Threat Defense Deployment with the Device Manager

Is This Chapter for You?

This chapter describes how to deploy a standalone the threat defense logical device with the device manager. To deploy a High Availability pair, see the Cisco Secure Firewall Device Manager Configuration Guide.

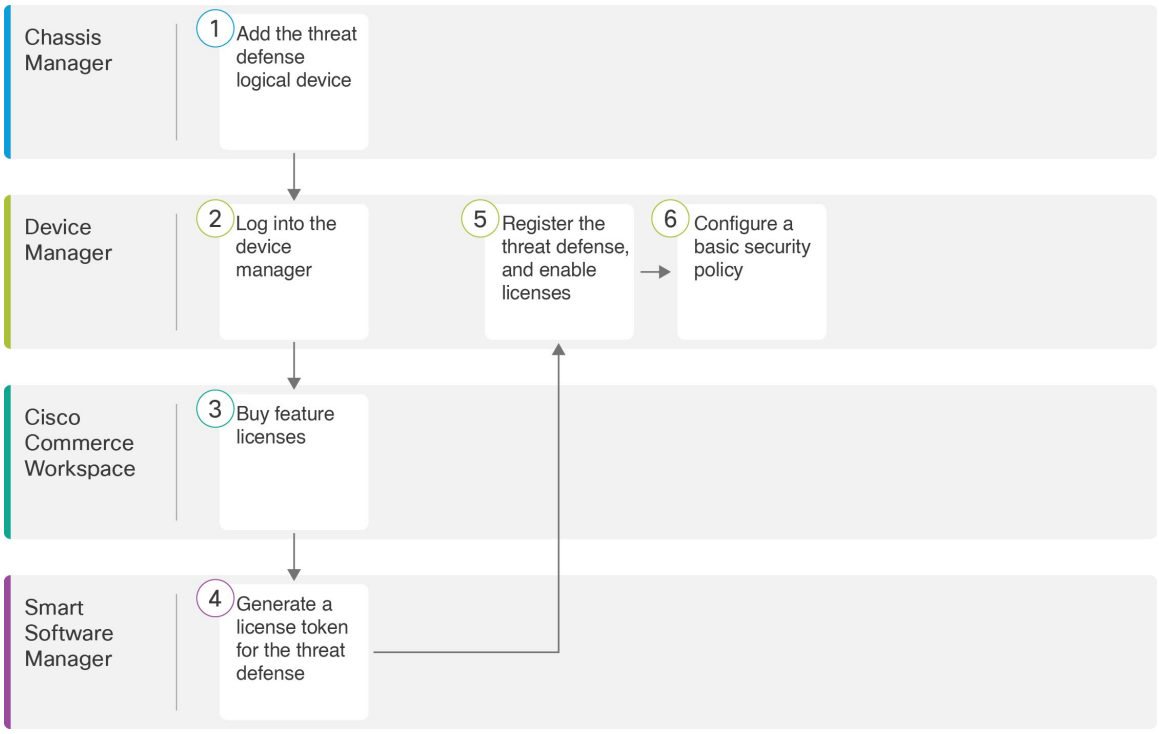
The device manager lets you configure the basic features of the software that are most commonly used for small networks. It is especially designed for networks that include a single device or just a few, where you do not want to use a high-powered multiple-device manager to control a large network containing many device manager devices.

If you are managing large numbers of devices, or if you want to use the more complex features and configurations that the threat defense allows, use the management center instead.

Privacy Collection Statement—The Firepower 4100 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 and configure the threat defense on your chassis.



	Workspace	Steps
1	Chassis Manager	Chassis Manager: Add the Threat Defense Logical Device, on page 2.
2	Device Manager	Log Into the Device Manager, on page 6.
3	Cisco Commerce Workspace	Configure Licensing, on page 6: Buy feature licenses.
4	Smart Software Manager	Configure Licensing, on page 6: Generate a license token for the device manager.
5	Device Manager	Configure Licensing, on page 6: Register the device manager with the Smart Licensing server, and enable feature licenses.
6	Device Manager	Configure a Basic Security Policy, on page 12.

Chassis Manager: Add the Threat Defense Logical Device

You can deploy the threat defense from the Firepower 4100 as a native instance. Container instances are not supported.

To add a High Availability pair, see the Cisco Secure Firewall Device Manager Configuration Guide.

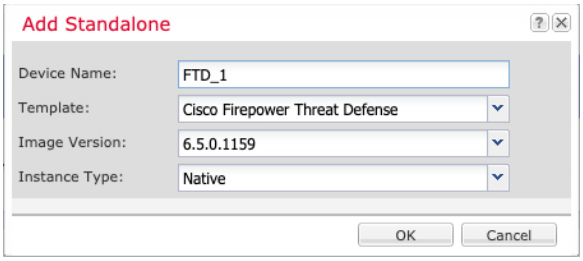
Before you begin

- Configure a Management interface to use with the threat defense; 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
  - Threat Defense hostname and domain name

Procedure

Step 1 In the 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.

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**.

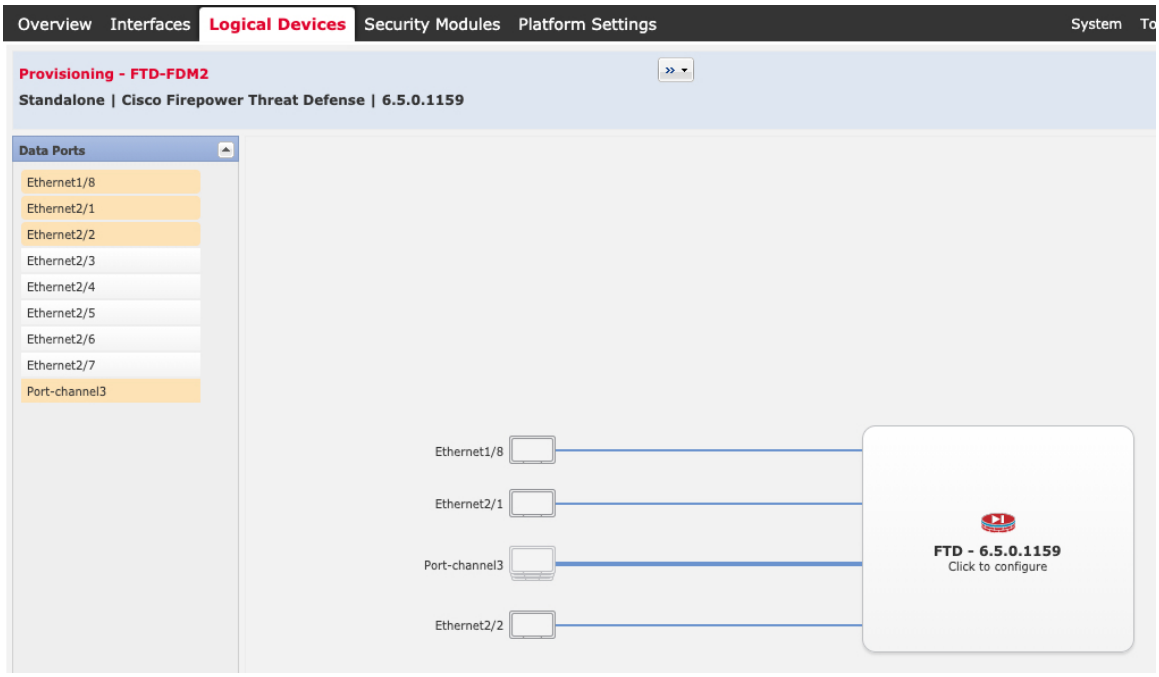
d) Choose the **Instance Type**: **Native**.

Container instances are not supported with the device manager.

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.

