



Threat Defense Deployment with the Management Center

Is This Chapter for You?

This chapter describes how to deploy a standalone threat defense logical device with the management center. To deploy a High Availability pair or a cluster, see the [Firepower Management Center Configuration Guide](#).

In a typical deployment on a large network, you install multiple managed devices on network segments. Each device controls, inspects, monitors, and analyzes traffic, and then reports to a managing the management center. The management center provides a centralized management console with a web interface that you can use to perform administrative, management, analysis, and reporting tasks in service to securing your local network.

For networks that include only a single device or just a few, where you do not need to use a high-powered multiple-device manager like the management center, you can use the integrated device manager. Use the device manager web-based device setup wizard to configure the basic features of the software that are most commonly used for small network deployments.

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.

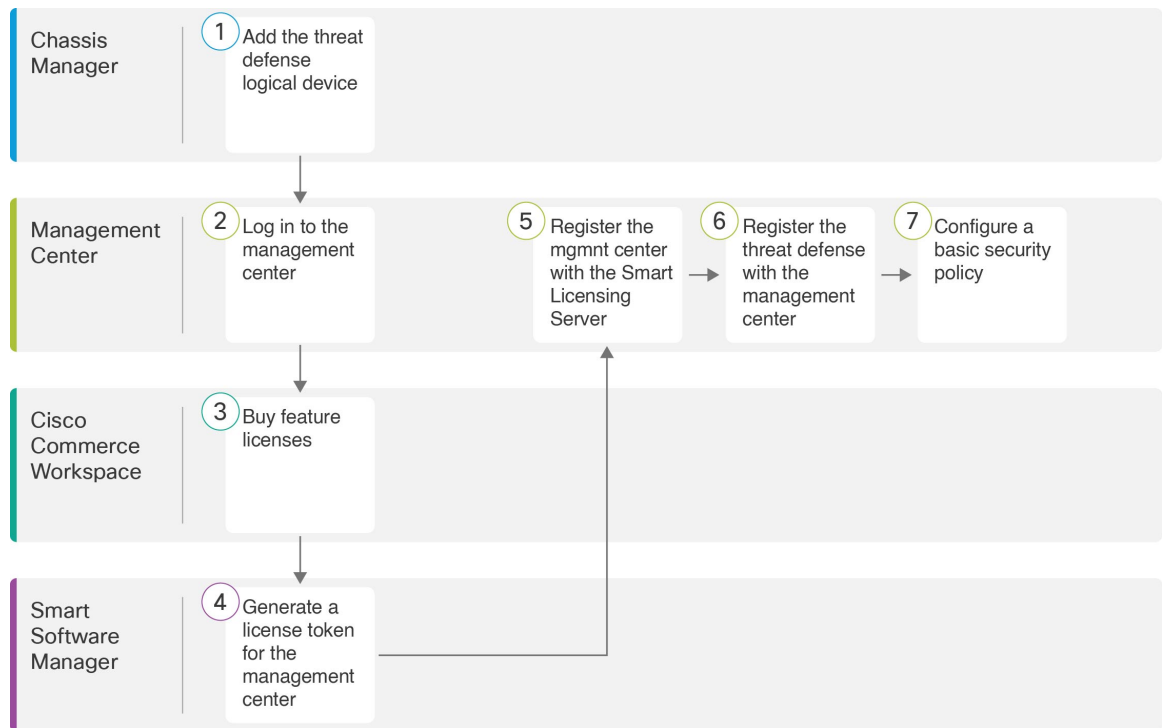
- [Before You Start, on page 2](#)
- [End-to-End Procedure, on page 2](#)
- [Chassis Manager: Add the Threat Defense Logical Device, on page 3](#)
- [Log Into the Management Center, on page 8](#)
- [Obtain Licenses for the Management Center, on page 9](#)
- [Register the Threat Defense with the Management Center, on page 11](#)
- [Configure a Basic Security Policy, on page 14](#)
- [Access the Threat Defense CLI, on page 25](#)
- [What's Next?, on page 27](#)
- [History for Threat Defense with the Management Center, on page 27](#)

Before You Start

Deploy and perform initial configuration of the management center. See the [Cisco Firepower Management Center 1600, 2600, and 4600 Hardware Installation Guide](#) or [Cisco Secure Firewall Management Center Virtual Getting Started Guide](#).

