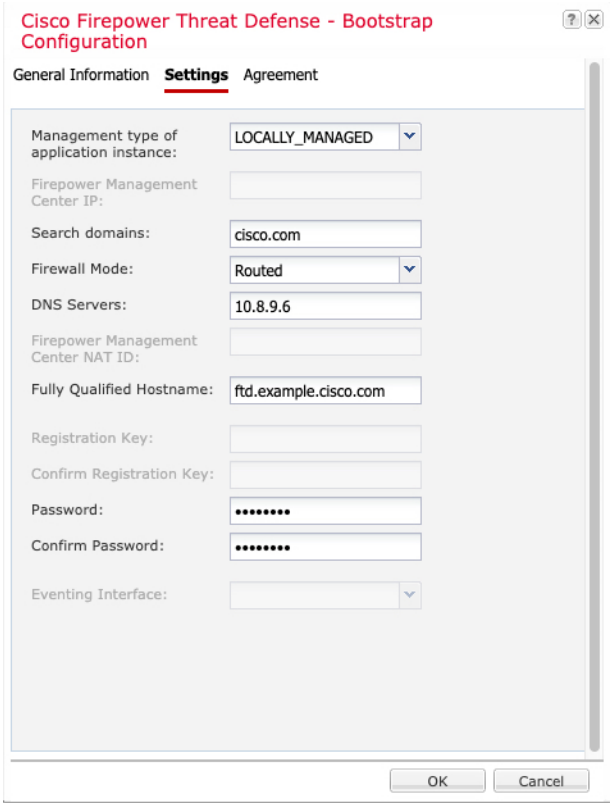
   This interface is used to manage the logical device. This interface is separate from the chassis management port.

c) Choose the management interface **Address Type**: **IPv4 only**, **IPv6 only**, or **IPv4 and IPv6**.
d) Configure the **Management IP** address.

   Set a unique IP address for this interface.

e) Enter a **Network Mask** or **Prefix Length**.
f) Enter a **Network Gateway** address.

Step 6 On the **Settings** tab, complete the following:



a) In the **Management type of application instance** drop-down list, choose **LOCALLY_MANAGED**.

   Native instances also support FMC as a manager. If you change the manager after you deploy the logical device, then your configuration is erased and the device is reinitialized.

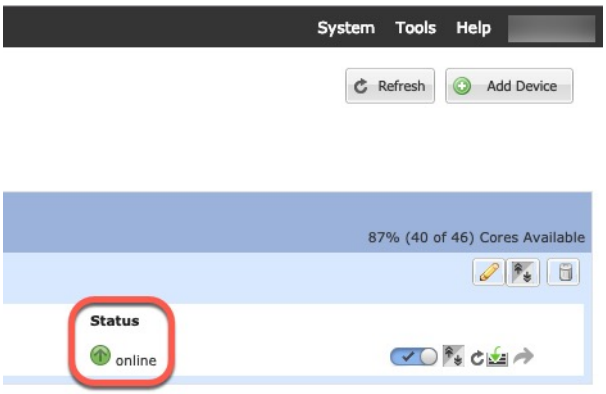
b) Enter the **Search Domains** as a comma-separated list.
c) The **Firewall Mode** only supports **Routed** mode.
d) Enter the **DNS Servers** as a comma-separated list.
e) Enter the **Fully Qualified Hostname** for the FTD.
f) Enter a **Password** for the FTD admin user for CLI access.

Step 7 On the **Agreement** tab, read and accept the end user license agreement (EULA).

Step 8 Click **OK** to close the configuration dialog box.

Step 9 Click **Save**.

The chassis deploys the logical device by downloading the specified software version and pushing the bootstrap configuration and management interface settings to the application instance. Check the **Logical Devices** page for the status of the new logical device. When the logical device shows its **Status** as **online**, you can start configuring the security policy in the application.



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 11.
- If you don't have a Cisco Secure Sign-On account, continue to Create a New Cisco Secure Sign-On Account, on page 8.

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.

