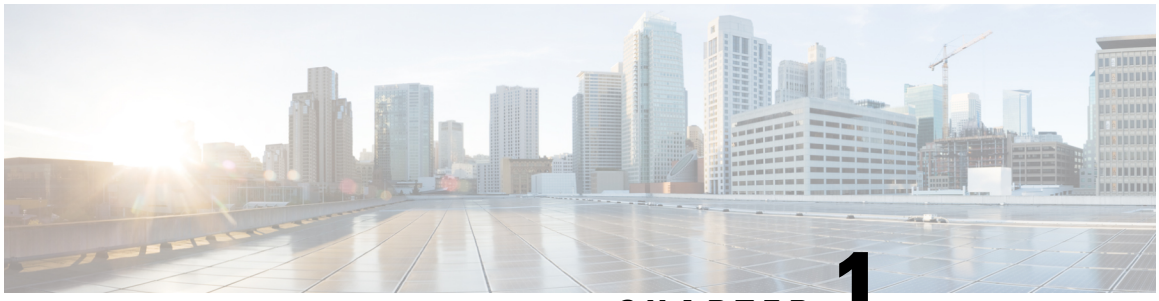
Cisco Firepower 2100 Getting Started Guide

First Published: 2019-09-25

Last Modified: 2023-01-23

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CHAPTER 1

Which Application and Manager is Right for You?

Your hardware platform can run one of two applications. For each application, you have a choice of managers. This chapter explains the application and manager choices.

Applications

You can use either the Secure Firewall ASA or the Secure Firewall Threat Defense (formerly Firepower Threat Defense) application on your hardware platform:

- ASA—The ASA is a traditional, advanced stateful firewall and VPN concentrator.
- Threat Defense—The threat defense is a next-generation firewall that combines an advanced stateful firewall, VPN concentrator, and next generation IPS.

Cisco provides ASA-to-threat defense migration tools to help you convert your ASA to the threat defense if you start with ASA and later reimage to threat defense.

To reimage between the ASA and the threat defense, see the Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide.

Managers

The threat defense and ASA support multiple managers.

Threat Defense Managers

Table 1: Threat Defense Managers

Manager	Description
Secure Firewall Management Center (formerly Firepower Management Center)	The management center is a multi-device manager that runs on its own server hardware, or as a virtual device on a hypervisor. To get started with the management center on the Management network, see Threat Defense Deployment with the Management Center, on page 5. To get started with the management center on a remote network, see Threat Defense Deployment with a Remote Management Center, on page 47.
Secure Firewall Device Manager (formerly Firepower Device Manager)	The device manager is a simplified, on-device manager. Some threat defense features are not supported using the device manager. To get started with the device manager, see Threat Defense Deployment with the Device Manager, on page 105.
Cisco Defense Orchestrator (CDO) Cloud-delivered Firewall Management Center	CDO's cloud-delivered Firewall Management Center has all of the configuration functionality of an on-premises management center. For the analytics functionality, you can use a cloud solution or an on-prem management center. CDO also manages other security devices, such as ASAs. To get started with CDO provisioning, see Threat Defense Deployment with CDO, on page 131.
Secure Firewall Threat Defense REST API	The threat defense REST API lets you automate direct configuration of the threat defense. You cannot use this API if you are managing the threat defense using the management center. The threat defense REST API is not covered in this guide. For more information, see the Cisco Secure Firewall Threat Defense REST API Guide.
Secure Firewall Management Center REST API	The management center REST API lets you automate configuration of management center policies that can then be applied to managed threat defenses. This API does not manage the threat defense directly. The management center REST API is not covered in this guide. For more information, see the Secure Firewall Management Center REST API Quick Start Guide.

ASA Managers

Table 2: ASA Managers

Manager	Description
Adaptive Security Device Manager (ASDM)	ASDM is a Java-based, on-device manager that provides full ASA functionality. To get started with ASDM, see ASA Appliance Mode Deployment with ASDM, on page 187. If you know you want to use the ASA in Platform mode, see ASA Platform Mode Deployment with ASDM and Chassis Manager, on page 207

Manager	Description
CLI	You can use the CLI to configure all ASA functionality. The CLI is not covered in this guide. For more information, see the ASA configuration guides.
CDO	CDO is a cloud-based, multi-device manager. CDO also manages other security devices, such as threat defenses. CDO for ASA is not covered in this guide. To get started with CDO, see the CDO home page.
Cisco Security Manager (CSM)	CSM is a multi-device manager that runs on its own server hardware. CSM does not support managing the threat defenses. CSM is not covered in this guide. For more information, see the CSM user guide.
ASA HTTP Interface	Using HTTP, an automation tool can execute commands on the ASAs by accessing specifically formatted URLs. The ASA HTTP interface is not covered in this guide. For more information, see the Cisco Secure Firewall ASA HTTP Interface for Automation.

CHAPTER 2

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?, on page 1. This chapter applies to the threat defense with the management center.

This chapter explains how to complete the initial configuration of your threat defense and how to register the firewall to the 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, on page 47.

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 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.

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.

