



# Threat Defense Deployment with CDO

## Is This Chapter for You?

To see all available operating systems and managers, see [Which Application and Manager is Right for You?](#). This chapter applies to the threat defense using Cisco Defense Orchestrator (CDO)'s cloud-delivered Secure Firewall Management Center. To use CDO using device manager functionality, see the CDO documentation.



---

**Note** The cloud-delivered management center supports threat defense 7.2 and later. For earlier versions, you can use CDO's device manager functionality. However, device manager mode is only available to existing CDO users who are already managing threat defenses using this mode.

---

Each threat defense controls, inspects, monitors, and analyzes traffic. CDO provides a centralized management console with a web interface that you can use to perform administrative and management tasks in service to securing your local network.

## About the Firewall

The hardware can run either threat defense software or ASA software. Switching between threat defense 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 Secure Firewall eXtensible Operating System (FXOS). The firewall does not support the FXOS Secure Firewall chassis manager; only a limited CLI is supported for troubleshooting purposes. See the [Cisco FXOS Troubleshooting Guide for the Firepower 1000/2100 and Secure Firewall 3100 with Firepower Threat Defense](#) 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.

- [About Threat Defense Management by CDO, on page 2](#)
- [End-to-End Procedure, on page 2](#)
- [Obtain Licenses, on page 3](#)
- [Log Into CDO, on page 4](#)
- [Onboard a Device with the Onboarding Wizard, on page 9](#)
- [Chassis Manager: Add the Threat Defense Logical Device, on page 10](#)
- [Configure a Basic Security Policy, on page 14](#)
- [Access the Threat Defense and FXOS CLI, on page 25](#)

- [What's Next, on page 27](#)

## About Threat Defense Management by CDO

The cloud-delivered management center offers many of the same functions as an on-premises management center and has the same look and feel. When you use CDO as the primary manager, you can use an on-prem management center for analytics only. The on-prem management center does not support policy configuration or upgrading.