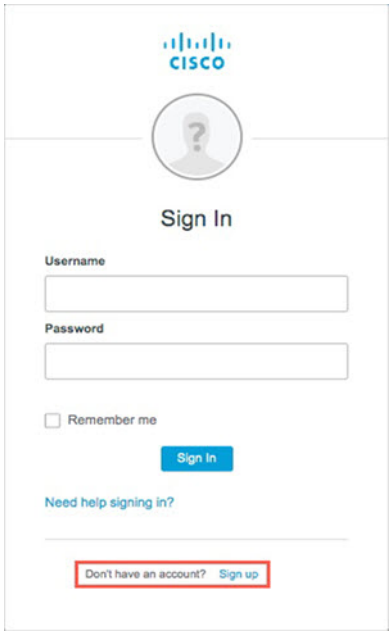
Procedure

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

a) Browse to https://sign-on.security.cisco.com.

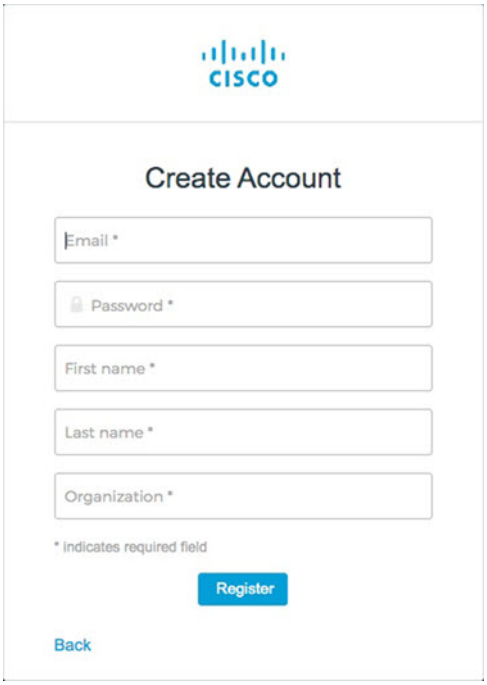
b) At the bottom of the Sign In screen, click **Sign up**.

Figure 1: Cisco SSO Sign Up



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

Figure 2: Create Account



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

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

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

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

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

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

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

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

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

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

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

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

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

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

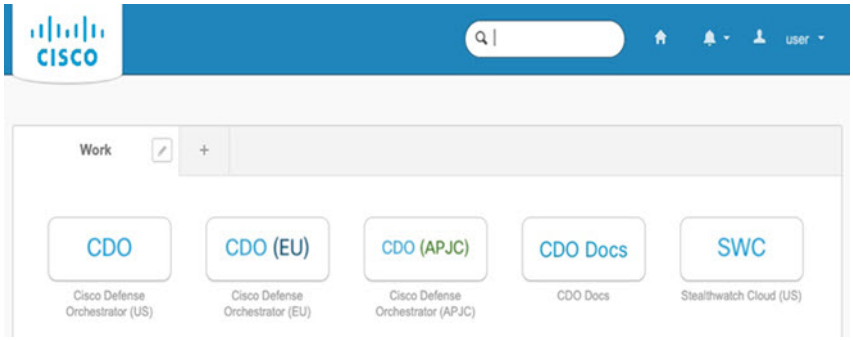
c) Choose a security image.

d) Click **Create My Account**.

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

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

Figure 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 8.
- Use a current version of Firefox or Chrome.

Procedure

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

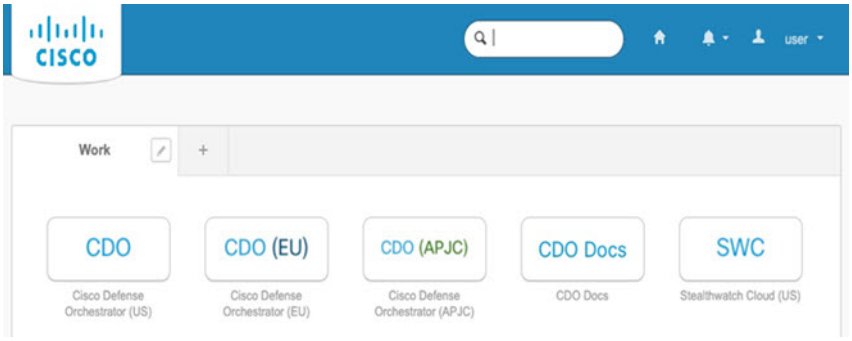
Step 2 Enter your **Username** and **Password**.

Step 3 Click **Log in**.

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

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

Figure 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 FTD to CDO

Use CDO's onboarding wizard to onboard your firewall.

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.
- Make sure the FTD logical device **Status** is **online** on the Firepower Chassis Manager **Logical Devices** page.