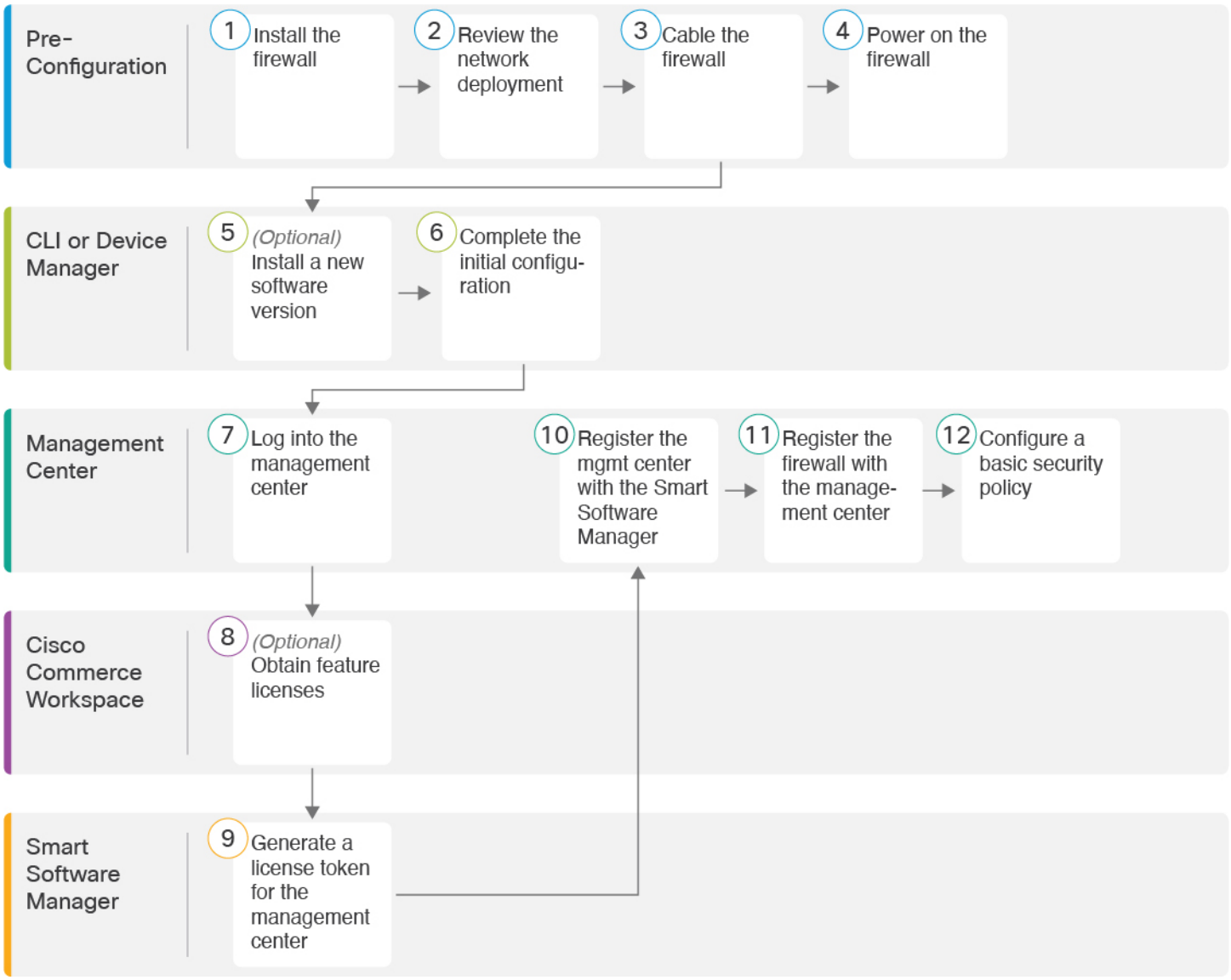
Privacy Collection Statement—The firewall does not require or actively collect personally identifiable information. However, you can use personally identifiable information in the configuration, for example for usernames. In this case, an administrator might be able to see this information when working 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

See the following tasks to deploy the threat defense with the management center.



1	Pre-Configuration	Install the firewall. See the hardware installation guide.
2	Pre-Configuration	Review the Network Deployment, on page 8.
3	Pre-Configuration	Cable the Device, on page 10.
4	Pre-Configuration	Power on the Device, on page 12.
5	CLI	(Optional) Check the Software and Install a New Version, on page 13.

6	CLI or Device Manager	Complete the Threat Defense Initial Configuration, on page 15
7	Management Center	Log Into the Management Center, on page 23.
8	Cisco Commerce Workspace	Obtain Licenses for the Management Center, on page 23: Buy feature licenses.
9	Smart Software Manager	Obtain Licenses for the Management Center, on page 23: Generate a license token for the management center.
10	Management Center	Obtain Licenses for the Management Center, on page 23: Register the Management Center with the Smart Licensing server.
11	Management Center	Register the Threat Defense with the Management Center, on page 25.
12	Management Center	Configure a Basic Security Policy, on page 28.

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.