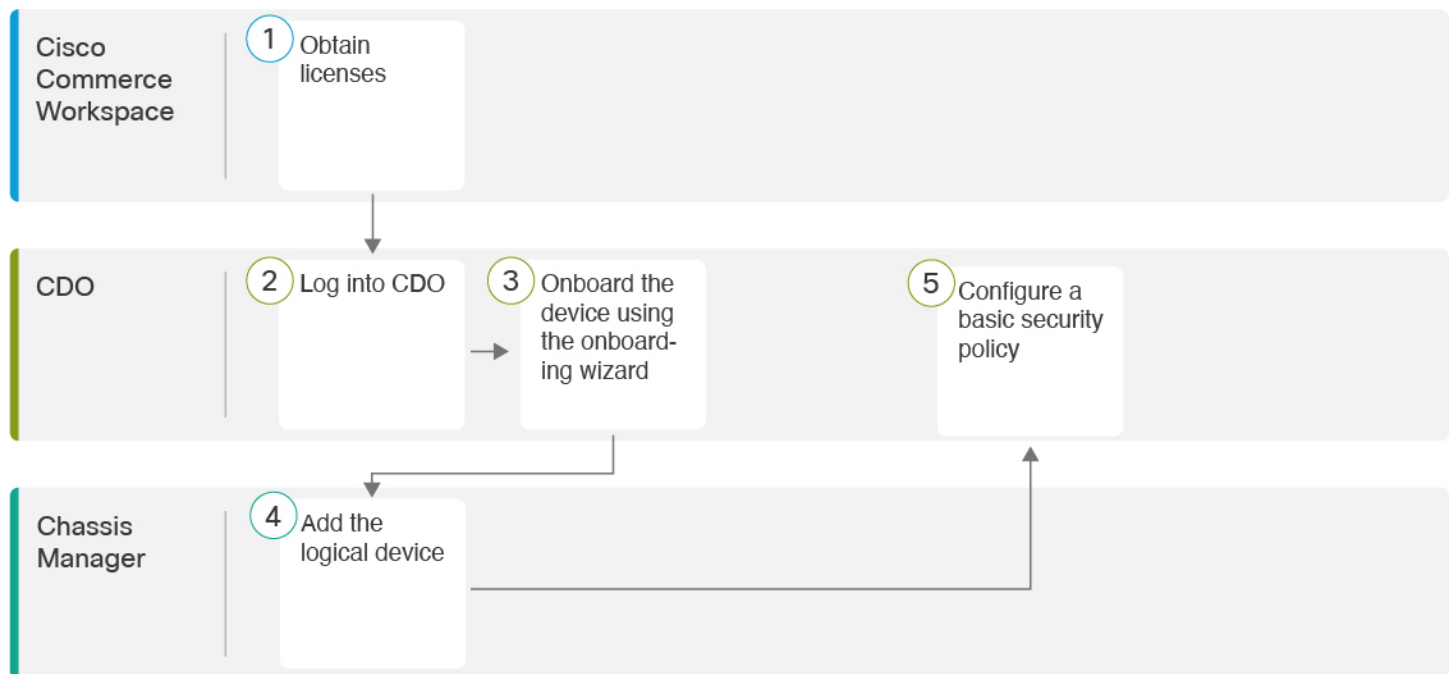


**Note** CDO does not support container instances or clusters.

## End-to-End Procedure

See the following tasks to onboard the threat defense to CDO using the onboarding wizard.

**Figure 1: End-to-End Procedure**



1	Cisco Commerce Workspace	<a href="#">Obtain Licenses, on page 3.</a>
2	CDO	<a href="#">Log Into CDO, on page 4.</a>
3	CDO	<a href="#">Onboard a Device with the Onboarding Wizard, on page 9.</a>

4	Chassis Manager	<a href="#">Chassis Manager: Add the Threat Defense Logical Device, on page 10.</a>
5	CDO	<a href="#">Configure a Basic Security Policy.</a>

## Obtain Licenses

All licenses are supplied to the threat defense by CDO. You can optionally purchase the following feature licenses:

- **IPS**—Security Intelligence and Next-Generation IPS
- **Malware Defense**—Malware defense
- **URL**—URL Filtering
- **Cisco Secure Client**—Secure Client Advantage, Secure Client Premier, or Secure Client VPN Only
- **Carrier**—Diameter, GTP/GPRS, M3UA, SCTP

For a more detailed overview on Cisco Licensing, go to [cisco.com/go/licensingguide](https://cisco.com/go/licensingguide)

### 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).

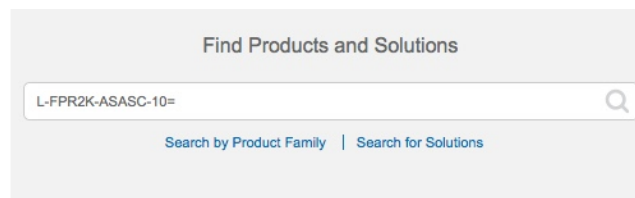
### Procedure

#### 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 2: License Search**



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

- IPS, Malware Defense, and URL license combination:
  - L-FPR4112T-TMC=
  - L-FPR4115T-TMC=
  - L-FPR4125T-TMC=
  - L-FPR4145T-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-FPR4112T-TMC-1Y
  - L-FPR4112T-TMC-3Y
  - L-FPR4112T-TMC-5Y
  - L-FPR4115T-TMC-1Y
  - L-FPR4115T-TMC-3Y
  - L-FPR4115T-TMC-5Y
  - L-FPR4125T-TMC-1Y
  - L-FPR4125T-TMC-3Y
  - L-FPR4125T-TMC-5Y
  - L-FPR4145T-TMC-1Y
  - L-FPR4145T-TMC-3Y
  - L-FPR4145T-TMC-5Y
- Cisco Secure Client—See the [Cisco Secure Client Ordering Guide](#).
  - Carrier license:
    - L-FPR4K-FTD-CAR=

**Step 2** If you have not already done so, register CDO with the Smart Software Manager.

Registering requires you to generate a registration token in the Smart Software Manager. See the CDO documentation for detailed instructions.

---

## 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 7](#).
- If you don't have a Cisco Secure Sign-On account, continue to [Create a New Cisco Secure Sign-On Account, on page 5](#).

## 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 3: Cisco SSO Sign Up

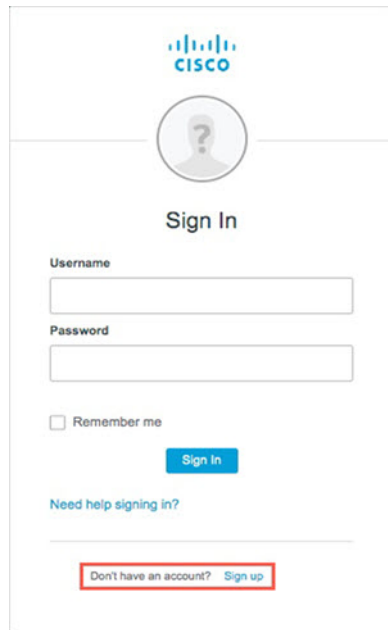


Figure 3 shows the Cisco SSO Sign In page. The page includes the Cisco logo, a placeholder for a profile picture, and the heading "Sign In". Below the heading are input fields for "Username" and "Password", a "Remember me" checkbox, and a "Sign in" button. A link for "Need help signing in?" is also present. At the bottom, a red-bordered box highlights the text "Don't have an account? Sign up".