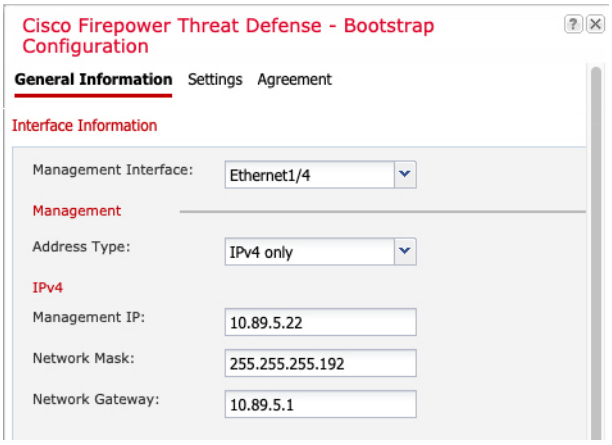


You can only assign data interfaces that you previously enabled on the **Interfaces** page. You will later enable and configure these interfaces in the device manager, including setting the IP addresses.

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) Choose the **Management Interface**.

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

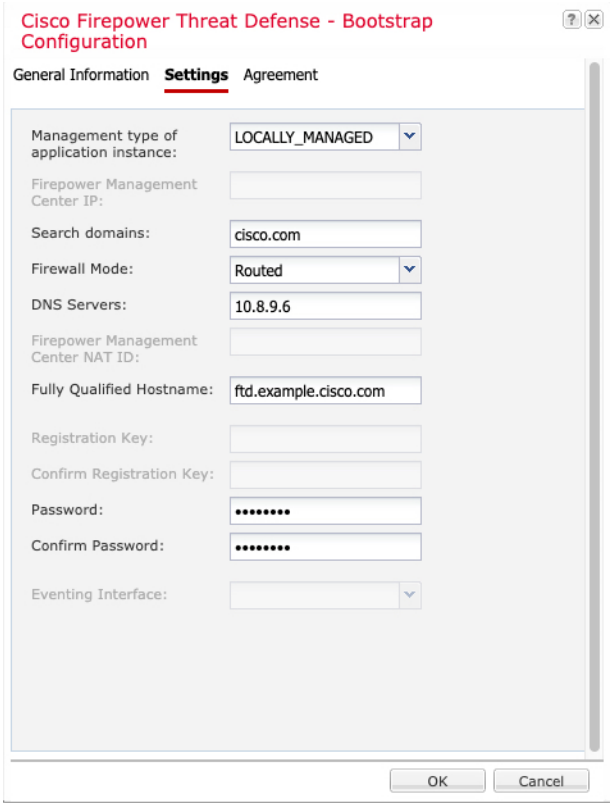
b) Choose the management interface **Address Type**: **IPv4 only**, **IPv6 only**, or **IPv4 and IPv6**.

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:



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

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

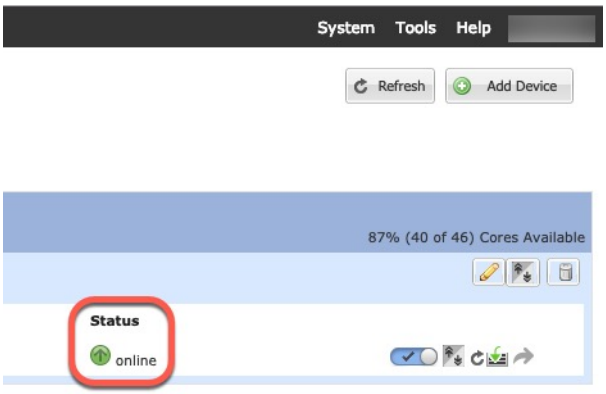
b) Enter the **Search Domains** as a comma-separated list.
c) The **Firewall Mode** only supports **Routed** mode.
d) Enter the **DNS Servers** as a comma-separated list.
e) Enter the **Fully Qualified Hostname** for the threat defense.
f) Enter a **Password** for the threat defense admin user for CLI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

Log into the device manager to configure your threat defense.

Before you begin

- Use a current version of Firefox, Chrome, Safari, Edge, or Internet Explorer.
- Make sure the threat defense logical device **Status** is **online** on the chassis manager **Logical Devices** page.

Procedure

Step 1 Enter the following URL in your browser.

- Management—**https://***management_ip*. Enter the interface IP address that you entered in the bootstrap configuration.

Step 2 Log in with the username **admin**, and the password you set when you deployed the threat defense.

Step 3 You are prompted to accept the 90-day evaluation license.

Configure Licensing

The threat defense 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 Essentials 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:

- **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

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.

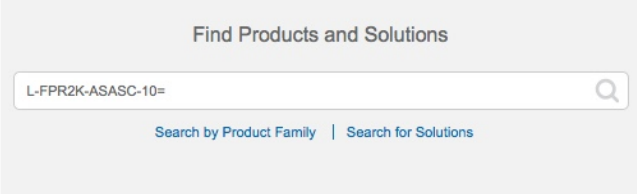
- Your Smart Software Licensing account must qualify for the Strong Encryption (3DES/AES) license to use some features (enabled using the export-compliance flag).

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 1: 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:

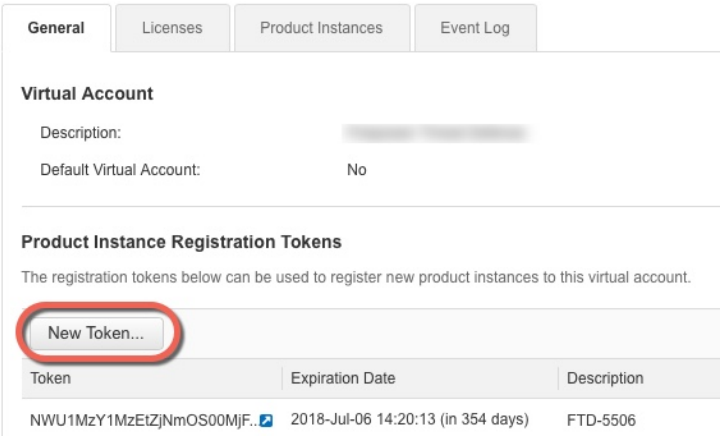
- L-FPR4112T-TMC-1Y
- L-FPR4112T-TMC-3Y
- L-FPR4112T-TMC-5Y
- L-FPR4115T-TMC-1Y
- L-FPR4115T-TMC-3Y
- L-FPR4115T-TMC-5Y
- L-FPR4125T-TMC-1Y
- L-FPR4125T-TMC-3Y
- L-FPR4125T-TMC-5Y
- L-FPR4145T-TMC-1Y
- L-FPR4145T-TMC-3Y
- L-FPR4145T-TMC-5Y

- Cisco Secure Client—See the Cisco Secure Client Ordering Guide.

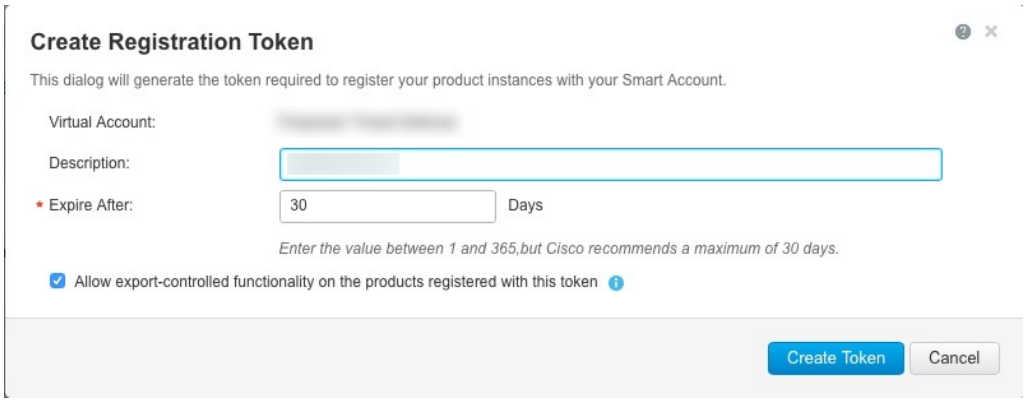
Step 2 In the Smart Software Manager, request and copy a registration token for the virtual account to which you want to add this device.