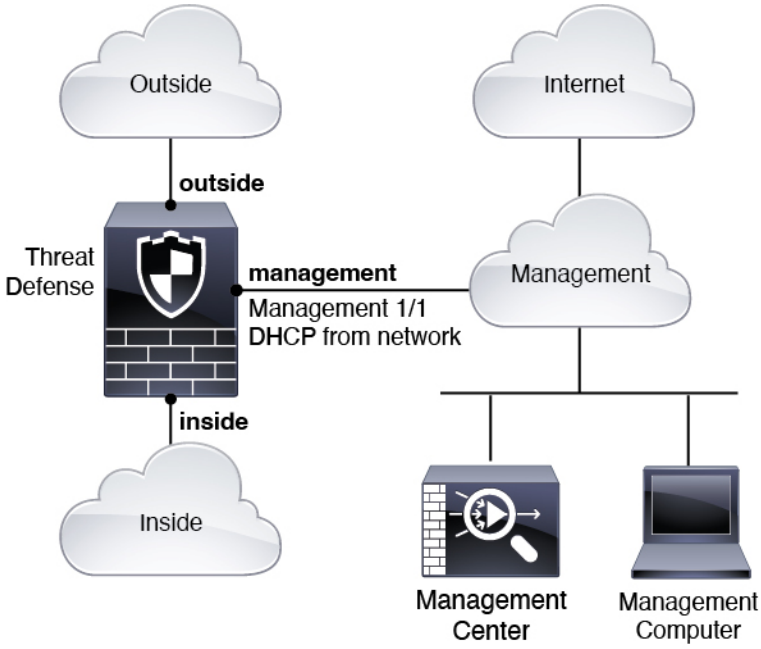
Typical Separate Management Network Deployment

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



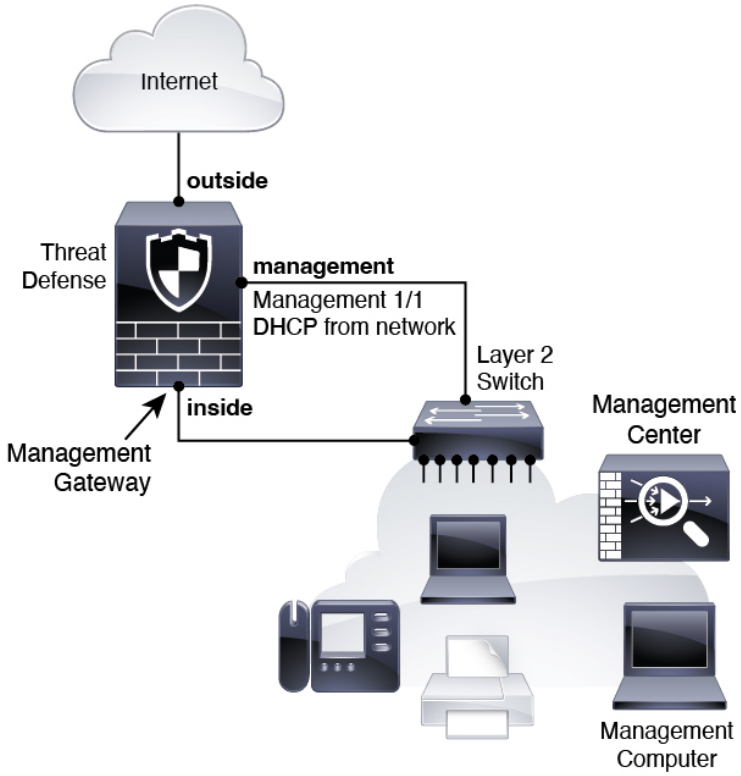
Typical Edge Network Deployment

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

- The inside interface acts as the internet gateway for Management and for the management center.
- Connects Management 1/1 to an inside interface through a Layer 2 switch.
- Connects the management center and management computer 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 Device

To cable one of the above scenarios on the Firepower 2100, see the following steps.

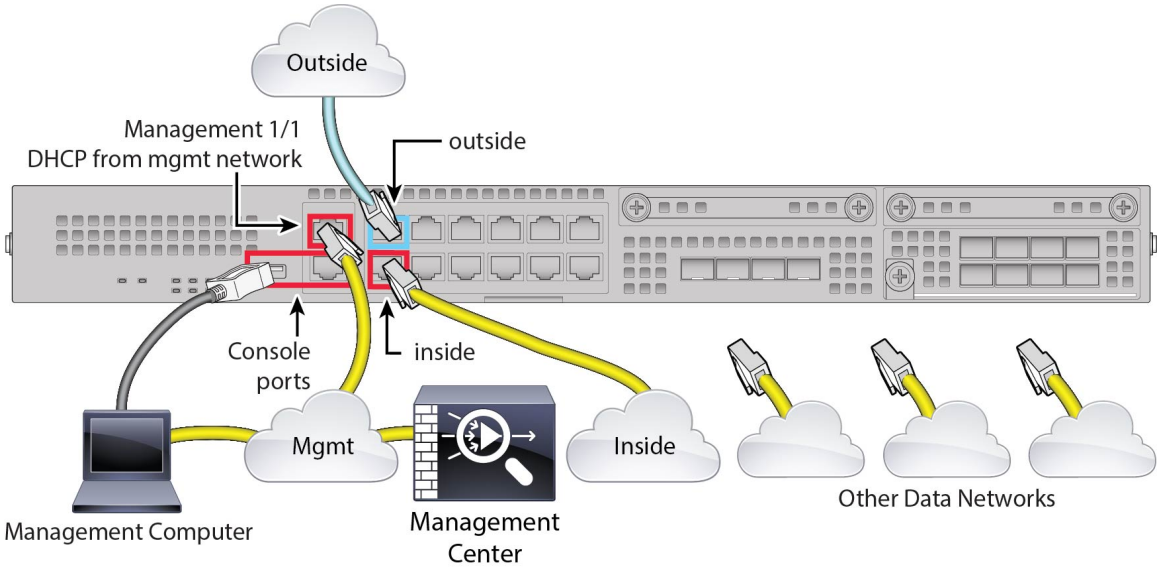
Note Other topologies can be used, and your deployment will vary depending on your basic logical network connectivity, ports, addressing, and configuration requirements.