Procedure

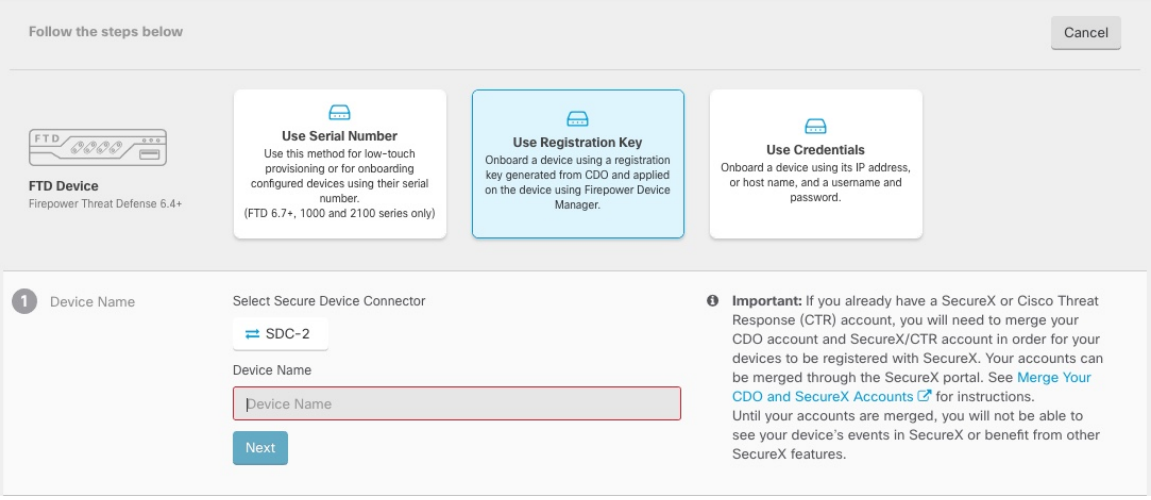
Step 1 In the CDO navigation pane, click **Devices & Services**, then click the blue plus button ( ) to **Onboard** a device.

Step 2 Click the **FTD** card.

Step 3 Click **Use Registration Key**.

Step 4 Complete the **Device Name** area fields.

Figure 5: Device Name



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) Enter the following URL in your browser to launch FDM: **https://***ftd_management_ip*. Enter the interface IP address that you entered in the bootstrap configuration.
b) Log in with the username **admin**, and the password you set when you deployed the FTD.
c) You are prompted to accept the 90-day evaluation license.
d) Under **System Settings**, click **Cloud Services**.
e) 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.
f) In the **Enrollment Type** area, click **Security/CDO Account**.

   For 6.6, this tab is called **Security Account**.

g) (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.

h) 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*.

i) In the **Registration Key** field, paste the registration key that you generated in CDO.
j) (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.m, on page 15).

k) (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.

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

m) (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 19. 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 6.5)

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

Before you begin

- This method is supported for the US, EU, and APJ (apj.cdo.cisco.com) 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 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.
- Make sure the FTD logical device **Status** is **online** on the Firepower Chassis Manager **Logical Devices** page.

Procedure

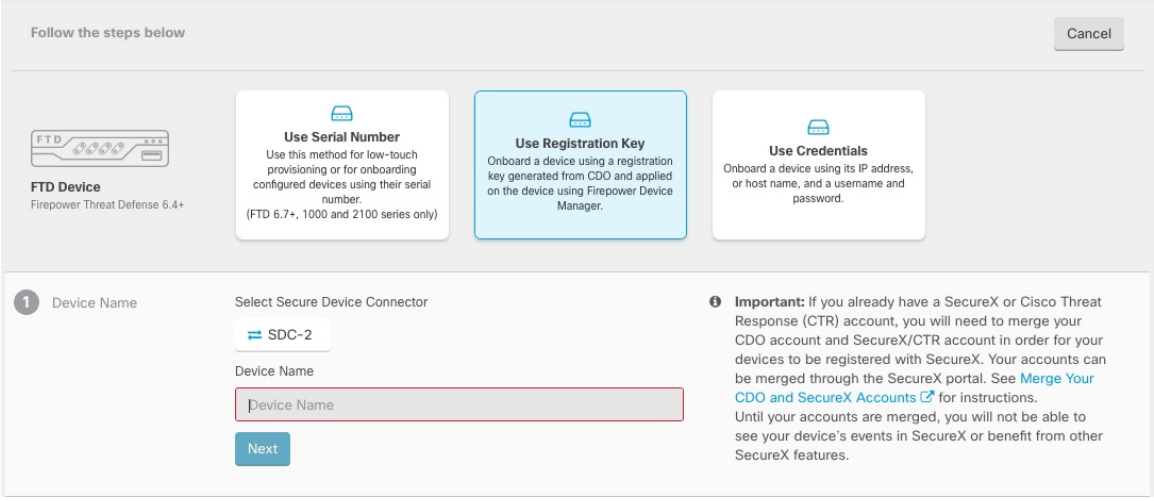
Step 1 In the CDO navigation pane, click **Devices & Services**, then click the blue plus button () to **Onboard** a device.

