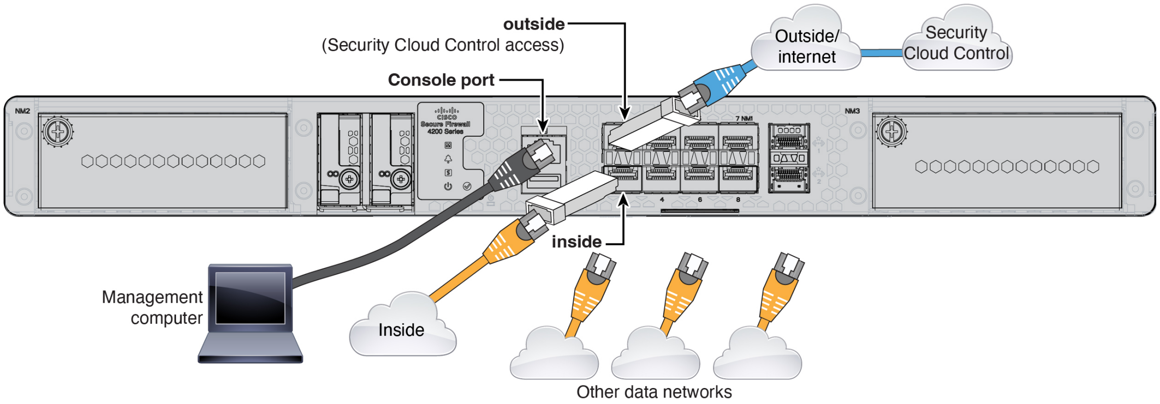
Cable and Onboard the Firewall

Cable and onboard the firewall to Security Cloud Control.

- Cable the Firewall, on page 1
- Onboard the Firewall, on page 1
- Perform Initial Configuration, on page 4

Cable the Firewall

- Obtain a console cable—The firewall does not ship with a console cable by default, so you will need to buy a third-party USB-to-RJ-45 serial cable, for example.
- Install SFPs into the data interface ports—The built-in ports are 1/10/25-Gb SFP28 ports that require SFP/SFP+/SFP28 modules.
- See the hardware installation guide for more information.



Onboard the Firewall

Onboard the firewall using a CLI registration key.

Procedure

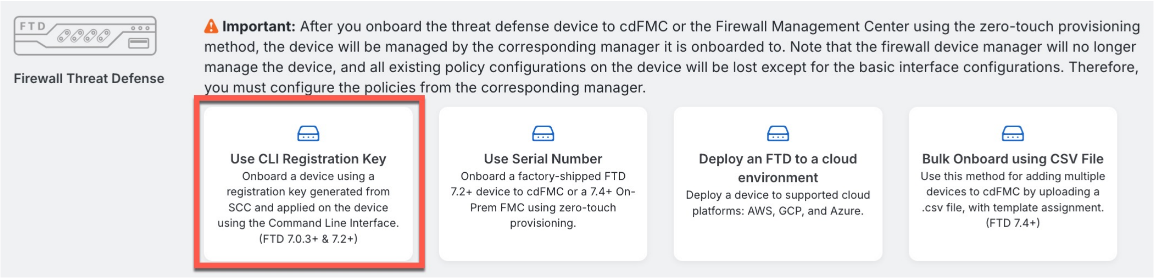
Step 1 In the Security Cloud Control navigation menu, click **Manage** > **Security Devices**, then click the blue plus button (+) to **Onboard** a device.

Step 2 Click the **FTD** tile.

Step 3 Under **Management Mode**, be sure **FTD** is selected.

Step 4 Select **Use CLI Registration Key** as the onboarding method.

Figure 1: Use CLI Registration Key



Firewall Threat Defense

⚠ **Important:** After you onboard the threat defense device to cdFMC or the Firewall Management Center using the zero-touch provisioning method, the device will be managed by the corresponding manager it is onboarded to. Note that the firewall device manager will no longer manage the device, and all existing policy configurations on the device will be lost except for the basic interface configurations. Therefore, you must configure the policies from the corresponding manager.

