Firepower Threat Defense Deployment with CDO and Low-Touch Provisioning

Is This Chapter for You?

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

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

Note This feature requires Firepower version 6.7 or later.

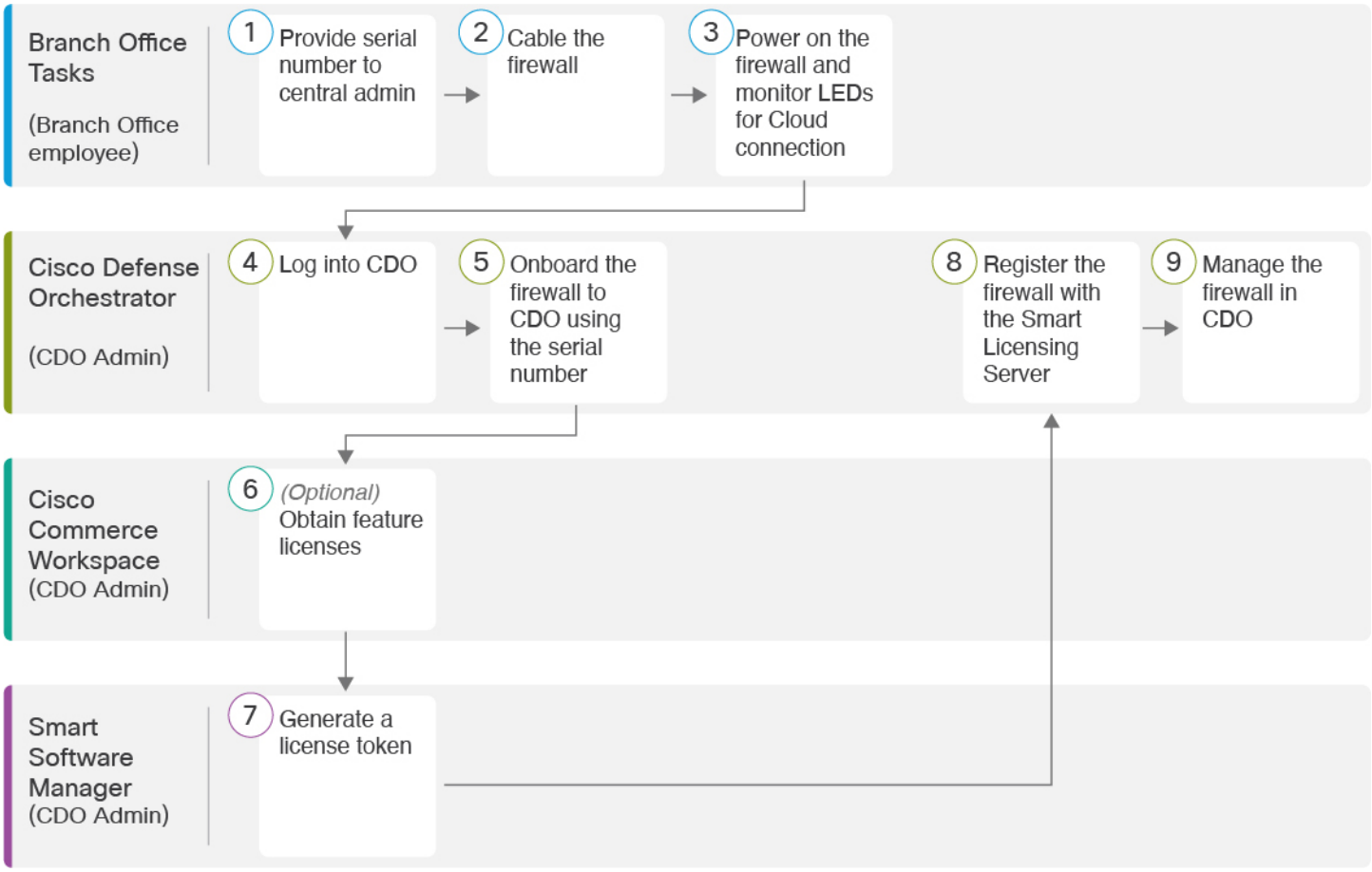
This document assumes the Firepower 2100 hardware has a pre-installed FTD image on it. The Firepower 2100 hardware can run either FTD software or ASA software. Switching between FTD and ASA requires you to reimage the device. See Reimage the Cisco ASA or Firepower Threat Defense Device.