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



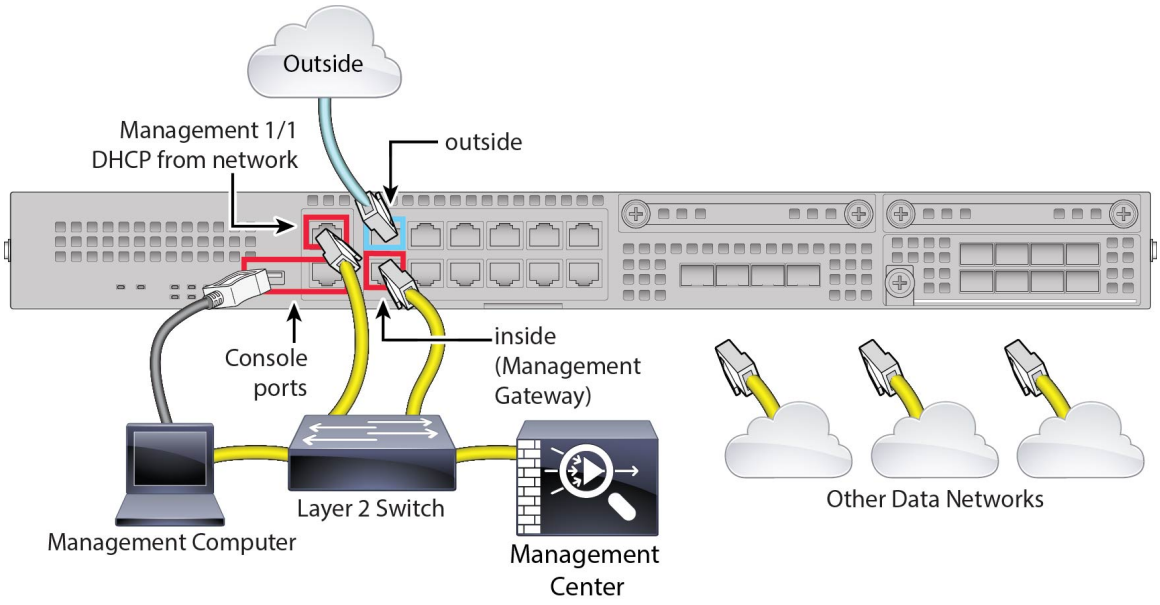
Note For version 6.5 and earlier, the Management 1/1 default IP address is 192.168.45.45.

a) Cable the following to your management network:
   - Management 1/1 interface
   - 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 or use the device manager for initial setup.
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



Note For version 6.5 and earlier, the Management 1/1 default IP address is 192.168.45.45.

a) Cable the following to a Layer 2 Ethernet switch:
   - Inside interface (for example, Ethernet 1/2)
   - Management 1/1 interface
   - 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 or use the device manager 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 Device

The power switch is located to the left of power supply module 1 on the rear of the chassis. It is a toggle switch that controls power to the system. If the power switch is in standby position, only the 3.3-V standby power is enabled from the power supply module and the 12-V main power is OFF. When the switch is in the ON position, the 12-V main power is turned on and the system boots.

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

Before you begin

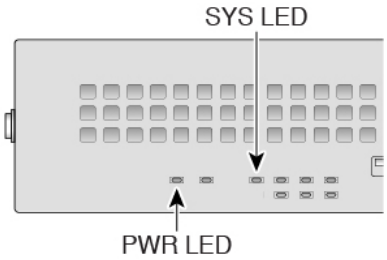
It's important that you provide reliable power for your device (for example, using an uninterruptable power supply (UPS)). Loss of power without first shutting down can cause serious file system damage. There are many processes running in the background all the time, and losing power does not allow the graceful shutdown of your system.

Procedure

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

Step 2 Press the power switch on the back of the device.

Step 3 Check the PWR LED on the front of the device; if it is solid green, the device is powered on.



Step 4 Check the SYS LED on the front of the device; after it is solid green, the system has passed power-on diagnostics.

Note Before you move the power switch to the OFF position, use the shutdown commands so that the system can perform a graceful shutdown. This may take several minutes to complete. After the graceful shutdown is complete, the console displays `It is safe to power off now`. The front panel blue locator beacon LED lights up indicating the system is ready to be powered off. You can now move the switch to the OFF position. The front panel PWR LED flashes momentarily and turns off. Do not remove the power until the PWR LED is completely off.

See the FXOS Configuration Guide for more information on using the shutdown commands.

(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 CLI. See Access the Threat Defense and FXOS CLI, on page 43 for more information. This procedure shows using the console port, but you can use SSH instead.

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               7.4.0.65        7.4.0.65
        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 19. 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 Device Manager

Connect to the device manager to perform initial setup of the threat defense. 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 settings. Note that other default configuration settings, such as the access control policy or security zones, are not retained. 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).

Before you begin

Deploy and perform initial configuration of the management center. You will need to know the management center IP address or hostname before you set up the threat defense.

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 End User License Agreement 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 Step 3, on page 16 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. Choose **Device**, then click the **System Settings** > **Management Interface** link.

If you want to configure a static IP address, 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.

