Threat Defense Deployment with the Management Center

Is This Chapter for You?

To see all available applications and managers, see Which Application and Manager is Right for You?. This chapter applies to the threat defense with the management center.

This chapter explains how to manage the threat defense with a management center located on your management network. For remote branch deployment, where the management center resides at a central headquarters, see Threat Defense Deployment with a Remote Management Center.

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 Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide.

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 3100/4200 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.
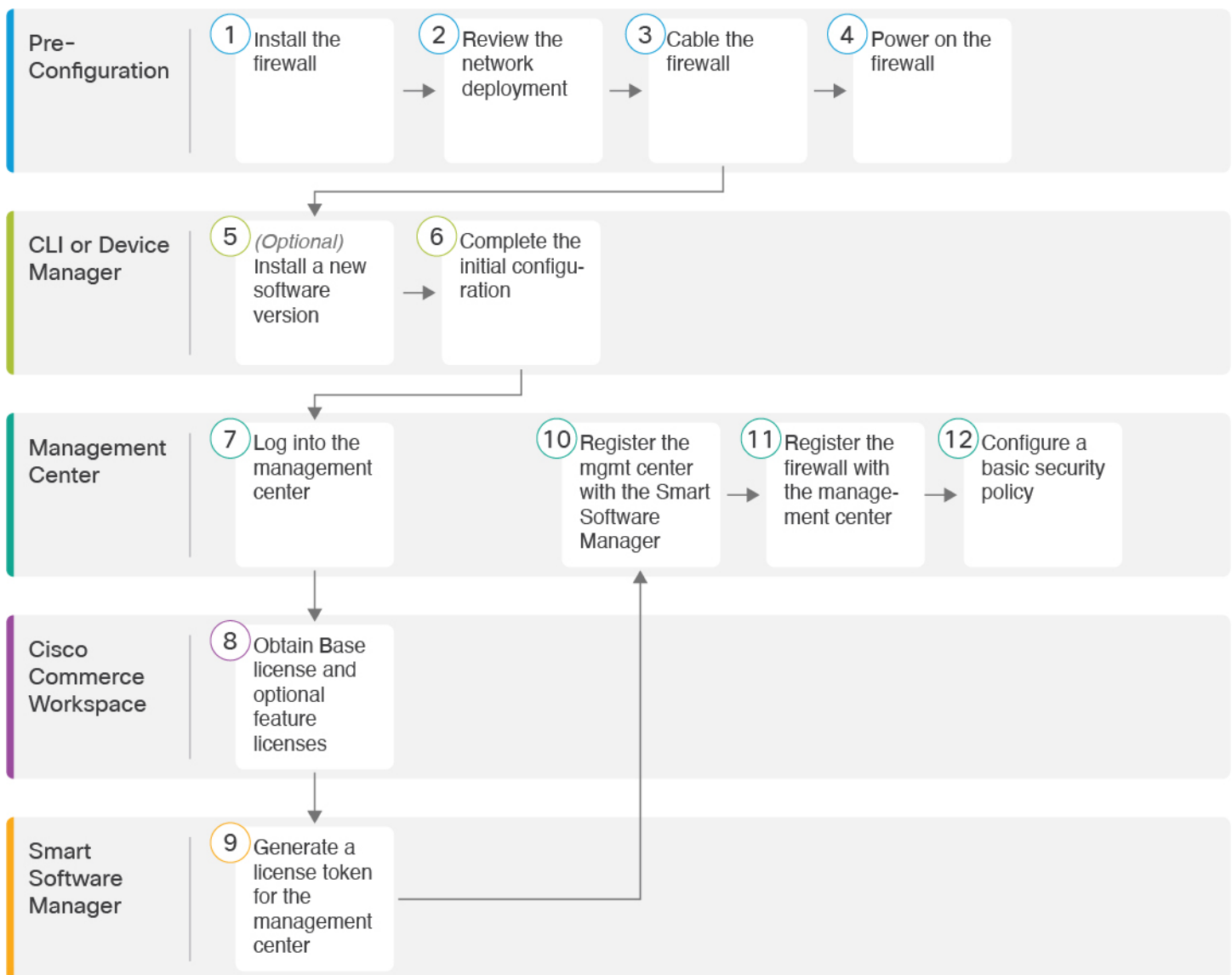
Before You Start

Deploy and perform initial configuration of the management center. See the getting started guide for your model.

End-to-End Tasks

1	Pre-Configuration	Install the firewall. See the hardware installation guide.
2	Pre-Configuration	Review the Network Deployment, on page 3.
3	Pre-Configuration	Cable the Firewall, on page 5.
4	Pre-Configuration	Power on the Firewall, on page 7.
5	CLI	(Optional) Check the Software and Install a New Version, on page 8.
6	CLI or Device Manager	Complete the Threat Defense Initial Configuration, on page 10.
7	Management Center	Log Into the Management Center, on page 18.
8	Cisco Commerce Workspace	Buy Base license and optional feature licenses (Obtain Licenses for the Management Center, on page 18).
9	Smart Software Manager	Generate a license token for the management center (Obtain Licenses for the Management Center, on page 18).
10	Management Center	Register the management center with the Smart Licensing server (Obtain Licenses for the Management Center, on page 18).
11	Management Center	Register the Threat Defense with the Management Center, on page 20.
12	Management Center	Configure a Basic Security Policy, on page 24.

Review the Network Deployment

Management Interface

The management center communicates with the threat defense on the Management interface.

The dedicated Management interface is a special interface with its own network settings:

- By default, the Management 1/1 interface is enabled and configured as a DHCP client. If your network does not include a DHCP server, you can set the Management interface to use a static IP address during initial setup at the console port.

- Both the threat defenseand the management center require internet access from their management interfaces for licensing and updates.

✎

Note   The management connection is a secure, TLS-1.3-encrypted communication channel between itself and the device. You do not need to run this traffic over an additional encrypted tunnel such as Site-to-Site VPN for security purposes. If the VPN goes down, for example, you will lose your management connection, so we recommend a simple management path.

Data Interfaces

You can configure other interfaces after you connect the threat defense to the management center.

Typical Separate Management Network Deployment

The following figure shows a typical network deployment for the firewall where the threat defense, management center, and management computer connect to the management network.

The management network has a path to the internet for licensing and updates.

*Figure 1: Separate Management Network*
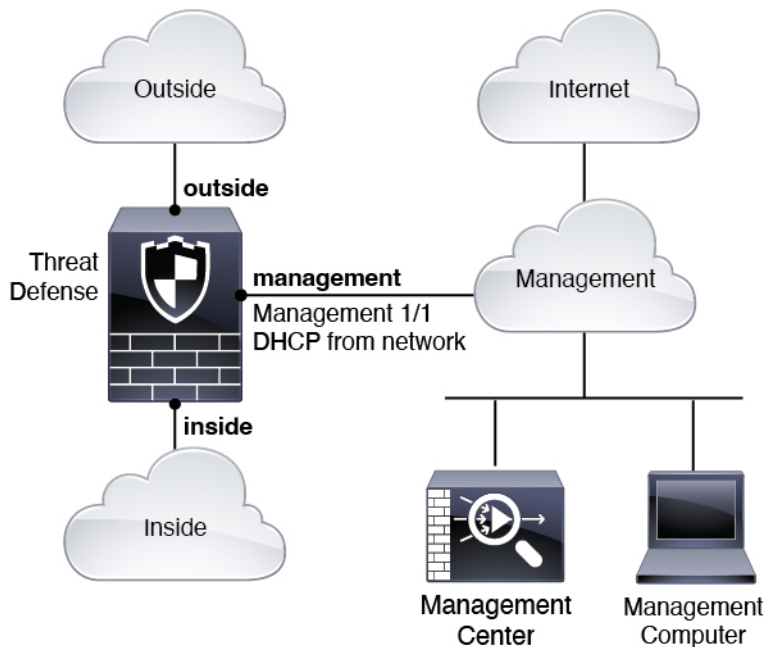
Typical Edge Network Deployment

The following figure shows a typical network deployment for the firewall where:

- Inside acts as the internet gateway for Management and for the management center.