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

Figure 4: Create Account

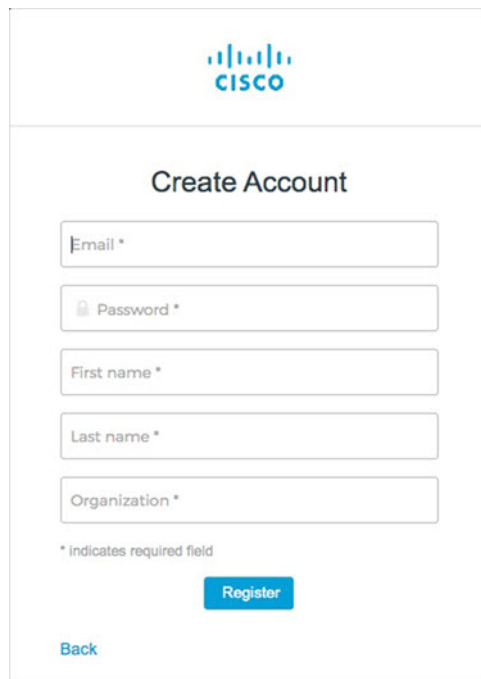


Figure 4 shows the Cisco Create Account page. The page includes the Cisco logo, the heading "Create Account", and input fields for "Email \*", "Password \*", "First name \*", "Last name \*", and "Organization \*". A note below the fields states "\* indicates required field". A "Register" button is at the bottom, along with a "Back" link.

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

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

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

- a) In the **Set up multi-factor authentication** screen, click **Configure**.
- b) Click **Start setup** and follow the prompts to choose a device and verify the pairing of that device with your account.

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

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

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

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

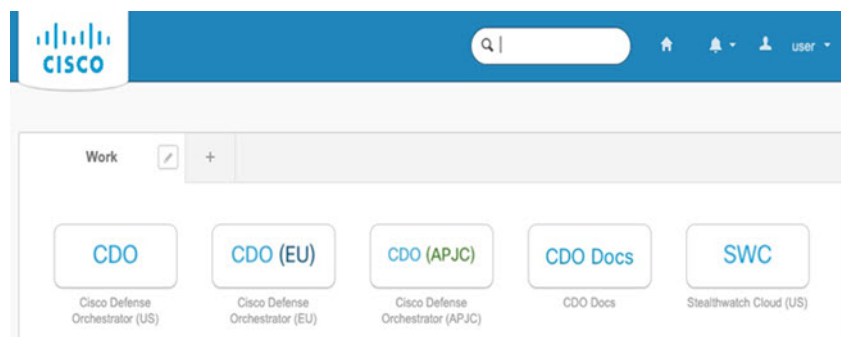
### Step 4 Configure Account Recovery Options for your Cisco Secure Sign-On Account.

- a) Choose a "forgot password" question and answer.
- b) Choose a recovery phone number for resetting your account using SMS.
- c) Choose a security image.
- d) Click **Create My Account**.

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

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

*Figure 5: Cisco SSO Dashboard*



## Log Into CDO with Cisco Secure Sign-On

Log into CDO to onboard and manage your device.

### Before you begin

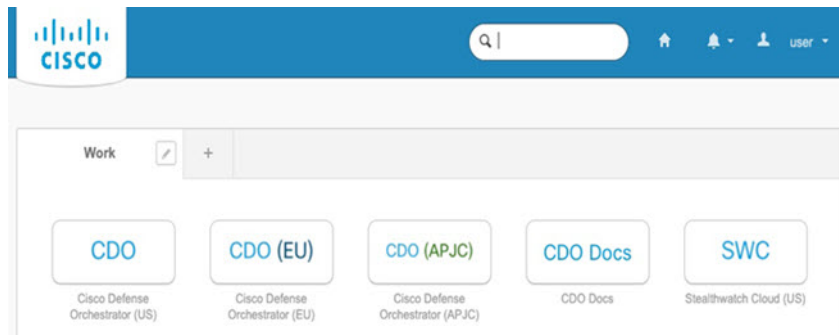
Cisco Defense Orchestrator (CDO) uses Cisco Secure Sign-On as its identity provider and Duo Security for multi-factor authentication (MFA).