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 3.
②	Management Center	Log Into the Management Center, on page 8.
③	Cisco Commerce Workspace	Obtain Licenses for the Management Center, on page 9: Buy feature licenses.
④	Smart Software Manager	Obtain Licenses for the Management Center, on page 9: Generate a license token for the management center.
⑤	Management Center	Obtain Licenses for the Management Center, on page 9: Register the management center with the Smart Licensing server.

	Workspace	Steps
6	Management Center	Register the Threat Defense with the Management Center, on page 11.
7	Management Center	Configure a Basic Security Policy, on page 14.

Chassis Manager: Add the Threat Defense Logical Device

You can deploy the threat defense from the Firepower 4100 as either a native or container instance. You can deploy multiple container instances per security engine, but only one native instance. See [Logical Device Application Instances: Container or Native](#) for the maximum container instances per model.

To add a High Availability pair or a cluster, see the [Firepower Management Center Configuration Guide](#).

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. In 6.7 and later, 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.
- For container instances, if you do not want to use the default profile, which uses the minimum resources, add a resource profile on **Platform Settings > Resource Profiles**.
- For container instances, before you can install a container instance for the first time, you may need to reinitialize the security engine so that the disk has the correct formatting. If this action is required, you will not be able to save your logical device. Click **Security Engine**, and then click the Reinitialize icon (🔄).
- Gather the following information:
 - Interface IDs for this device
 - Management interface IP address and network mask
 - Gateway IP address
 - Management Center IP address and/or NAT ID of your choosing
 - DNS server IP address

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**.

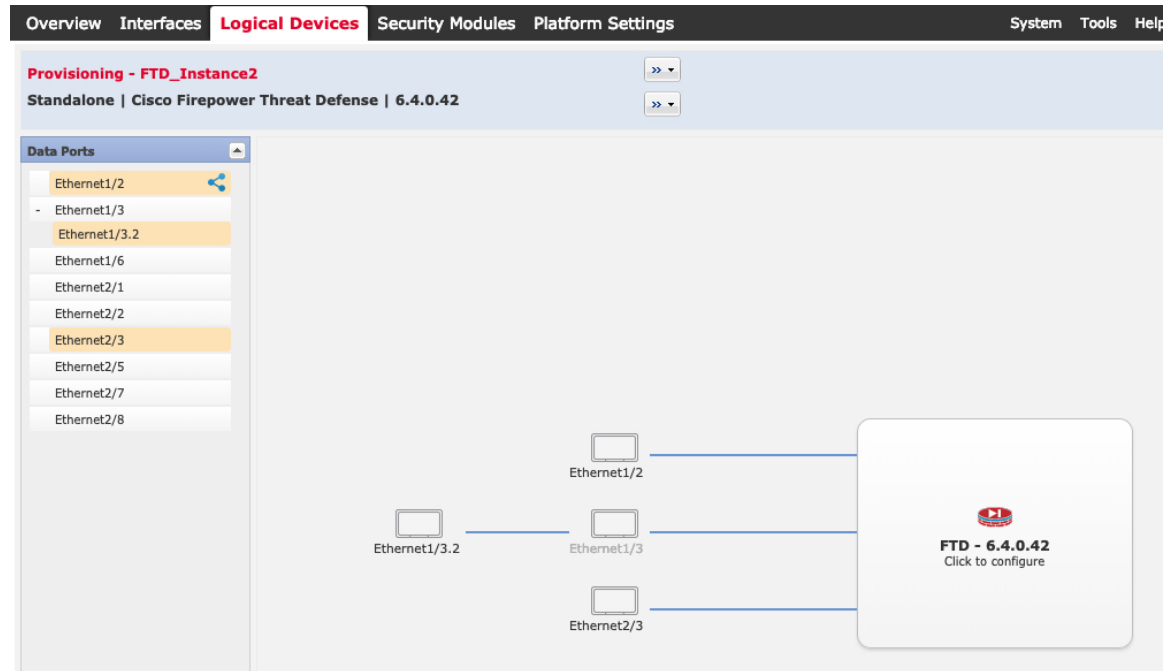
d) Choose the **Instance Type**: **Container** or **Native**.

A native instance uses all of the resources (CPU, RAM, and disk space) of the security module/engine, so you can only install one native instance. A container instance uses a subset of resources of the security module/engine, so you can install multiple container instances.


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 and Data-sharing interfaces that you previously enabled on the **Interfaces** page. You will later enable and configure these interfaces in the management center, including setting the IP addresses.