Step 2 Click the **FTD** card.

Step 3 Click **Use Registration Key**.

Step 4 Complete the **Device Name** area fields.

Figure 6: Device Name



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) Enter the following URL in your browser to launch FDM: **https://***ftd_management_ip*. Enter the interface IP address that you entered in the bootstrap configuration.
b) Log in with the username **admin**, and the password you set when you deployed the FTD.
c) You are prompted to accept the 90-day evaluation license.
d) Under **System Settings**, click **Cloud Services**.
e) Click **Get Started** in the **Cisco Defense Orchestrator** group.
f) 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).

g) In the **Registration Key** field, paste the registration key that you generated in CDO.
h) 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 19. 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 12.

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 Management interface.
- Make sure the FTD logical device **Status** is **online** on the Firepower Chassis Manager **Logical Devices** page.

Procedure

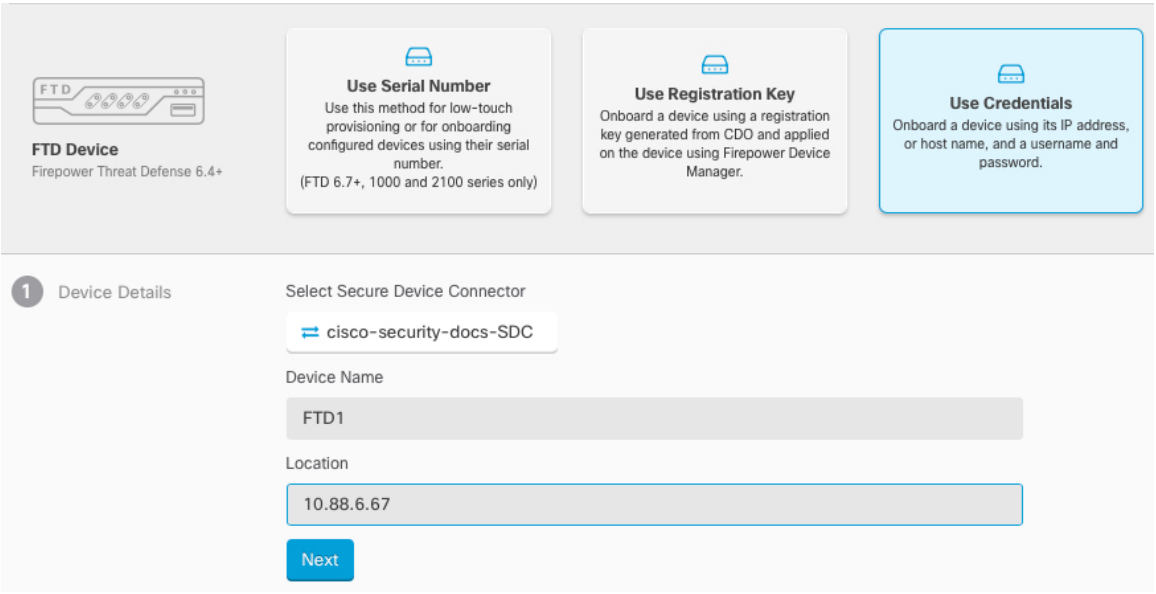
Step 1 In the CDO navigation pane, click **Devices & Services**, then click the blue plus button ( ) to **Onboard** a device.

Step 2 Click the **FTD** card.

Step 3 Click **Use Credentials**.

Step 4 Complete the **Device Name** area fields.

Figure 7: Device Name



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) 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.

d) 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 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.