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 threat defense.

Figure 2: View Token

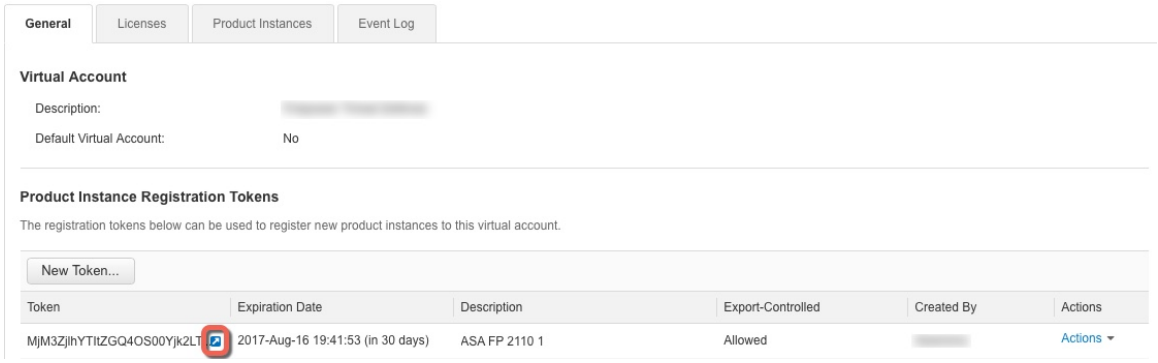
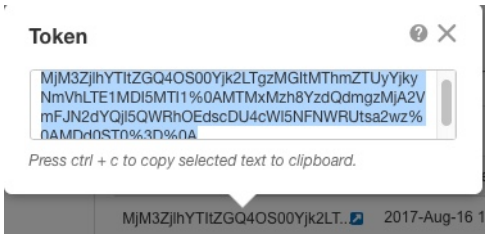


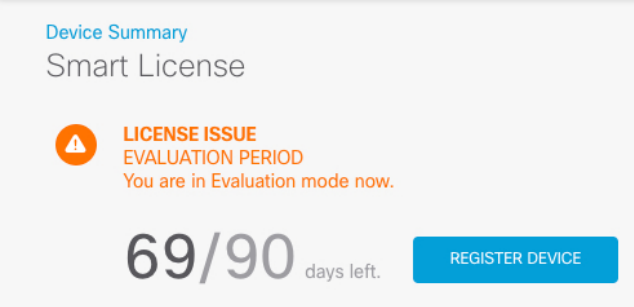
Figure 3: Copy Token



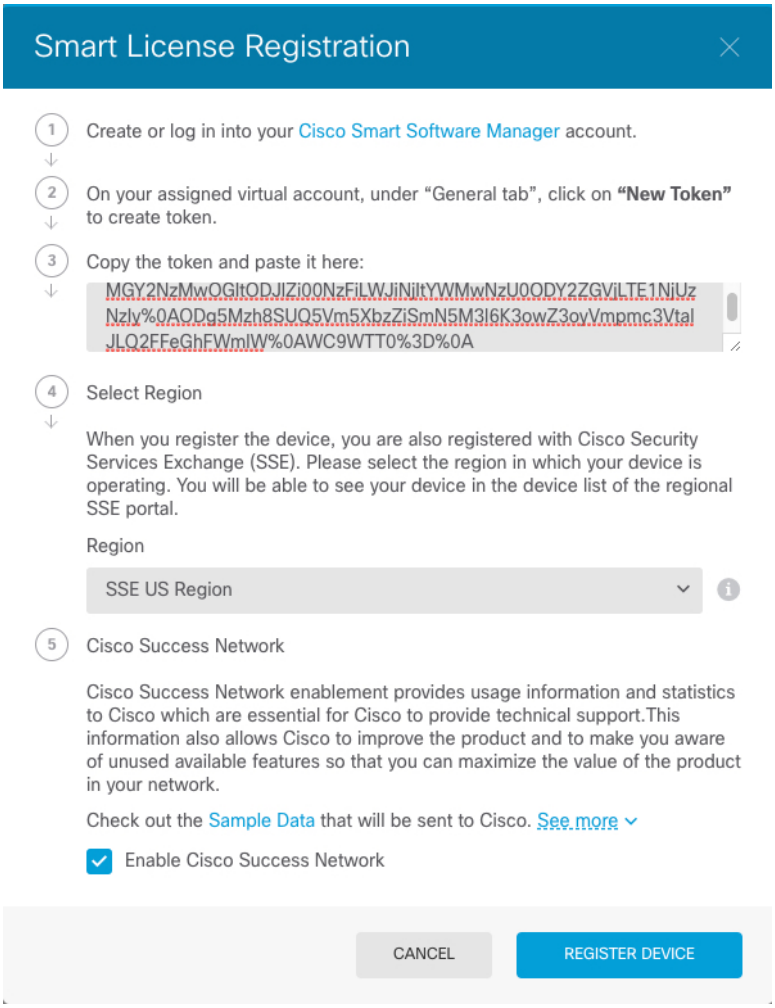
Step 3 In the device manager, click **Device**, and then in the **Smart License** summary, click **View Configuration**.

You see the **Smart License** page.

Step 4 Click **Register Device**.

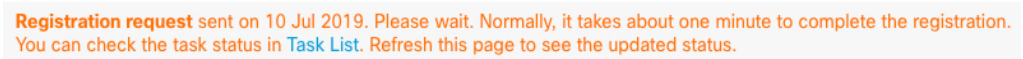


Then follow the instructions on the **Smart License Registration** dialog box to paste in your token:

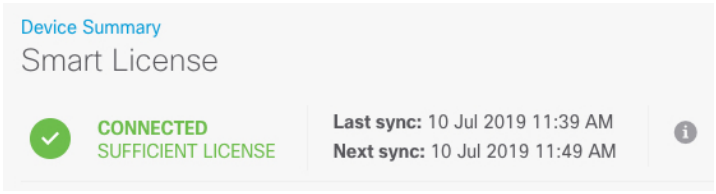


Step 5 Click **Register Device**.

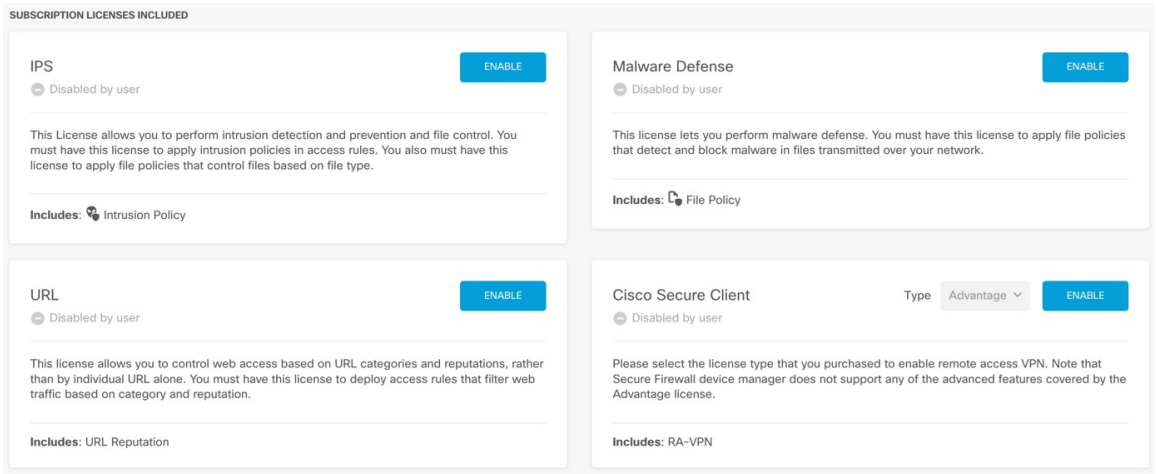
You return to the **Smart License** page. While the device registers, you see the following message:



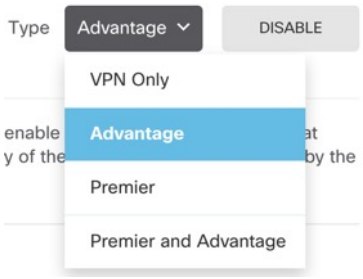
After the device successfully registers and you refresh the page, you see the following:



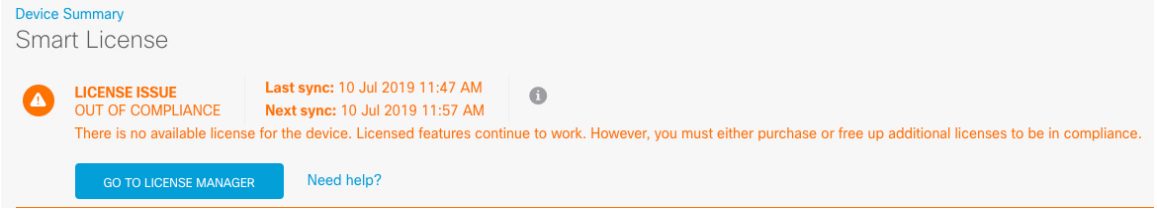
Step 6 Click the **Enable/Disable** control for each optional license as desired.



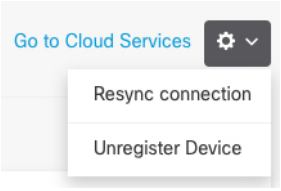
- **Enable**—Registers the license with your Cisco Smart Software Manager account and enables the controlled features. You can now configure and deploy policies controlled by the license.
- **Disable**—Unregisters the license with your Cisco Smart Software Manager account and disables the controlled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



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:



Step 7 Choose **Resync Connection** from the gear drop-down list to synchronize license information with Cisco Smart Software Manager.



Configure a Basic Security Policy

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

1	Configure Interfaces, on page 13. Assign a static IP address to the inside interface, and use DHCP for the outside interface.
2	Add Interfaces to Security Zones, on page 15. Add the inside and outside interfaces to inside and outside security zones, which are required for access control.
3	Add the Default Route, on page 17. If you do not receive the default route from the outside DHCP server, you need to manually add it.
4	Configure NAT, on page 19. Use interface PAT on the outside interface.
5	Allow Traffic from Inside to Outside, on page 21. Allow traffic from inside to outside.
6	(Optional) Configure the DHCP Server, on page 22. Use a DHCP server on the inside interface for clients.
7	(Optional) Configure the Management Gateway and Allow Management on Data Interfaces, on page 23. Change the management gateway and/or allow management from a data interface.
8	Deploy the Configuration, on page 25.

Configure Interfaces

Enable the threat defense interfaces 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 an inside interface with a static address and an outside interface using DHCP.

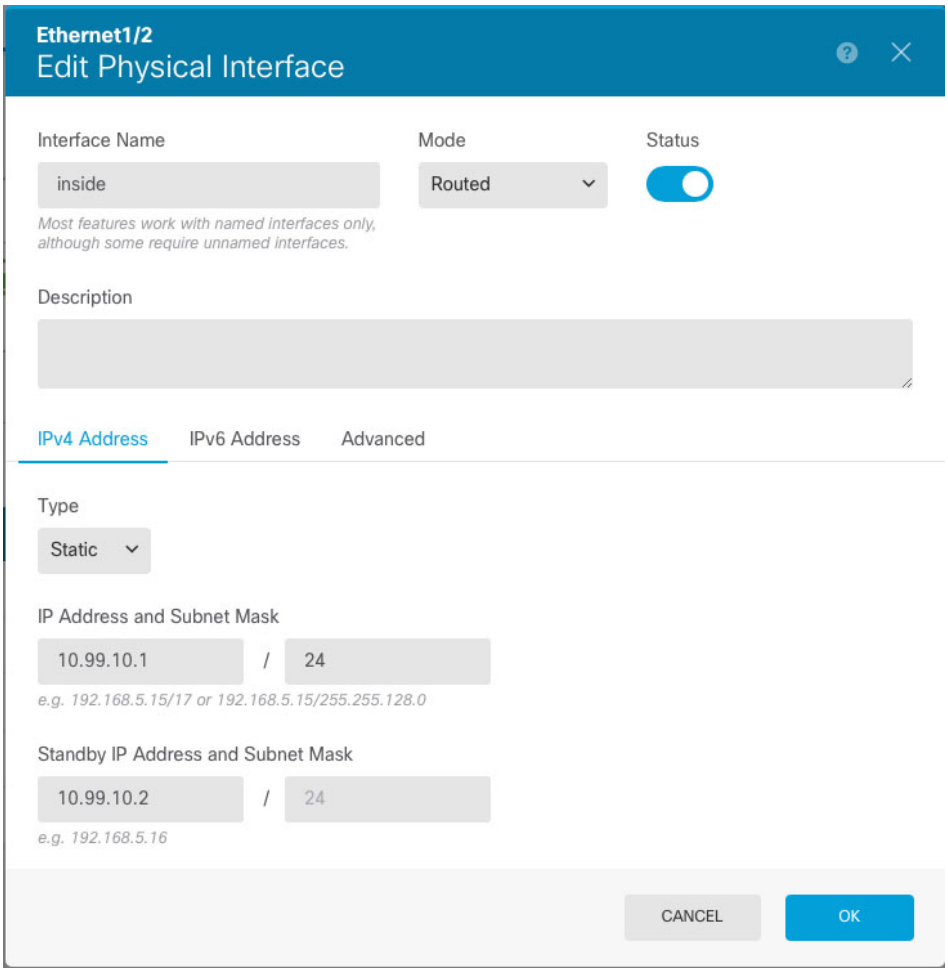
Procedure

Step 1 Click **Device**, and then click the link in the **Interfaces** summary.

The **Interfaces** page is selected by default. The interfaces list shows physical interfaces, their names, addresses, and states.

Step 2 Click the edit icon () for the interface that you want to use for *inside*

Step 3 Set the following:



a) Set the **Interface Name**.

Set the name for the interface, up to 48 characters. Alphabetic characters must be lower case. For example, **inside** or **outside**. Without a name, the rest of the interface configuration is ignored. Unless you configure subinterfaces, the interface should have a name.

b) Set the **Mode** to **Routed**.

If you want to use Passive interfaces, see the Cisco Secure Firewall Device Manager Configuration Guide.

c) Set the **Status** slider to the enabled setting ( ).

Important You must also enable the interface in FXOS.

d) (Optional) Set the **Description**.