You can only assign up to 10 Data-sharing interfaces to a container instance. Also, each Data-sharing interface can be assigned to at most 14 container instances. A Data-sharing interface is indicated by the sharing icon ()

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 (see the [Firepower Management Center Configuration Guide](#) for information about Inline Sets). 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:

Cisco Firepower Threat Defense - Bootstrap Configuration

General Information Settings Agreement

SM 1 - 22 Cores Available

Resource Profile:

Interface Information

Management Interface:

Management

Address Type:

IPv4

Management IP:

Network Mask:

Network Gateway:

- a) For a container instance, specify the **Resource Profile**.
If you later assign a different resource profile, then the instance will reload, which can take approximately 5 minutes. Note that for established High Availability pairs or clusters, if you assign a different-sized resource profile, be sure to make all members the same size as soon as possible.
- b) Choose the **Management Interface**.
This interface is used to manage the logical device. This interface is separate from the chassis management port.
- c) Choose the management interface **Address Type**: **IPv4 only**, **IPv6 only**, or **IPv4 and IPv6**.
- d) Configure the **Management IP** address.
Set a unique IP address for this interface.
- e) Enter a **Network Mask** or **Prefix Length**.
- f) Enter a **Network Gateway** address.

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

Cisco Firepower Threat Defense - Bootstrap Configuration

General Information **Settings** Agreement

Management type of application instance:	FMC
Firepower Management Center IP:	10.89.5.35
Search domains:	cisco.com
Firewall Mode:	Routed
DNS Servers:	10.89.5.67
Firepower Management Center NAT ID:	test
Fully Qualified Hostname:	ftd2.cisco.com
Registration Key:
Confirm Registration Key:
Password:
Confirm Password:
Eventing Interface:	

- a) For a native instance, in the **Management type of application instance** drop-down list, choose **FMC**.
Native instances also support the device manager as a manager. After you deploy the logical device, you cannot change the manager type.
- b) Enter the **Firepower Management Center IP** or hostname of the managing the management center. If you do not know the management center IP address, leave this field blank and enter a passphrase in the **Firepower Management Center NAT ID** field.
- c) For a container instance, **Permit Expert mode from FTD SSH sessions: Yes or No**. Expert Mode provides the threat defense shell access for advanced troubleshooting.

If you choose **Yes** for this option, then users who access the container instance directly from an SSH session can enter Expert Mode. If you choose **No**, then only users who access the container instance from the FXOS CLI can enter Expert Mode. We recommend choosing **No** to increase isolation between instances.

Use Expert Mode only if a documented procedure tells you it is required, or if the Cisco Technical Assistance Center asks you to use it. To enter this mode, use the **expert** command in the threat defense CLI.

- d) Enter the **Search Domains** as a comma-separated list.
- e) 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.
- f) 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.
- g) Enter the **Fully Qualified Hostname** for the threat defense.

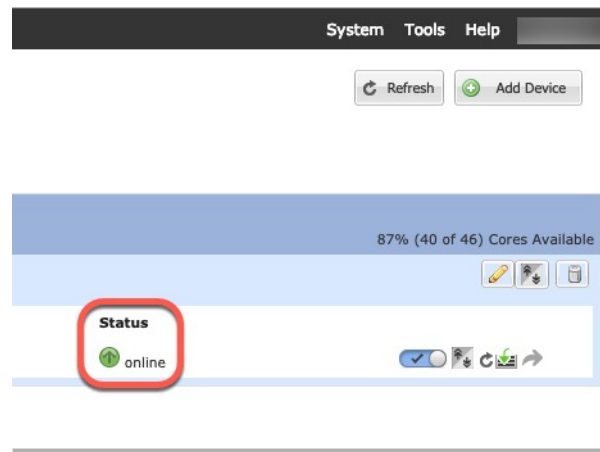
- h) Enter a **Registration Key** to be shared between the management center and the device during registration.
You can choose any text string for this key between 1 and 37 characters; you will enter the same key on the management center when you add the threat defense.
- i) Enter a **Password** for the threat defense admin user for CLI access.
- j) Choose the **Eventing Interface** on which events should be sent. If not specified, the management interface will be used.
This interface must be defined as a Firepower-eventing interface.
- k) For a container instance, set the **Hardware Crypto** as **Enabled** or **Disabled**.
This setting enables TLS crypto acceleration in hardware, and improves performance for certain types of traffic. For more information, see the [Firepower Management Center Configuration Guide](#). This feature is not supported for native instances. To view the percentage of hardware crypto resources allocated to this instance, enter the **show hw-crypto** command.