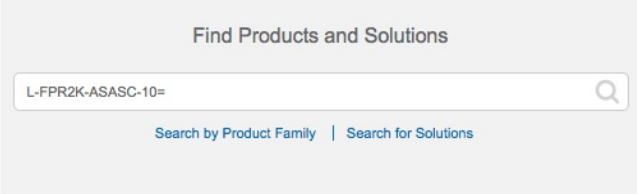
- Your Smart Software Licensing account must qualify for the Strong Encryption (3DES/AES) license to use some features (enabled using the export-compliance flag).

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 8: 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-FPR9K-24T-TMC=
  - L-FPR9K-36T-TMC=
  - L-FPR9K-40T-TMC=
  - L-FPR9K-44T-TMC=
  - L-FPR9K-48T-TMC=
  - L-FPR9K-56T-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-FPR9K-24T-TMC-1Y
  - L-FPR9K-24T-TMC-3Y
  - L-FPR9K-24T-TMC-5Y
  - L-FPR9K-36T-TMC-1Y
  - L-FPR9K-36T-TMC-3Y
  - L-FPR9K-36T-TMC-5Y
  - L-FPR9K-40T-TMC-1Y
  - L-FPR9K-40T-TMC-3Y
  - L-FPR9K-40T-TMC-5Y
  - L-FPR9K-44T-TMC-1Y
  - L-FPR9K-44T-TMC-3Y
  - L-FPR9K-44T-TMC-5Y
  - L-FPR9K-48T-TMC-1Y
  - L-FPR9K-48T-TMC-3Y
  - L-FPR9K-48T-TMC-5Y
  - L-FPR9K-56T-TMC-1Y
  - L-FPR9K-56T-TMC-3Y

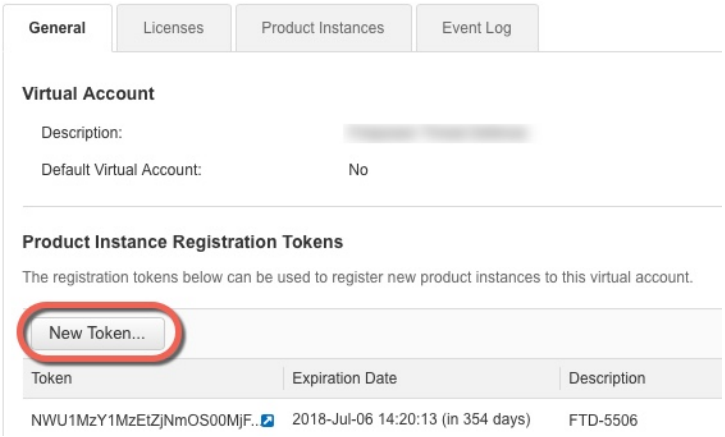
- L-FPR9K-56T-TMC-5Y

- RA VPN—See the Cisco AnyConnect Ordering Guide.

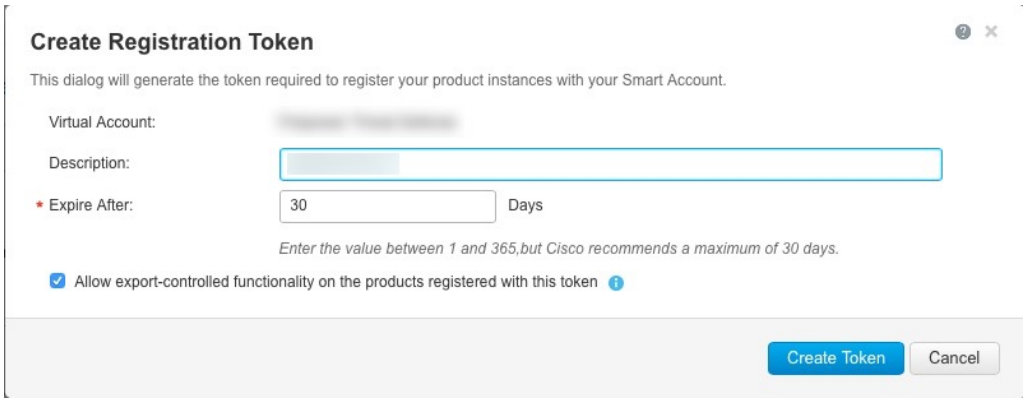
Step 2 In the Smart Software Manager, request and copy a registration token for the virtual account to which you want to add this device.

a) Click **Inventory**.