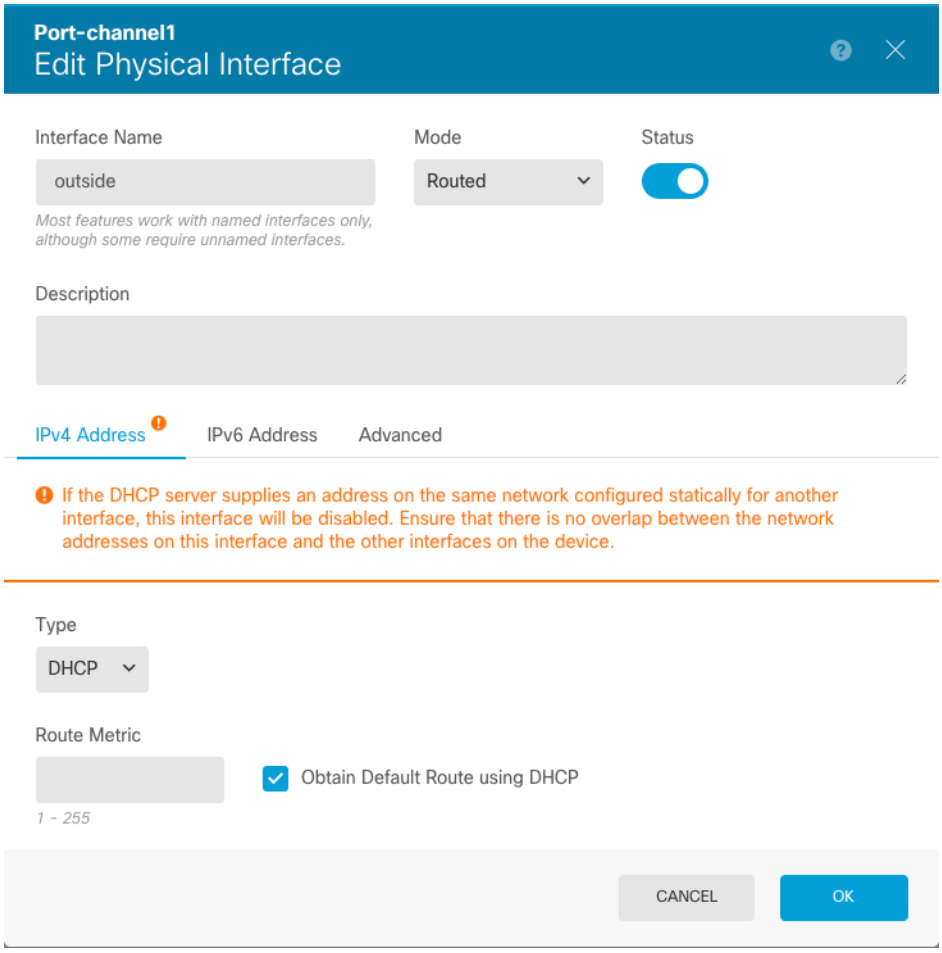
The description can be up to 200 characters on a single line, without carriage returns.

e) On the **IPv4 Address** page, configure a static IP address.

f) (Optional) Click **IPv6 Address**, and configure IPv6.

Step 4 Click **OK**.

Step 5 Click the edit icon ( ) for the interface that you want to use for *outside*, and set the same fields as for inside; for this interface, choose **DHCP** for the IPv4 Address.



Note If you use a static IP address or do not receive the default route from DHCP, you will need to manually set a default route; see the Cisco Secure Firewall Device Manager Configuration Guide.

Add Interfaces to Security Zones

A security zone is a grouping of interfaces. Zones divide the network into segments to help you manage and classify traffic. You can define multiple zones, but a given interface can be in one zone only.

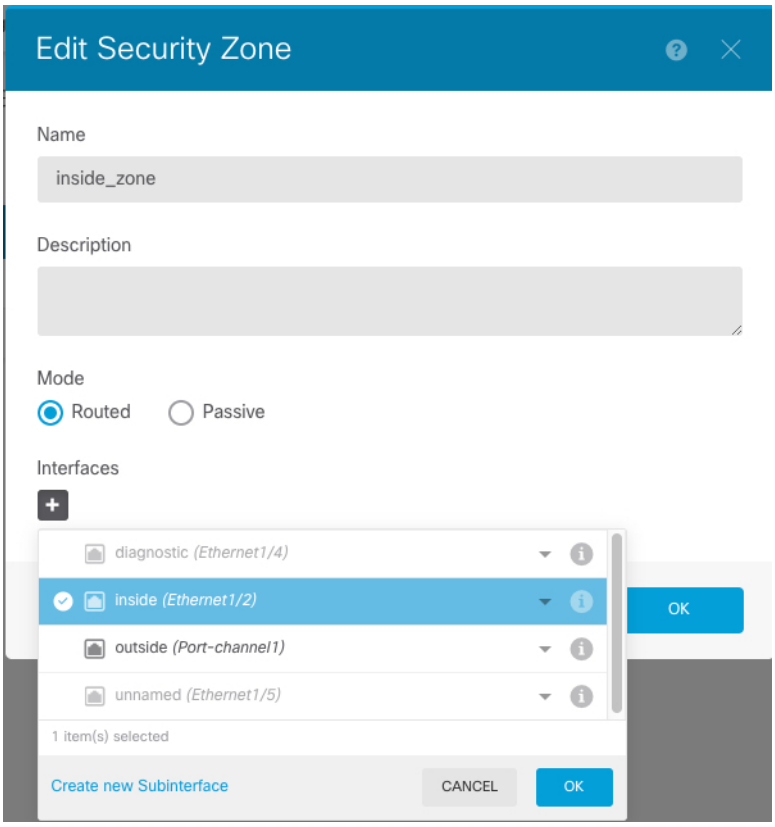
This procedure tells you how to add interfaces to the following pre-configured zones:

- **inside_zone**—This zone is intended to represent internal networks.
- **outside_zone**—This zone is intended to represent networks external to your control, such as the Internet.

Procedure

Step 1 Select **Objects**, then select **Security Zones** from the table of contents.

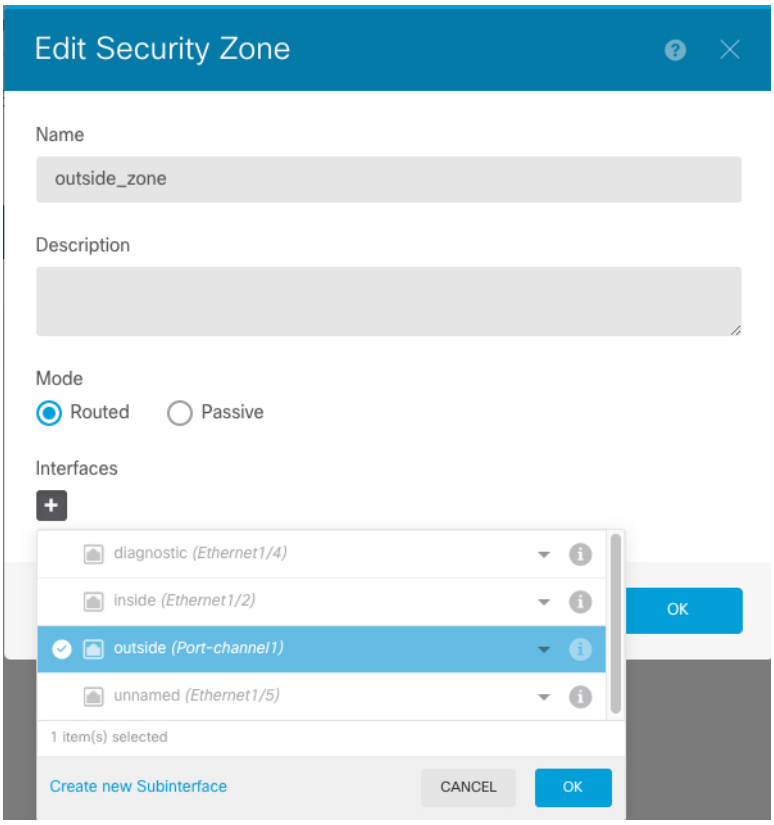
Step 2 Click the edit icon ( ) for the **inside_zone**.