The Firepower 2100 runs an underlying operating system called the Firepower eXtensible Operating System (FXOS). The Firepower 2100 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 Firepower 2100 Series does not require or actively collect personally-identifiable information. However, you can use personally-identifiable information in the configuration, for example for usernames. In this case, an administrator might be able to see this information when working with the configuration or when using SNMP.

End-to-End Procedure

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



1	Branch Office Tasks (Branch Office Employee)	Provide the Firewall Serial Number to the Central Administrator, on page 3.
2	Branch Office Tasks (Branch Office Employee)	Cable the Device, on page 4.
3	Branch Office Tasks (Branch Office Employee)	Power On the Device, on page 5.
4	Cisco Defense Orchestrator (CDO Admin)	Log Into CDO with Cisco Secure Sign-On, on page 9.

5	Cisco Defense Orchestrator (CDO Admin)	Onboard the Device Using Low-Touch Provisioning and the Serial Number, on page 11.
6	Cisco Commerce Workspace (CDO Admin)	(Optional) Obtain feature licenses (Configure Licensing, on page 12).
7	Smart Software Manager (CDO Admin)	Generate a license token (Configure Licensing, on page 12).
8	Cisco Defense Orchestrator (CDO Admin)	Register the device with the Smart Licensing Server (Configure Licensing, on page 12).
9	Cisco Defense Orchestrator (CDO Admin)	Manage the Device with CDO, on page 17.

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 adminstrator.

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.

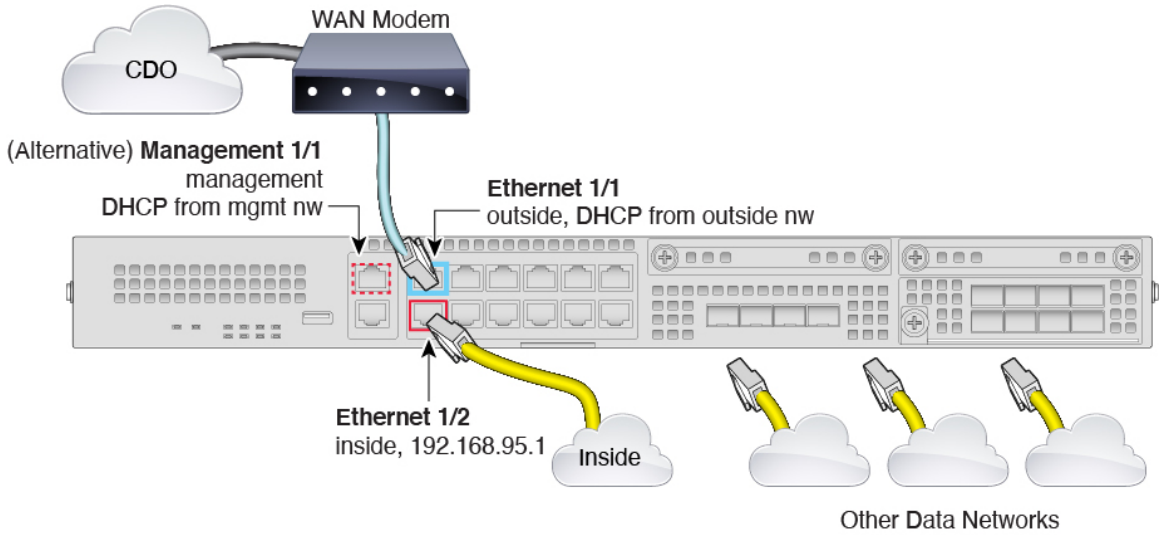
Cable the Device

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 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. The outside Ethernet 1/1 interface only supports IPv4 for low-touch provisioning.