- 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 5](#).
- 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 6: 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.
-



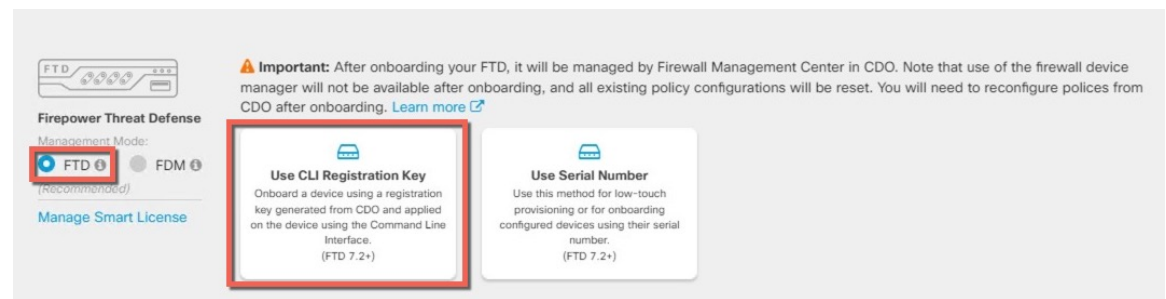
# Onboard a Device with the Onboarding Wizard

Onboard the threat defense using CDO's onboarding wizard using a CLI registration key.

## Procedure

- Step 1** In the CDO navigation pane, click **Inventory**, then click the blue plus button (  ) to **Onboard** a device.
- Step 2** Select the **FTD** tile.
- Step 3** Under **Management Mode**, be sure **FTD** is selected.
- At any point after selecting **FTD** as the management mode, you can click **Manage Smart License** to enroll in or modify the existing smart licenses available for your device. See [Obtain Licenses, on page 3](#) to see which licenses are available.
- Step 4** Select **Use CLI Registration Key** as the onboarding method.

**Figure 7: Use CLI Registration Key**



- Step 5** Enter the **Device Name** and click **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**.
- 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**.
- Step 8** For the **CLI Registration Key**, CDO generates a command with the registration key and other parameters. You must copy this command and use it in the initial configuration of the threat defense.

```
configure manager add cdo_hostname registration_key nat_id display_name
```


In the chassis manager when you deploy the logical device (see [Chassis Manager: Add the Threat Defense Logical Device, on page 10](#)), copy this command into the **CDO Onboard** and **Confirm CDO Onboard** fields.