- Management 1/1 connects to an inside interface through a Layer 2 switch.

- The management center and management computer connect to the switch.

This direct connection is allowed because the Management interface has separate routing from the other interfaces on the threat defense.

Figure 2: Edge Network Deployment
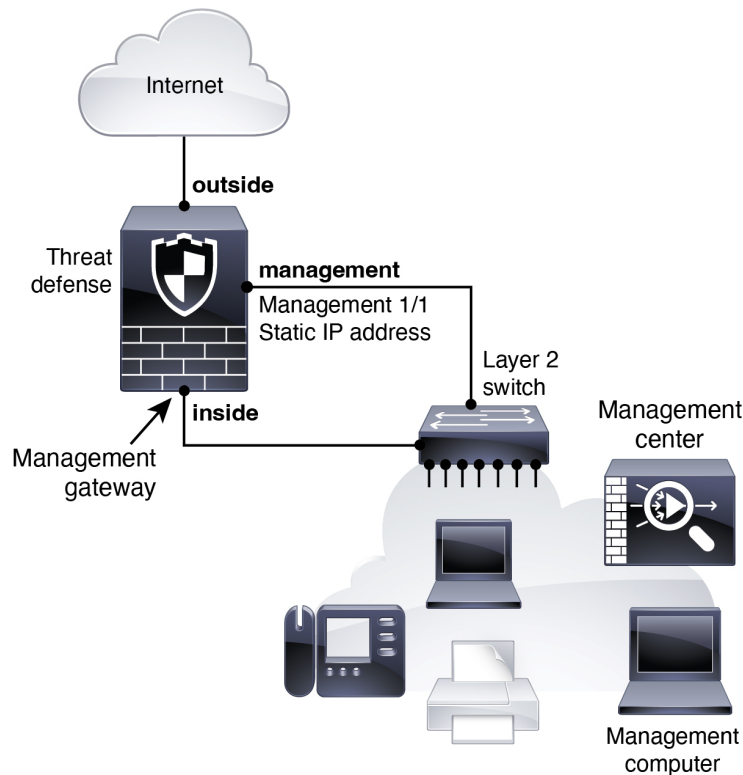
Cable the Firewall

To cable one of the recommended scenarios on the Secure Firewall 3100, see the following steps.

> **Note**   Other topologies can be used, and your deployment will vary depending on your basic logical network connectivity, ports, addressing, and configuration requirements.

Before you begin

- Install an SFP for the Management port—The Management port is a 1/10-Gb SFP port that requires an SFP module.

- Obtain a console adapter—The Secure Firewall 3100 ships with a DB-9 to RJ-45 serial cable, so you may need to buy a third party DB-9-to-USB serial cable to make the connection.

Procedure

Step 1   Install the chassis. See the hardware installation guide.

**Step 2**   Cable for a separate management network:

Figure 3: Cabling a Separate Management Network
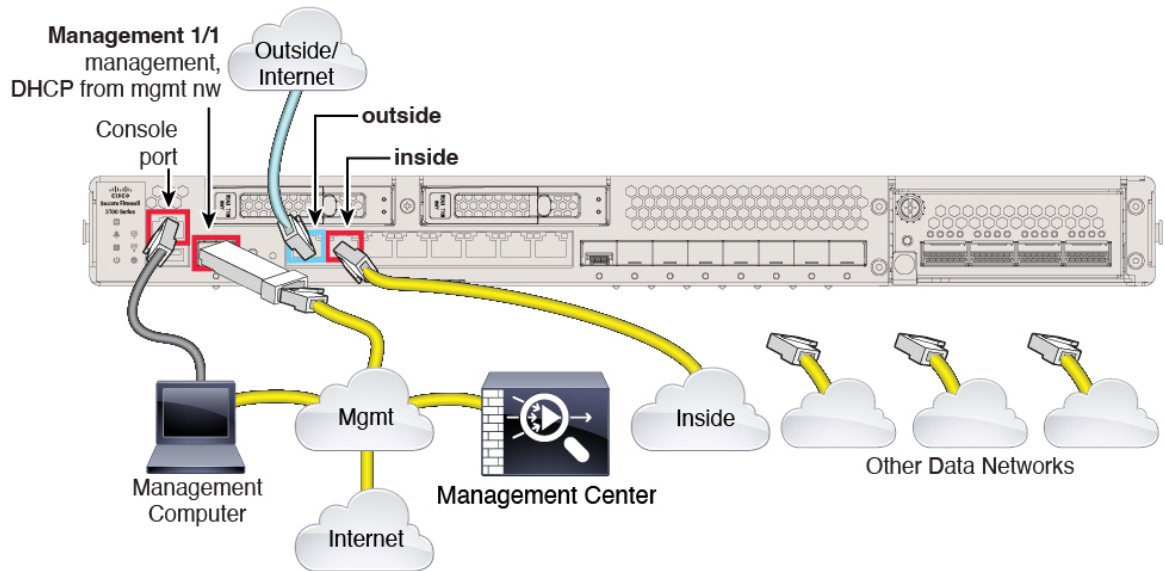
a) Cable the following to your management network:

   • Management 1/1 interface

   • Secure Firewall Management Center

   • Management computer

b) Connect the management computer to the console port. You need to use the console port to access the CLI for initial setup if you do not use SSH to the Management interface.

c) Connect the inside interface (for example, Ethernet 1/2) to your inside router.

d) Connect the outside interface (for example, Ethernet 1/1) to your outside router.

e) Connect other networks to the remaining interfaces.

Step 3 Cable for an edge deployment:

Figure 4: Cabling an Edge Deployment
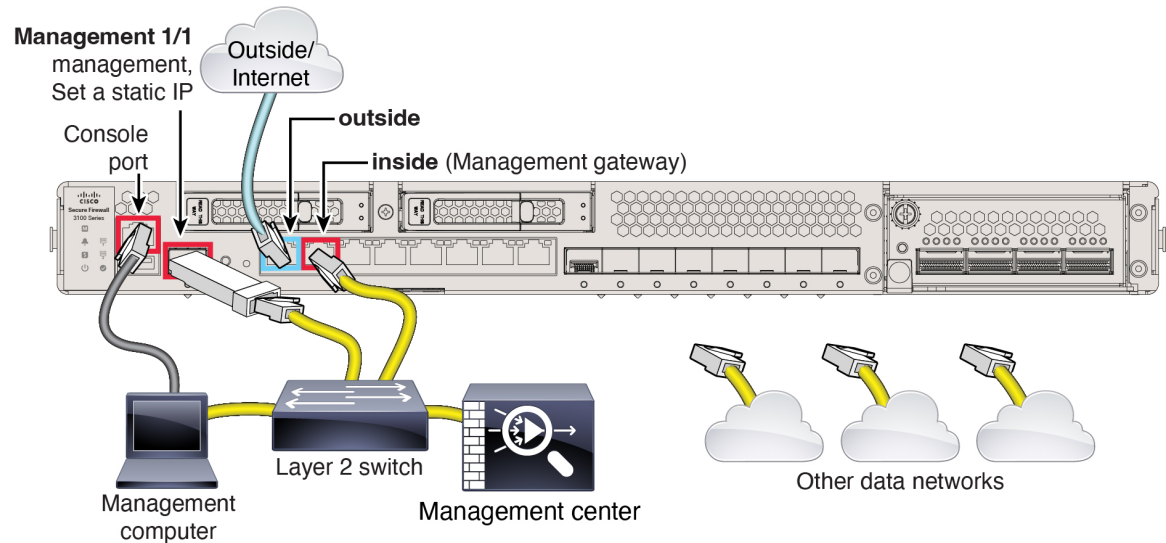
a) Cable the following to a Layer 2 Ethernet switch:

- Inside interface (for example, Ethernet 1/2)
- Management 1/1 interface
- Secure Firewall Management Center
- Management computer

b) Connect the management computer to the console port. You need to use the console port to access the CLI for initial setup.

c) Connect the outside interface (for example, Ethernet 1/1) to your outside router.

d) Connect other networks to the remaining interfaces.