Step 2 Connect the inside network to Ethernet 1/2.

Step 3 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.

Before you begin

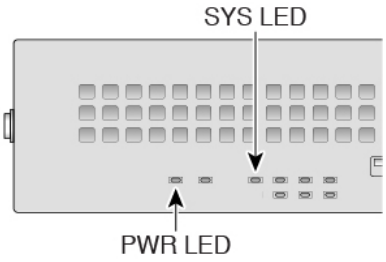
It's important that you provide reliable power for your device (for example, using an uninterruptable power supply (UPS)). Loss of power without first shutting down can cause serious file system damage. There are many processes running in the background all the time, and losing power does not allow the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

CDO Administrator Onboarding and Management

After the remote branch administrator sends the serial number information to the central headquarters, the CDO administrator onboards the FTD to CDO. When you onboard the firewall in CDO using the serial number, the firewall is associated with your CDO tenant in the Cisco cloud.

After the branch office administrator cables and powers on the FTD, the firewall connects to the Cisco cloud, and CDO syncs the firewall's configuration automatically.

You can then license your firewall, and configure and manage your firewall with CDO.

Log Into CDO

CDO uses Cisco Secure Sign-On as its identity provider and Duo Security for multi-factor authentication (MFA). CDO requires MFA which provides an added layer of security in protecting your user identity. Two-factor authentication, a type of MFA, requires two components, or factors, to ensure the identity of the user logging into CDO.

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

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

- If you have a Cisco Secure Sign-On account, skip ahead to Log Into CDO with Cisco Secure Sign-On, on page 9.
- If you don't have a Cisco Secure Sign-On account, continue to Create a New Cisco Secure Sign-On Account.

Create a New Cisco Secure Sign-On Account

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

Before you begin

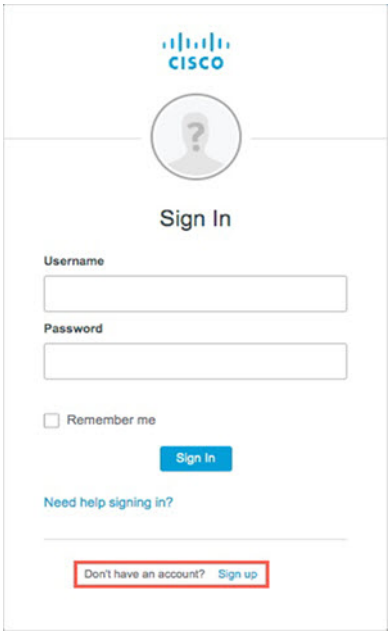
- **Install DUO Security—**We recommend that you install the Duo Security app on a mobile phone. Review Duo Guide to Two Factor Authentication: Enrollment Guide if you have questions about installing Duo.
- **Time Synchronization—**You are going to use your mobile device to generate a one-time password.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

Procedure

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

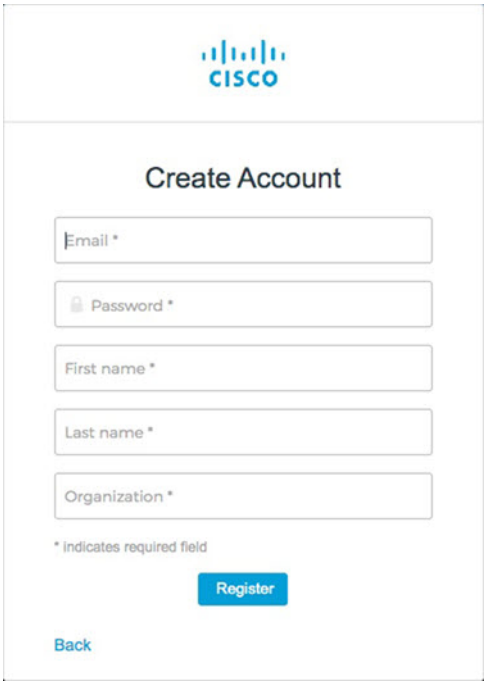
a) Browse to https://sign-on.security.cisco.com.
b) At the bottom of the Sign In screen, click **Sign up**.