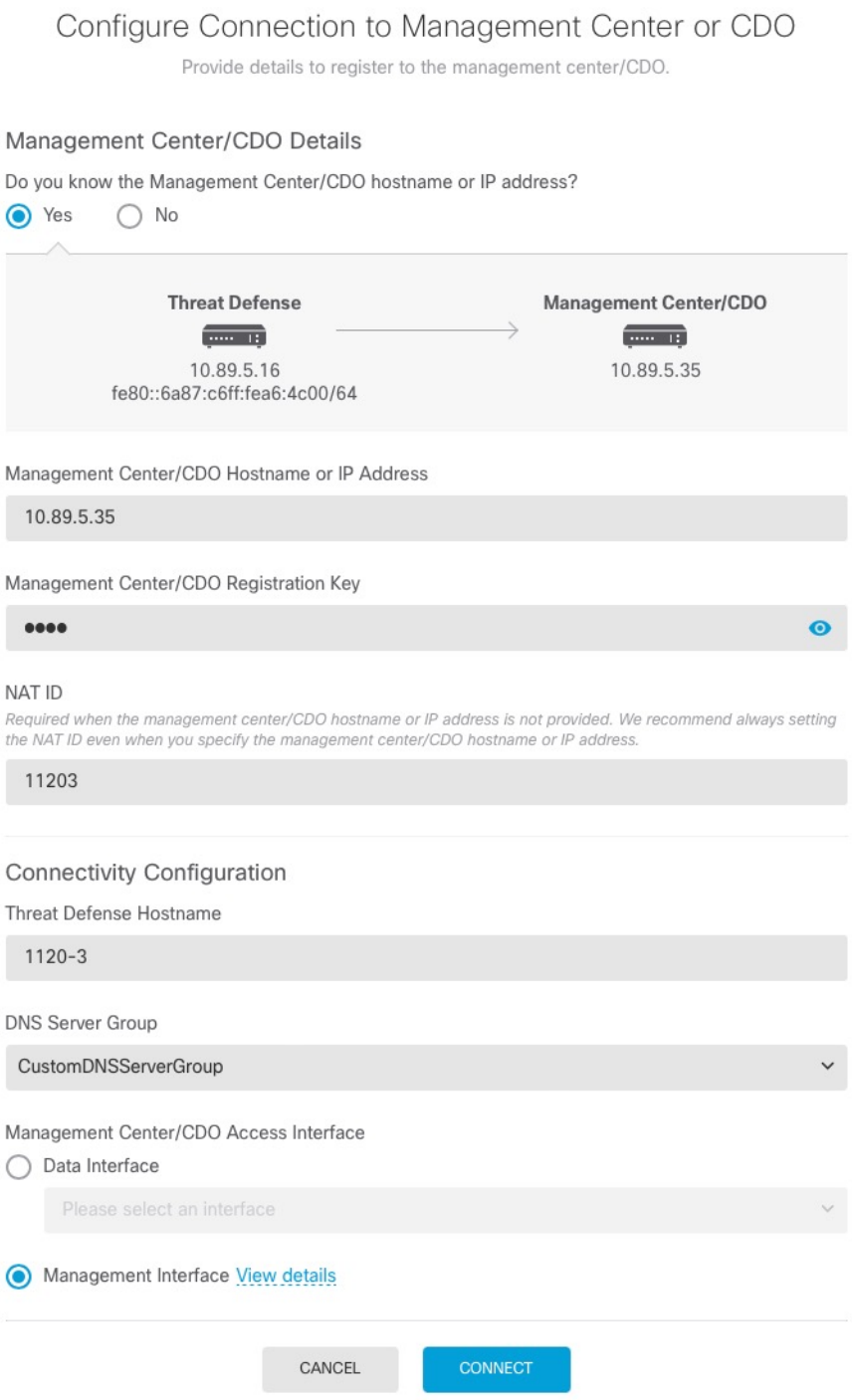
Step 4 If you want to configure additional interfaces, including an interface other than outside or inside, choose **Device**, and then click the link in the **Interfaces** summary.

See Configure the Firewall in the Device Manager, on page 124 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 5: Management Center/CDO Details



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, SSL-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.

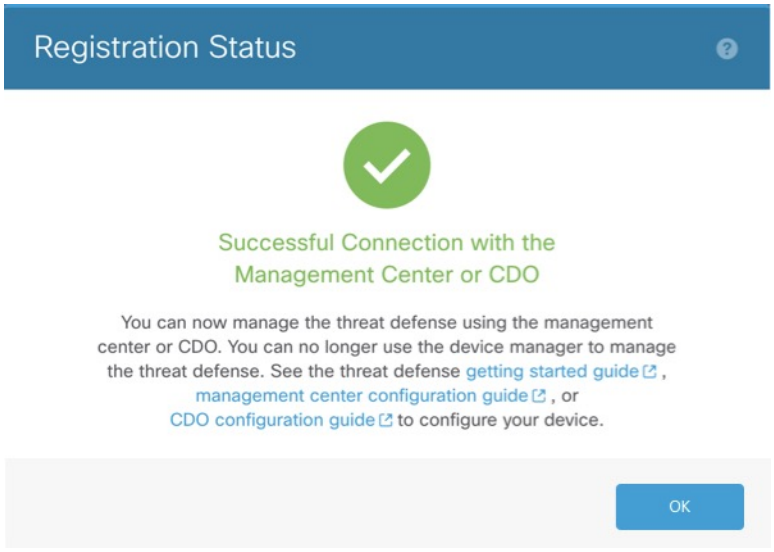
c) For the **Management Center/CDO Access Interface**, choose **management**.

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 6: Successful Connection



Complete the Threat Defense Initial Configuration Using the CLI

Connect to the threat defense CLI to perform initial setup, including setting 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. In 6.7 and later: 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 (7.1 and later), *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.
- **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.