Step 3 In the **Interfaces** list, click + and select the inside interface to add to the zone.

Step 4 Click **OK** to save your changes.

Step 5 Repeat these steps to add the outside interface to the **outside_zone**.



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 on the **Device Summary** > **Static Routing** page.

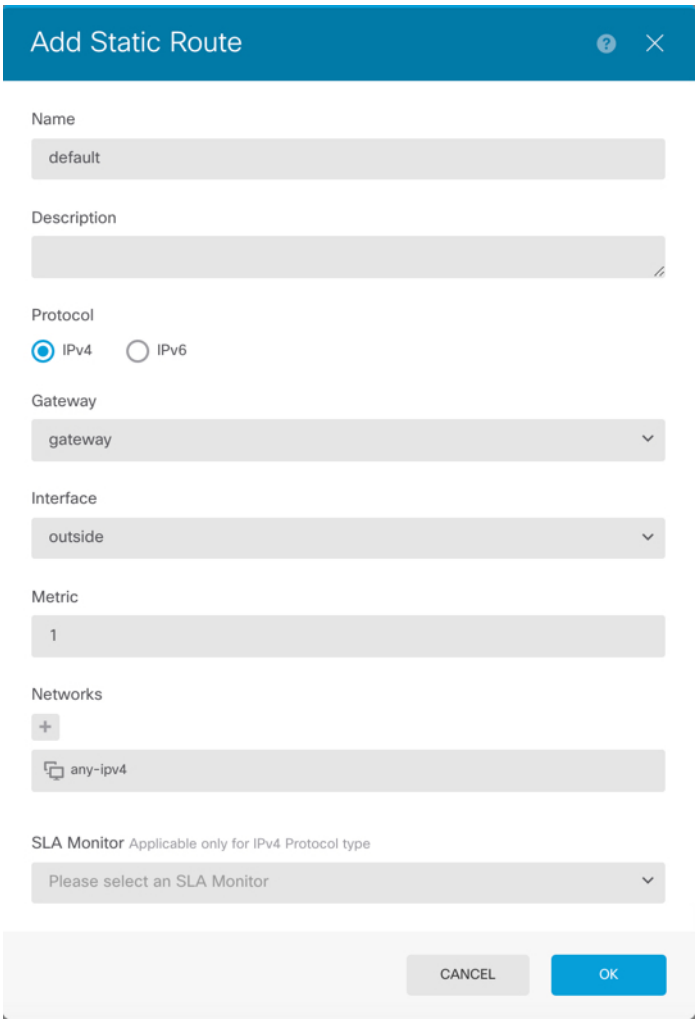
Procedure

Step 1 Click **Device**, then click the link in the **Routing** summary.

The **Static Routing** page appears.

Step 2 Click + or **Create Static Route**.

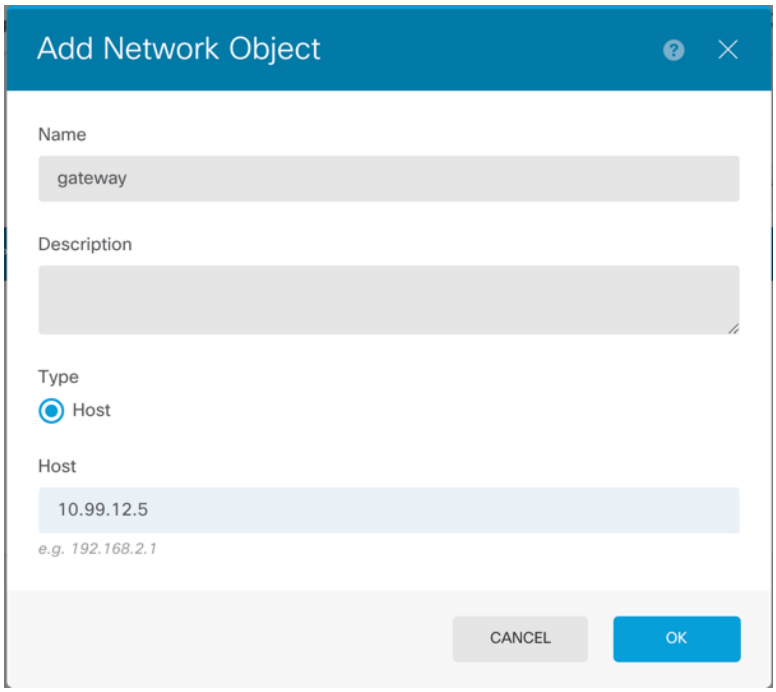
Step 3 Configure the default route properties.



a) Enter a **Name**, for example, **default**.
b) Click either the **IPv4** or **IPv6** radio button.

   You need to create separate default routes for IPv4 and IPv6.

c) Click **Gateway**, and then click **Create New Network** to add the gateway IP address as a host object.



d) Choose the gateway **Interface**, for example **outside**.

e) Click the **Networks** + icon, and choose **any-ipv4** for an IPv4 default route or **any-ipv6** for an IPv6 default route.

Step 4 Click **OK**.

Configure NAT

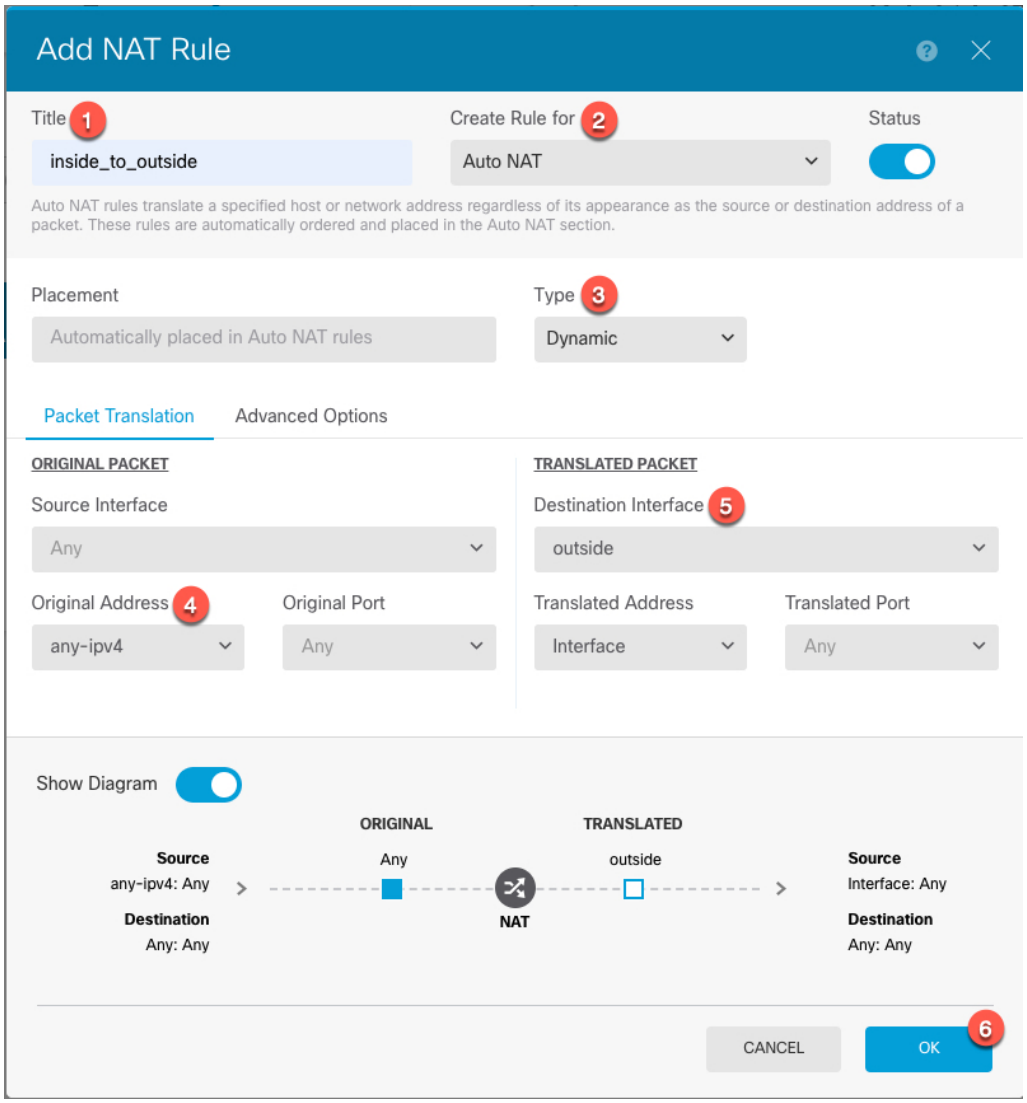
A typical NAT rule converts internal addresses to a port on the outside interface IP address. This type of NAT rule is called *interface Port Address Translation (PAT)*. You cannot use interface PAT for IPv6.