Figure 2: Cisco SSO Sign Up



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

Figure 3: Create Account



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

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

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

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

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

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

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

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

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

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

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

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

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

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

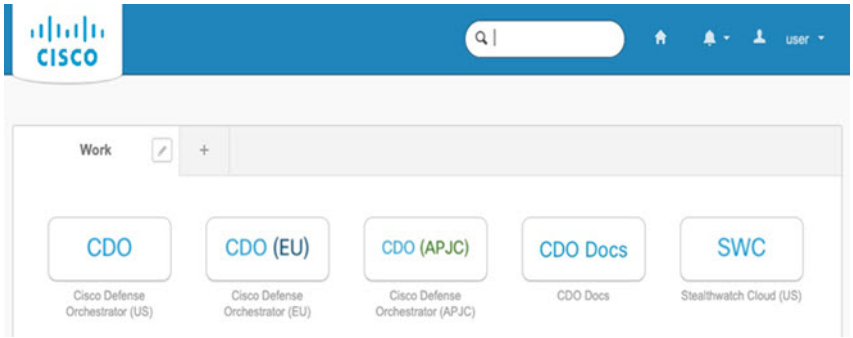
c) Choose a security image.

d) Click **Create My Account**.

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

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

Figure 4: Cisco SSO Dashboard



Log Into CDO with Cisco Secure Sign-On

Log into CDO to onboard and manage your FTD.

Before you begin

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

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

Procedure

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

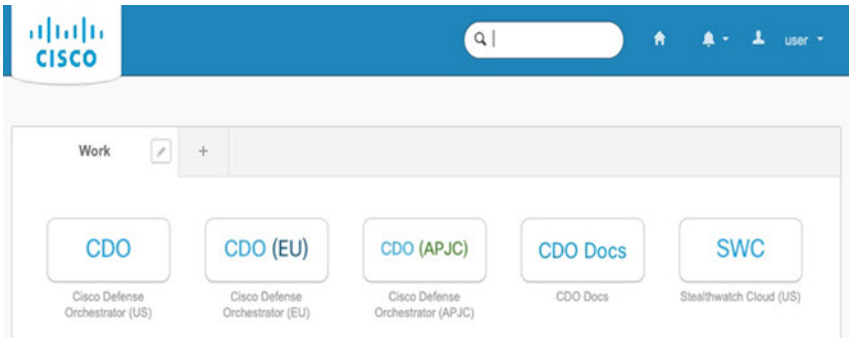
Step 2 Enter your **Username** and **Password**.

Step 3 Click **Log in**.

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

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

Figure 5: Cisco SSO Dashboard



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

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

Onboard the Device 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:

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

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

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

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

Step 5 Click **Next**.

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

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

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

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

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

Step 7 Click **Next**.

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

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

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

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

Step 9 Click **Next**.

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

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

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

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

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

What to do next

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

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.

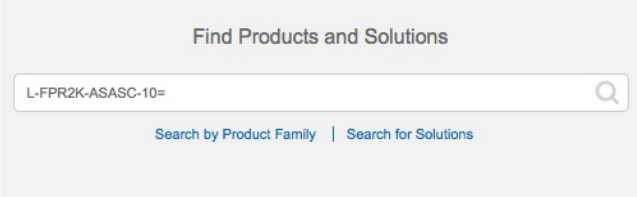
- Your Smart Software Licensing account must qualify for the Strong Encryption (3DES/AES) license to use some features (enabled using the export-compliance flag).