Power on the Firewall

System power is controlled by a rocker power switch located on the rear of the firewall. The power switch is implemented as a soft notification switch that supports graceful shutdown of the system to reduce the risk of system software and data corruption.

Note The first time you boot up the threat defense, initialization can take approximately 15 to 30 minutes.

Before you begin

It's important that you provide reliable power for your firewall (for example, using an uninterruptable power supply (UPS)). Loss of power without first shutting down can cause serious file system damage. There are

many processes running in the background all the time, and losing power does not allow the graceful shutdown of your system.

Procedure

Step 1   Attach the power cord to the firewall, and connect it to an electrical outlet.

Step 2   Turn the power on using the standard rocker-type power on/off switch located on the rear of the chassis, adjacent to the power cord.

Step 3   Check the Power LED on the back of the firewall; if it is solid green, the firewall is powered on.

Figure 5: System and Power LEDs
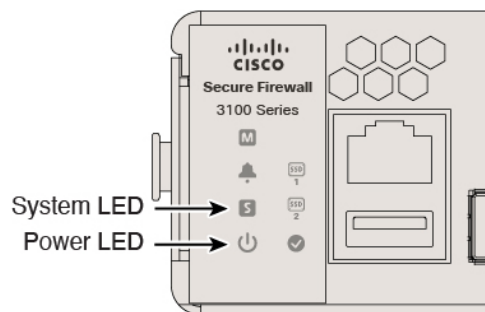
Step 4   Check the System LED on the back of the firewall; after it is solid green, the system has passed power-on diagnostics.

Note   When the switch is toggled from ON to OFF, it may take several seconds for the system to eventually power off. During this time, the Power LED on the front of the chassis blinks green. Do not remove the power until the Power LED is completely off.

(Optional) Check the Software and Install a New Version

To check the software version and, if necessary, install a different version, perform these steps. We recommend that you install your target version before you configure the firewall. Alternatively, you can perform an upgrade after you are up and running, but upgrading, which preserves your configuration, may take longer than using this procedure.

What Version Should I Run?

Cisco recommends running a Gold Star release indicated by a gold star next to the release number on the software download page. You can also refer to the release strategy described in https://www.cisco.com/c/en/us/products/collateral/security/firewalls/bulletin-c25-743178.html; for example, this bulletin describes short-term release numbering (with the latest features), long-term release numbering (maintenance releases and patches for a longer period of time), or extra long-term release numbering (maintenance releases and patches for the longest period of time, for government certification).

Procedure

Step 1 Connect to the console port. See Access the Threat Defense and FXOS CLI, on page 39 for more information.

Log in with the **admin** user and the default password, **Admin123**.

You connect to the FXOS CLI. The first time you log in, you are prompted to change the password. This password is also used for the threat defense login for SSH.

Note If the password was already changed, and you do not know it, you must perform a factory reset to reset the password to the default. See the FXOS troubleshooting guide for the factory reset procedure.

Example:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

Step 2 At the FXOS CLI, show the running version.

scope ssa

show app-instance

Example:

```
Firepower# scope ssa
Firepower /ssa # show app-instance

Application Name     Slot ID    Admin State     Operational State    Running Version Startup
 Version Cluster Oper State
-------------------- ---------- --------------- -------------------- ---------------
--------------- -----------------
ftd                  1          Enabled         Online               7.6.0.65        7.6.0.65
        Not Applicable
```

Step 3 If you want to install a new version, perform these steps.

a) If you need to set a static IP address for the Management interface, see Complete the Threat Defense Initial Configuration Using the CLI, on page 10. By default, the Management interface uses DHCP.

You will need to download the new image from a server accessible from the Management interface.

b) Perform the reimage procedure in the FXOS troubleshooting guide.

After the firewall reboots, you connect to the FXOS CLI again.

c) At the FXOS CLI, you are prompted to set the admin password again.

Complete the Threat Defense Initial Configuration

You can complete the threat defense initial configuration using the CLI or device manager.

Complete the Threat Defense Initial Configuration Using the CLI

Set the Management IP address, gateway, and other basic networking settings using the setup wizard. The dedicated Management interface is a special interface with its own network settings. If you do not want to use the Management interface for the manager access, you can use the CLI to configure a data interface instead. You will also configure the management center communication settings. When you perform initial setup using the device manager, *all* interface configuration completed in the device manager is retained when you switch to the management center for management, in addition to the Management interface and manager access interface settings. Note that other default configuration settings, such as the access control policy, are not retained.

Procedure

Step 1 Connect to the threat defense CLI, either from the console port or using SSH to the Management interface, which obtains an IP address from a DHCP server by default. If you intend to change the network settings, we recommend using the console port so you do not get disconnected.

The console port connects to the FXOS CLI. The SSH session connects directly to the threat defense CLI.

Step 2 Log in with the username **admin** and the password **Admin123**.

At the console port, you connect to the FXOS CLI. The first time you log in to FXOS, you are prompted to change the password. This password is also used for the threat defense login for SSH.

Note If the password was already changed, and you do not know it, you must reimage the device to reset the password to the default. See the FXOS troubleshooting guide for the reimage procedure.

Example:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

Step 3   If you connected to FXOS on the console port, connect to the threat defense CLI.

connect ftd

Example:

```
firepower# connect ftd
>
```

Step 4   The first time you log in to the threat defense, you are prompted to accept the End User License Agreement (EULA) and, if using an SSH connection, to change the admin password. You are then presented with the CLI setup script.

Note   You cannot repeat the CLI setup wizard unless you clear the configuration; for example, by reimaging. However, all of these settings can be changed later at the CLI using **configure network** commands. See Cisco Secure Firewall Threat Defense Command Reference.

Defaults or previously entered values appear in brackets. To accept previously entered values, press **Enter**.

See the following guidelines:

- **Do you want to configure IPv4?** and/or **Do you want to configure IPv6?**—Enter **y** for at least one of these types of addresses. For the edge deployment example shown in the network deployment section, set a static IP address because the gateway inside interface does not yet have a DHCP server running.

- **Enter the IPv4 default gateway for the management interface** and/or **Enter the IPv6 gateway for the management interface**—Set a gateway IP address for Management 1/1 on the management network. In the edge deployment example shown in the network deployment section, the inside interface acts as the management gateway. In this case, you should set the gateway IP address to be the *intended* inside interface IP address; you must later use the management center to set the inside IP address. The **data-interfaces** setting applies only to the remote management center or device manager management.

- **If your networking information has changed, you will need to reconnect**—If you are connected with SSH but you change the IP address at initial setup, you will be disconnected. Reconnect with the new IP address and password. Console connections are not affected.

- **Manage the device locally?**—Enter **no** to use the management center. A **yes** answer means you will use the device manager instead.