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 Management Center

Use the management center to configure and monitor the threat defense.

Before you begin

For information on supported browsers, refer to the release notes for the version you are using (see <https://www.cisco.com/go/firepower-notes>).

Procedure

- Step 1** Using a supported browser, enter the following URL.
- https://fmc_ip_address**
- Step 2** Enter your username and password.
- Step 3** Click **Log In**.
-

Obtain Licenses for the Management Center

All licenses are supplied to the threat defense by the management center. You can purchase 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
- **Carrier**—Diameter, GTP/GPRS, M3UA, SCTP

For a more detailed overview on Cisco Licensing, go to 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 1: License Search

Find Products and Solutions

L-FPR2K-ASASC-10=

Search by Product Family | Search for Solutions

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 the management center with the Smart Licensing server.

Registering requires you to generate a registration token in the Smart Software Manager. See the [Cisco Secure Firewall Management Center Administration Guide](#) for detailed instructions.

Register the Threat Defense with the Management Center

Register each logical device individually to the same management center.

Before you begin

- Make sure the threat defense logical device **Status** is **online** on the chassis manager **Logical Devices** page.
- Gather the following information that you set in the threat defense initial bootstrap configuration (see [Chassis Manager: Add the Threat Defense Logical Device, on page 3](#)):
 - The threat defense management IP address or hostname, and NAT ID
 - The management center registration key
- In 6.7 and later, if you want to use a data interface for management, use the **configure network management-data-interface** command at the threat defense CLI. See the [Cisco Secure Firewall Threat Defense Command Reference](#) for more information.

Procedure

- Step 1** In the management center, choose **Devices > Device Management**.
- Step 2** From the **Add** drop-down list, choose **Add Device**.

Add Device

Host:†
ftd-1.cisco.com

Display Name:
ftd-1.cisco.com

Registration Key:†

Group:
None

Access Control Policy:†
inside-outside

Smart Licensing

Malware
 Threat
 URL Filtering

Advanced

Unique NAT ID:†
natid56

Transfer Packets

Cancel Register

Set the following parameters:

- **Host**—Enter the IP address or hostname of the threat defense you want to add. You can leave this field blank if you specified both the management center IP address and a NAT ID in the threat defense initial bootstrap configuration.

Note In an HA environment, when both the management centers are behind a NAT, you can register the threat defense without a host IP or name in the primary management center. However, for registering the threat defense in a secondary management center, you must provide the IP address or hostname for the threat defense.
- **Display Name**—Enter the name for the threat defense as you want it to display in the management center.
- **Registration Key**—Enter the same registration key that you specified in the threat defense initial bootstrap configuration.
- **Domain**—Assign the device to a leaf domain if you have a multidomain environment.
- **Group**—Assign it to a device group if you are using groups.
- **Access Control Policy**—Choose an initial policy. Unless you already have a customized policy you know you need to use, choose **Create new policy**, and choose **Block all traffic**. You can change this later to allow traffic; see [Allow Traffic from Inside to Outside](#), on page 22.

Figure 2: New Policy

New Policy ?

Name:

Description:

Select Base Policy:

Default Action:
 Block all traffic
 Intrusion Prevention
 Network Discovery

- **Smart Licensing**—Assign the Smart Licenses you need for the features you want to deploy: **Malware** (if you intend to use malware inspection), **Threat** (if you intend to use intrusion prevention), and **URL** (if you intend to implement category-based URL filtering). **Note:** You can apply an Secure Client remote access VPN license after you add the device, from the **System > Licenses > Smart Licenses** page.
- **Unique NAT ID**—Specify the NAT ID that you specified in the threat defense initial bootstrap configuration.
- **Transfer Packets**—Allow the device to transfer packets to the management center. When events like IPS or Snort are triggered with this option enabled, the device sends event metadata information and packet data to the management center for inspection. If you disable it, only event information will be sent to the management center, but packet data is not sent.

Step 3 Click **Register**, or if you want to add another device, click **Register and Add Another** and confirm a successful registration.