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:

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

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.

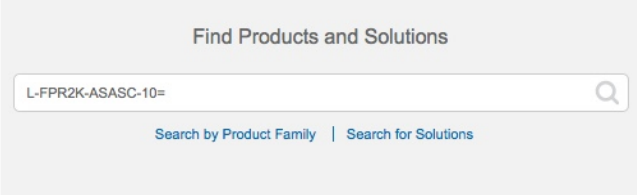
- Your Smart Software Licensing account must qualify for the Strong Encryption (3DES/AES) license to use some features (enabled using the export-compliance flag).

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 7: License Search



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

- IPS, Malware Defense, and URL license combination:
  - L-FPR2110T-TMC=
  - L-FPR2120T-TMC=
  - L-FPR2130T-TMC=
  - L-FPR2140T-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-FPR2110T-TMC-1Y
  - L-FPR2110T-TMC-3Y
  - L-FPR2110T-TMC-5Y
  - L-FPR2120T-TMC-1Y
  - L-FPR2120T-TMC-3Y
  - L-FPR2120T-TMC-5Y
  - L-FPR2130T-TMC-1Y
  - L-FPR2130T-TMC-3Y
  - L-FPR2130T-TMC-5Y
  - L-FPR2140T-TMC-1Y
  - L-FPR2140T-TMC-3Y
  - L-FPR2140T-TMC-5Y
- 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

- Gather the following information that you set in the threat defense initial configuration:
  - The threat defense management IP address or hostname, and NAT ID
  - The management center registration key

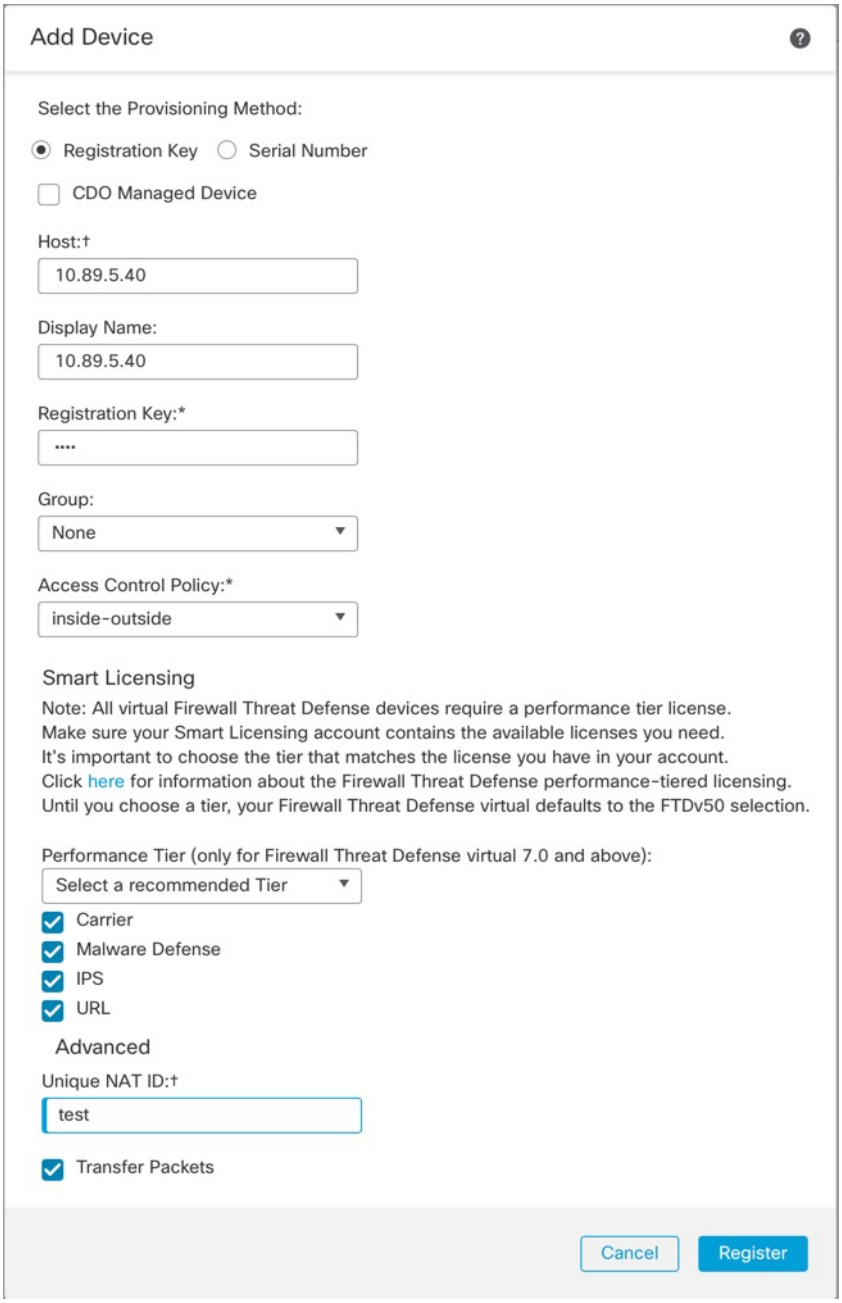
Procedure

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

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

The **Registration Key** method is selected by default.