Use CLI Registration Key
Onboard a device using a registration key generated from SCC and applied on the device using the Command Line Interface. (FTD 7.0.3+ & 7.2+)

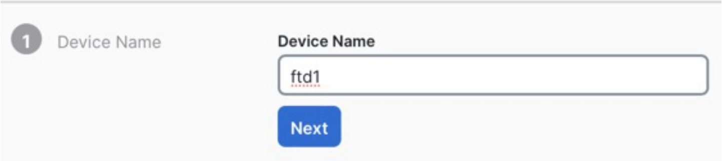
Use Serial Number
Onboard a factory-shipped FTD 7.2+ device to cdFMC or a 7.4+ On-Prem FMC using zero-touch provisioning.

Deploy an FTD to a cloud environment
Deploy a device to supported cloud platforms: AWS, GCP, and Azure.

Bulk Onboard using CSV File
Use this method for adding multiple devices to cdFMC by uploading a .csv file, with template assignment. (FTD 7.4+)

Step 5 Enter the **Device Name** and click **Next**.

Figure 2: Device Name



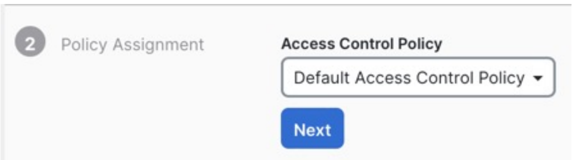
1 Device Name

Device Name: ftd1

Next

Step 6 For the **Policy Assignment**, use the drop-down menu to choose an access control policy for the device. If you have no policies configured, choose the **Default Access Control Policy**.

Figure 3: Access Control Policy



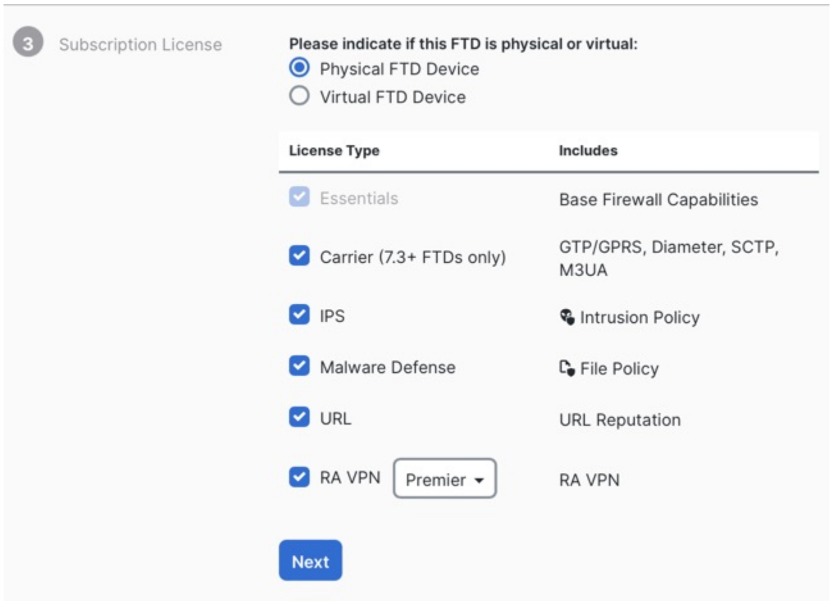
2 Policy Assignment

Access Control Policy: Default Access Control Policy

Next

Step 7 For the **Subscription License**, click the **Physical FTD Device** radio button, and then check each of the feature licenses you want to enable. Click **Next**.