If the registration succeeds, the device is added to the list. If it fails, you will see an error message. If the threat defense fails to register, check the following items:

- **Ping**—Access the threat defense CLI ([Access the Threat Defense CLI, on page 25](#)), and ping the management center IP address using the following command:

```
ping system ip_address
```

If the ping is not successful, check your network settings using the **show network** command. If you need to change the threat defense Management IP address, use the **configure network {ipv4 | ipv6} manual** command. If you configured a data interface for the management center access, use the **configure network management-data-interface** command.

- **NTP**—Make sure the Firepower 4100 NTP server matches the management center server set on the **System > Configuration > Time Synchronization** page.

- Registration key, NAT ID, and the management center IP address—Make sure you are using the same registration key, and if used, NAT ID, on both devices. You can set the registration key and NAT ID on the management center using the **configure manager add** command.

For more troubleshooting information, see <https://cisco.com/go/fmc-reg-error>.

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, on page 14.
2	Configure the DHCP Server, on page 18.
3	Add the Default Route, on page 19.
4	Configure NAT, on page 20.
5	Allow Traffic from Inside to Outside, on page 22.
6	Deploy the Configuration, on page 23.

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.

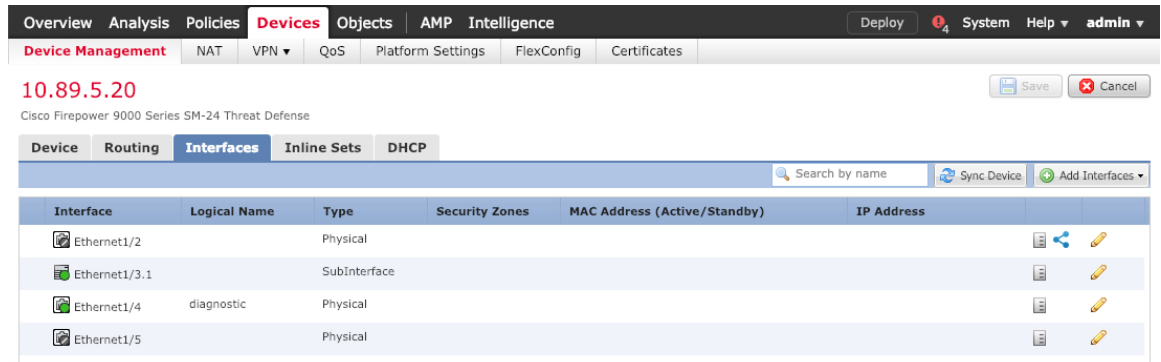
A typical edge-routing situation is to obtain the outside interface address through DHCP from your ISP, while you define static addresses on the inside interfaces.

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

Procedure

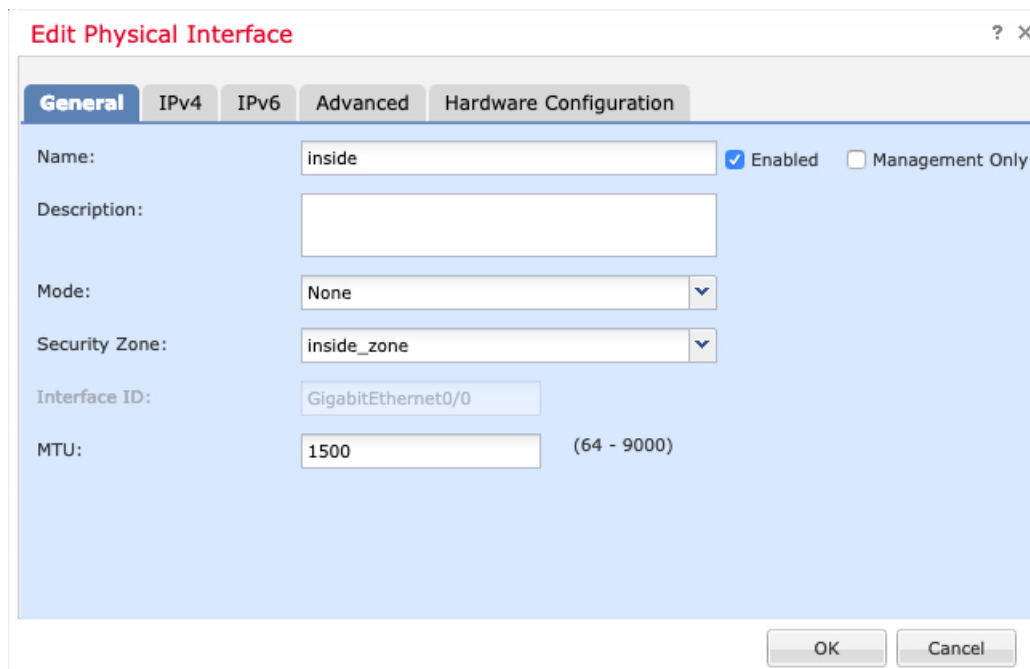
Step 1 Choose **Devices > Device Management**, and click the **Edit** (✎) for the firewall.