### Example:

Sample command:

```
configure manager add account1.app.us.cdo.cisco.com KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
Lzm1HOynhVUWhXYWz2swmkj2ZWsn3Lb account1.app.us.cdo.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 **Inventory** page. Enter a label and select the blue plus button () . Labels are applied to the device after it's onboarded to CDO.

---

#### What to do next

From the **Inventory** page, select the device you just onboarded and select any of the option listed under the **Management** pane located to the right.

## Chassis Manager: Add the Threat Defense Logical Device

You can deploy the threat defense from the Firepower 4100 as a standalone, native instance. CDO does not support container instances or clusters.

This procedure lets you configure the logical device characteristics, including the bootstrap configuration used by the application.

#### Before you begin

- Configure a Management interface to use with the threat defense; see [Configure Interfaces](#). The Management interface is required. You can later enable management from a data interface; but you must assign a Management interface to the logical device even if you don't intend to use it after you enable data management. 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
  - CDO hostname, registration key, and NAT ID generated by CDO. See [Onboard a Device with the Onboarding Wizard, on page 9](#).
  - DNS server IP address

#### Procedure

---

**Step 1** In the chassis manager, choose **Logical Devices**.

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

Figure 8: Add a Standalone Device

- 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.


**Note** You cannot change this name after you add the logical device.

- b) For the **Template**, choose **Cisco Firepower Threat Defense**.  
 c) Choose the **Image Version**.  
 d) Choose the **Instance Type: Native**.  
 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 CDO, including setting the IP addresses.

Hardware Bypass–capable ports are shown with the following icon: . For certain interface modules, you can enable the Hardware Bypass feature for Inline Set interfaces only. Hardware Bypass ensures that traffic

continues to flow between an inline interface pair during a power outage. This feature can be used to maintain network connectivity in the case of software or hardware failures. If you do not assign both interfaces in a Hardware Bypass pair, you see a warning message to make sure your assignment is intentional. You do not need to use the Hardware Bypass feature, so you can assign single interfaces if you prefer.

**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:

*Figure 9: General Information*

The screenshot shows the 'Cisco Firepower Threat Defense - Bootstrap Configuration' dialog box with the 'General Information' tab selected. The 'Security Module(SM) Selection' section has three buttons: 'SM 1 - Ok' (highlighted in blue), 'SM 2 - Ok', and 'SM 3 - Empty'. Below this, it says 'SM 1 - 0 Cores Available'. The 'Interface Information' section contains the following fields:

- Management Interface: Ethernet1/4
- Address Type: IPv4 only
- Management IP: 10.89.5.20
- Network Mask: 255.255.255.192
- Network Gateway: 10.89.5.1

At the bottom of the dialog are 'OK' and 'Cancel' buttons.

a) Choose the **Management Interface**.

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

b) Choose the management interface **Address Type**: **IPv4 only**, **IPv6 only**, or **IPv4 and IPv6**.

c) Configure the **Management IP** address.

Set a unique IP address for this interface.

d) Enter a **Network Mask** or **Prefix Length**.

e) Enter a **Network Gateway** address.

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

Figure 10: Settings

The screenshot shows the 'Cisco Secure Firewall Threat Defense - Bootstrap Configuration' dialog box with the 'Settings' tab selected. The fields are as follows:

- Management type of application instance: CDO (dropdown)
- Search domains: cisco.com (text)
- Firewall Mode: Routed (dropdown)
- DNS Servers: 72.163.47.11 (text)
- Fully Qualified Hostname: 9300-2.cisco.com (text)
- Password: [masked] (text) Set: Yes
- Confirm Password: [masked] (text)
- Registration Key: [empty] (text) Set: Yes
- Confirm Registration Key: [empty] (text)
- CDO Onboard: [masked] (text)
- Confirm CDO Onboard: [masked] (text)
- Firepower Management Center IP: [empty] (text)
- Firepower Management Center NAT ID: [empty] (text)
- Eventing Interface: None (dropdown)

Buttons: OK, Cancel

- a) In the **Management type of application instance** drop-down list, choose **CDO**.
- b) Enter the **Search Domains** as a comma-separated list.