Procedure

Step 1 Click **Policies** and then click **NAT**.

Step 2 Click + or **Create NAT Rule**.

Step 3 Configure the basic rule options:



a) Set the **Title**.
b) Choose **Create Rule For** > **Auto NAT**.
c) Choose **Type** > **Dynamic**.

Step 4 Configure the following packet translation options:

a) For the **Original Packet**, set the **Original Address** as **any-ipv4**.

This rule will translate all IPv4 traffic originating on any interface. If you want to restrict the interfaces or the addresses, you can choose a specific **Source Interface** and specify IP addresses for the **Original Address**.

b) For the **Translated Packet**, set the **Destination Interface** to the outside interface.

By default, the interface IP address is used for the translated address.

Step 5 (Optional) Click **Show Diagram** to view a visual representation of the rule.

Step 6 Click **OK**.

Allow Traffic from Inside to Outside

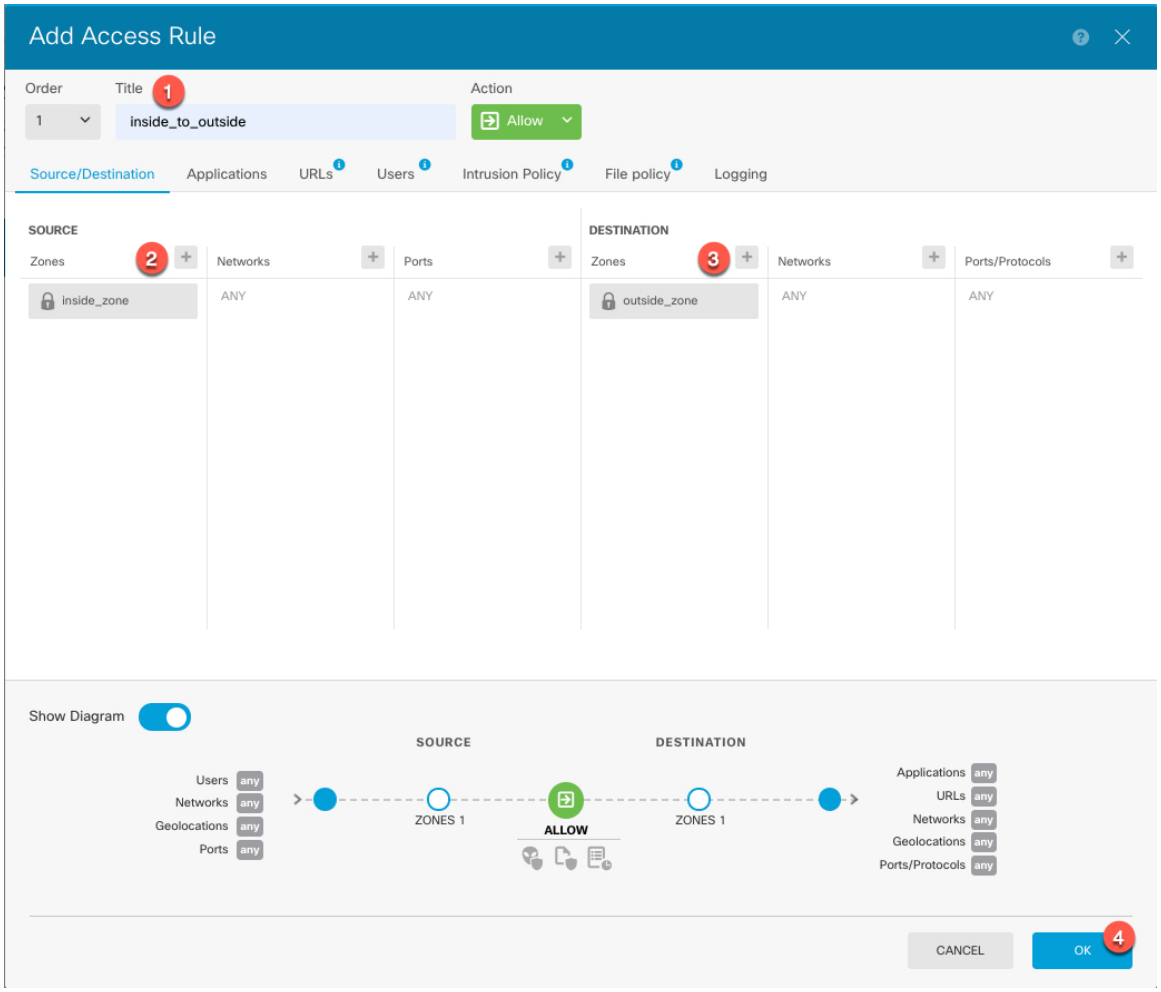
By default, traffic is blocked between security zones. This procedure shows how to allow traffic from inside to outside.

Procedure

Step 1 Choose **Policies** > **Access Control**.

Step 2 Click + or **Create Access Rule**.

Step 3 Configure the basic rule options:



a) Set the **Title**.

b) For the **Source**, click the **Zones** + icon, and choose the inside zone.

c) For the **Destination**, click the **Zones** + icon, and choose the outside zone.
d) (Optional) Click **Show Diagram** to view a visual representation of the rule.
e) Click **OK**.

(Optional) Configure the DHCP Server

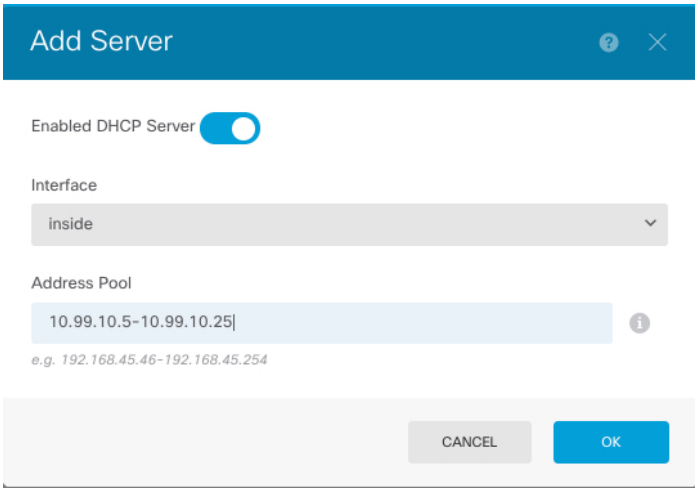
Enable the DHCP server if you want clients to use DHCP to obtain IP addresses from the threat defense.

Procedure

Step 1 Click **Device**, then click the **System Settings** > **DHCP Server** link.

Step 2 Click + or **Create DHCP Server**.