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 6: License Search



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

- Threat, Malware, and URL license combination:
  - L-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

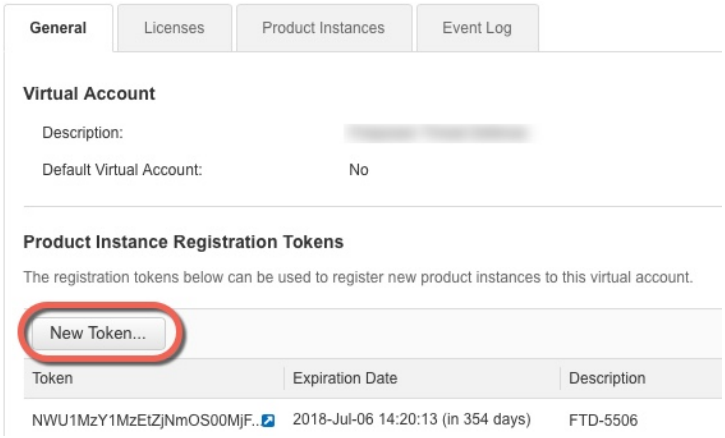
- L-FPR2130T-TMC-5Y
- L-FPR2140T-TMC-1Y
- L-FPR2140T-TMC-3Y
- L-FPR2140T-TMC-5Y

- RA VPN—See the Cisco AnyConnect Ordering Guide.

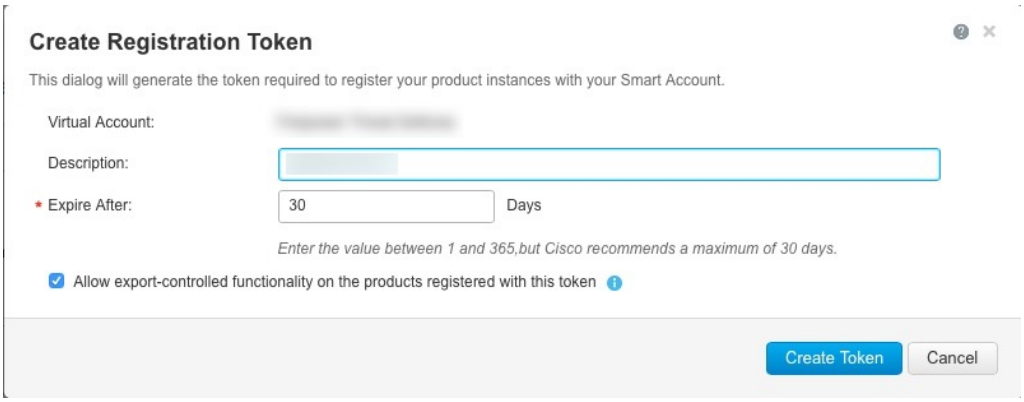
Step 2 In the Smart Software Manager, request and copy a registration token for the virtual account to which you want to add this device.

a) Click **Inventory**.

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



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



- **Description**

- **Expire After**—Cisco recommends 30 days.
- **Allow export-controlled functionaility on the products registered with this token**—Enables the export-compliance flag if you are in a country that allows for strong encryption. 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 7: View Token

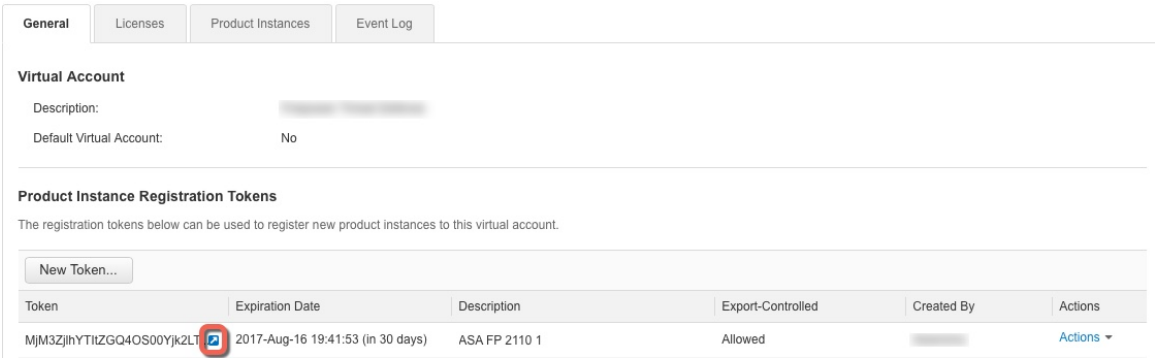
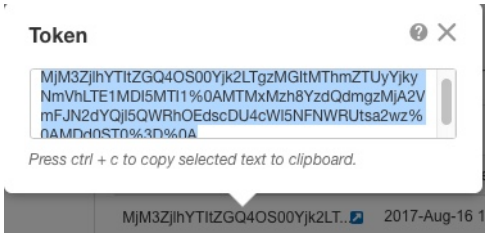