- c) Choose the **Firewall Mode**: **Transparent** or **Routed**.

In routed mode, the threat defense is considered to be a router hop in the network. Each interface that you want to route between is on a different subnet. A transparent firewall, on the other hand, is a Layer 2 firewall that acts like a “bump in the wire,” or a “stealth firewall,” and is not seen as a router hop to connected devices.

The firewall mode is only set at initial deployment. If you re-apply the bootstrap settings, this setting is not used.

- d) Enter the **DNS Servers** as a comma-separated list.  
The threat defense uses DNS if you specify a hostname for the management center, for example.
- e) Enter the **Fully Qualified Hostname** for the threat defense.
- f) Enter a **Password** for the threat defense admin user for CLI access.
- g) Copy the command generated by CDO into the **CDO Onboard** and **Confirm CDO Onboard** fields.
- h) A separate **Eventing Interface** is not supported for CDO, so this setting will be ignored.

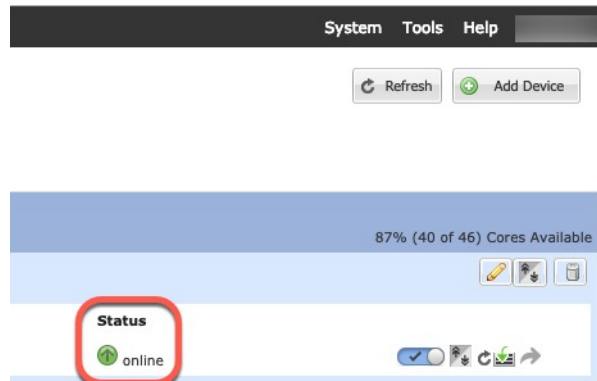
**Step 7** On the **Agreement** tab, read and accept the end user license agreement (EULA).

**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.



## Configure a Basic Security Policy

This section describes how to configure a basic security policy with the following settings:

- Inside and outside interfaces—Assign a static IP address to the inside interface, and use DHCP for the outside interface.
- DHCP server—Use a DHCP server on the inside interface for clients.
- Default route—Add a default route through the outside interface.
- NAT—Use interface PAT on the outside interface.
- Access control—Allow traffic from inside to outside.

To configure a basic security policy, complete the following tasks.

1	Configure Interfaces.
2	Configure the DHCP Server.
3	Add the Default Route.
4	Configure NAT.
5	Allow Traffic from Inside to Outside.
6	Deploy the Configuration.

## Configure Interfaces

Enable the threat defense interfaces, assign them to security zones, and set the IP addresses. Typically, you must configure at least a minimum of two interfaces to have a system that passes meaningful traffic. Normally, you would have an outside interface that faces the upstream router or internet, and one or more inside interfaces for your organization's networks. Some of these interfaces might be "demilitarized zones" (DMZs), where you place publically-accessible assets such as your web server.

A typical edge-routing situation is to obtain the outside interface address through DHCP from your ISP, while you define static addresses on the inside interfaces.

The following example configures a routed mode inside interface with a static address and a routed mode outside interface using DHCP.

### Procedure

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

**Step 2** Click **Interfaces**.

10.89.5.20

Cisco Firepower 9000 Series SM-24 Threat Defense

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

**Step 3** Click **Edit** (✎) for the interface that you want to use for *inside*.

The **General** tab appears.

**Edit Physical Interface** ? X

**General** IPv4 IPv6 Advanced Hardware Configuration

Name:   Enabled  Management Only

Description:

Mode:  ▼

Security Zone:  ▼

Interface ID:

MTU:  (64 - 9000)

OK Cancel

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

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

- Click the **IPv4** and/or **IPv6** tab.
  - IPv4**—Choose **Use Static IP** from the drop-down list, and enter an IP address and subnet mask in slash notation.

For example, enter **192.168.1.1/24**

**Edit Physical Interface**

**General** **IPv4** IPv6 Advanced Hardware Configuration

IP Type:  ▼

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



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

f) Click **OK**.

**Step 4** Click the **Edit** (✎) for the interface that you want to use for *outside*.

The **General** tab appears.

The screenshot shows the 'Edit Physical Interface' dialog box with the following configuration:

- Name:** outside
- Description:** (empty)
- Mode:** None
- Security Zone:** outside\_zone
- Interface ID:** GigabitEthernet0/0
- MTU:** 1500 (64 - 9000)
- Enabled:**  Enabled
- Management Only:**  Management Only

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

a) Enter a **Name** up to 48 characters in length.

For example, name the interface **outside**.

b) Check the **Enabled** check box.

c) Leave the **Mode** set to **None**.

d) From the **Security Zone** drop-down list, choose an existing outside security zone or add a new one by clicking **New**.