Step 3 Configure the server properties.



a) Click the **Enable DHCP Server** slider so that it shows enabled ( ).
b) Choose the **Interface** on which you want to enable the DHCP server.

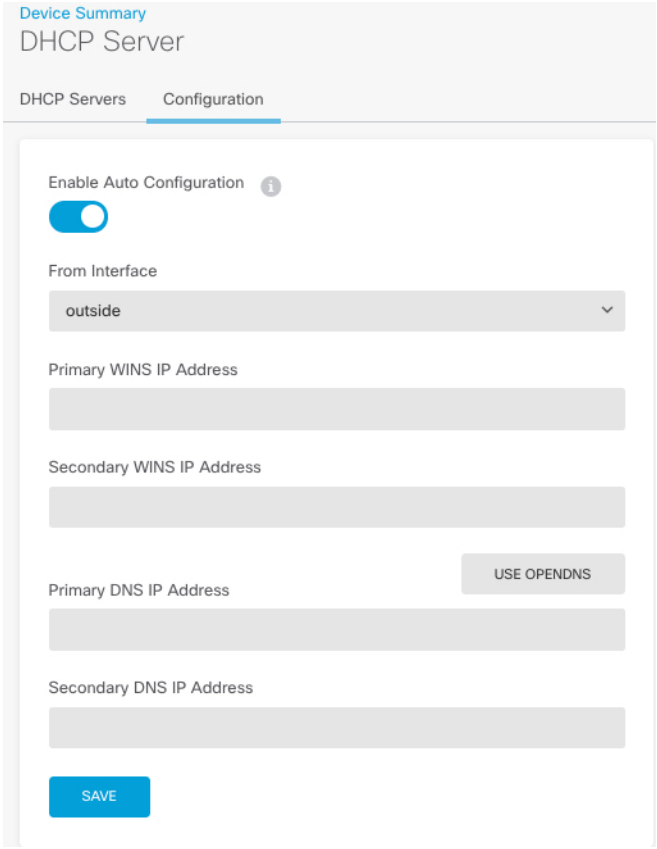
The interface must have a static IP address; you cannot be using DHCP to obtain the interface address if you want to run a DHCP server on the interface.

c) Enter the **Address Pool**

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, the broadcast address, or the subnet network address.

d) Click **OK**.

Step 4 (Optional) Click **Configuration** to configure auto-configuration and global settings.



DHCP auto configuration enables the DHCP Server to provide DHCP clients with DNS server, domain name, and WINS server information obtained from a DHCP client that is running on the specified interface. Typically, you would use auto-configuration if you are obtaining an address using DHCP on the outside interface, but you could choose any interface that obtains its address through DHCP. If you cannot use auto-configuration, you can manually define the required options.

a) Click the **Enable Auto Configuration** slider so that it shows enabled ( ).
b) Choose the interface in the **From Interface** drop-down menu from which you want clients to inherit server settings.
c) If you do not enable auto-configuration, or if you want to override any of the automatically configured settings, configure one or more global options. These settings will be sent to DHCP clients on all interfaces that run a DHCP server.
d) Click **Save**.

(Optional) Configure the Management Gateway and Allow Management on Data Interfaces

When you deployed the threat defense, you configured the management address and an external gateway. The following procedure lets you configure the threat defense to send management traffic over the backplane through the data interfaces instead of through the management interface. In this case, you can still manage

the threat defense if you are on a directly-connected management network, but management traffic destined for any other network will be routed out the data interfaces instead of through management.

Also, by default, you can only manage the threat defense through the management interface (device manager or CLI access). The following procedure also lets you enable management on one or more data interfaces. Note that the management interface gateway does not affect the device manager management traffic on data interfaces; in this case, the threat defense uses the regular routing table.

Before you begin

Configure data interfaces according to Configure Interfaces, on page 13.

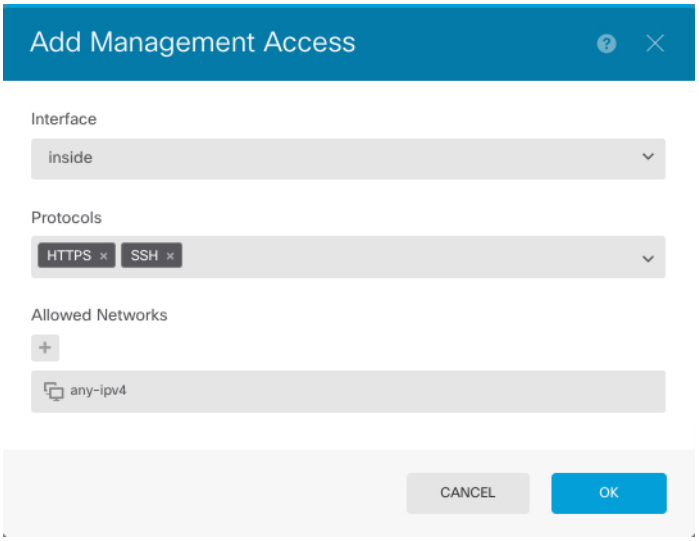
Procedure

Step 1 Allow management from a data interface.

a) Click **Device**, then click the **System Settings** > **Management Access** link.

b) Click **Data Interfaces**.

c) Click + or **Create Data Interface**, and create a rule for each interface:



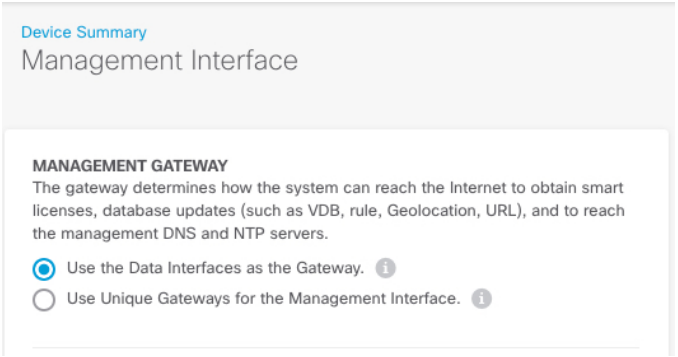
- **Interface**—Choose the interface on which you want to allow management access.
- **Protocols**—Choose whether the rule is for HTTPS (port 443), SSH (port 22), or both.
- **Allowed Networks**—Choose the network objects that define the IPv4 or IPv6 network or host that should be able to access the system. To specify "any" address, select **any-ipv4** (0.0.0.0/0) and **any-ipv6** (::/0).

d) Click **OK**.

Step 2 Set the management gateway to use the data interfaces.

a) Click **Device**, then click the **System Settings** > **Management Interface** link.

b) Choose **Use the Data Interfaces as the Gateway**.



c) Click **Save**, read the warning, and click **OK**.

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 the **Deploy Changes** icon in the upper right of the web page.

The icon is highlighted with a dot when there are undeployed changes.

The Pending Changes window shows a comparison of the deployed version of the configuration with the pending changes. These changes are color-coded to indicate removed, added, or edited elements. See the legend in the window for an explanation of the colors.

Step 2 If you are satisfied with the changes, you can click **Deploy Now** to start the job immediately.

The window will show that the deployment is in progress. You can close the window, or wait for deployment to complete. If you close the window while deployment is in progress, the job does not stop. You can see results in the task list or audit log. If you leave the window open, click the **Deployment History** link to view the results.

Access the Threat Defense 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, see the documents available for your software version at Navigating the Cisco Firepower Documentation.

For information related to using the device manager, see Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager.

History for Threat Defense with the Device Manager

Feature Name	Version	Feature Information
Support for device manager with native instances	6.5.0	You can now deploy a native instance using the device manager. New/Modified screens: **Logical Devices** > **Add Device** **Note** Requires FXOS 2.7.1.