Figure 8: Add Device Using a Registration Key



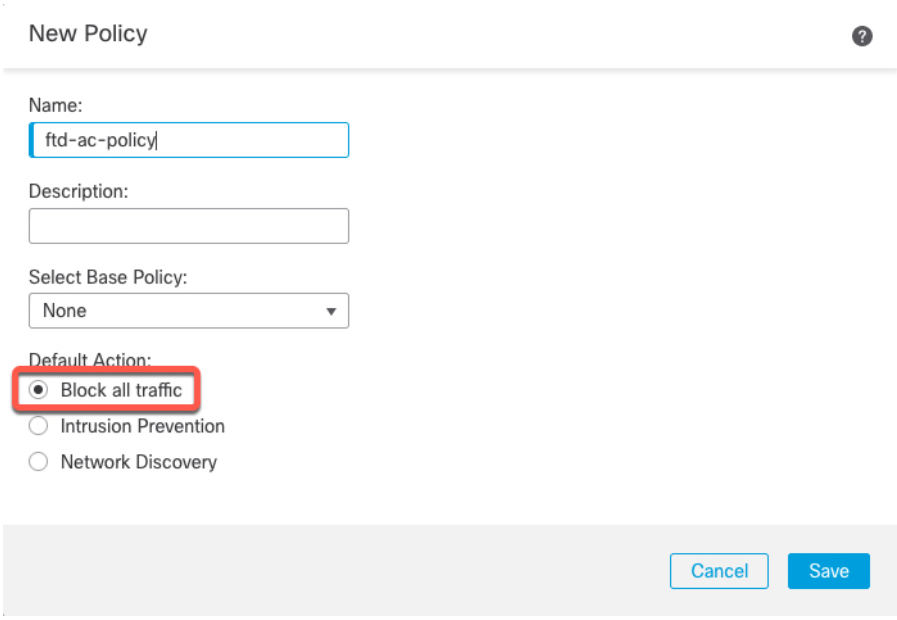
Set the following parameters:

- **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 40.

Figure 9: New Policy



- **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 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 29.
2	Configure the DHCP Server, on page 33.
3	Add the Default Route, on page 35.
4	Configure NAT, on page 37.
5	Allow Traffic from Inside to Outside, on page 40.
6	Deploy the Configuration, on page 41.

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.

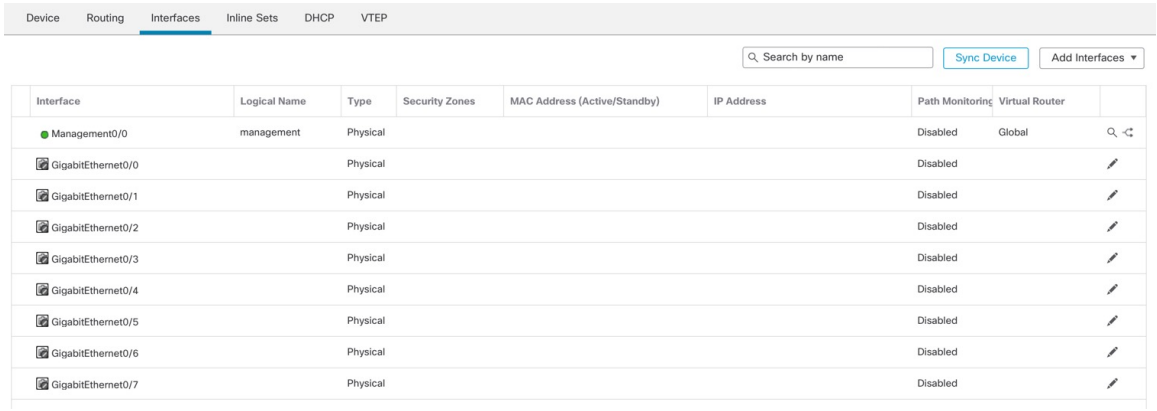
The following example configures a routed mode inside interface with a static address and a routed mode outside interface using DHCP.

Procedure

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

Step 2 Click **Interfaces**.

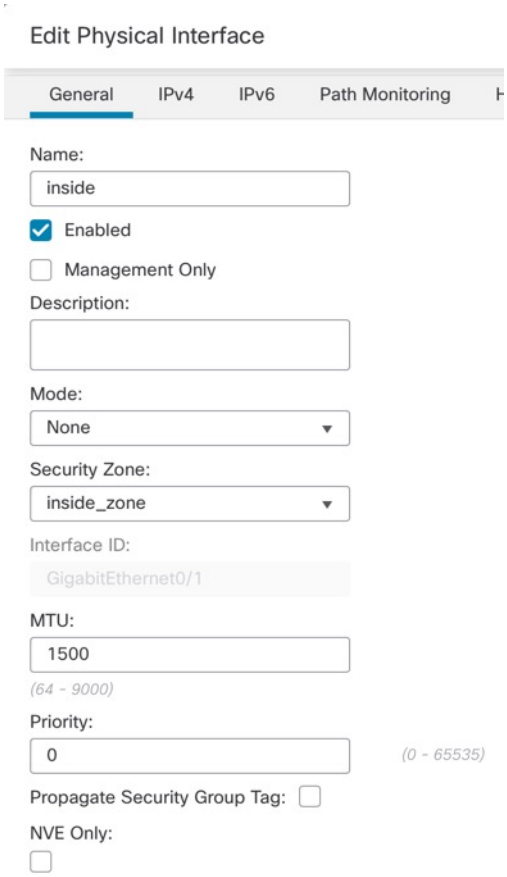
Figure 10: Interfaces



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

The **General** tab appears.

Figure 11: 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**.