For example, add a zone called **outside\_zone**.

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

- **IPv4**—Choose **Use DHCP**, and configure the following optional parameters:

- **Obtain default route using DHCP**—Obtains the default route from the DHCP server.

- **DHCP route metric**—Assigns an administrative distance to the learned route, between 1 and 255. The default administrative distance for the learned routes is 1.

**Edit Physical Interface**

General **IPv4** IPv6 Advanced Hardware Configuration

IP Type: Use DHCP

Obtain default route using DHCP:

DHCP route metric: 1 (1 - 255)

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

f) Click **OK**.

**Step 5** Click **Save**.

## Configure the DHCP Server

Enable the DHCP server if you want clients to use DHCP to obtain IP addresses from the threat defense.

### Procedure

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

**Step 2** Choose **DHCP > DHCP Server**.

**Step 3** On the **Server** page, click **Add**, and configure the following options:

**Add Server** ? x

Interface\* inside

Address Pool\* 10.9.7.9-10.9.7.25 (2.2.2.10-2.2.2.20)

Enable DHCP Server

OK Cancel

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

**Step 4** Click **OK**.

**Step 5** Click **Save**.

## Add the Default Route

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

### Procedure

- Step 1** Choose **Devices > Device Management**, and click the **Edit** (✎) for the device.
- Step 2** Choose **Routing > Static Route**, click **Add Route**, and set the following:

The screenshot shows the 'Add Static Route Configuration' dialog box. It has a title bar with a question mark and a close button. The 'Type' section has radio buttons for 'IPv4' (selected) and 'IPv6'. The 'Interface\*' dropdown is set to 'outside'. Below this are two panes: 'Available Network' and 'Selected Network'. The 'Available Network' pane has a search bar and a list of network objects, with 'any-ipv4' selected. An 'Add' button is between the panes. The 'Selected Network' pane shows 'any-ipv4'. Below the panes are fields for 'Gateway\*' (set to 'default-gateway'), 'Metric' (set to '1'), 'Tunneled' (checkbox), and 'Route Tracking' (dropdown). 'OK' and 'Cancel' buttons are at the bottom.

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

- Step 3** Click **OK**.

The route is added to the static route table.

The screenshot shows the configuration interface for a Cisco Firepower 9000 Series SM-24 Threat Defense device. The 'Devices' tab is active, and the 'Static Route' configuration page is displayed. The interface includes a navigation menu on the left with options like OSPF, OSPFv3, RIP, BGP, Static Route (selected), and Multicast Routing. The main area shows a table of routes with columns for Network, Interface, Gateway, Tunneled, Metric, and Tracked. A single IPv4 route is listed: any-ipv4 on the outside interface with a gateway of 10.99.10.1 and a metric of 1. An 'Add Route' button is visible in the top right corner of the table area.

Network	Interface	Gateway	Tunneled	Metric	Tracked
<b>IPv4 Routes</b>					
any-ipv4	outside	10.99.10.1	false	1	
<b>IPv6 Routes</b>					

**Step 4** Click **Save**.

## Configure NAT

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

### Procedure

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

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

The screenshot shows the 'New Policy' configuration dialog box. The 'Name' field is set to 'interface\_PAT'. The 'Description' field is empty. Under the 'Targeted Devices' section, there are two panes: 'Available Devices' and 'Selected Devices'. The 'Available Devices' pane contains a search box and a list with one item: 192.168.0.16. The 'Selected Devices' pane contains a list with one item: 192.168.0.16, which is circled in red. An 'Add to Policy' button is located between the two panes. At the bottom of the dialog, there are 'Save' and 'Cancel' buttons.

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

**Step 3** Click **Add Rule**.

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

**Step 4** Configure the basic rule options:

The screenshot shows the 'Add NAT Rule' dialog box with the following settings:

- NAT Rule: Auto NAT Rule
- Type: Dynamic
- Enable:
- Interface Objects: Translation (selected), PAT Pool, Advanced

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

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

The screenshot shows the 'Add NAT Rule' dialog box with the 'Interface Objects' tab selected. The configuration is as follows:

- NAT Rule: Auto NAT Rule
- Type: Dynamic
- Enable:
- Interface Objects: Translation (selected), PAT Pool, Advanced