- **Configure firewall mode?**—We recommend that you set the firewall mode at initial configuration. Changing the firewall mode after initial setup erases your running configuration.

Example:

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
End User License Agreement
[...]

Please enter 'YES' or press <ENTER> to AGREE to the EULA:

System initialization in progress.  Please stand by.
You must change the password for 'admin' to continue.
Enter new password: ********
Confirm new password: ********
You must configure the network to continue.
Configure at least one of IPv4 or IPv6 unless managing via data interfaces.
Do you want to configure IPv4? (y/n) [y]:
```

```
Do you want to configure IPv6? (y/n) [y]:n
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.10.15
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]: 10.10.10.1
Enter a fully qualified hostname for this system [firepower]: ftd-1.cisco.com
Enter a comma-separated list of DNS servers or 'none'
[208.67.222.222,208.67.220.220,2620:119:35::35]:
Enter a comma-separated list of search domains or 'none' []:cisco.com
If your networking information has changed, you will need to reconnect.
Disabling IPv6 configuration: management0
Setting DNS servers: 208.67.222.222,208.67.220.220,2620:119:35::35
Setting DNS domains:cisco.com
Setting hostname as ftd-1.cisco.com
Setting static IPv4: 10.10.10.15 netmask: 255.255.255.192 gateway: 10.10.10.1 on management0
Updating routing tables, please wait...
All configurations applied to the system. Took 3 Seconds.
Saving a copy of running network configuration to local disk.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: no
DHCP server is already disabled
DHCP Server Disabled
Configure firewall mode? (routed/transparent) [routed]:
Configuring firewall mode ...


Device is in OffBox mode - disabling/removing port 443 from iptables.
Update policy deployment information
    - add device configuration
    - add network discovery
    - add system policy

You can register the sensor to a Firepower Management Center and use the
Firepower Management Center to manage it. Note that registering the sensor
to a Firepower Management Center disables on-sensor Firepower Services
management capabilities.

When registering the sensor to a Firepower Management Center, a unique
alphanumeric registration key is always required.  In most cases, to register
a sensor to a Firepower Management Center, you must provide the hostname or
the IP address along with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'

However, if the sensor and the Firepower Management Center are separated by a
NAT device, you must enter a unique NAT ID, along with the unique registration
key.
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'

Later, using the web interface on the Firepower Management Center, you must
use the same registration key and, if necessary, the same NAT ID when you add
this sensor to the Firepower Management Center.
>
```

Step 5   Identify the management center that will manage this threat defense.

configure manager add {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} *reg_key* [*nat_id*]

- {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**}—Specifies either the FQDN or IP address of the management center. If the management center is not directly addressable, use **DONTRESOLVE** and also specify the *nat_id*. At least one of the devices, either the management center or the threat defense, must have a reachable IP address to establish the two-way, SSL-encrypted communication channel

between the two devices. If you specify **DONTRESOLVE** in this command, then the threat defense must have a reachable IP address or hostname.

- *reg_key*—Specifies a one-time registration key of your choice that you will also specify on the management center when you register the threat defense. The registration key must not exceed 37 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-).

- *nat_id*—Specifies a unique, one-time string of your choice that you will also specify on the management center when you register the threat defense when one side does not specify a reachable IP address or hostname. It is required if you set the management center to **DONTRESOLVE**. The NAT ID must not exceed 37 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-). This ID cannot be used for any other devices registering to the management center.

Example:

```
> configure manager add MC.example.com 123456
Manager successfully configured.
```

If the management center is behind a NAT device, enter a unique NAT ID along with the registration key, and specify DONTRESOLVE instead of the hostname, for example:

Example:

```
> configure manager add DONTRESOLVE regk3y78 natid90
Manager successfully configured.
```

If the threat defense is behind a NAT device, enter a unique NAT ID along with the management center IP address or hostname, for example:

Example:

```
> configure manager add 10.70.45.5 regk3y78 natid56
Manager successfully configured.
```

What to do next

Register your firewall to the management center.

Complete the Threat Defense Initial Configuration Using the Device Manager

When you use the device manager for initial setup, the following interfaces are preconfigured in addition to the Management interface and manager access settings. Note that other settings, such as the DHCP server on inside, access control policy, or security zones, are not configured.

- Ethernet 1/1—"outside", IP address from DHCP, IPv6 autoconfiguration

- Ethernet 1/2— "inside", 192.168.95.1/24

- Default route—Obtained through DHCP on the outside interface

If you perform additional interface-specific configuration within device manager before registering with the management center, then that configuration is preserved.

When you use the CLI, only the Management interface and manager access settings are retained (for example, the default inside interface configuration is not retained).

Procedure

Step 1 Log in to the device manager.

a) Enter one of the following URLs in your browser.

   • Inside (Ethernet 1/2)—**https://192.168.95.1**.

   • Management—**https://***management_ip*. The Management interface is a DHCP client, so the IP address depends on your DHCP server. You might have to set the Management IP address to a static address as part of this procedure, so we recommend that you use the inside interface so you do not become disconnected.

b) Log in with the username **admin**, and the default password **Admin123**.

c) You are prompted to read and accept the General Terms and change the admin password.

Step 2 Use the setup wizard when you first log into the device manager to complete the initial configuration. You can optionally skip the setup wizard by clicking **Skip device setup** at the bottom of the page.

After you complete the setup wizard, in addition to the default configuraton for the inside interface (Ethernet1/2), you will have configuration for an outside (Ethernet1/1) interface that will be maintained when you switch to management center management.

a) Configure the following options for the outside and management interfaces and click **Next**.

   1. Outside Interface Address—This interface is typically the internet gateway, and might be used as your manager access interface. You cannot select an alternative outside interface during initial device setup. The first data interface is the default outside interface.

   If you want to use a different interface from outside (or inside) for manager access, you will have to configure it manually after completing the setup wizard.

   Configure IPv4—The IPv4 address for the outside interface. You can use DHCP or manually enter a static IP address, subnet mask, and gateway. You can also select **Off** to not configure an IPv4 address. You cannot configure PPPoE using the setup wizard. PPPoE may be required if the interface is connected to a DSL modem, cable modem, or other connection to your ISP, and your ISP uses PPPoE to provide your IP address. You can configure PPPoE after you complete the wizard.

   Configure IPv6—The IPv6 address for the outside interface. You can use DHCP or manually enter a static IP address, prefix, and gateway. You can also select **Off** to not configure an IPv6 address.

   2. Management Interface

   You will not see Management Interface settings if you performed intial setup at the CLI. Note that setting the Management interface IP address is not part of the setup wizard. See Step to set the Management IP address.

   DNS Servers—The DNS server for the firewall's Management interface. Enter one or more addresses of DNS servers for name resolution. The default is the OpenDNS public DNS servers. If you edit the fields and want to return to the default, click **Use OpenDNS** to reload the appropriate IP addresses into the fields.

   Firewall Hostname—The hostname for the firewall's Management interface.

b) Configure the **Time Setting (NTP)** and click **Next**.

1. **Time Zone**—Select the time zone for the system.

2. **NTP Time Server**—Select whether to use the default NTP servers or to manually enter the addresses of your NTP servers. You can add multiple servers to provide backups.

c) Select **Start 90 day evaluation period without registration**.

Do not register the threat defense with the Smart Software Manager; all licensing is performed on the management center.

d) Click **Finish**.

e) You are prompted to choose **Cloud Management** or **Standalone**. For management center management, choose **Standalone**, and then **Got It**.

Step 3   (Might be required) Configure a static IP address for the Management interface. See the Management interface on **Device** > **Interfaces**.

If you want to configure a static IP address, for example for an edge deployment where there is not DHCP server on the network yet, be sure to also set the default gateway to be a unique gateway instead of the data interfaces. If you use DHCP, you do not need to configure anything.

Step 4   If you want to configure additional interfaces, including an interface other than outside or inside, choose **Device**, and then click the link in the **Interfaces** summary.

See Configure the Firewall in the Device Manager for more information about configuring interfaces in the device manager. Other device manager configuration will not be retained when you register the device to the management center.

Step 5   Choose **Device** > **System Settings** > **Central Management**, and click **Proceed** to set up the management center management.

Step 6   Configure the **Management Center/CDO Details**.

Figure 6: Management Center/CDO Details

Configure Connection to Management Center or CDO

Provide details to register to the management center/CDO.

Management Center/CDO Details

Do you know the Management Center/CDO hostname or IP address?

◉ Yes   ○ No

Threat Defense → **Management Center/CDO**

10.89.5.16
fe80::6a87:c6ff:fea6:4c00/64

10.89.5.35

Management Center/CDO Hostname or IP Address

10.89.5.35

Management Center/CDO Registration Key

••••   👁

NAT ID

Required when the management center/CDO hostname or IP address is not provided. We recommend always setting the NAT ID even when you specify the management center/CDO hostname or IP address.

11203

Connectivity Configuration

Threat Defense Hostname

1120-3

DNS Server Group

CustomDNSServerGroup   ⌄

Management Center/CDO Access Interface

○ Data Interface

Please select an interface   ⌄

◉ Management Interface View details

CANCEL   CONNECT

a) For **Do you know the Management Center/**CDO **hostname or IP address**, click **Yes** if you can reach the management center using an IP address or hostname, or **No** if the management center is behind NAT or does not have a public IP address or hostname.