Figure 4: Subscription License



3 Subscription License

Please indicate if this FTD is physical or virtual:

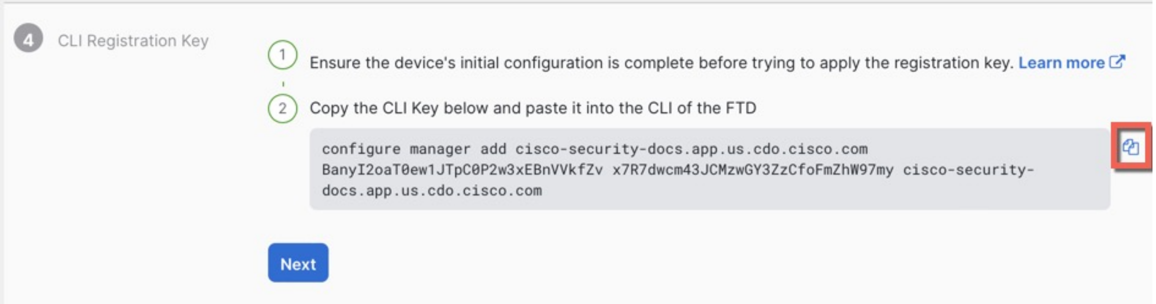
● Physical FTD Device

○ Virtual FTD Device

License Type	Includes
☑ Essentials	Base Firewall Capabilities
☑ Carrier (7.3+ FTDs only)	GTP/GPRS, Diameter, SCTP, M3UA
☑ IPS	Intrusion Policy
☑ Malware Defense	File Policy
☑ URL	URL Reputation
☑ RA VPN Premier ▾	RA VPN

Step 8 For the **CLI Registration Key**, Security Cloud Control generates a command with the registration key and other parameters. You must copy this command and use it in the intial configuration of the Firewall Threat Defense.

Figure 5: CLI Registration Key



4 CLI Registration Key

1 Ensure the device's initial configuration is complete before trying to apply the registration key. Learn more

2 Copy the CLI Key below and paste it into the CLI of the FTD

```
configure manager add cisco-security-docs.app.us.cdo.cisco.com
BanyI2oaT0ew1JTpC0P2w3xEBnVVkfZv x7R7dwcm43JCMzwGY3ZzCfoFmZhW97my cisco-security-
docs.app.us.cdo.cisco.com
```

configure manager add Security Cloud Control_*hostname registration_key nat_id display_name*

Copy this command at the Firewall Threat Defense CLI after you complete the startup script. See Perform Initial Configuration, on page 4.

Example:

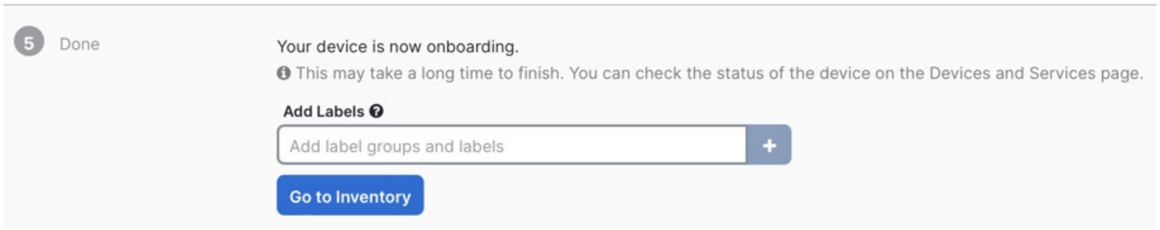
Sample command for CLI setup:

```
configure manager add account1.app.us.scc.cisco.com KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
Lzm1HOynhVUWhXYWz2swmkj2ZWsN3Lb account1.app.us.scc.cisco.com
```

Step 9 Click **Next** in the onboarding wizard to start registering the device.

Step 10 (Optional) Add labels to your device to help sort and filter the **Security Devices** page. Enter a label and select the blue plus button (+). Labels are applied to the device after it's onboarded to Security Cloud Control.

Figure 6: Done



5 Done

Your device is now onboarding.

ℹ This may take a long time to finish. You can check the status of the device on the Devices and Services page.

Perform Initial Configuration

Set the dedicated Management IP address, gateway, and other basic networking settings using the CLI setup script.

Procedure

Connect to the console port and access the Firewall Threat Defense CLI. See Access the Firewall Threat Defense CLI.