- Available Interface Objects:
  - inside\_zone
  - outside\_zone (highlighted with a red circle and '1')
- Source Interface Objects (0): any
- Destination Interface Objects (1): outside\_zone (added with a red circle and '3')
- Buttons: Add to Source, Add to Destination (with a red circle and '2')

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

The screenshot shows the 'Add NAT Rule' dialog box with the 'Translation' tab selected. The configuration is as follows:

- NAT Rule: Auto NAT Rule
- Type: Dynamic
- Enable:
- Interface Objects: Translation (selected), PAT Pool, Advanced
- Original Packet:
  - Original Source:\* all-ipv4 (circled in red)
  - Original Port: TCP
- Translated Packet:
  - Translated Source: Destination Interface IP (circled in red)
  - Translated Port: (empty)

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

**New Network Object** ? x

Name: all-ipv4

Description:

Network:  Host  Range  Network  FQDN

0.0.0.0/0

Allow Overrides:

Save Cancel

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

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

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

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

#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options
NAT Rules Before											
Auto NAT Rules											
#	→	Dynamic	any	outside_zone	all-ipv4			interface			Dns:false
NAT Rules After											

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

## Allow Traffic from Inside to Outside

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

### Procedure

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

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

The screenshot shows the 'Add Rule' configuration window. The rule name is 'inside\_to\_outside', it is enabled, and its action is 'Allow'. The source zone is 'inside\_zone' and the destination zone is 'outside\_zone'. The window also shows tabs for 'Zones', 'Networks', 'VLAN Tags', 'Users', 'Applications', 'Ports', 'URLs', 'SGT/ISE Attributes', 'Inspection', 'Logging', and 'Comments'.

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

Leave the other settings as is.

**Step 3** Click **Add**.

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

The screenshot shows the 'Rules' table in the Threat Defense console. The table has columns for Name, Source Zone, Dest Zones, Source Net..., Dest Netw..., VLAN Tags, Users, Applications, Source Po..., Dest Ports, URLs, ISE/SGT A..., and Action. The rule 'inside\_to\_outside' is listed with source zone 'inside\_zone' and destination zone 'outside\_zone'.

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

**Step 4** Click **Save**.

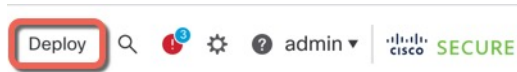
## Deploy the Configuration

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

### Procedure

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

Figure 11: Deploy



**Step 2** Either click **Deploy All** to deploy to all devices or click **Advanced Deploy** to deploy to selected devices.

Figure 12: Deploy All

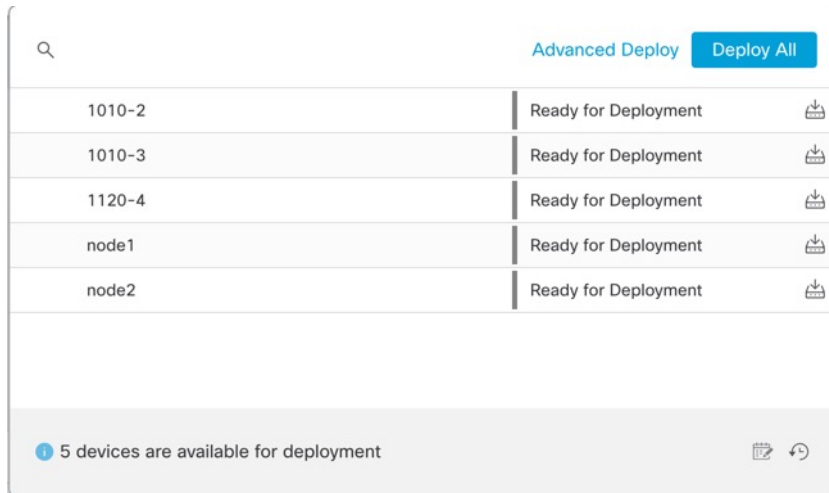


Figure 13: Advanced Deploy

1 device selected

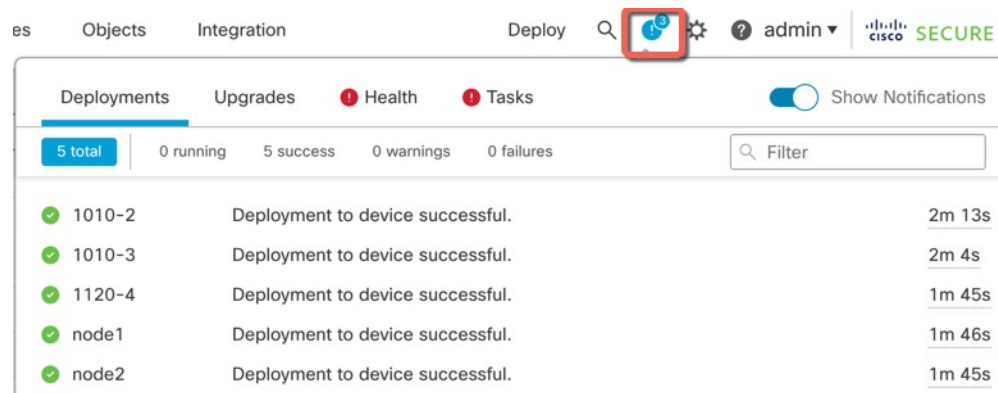
Search using device name, user name, type, group or status Deploy time: Estimate **Deploy**

Device	Modified by	Inspect Interruption	Type	Group	Last Deploy Time	Preview	Status
<input checked="" type="checkbox"/> node1	System		FTD		May 23, 2022 6:49 PM		Ready for Deployment
<input type="checkbox"/> 1010-2	admin, System		FTD		May 23, 2022 7:09 PM		Ready for Deployment
<input type="checkbox"/> node2	System		FTD		May 23, 2022 6:49 PM		Ready for Deployment
<input type="checkbox"/> 1010-3	System		FTD		May 23, 2022 6:49 PM		Ready for Deployment
<input type="checkbox"/> 1120-4	System		FTD		May 23, 2022 6:49 PM		Ready for Deployment

**Step 3** Ensure that the deployment succeeds. Click the icon to the right of the **Deploy** button in the menu bar to see status for deployments.



Figure 14: Deployment Status



## Access the Threat Defense and FXOS CLI

You can use the threat defense 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 threat defense management interface IP address.
- You set the management IP address when you deployed the logical device. Log into the threat defense 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 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 engine.

```
connect module 1 { 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 threat defense 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 the threat defense 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 threat defense using CDO, see the [Cisco Defense Orchestrator](#) home page.