At least one of the devices, either the management center or the threat defense device, must have a reachable IP address to establish the two-way, TLS-1.3-encrypted communication channel between the two devices.

b) If you chose **Yes**, then enter the **Management Center/**CDO **Hostname/IP Address**.

c) Specify the **Management Center/**CDO **Registration Key**.

This key is a one-time registration key of your choice that you will also specify on the management center when you register the threat defense device. The registration key must not exceed 37 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-). This ID can be used for multiple devices registering to the management center.

d) Specify a **NAT ID**.

This ID is a unique, one-time string of your choice that you will also specify on the management center. This field is required if you only specify the IP address on one of the devices; but we recommend that you specify the NAT ID even if you know the IP addresses of both devices. The NAT ID must not exceed 37 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-). This ID *cannot* be used for any other devices registering to the management center. The NAT ID is used in combination with the IP address to verify that the connection is coming from the correct device; only after authentication of the IP address/NAT ID will the registration key be checked.

Step 7 Configure the **Connectivity Configuration**.

a) Specify the **FTD Hostname**.

b) Specify the **DNS Server Group**.

Choose an existing group, or create a new one. The default DNS group is called **CiscoUmbrellaDNSServerGroup**, which includes the OpenDNS servers.

c) For the **Management Center/CDO Access Interface**, choose **management**.

Step 8 Click **Connect**. The **Registration Status** dialog box shows the current status of the switch to the management center. After the **Saving Management Center/**CDO **Registration Settings** step, go to the management center, and add the firewall.

If you want to cancel the switch to the management center, click **Cancel Registration**. Otherwise, do not close the device manager browser window until after the **Saving Management Center/**CDO **Registration Settings** step. If you do, the process will be paused, and will only resume when you reconnect to the device manager.

If you remain connected to the device manager after the **Saving Management Center/**CDO **Registration Settings** step, you will eventually see the **Successful Connection with Management Center or** CDO dialog box, after which you will be disconnected from the device manager.

Figure 7: Successful Connection
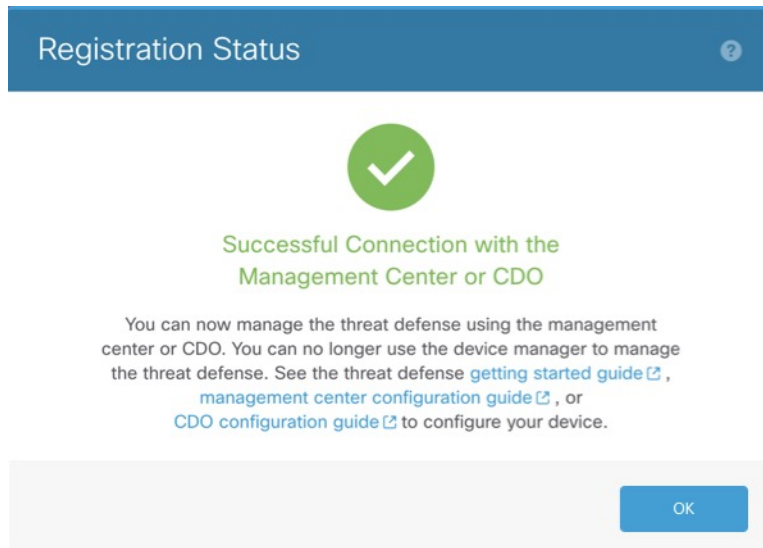
Log Into the Management Center

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

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:

- **Essentials**—(Required) Essentials license.

- **IPS**—Security Intelligence and Next-Generation IPS

- **Malware Defense**—Malware defense

- **URL Filtering**—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 an 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 an 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 **Search All** field on the Cisco Commerce Workspace.

Figure 8: License Search
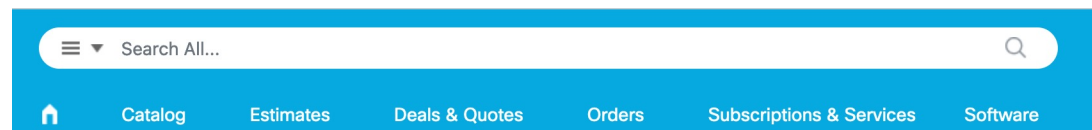
Choose **Products & Services** from the results.

Figure 9: Results
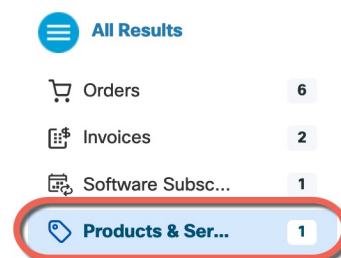
Search for the following license PIDs:

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

- Essentials:

    - *Included automatically*

- IPS, Malware Defense, and URL license combination:

- L-FPR3110T-TMC=

- L-FPR3120T-TMC=

- L-FPR3130T-TMC=

- L-FPR3140T-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-FPR3110T-TMC-1Y

- L-FPR3110T-TMC-3Y

- L-FPR3110T-TMC-5Y

- L-FPR3120T-TMC-1Y

- L-FPR3120T-TMC-3Y

- L-FPR3120T-TMC-5Y

- L-FPR3130T-TMC-1Y

- L-FPR3130T-TMC-3Y

- L-FPR3130T-TMC-5Y

- L-FPR3140T-TMC-1Y

- L-FPR3140T-TMC-3Y

- L-FPR3140T-TMC-5Y

- Carrier license:

  - L-FPR3K-FTD-CAR=

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

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 the threat defense to the management center manually using the device IP address or hostname.

Before you begin

Procedure

Step 1   In the management center, choose **Devices** > **Device Management**.

Step 2   From the **Add** drop-down list, choose **Add Device**.

Figure 10: Add Device Using a Registration Key

Add Device ⓘ

☐ CDO Managed Device

Host:†

10.89.5.41

Display Name:

3110-1

Registration Key:*

••••

Group:

None ⌄

Access Control Policy:*

wfx_automationPolicy123 ⌄

Smart Licensing

Note: All virtual Firewall Threat Defense devices require a performance tier license.
Make sure your Smart Licensing account contains the available licenses you need.
It's important to choose the tier that matches the license you have in your account.
Click here for information about the Firewall Threat Defense performance-tiered licensing.
Until you choose a tier, your Firewall Threat Defense virtual defaults to the FTDv50 selection.

Performance Tier (only for Firewall Threat Defense virtual 7.0 and above):

Select a recommended Tier ⌄

☑ Carrier
☑ Malware Defense
☑ IPS
☑ URL

 Advanced

Unique NAT ID:†

31101

☑ Transfer Packets

Cancel   **Register**

Figure 11: Add Device

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 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 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 36.

Figure 12: New Policy

New Policy

Name:

ftd-ac-policy

Description:

Select Base Policy:

None ▼

Default Action:

- ⦿ Block all traffic
- ○ Intrusion Prevention
- ○ Network Discovery

Cancel   Save

- **Smart Licensing**—Assign the Smart Licenses you need for the features you want to deploy. **Note:** You can apply the 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 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**, 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, 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.

- 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 threat defense 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 24.
2	Configure the DHCP Server, on page 29.
3	Add the Default Route, on page 31.
4	Configure NAT, on page 33.
5	Allow Traffic from Inside to Outside, on page 36.
6	Deploy the Configuration, on page 38.

Configure Interfaces

When you use the device manager for initial setup, the following interfaces are preconfigured:

- Ethernet 1/1—"outside", IP address from DHCP, IPv6 autoconfiguration

- Ethernet 1/2— "inside", 192.168.95.1/24

• Default route—Obtained through DHCP on the outside interface

If you performed additional interface-specific configuration within device manager before registering with the management center, then that configuration is preserved.