Step 2 Click **Interfaces**.



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

The **General** tab appears.



- 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**.

- d) 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.

- e) 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**

The screenshot shows the 'Edit Physical Interface' configuration window with the 'IPv4' tab selected. The 'IP Type' dropdown is set to 'Use Static IP'. The 'IP Address' field contains '192.168.1.1/24'. To the right of the IP address field, there are example addresses: 'eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25'. The window has tabs for 'General', 'IPv4', 'IPv6', 'Advanced', and 'Hardware Configuration'.

- **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.

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

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. The 'Selected Network' pane has a list with 'any-ipv4' selected. An 'Add' button is between the panes. At the bottom, there 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 right.

- **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.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy 4 System Help admin

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates

10.89.5.20 You have unsaved changes Save Cancel

Cisco Firepower 9000 Series SM-24 Threat Defense

Device **Routing** Interfaces Inline Sets DHCP

OSPF
OSPFv3
RIP
BGP
Static Route
Multicast Routing

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

Add Route

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**.

New Policy ? x

Name:

Description:

Targeted Devices

Select devices to which you want to apply this policy.

Available Devices

Selected Devices

The policy is added to 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: Interface Objects (selected), Translation, PAT Pool, Advanced
- Available Interface Objects: Search by name, inside_zone, outside_zone (highlighted with a red circle and '1').
- Source Interface Objects (0): any
- Destination Interface Objects (1): outside_zone (highlighted with a red circle and '3').
- Buttons: Add to Source, Add to Destination (highlighted with a red circle and '2').
- Bottom buttons: OK, Cancel

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: Interface Objects, Translation (selected), PAT Pool, Advanced
- Original Packet: Original Source:* all-ipv4 (highlighted with a red circle), Original Port: TCP
- Translated Packet: Translated Source: Destination Interface IP (highlighted with a red circle), 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.

interface_PAT

Rules

#	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 'Name' field is 'inside_to_outside', 'Enabled' is checked, and 'Insert' is set to 'into Mandatory'. The 'Action' is 'Allow'. The 'Zones' tab is selected, showing 'Available Zones' with 'inside_zone' and 'outside_zone'. 'Source Zones' contains 'inside_zone' and 'Destination Zones' contains 'outside_zone'.

- **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 'Policies' configuration page. The 'Rules' table is visible, showing the rule 'inside_to_outside' under the 'Mandatory - ftd_ac_policy (1-1)' category. The table has columns for Name, Source Zones, Dest Zones, Source Net..., Dest Netw..., VLAN Tags, Users, Applications, Source Po..., Dest Ports, URLs, ISE/SGT A..., and Action.