Figure 8: Copy Token



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

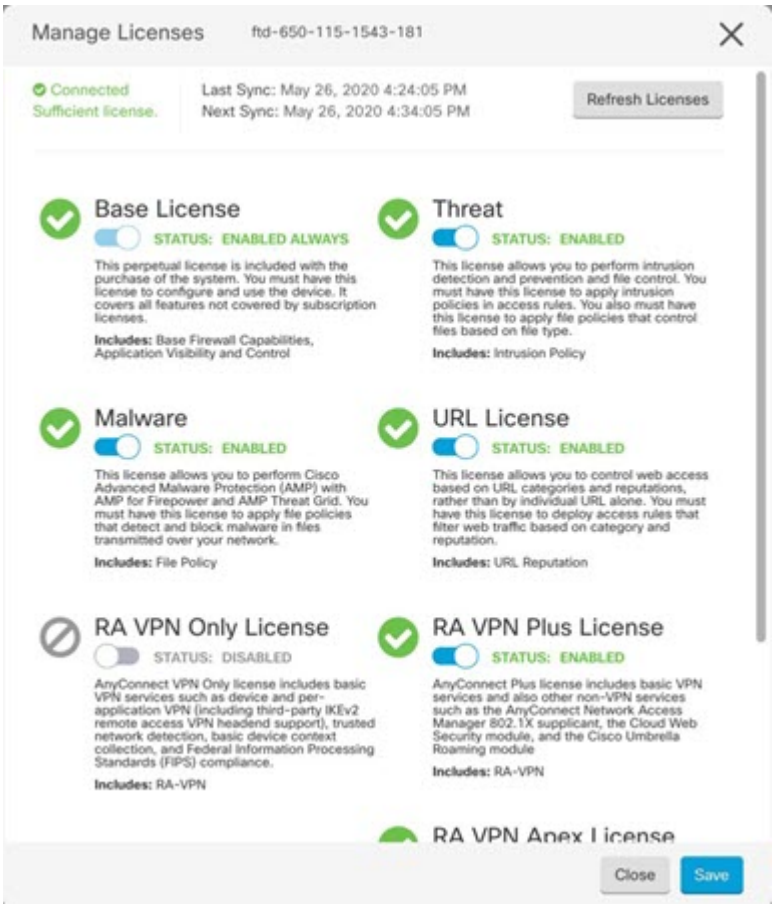
Step 4 In the **Device Actions** pane, click **Manage Licenses**, and follow the on-screen instructions to enter the smart-license generated from Smart Software Manager.

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

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

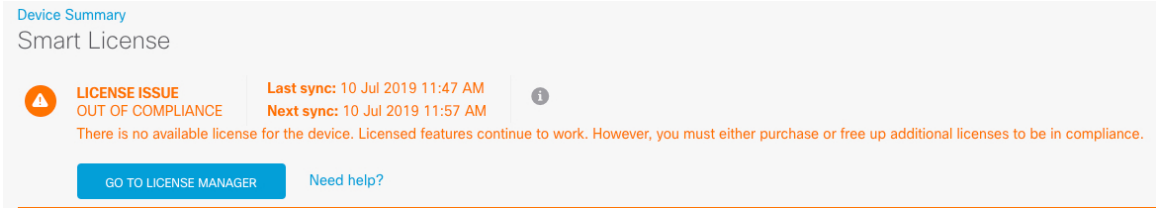
Registration request sent on 10 Jul 2019. Please wait. Normally, it takes about one minute to complete the registration. You can check the task status in Task List. Refresh this page to see the updated status.

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



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

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



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

Manage the Device with CDO

After onboarding the firewall to CDO, you can manage the firewall with CDO. To manage the FTD with CDO:

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

What to do Next

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