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



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



- **Description**
- **Expire After**—Cisco recommends 30 days.
- **Allow export-controlled 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 9: View Token

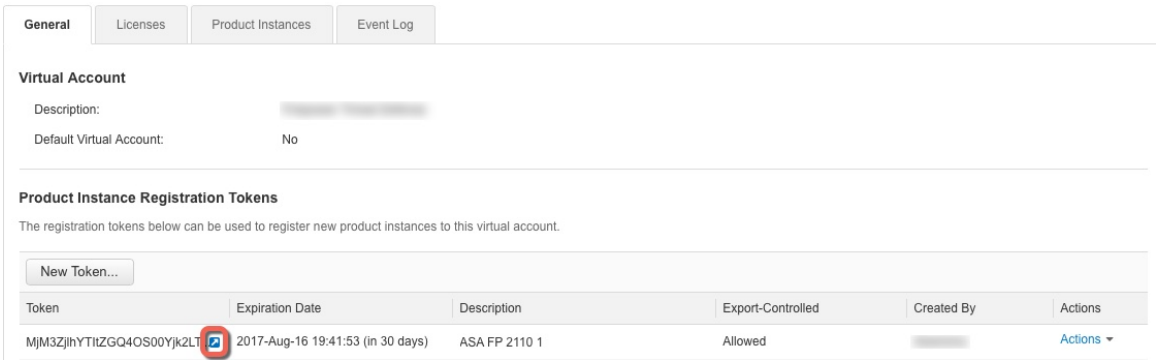
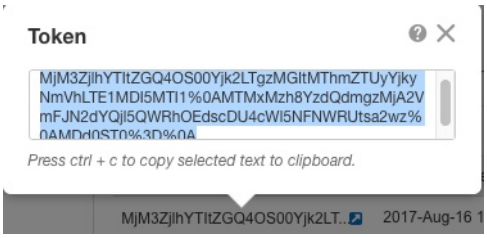


Figure 10: Copy Token



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

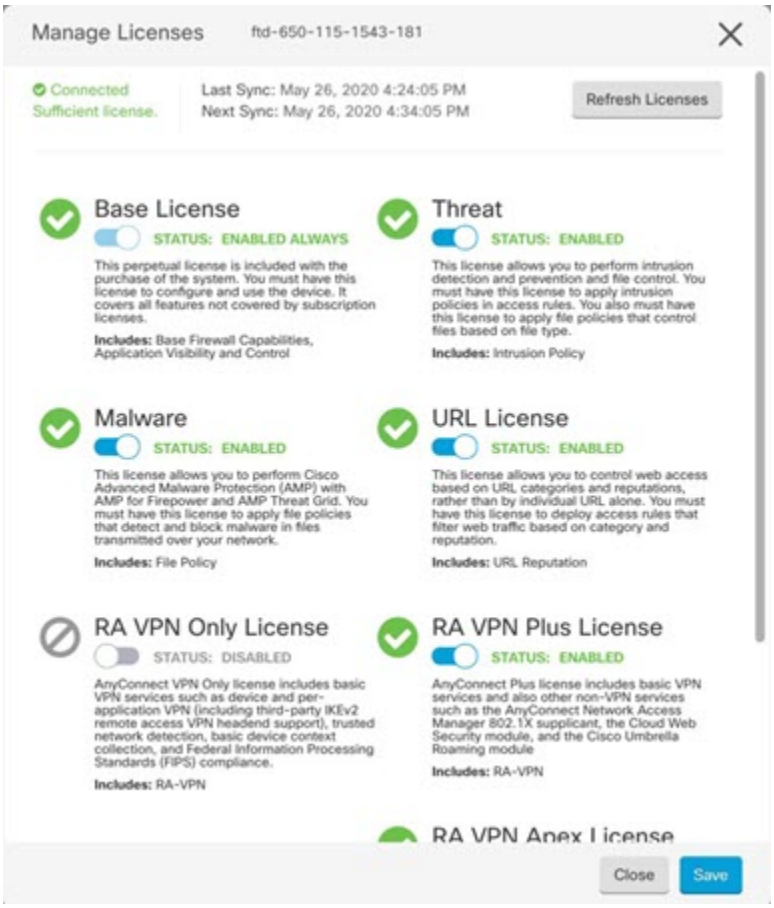
Step 4 In the **Device Actions** pane, click **Manage Licenses**, and follow the on-screen instructions to enter the smart-license generated from Smart Software Manager.