#	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**.

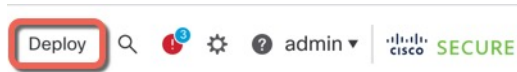
Deploy the Configuration

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 3: Deploy



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

Figure 4: Deploy All

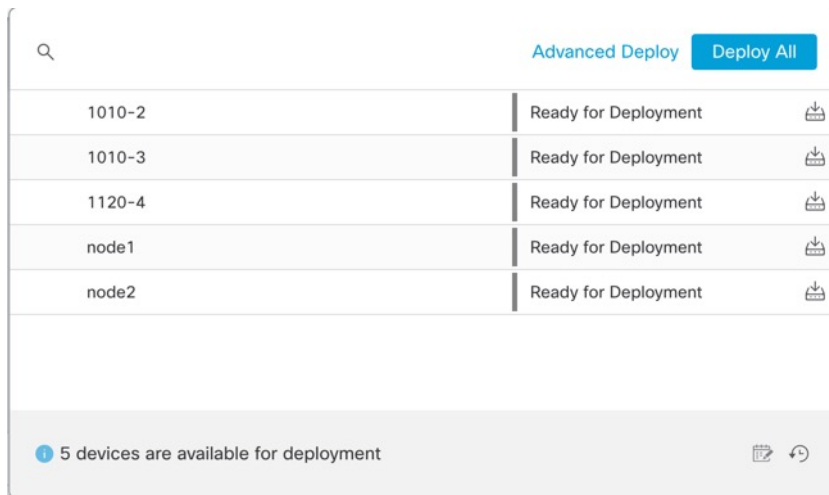
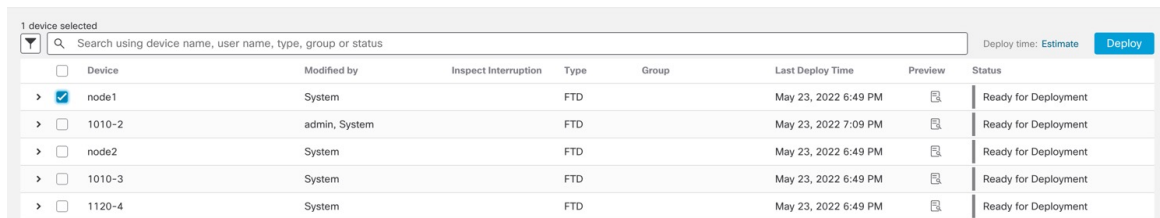
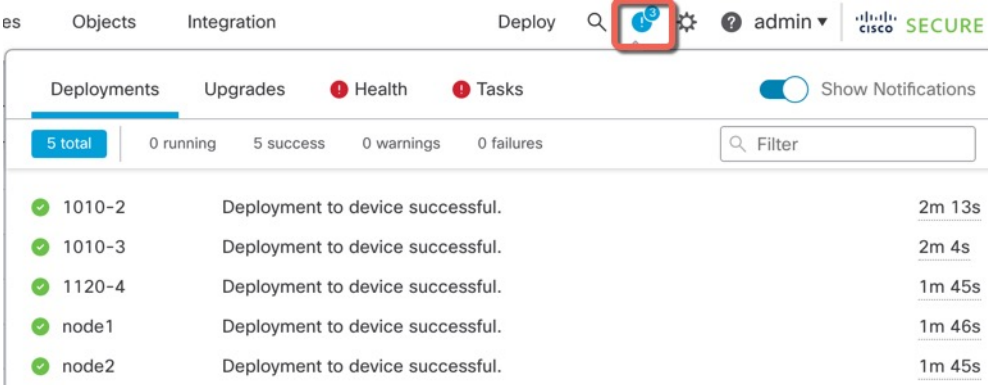


Figure 5: Advanced Deploy



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 6: Deployment Status



Deployment ID	Status	Message	Time
1010-2	Success	Deployment to device successful.	2m 13s
1010-3	Success	Deployment to device successful.	2m 4s
1120-4	Success	Deployment to device successful.	1m 45s
node1	Success	Deployment to device successful.	1m 46s
node2	Success	Deployment to device successful.	1m 45s

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 management center, see the [Firepower Management Center Configuration Guide](#).

History for Threat Defense with the Management Center

Feature Name	Version	Feature Information
Support for ASA and threat defense on separate modules of the same Firepower 9300	6.4	You can now deploy the ASA and the threat defense logical devices on the same Firepower 9300. Note Requires FXOS 2.6.1.
Threat Defense for the Firepower 4115, 4125, and 4145	6.4	We introduced the Firepower 4115, 4125, and 4145. Note Requires FXOS 2.6.1.

Feature Name	Version	Feature Information
Multi-instance capability for threat defense on the Firepower 4100/9300	6.3.0	<p>You can now deploy multiple logical devices, each with the threat defense container instance, on a single security engine/module. Formerly, you could only deploy a single native application instance.</p> <p>To provide flexible physical interface use, you can create VLAN subinterfaces in FXOS and also share interfaces between multiple instances. Resource management lets you customize performance capabilities for each instance.</p> <p>You can use High Availability using a container instance on 2 separate chassis. Clustering is not supported.</p> <p>Note Multi-instance capability is similar to ASA multiple context mode, although the implementation is different. Multiple context mode is not available on the threat defense.</p> <p>New/Modified management center screens:</p> <ul style="list-style-type: none"> • Devices > Device Management > Edit icon > Interfaces tab <p>New/Modified chassis manager screens:</p> <ul style="list-style-type: none"> • Overview > Devices • Interfaces > All Interfaces > Add New drop-down menu > Subinterface • Interfaces > All Interfaces > Type • Logical Devices > Add Device • Platform Settings > Mac Pool • Platform Settings > Resource Profiles