In any case, you need to perform additional interface configuration after you register the device. Enable the threat defense interfaces, assign them to security zones, and set the IP addresses. Also configure breakout 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**.

Figure 13: Interfaces

Step 3   To create breakout ports from a 40-Gb or larger interface, click the **Break** icon for the interface.

If you already used the full interface in your configuration, you will have to remove the configuration before you can proceed with the breakout.

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

The **General** tab appears.

Figure 14: General Tab

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

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

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

c) 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**

Figure 15: IPv4 Tab

Edit Physical Interface

General   IPv4   IPv6   Path Monitoring

IP Type:

Use Static IP   ▼

IP Address:

192.168.1.1/24

eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25

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

Figure 16: IPv6 Tab

Edit Physical Interface

General   IPv4   IPv6   Path Monitoring   Hardware Configu

Basic   Address   Prefixes   Settings   DHCP

Enable IPV6: ☐

Enforce EUI 64: ☐

Link-Local address: [   ]

Autoconfiguration: ☑

Obtain Default Route: ☐

    f)   Click **OK**.

Step 5   Click the **Edit** (✐) for the interface that you want to use for *outside*.

The **General** tab appears.

Figure 17: General Tab

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.

Figure 18: IPv4 Tab

Edit Physical Interface

| General | **IPv4** | IPv6 | Path Mc |

IP Type:

Use DHCP ▾

Obtain default route
using DHCP: ☑

DHCP route metric:

1

(1 – 255)

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

Figure 19: IPv6 Tab

Edit Physical Interface

| General | IPv4 | **IPv6** | Path Monitoring | Hardware Configu |

| **Basic** | Address | Prefixes | Settings | DHCP |

Enable IPV6: ☐

Enforce EUI 64: ☐

Link-Local address:

Autoconfiguration: ☑

Obtain Default Route: ☐

    f)   Click **OK**.

Step 6   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 **Edit** (✐) for the device.

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

Figure 20: DHCP Server

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

Figure 21: Add Server

- **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 **Edit** (✐) for the device.

Step 2   Choose **Routing** > **Static Route**.

Figure 22: Static Route
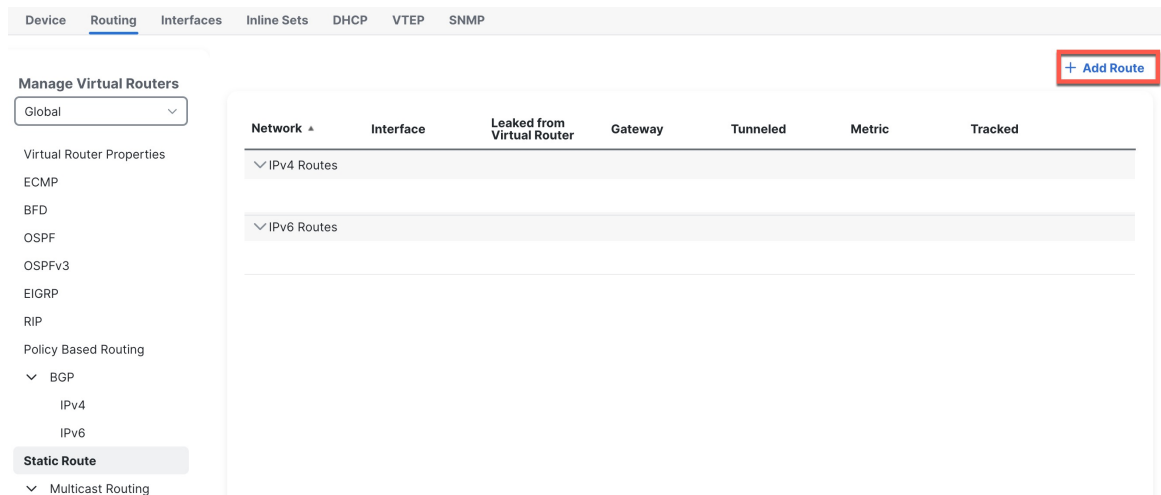
Step 3   Click **Add Route**, and set the following:

Figure 23: Add Static Route Configuration

- **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 4   Click **OK**.

The route is added to the static route table.

Step 5   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**.

Figure 24: New Policy

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

Figure 25: NAT Policy

Step 3 Click **Add Rule**.

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

Step 4 Configure the basic rule options:

Figure 26: Basic Rule Options

- **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.

Figure 27: Interface Objects

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

Figure 28: Translation

Interface Objects	Translation	PAT Pool	Advanced

Original Packet

Translated Packet

Original Source:*

all-ipv4 ▼ ＋

Original Port:

TCP ▼

Translated Source:

Destination Interface IP ▼

ⓘ The values selected for Destination Interface Objects in 'Interface Objects' tab will be used

Translated Port:

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

Figure 29: New Network Object

New Network Object ⑦

Name

all-ipv4

Description

Network

○ Host ○ Range ⦿ Network ○ FQDN

0.0.0.0/0

☐ Allow Overrides

Cancel **Save**

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.

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 **Edit** (✎) for the access control policy assigned to the threat defense.

Step 2   Click **Add Rule**, and set the following parameters:
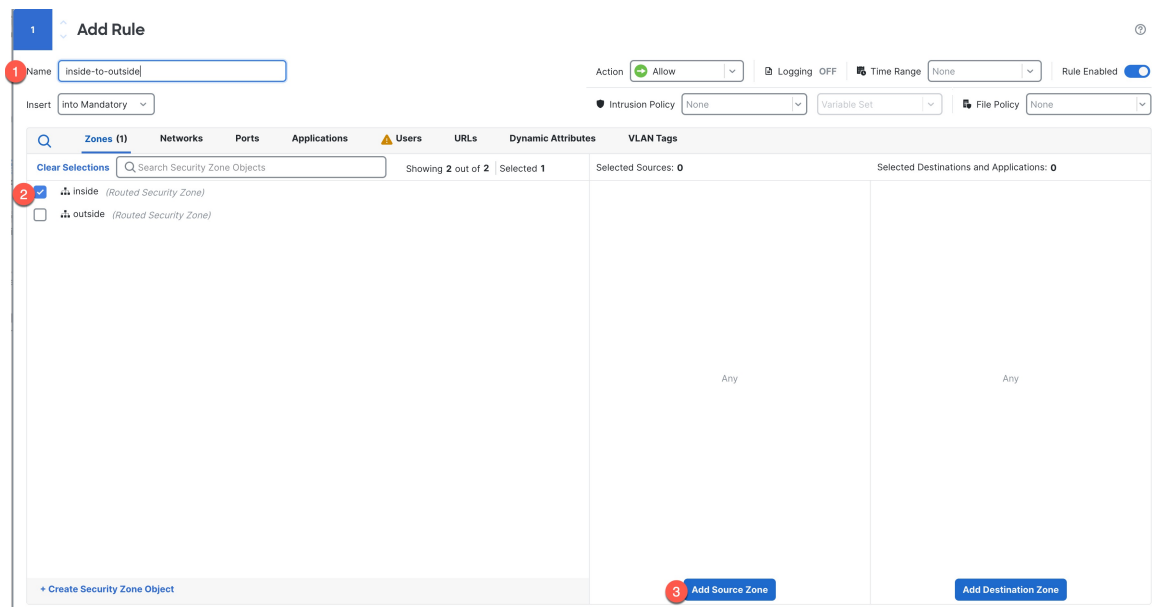
Figure 30: Source Zone

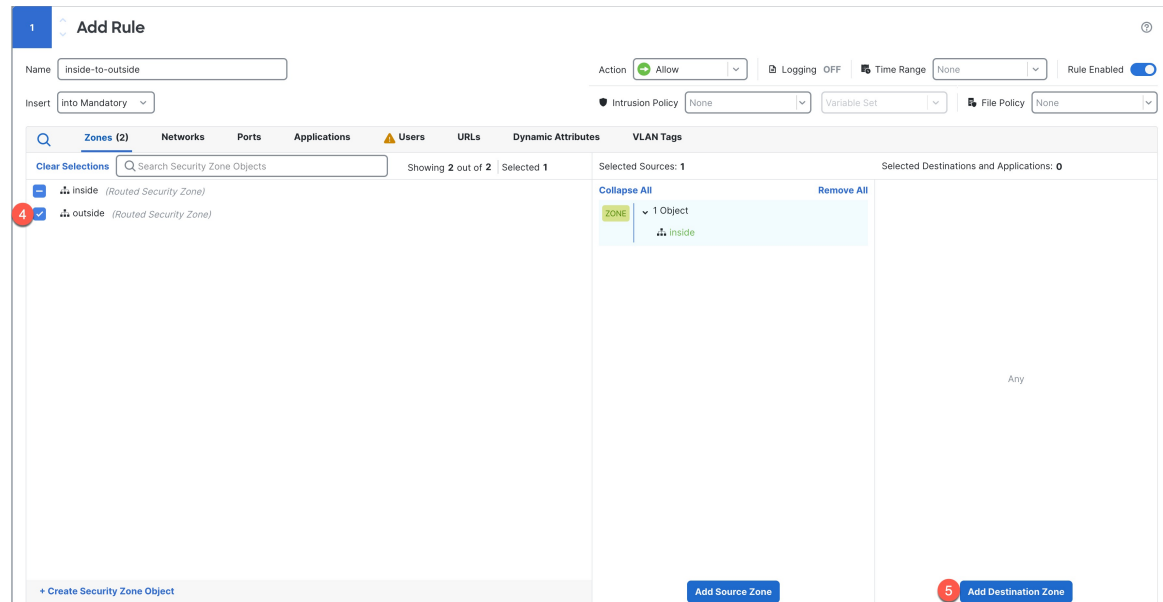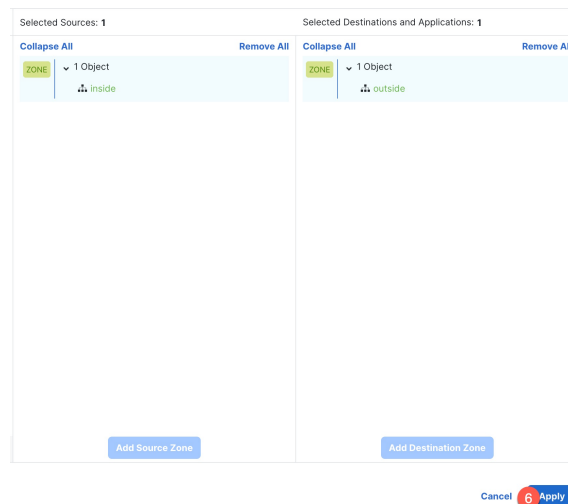**Figure 31: Destination Zone**

Figure 32: Apply

- **Name**—Name this rule, for example, **inside-to-outside**.

- **Selected Sources**—Select the inside zone from **Zones**, and click **Add Source Zone**.

- **Selected Destinations and Applications**—Select the outside zone from **Zones**, and click **Add Destination Zone**.

Leave the other settings as is.

Step 3   Click **Apply**.

The rule is added to the **Rules** table.
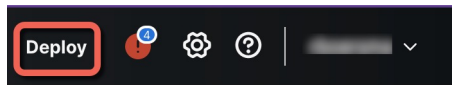
Step 4   Click **Save**.

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 33: Deploy

Step 2   For a quick deployment, check specific devices and then click **Deploy**, or click **Deploy All** to deploy to all devices. Otherwise, for additional deployment options, click **Advanced Deploy**.
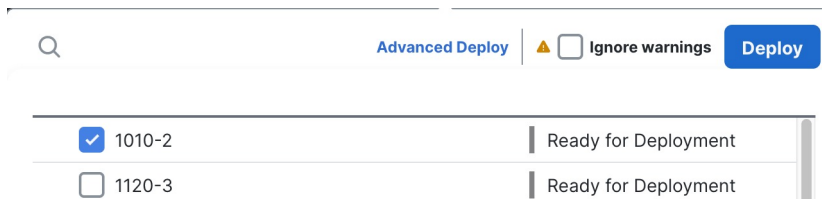
Figure 34: Deploy Selected
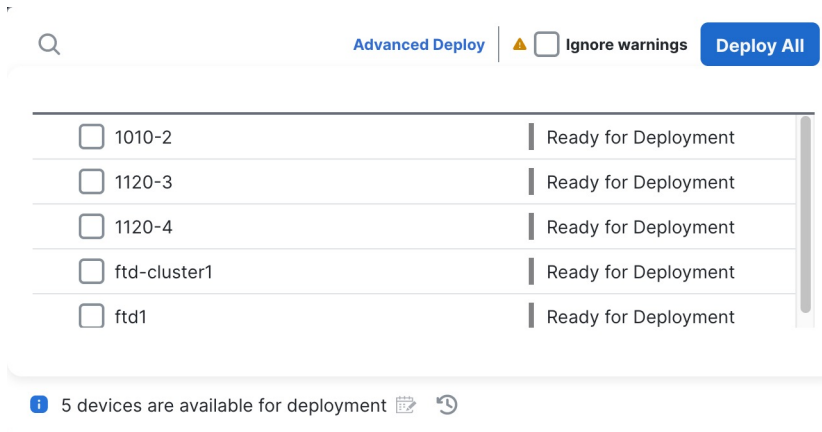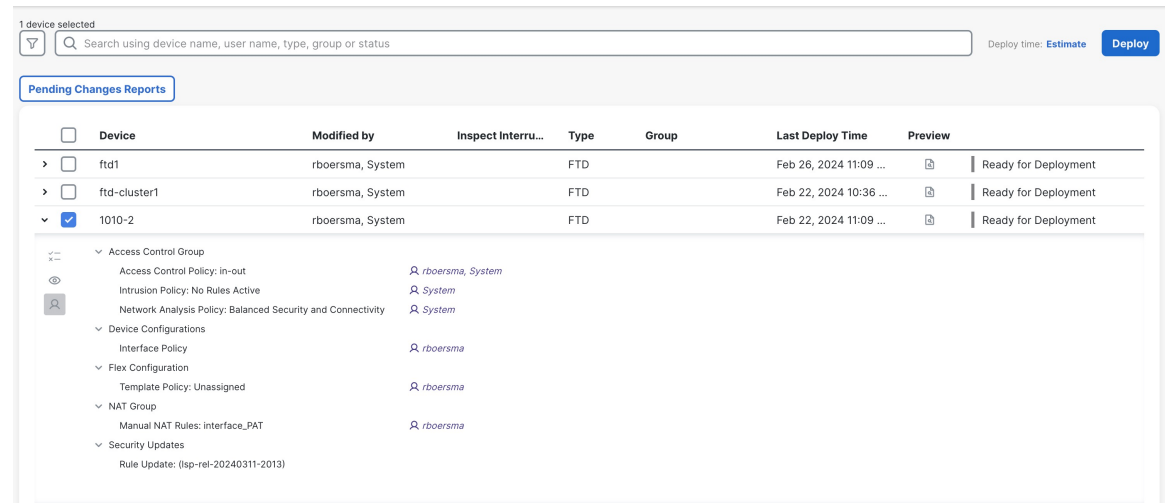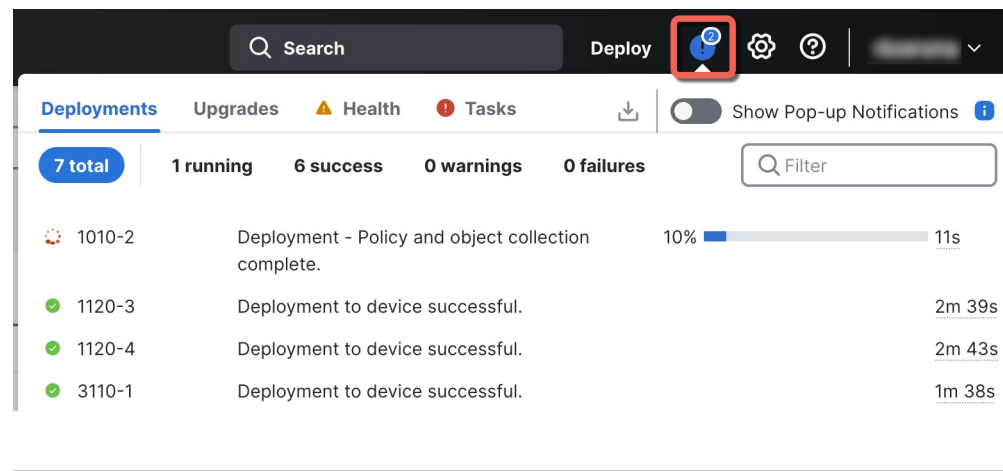

Figure 35: Deploy All

Figure 36: 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 37: Deployment Status

Access the Threat Defense and FXOS CLI

Use the command-line interface (CLI) to set up the system and do basic system troubleshooting. You cannot configure policies through a CLI session. You can access the CLI by connecting to the console port.

You can also access the FXOS CLI for troubleshooting purposes.

Note　You can alternatively SSH to the Management interface of the threat defense device. Unlike a console session, the SSH session defaults to the threat defense CLI, from which you can connect to the FXOS CLI using the **connect fxos** command. You can later connect to the address on a data interface if you open the interface for SSH connections. SSH access to data interfaces is disabled by default. This procedure describes console port access, which defaults to the FXOS CLI.

Procedure

Step 1　To log into the CLI, connect your management computer to the console port. The Secure Firewall 3100 ships with a DB-9 to RJ-45 serial cable, so you may need to buy a third party DB-9-to-USB serial cable to make the connection. Be sure to install any necessary USB serial drivers for your operating system. The console port defaults to the FXOS CLI. Use the following serial settings:

- 9600 baud
- 8 data bits
- No parity
- 1 stop bit

You connect to the FXOS CLI. Log in to the CLI using the **admin** username and the password you set at initial setup (the default is **Admin123**).

Example:

```
firepower login: admin
Password:
Last login: Thu May 16 14:01:03 UTC 2019 on ttyS0
Successful login attempts for user 'admin' : 1

firepower#
```

Step 2　Access the threat defense CLI.

connect ftd

Example:

```
firepower# connect ftd
>
```

After logging in, for information on the commands available in the CLI, enter **help** or **?**. For usage information, see Cisco Secure Firewall Threat Defense Command Reference.

Step 3　To exit the threat defense CLI, enter the **exit** or **logout** command.

This command returns you to the FXOS CLI prompt. For information on the commands available in the FXOS CLI, enter **?**.

Example:

```
> exit
firepower#
```

Power Off the Firewall

It's important that you shut down your system properly. Simply unplugging the power or pressing the power switch can cause serious file system damage. Remember that there are many processes running in the background all the time, and unplugging or shutting off the power does not allow the graceful shutdown of your firewall system.

You can power off the device using the management center device management page, or you can use the FXOS CLI.

Power Off the Firewall Using the Management Center

It's important that you shut down your system properly. Simply unplugging the power or pressing the power switch can cause serious file system damage. Remember that there are many processes running in the background all the time, and unplugging or shutting off the power does not allow the graceful shutdown of your firewall.

You can shut down your system properly using the management center.

Procedure

Step 1 Choose **Devices** > **Device Management**.

Step 2 Next to the device that you want to restart, click **Edit** (✐).

Step 3 Click the **Device** tab.

Step 4 Click **Shut Down Device** (⊗) in the **System** section.

Step 5 When prompted, confirm that you want to shut down the device.

Step 6 If you have a console connection to the firewall, monitor the system prompts as the firewall shuts down. You will see the following prompt:

```
System is stopped.
It is safe to power off now.

Do you want to reboot instead? [y/N]
```

If you do not have a console connection, wait approximately 3 minutes to ensure the system has shut down.

Step 7 You can now turn off the power switch and unplug the power to physically remove power from the chassis if necessary.

Power Off the Firewall at the CLI

You can use the FXOS CLI to safely shut down the system and power off the device. You access the CLI by connecting to the console port; see Access the Threat Defense and FXOS CLI, on page 39.

Procedure

Step 1   In the FXOS CLI, connect to local-mgmt:

firepower # **connect local-mgmt**

Step 2   Issue the **shutdown** command:

firepower(local-mgmt) # **shutdown**

Example:

```
firepower(local-mgmt)# shutdown
This command will shutdown the system.  Continue?
Please enter 'YES' or 'NO': yes
INIT: Stopping Cisco Threat Defense......ok
```

Step 3   Monitor the system prompts as the firewall shuts down. You will see the following prompt:

```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

Step 4   You can now turn off the power switch and unplug the power to physically remove power from the chassis if necessary.

What's Next?

To continue configuring your threat defense, see the documents available for your software version at Navigating the Cisco Secure Firewall Threat Defense Documentation.

For information related to using the management center, see the Cisco Secure Firewall Management Center Device Configuration Guide.