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:

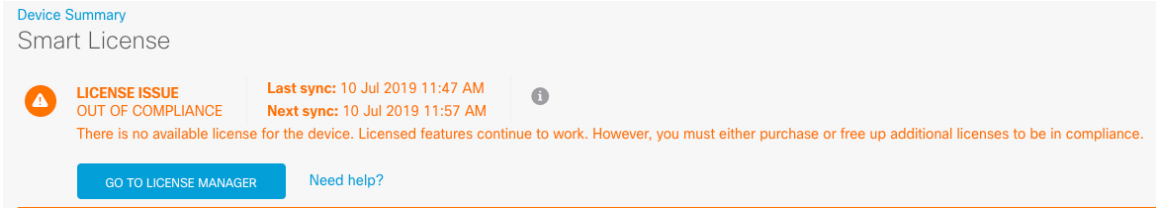
Registration request sent on 10 Jul 2019. Please wait. Normally, it takes about one minute to complete the registration. You can check the task status in Task List. Refresh this page to see the updated status.

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.



- **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.

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**.

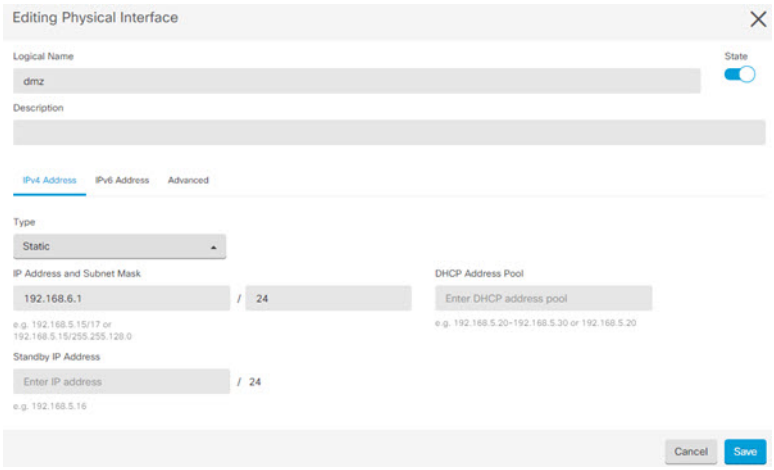
Unless you configure subinterfaces, the interface should have a name.

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

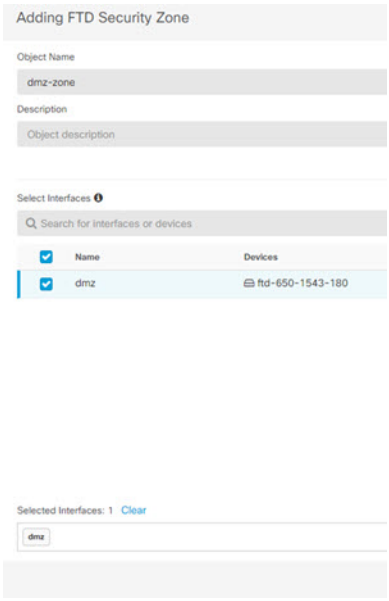


Step 5 If you configured new interfaces, choose **Management** > **Objects**.

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



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

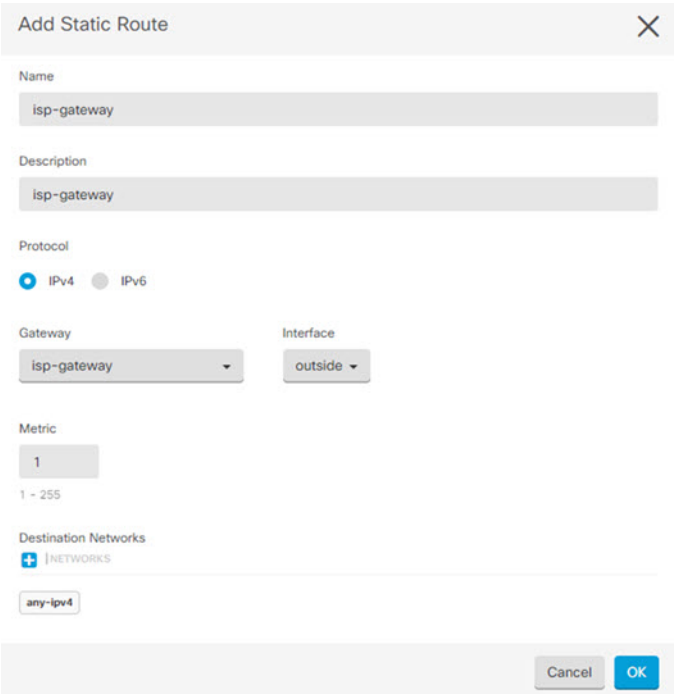
Step 7 Choose **Management** > **Routing**, then click the Add icon to configure a default route.

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



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.

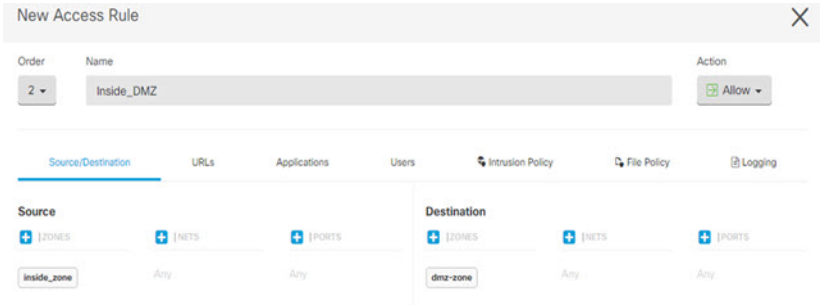
In addition, you can configure other policies to provide additional services, and fine-tune NAT and access rules to get the results that your organization requires. You can configure the following policies:

- **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.

Access the Firepower Threat Defense CLI

You can use the FTD CLI to change management interface parameters and for troubleshooting purposes. You can access the CLI using SSH to the Management interface, or by connecting from the FXOS CLI.

Procedure

Step 1 (Option 1) SSH directly to the FTD management interface IP address.

You set the management IP address when you deployed the logical device. Log into the FTD with the admin account and the password you set during initial deployment.

If you forgot the password, you can change it by editing the logical device in the Firepower Chassis Manager.

Step 2 (Option 2) From the FXOS CLI, connect to the module CLI using a console connection or a Telnet connection.

a) Connect to the security module.

connect module *slot_number* {**console** | **telnet**}

The benefits of using a Telnet connection is that you can have multiple sessions to the module at the same time, and the connection speed is faster.

Example:

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

b) Connect to the FTD console.

connect ftd *name*

If you have multiple application instances, you must specify the name of the instance. To view the instance names, enter the command without a name.

Example:

```
Firepower-module1> connect ftd FTD_Instance1

============================ ATTENTION ==============================
You are connecting to ftd from a serial console. Please avoid
executing any commands which may produce large amount of output.
Otherwise, data cached along the pipe may take up to 12 minutes to be
drained by a serial console at 9600 baud rate after pressing Ctrl-C.

To avoid the serial console, please login to FXOS with ssh and use
'connect module <slot> telnet' to connect to the security module.
=====================================================================

Connecting to container ftd(FTD_Instance1) console... enter "exit" to return to bootCLI
>
```

c) Exit the application console to the FXOS module CLI by entering **exit**.

Note For pre-6.3 versions, enter **Ctrl-a, d**.

d) Return to the supervisor level of the FXOS CLI.

To exit the console:

1. Enter **~**

   You exit to the Telnet application.

2. To exit the Telnet application, enter:

   telnet>**quit**

To exit the Telnet session:

Enter **Ctrl-], .**

Example

The following example connects to an FTD on security module 1 and then exits back to the supervisor level of the FXOS CLI.

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>connect ftd FTD_Instance1

============================ ATTENTION ============================
You are connecting to ftd from a serial console. Please avoid
executing any commands which may produce large amount of output.
Otherwise, data cached along the pipe may take up to 12 minutes to be
drained by a serial console at 9600 baud rate after pressing Ctrl-C.

To avoid the serial console, please login to FXOS with ssh and use
'connect module <slot> telnet' to connect to the security module.
===================================================================

Connecting to container ftd(FTD_Instance1) console... enter "exit" to return to bootCLI
> ~
telnet> quit
Connection closed.
Firepower#
```

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.

History for FTD with CDO

Feature Name	Version	Feature Information
Support for CDO with native instances	6.5.0	You can now onboard and manage a native instance using CDO.