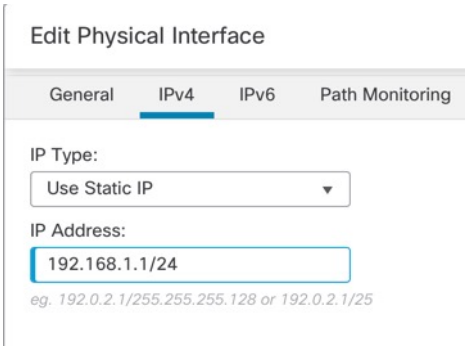
   For example, add a zone called **inside_zone**. Each interface must be assigned to a security zone and/or interface group. An interface can belong to only one security zone, but can also belong to multiple interface groups. You apply your security policy based on zones or groups. For example, you can 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.

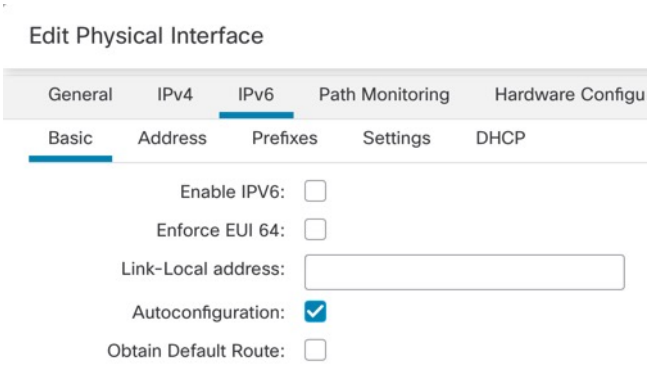
     For example, enter **192.168.1.1/24**

Figure 12: IPv4 Tab



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

Figure 13: IPv6 Tab

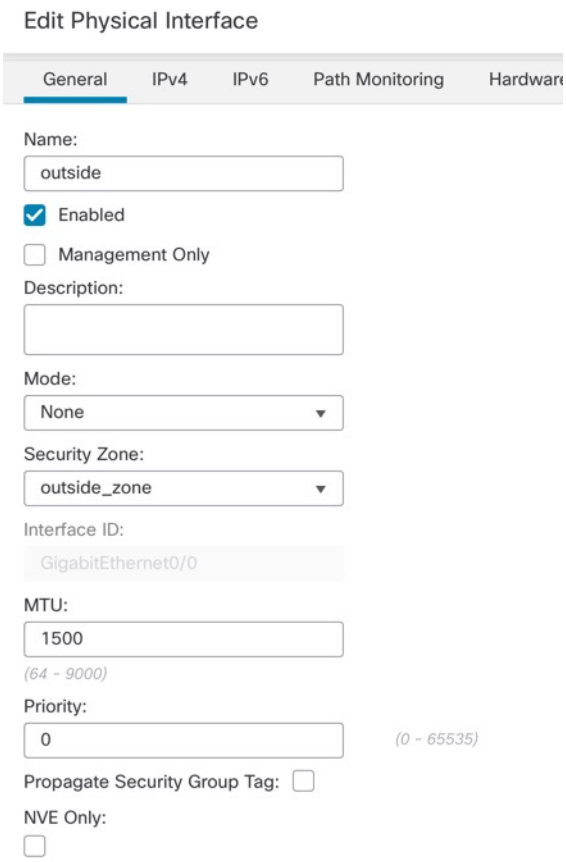


f) Click **OK**.

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

The **General** tab appears.

Figure 14: 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**.

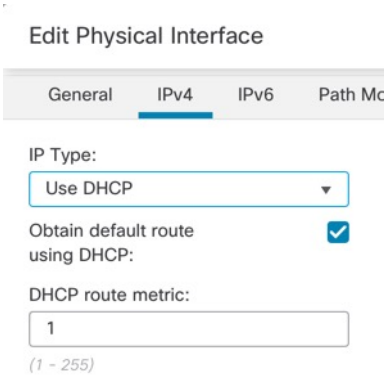
d) From the **Security Zone** drop-down list, choose an existing outside security zone or add a new one by clicking **New**.

   For example, add a zone called **outside_zone**.

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

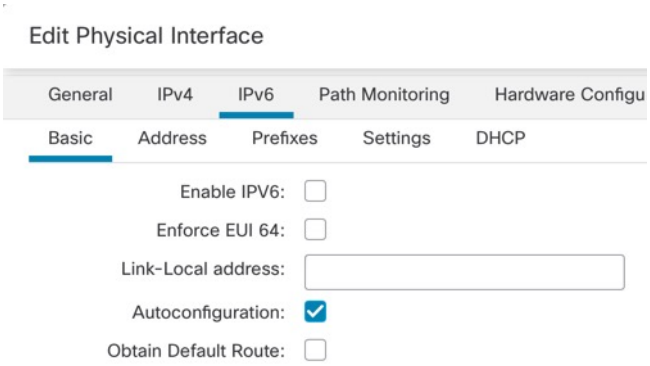
   - **IPv4**—Choose **Use DHCP**, and configure the following optional parameters:
     - **Obtain default route using DHCP**—Obtains the default route from the DHCP server.
     - **DHCP route metric**—Assigns an administrative distance to the learned route, between 1 and 255. The default administrative distance for the learned routes is 1.

Figure 15: IPv4 Tab



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

Figure 16: IPv6 Tab



f) Click **OK**.

Step 5 Click **Save**.

Configure the DHCP Server

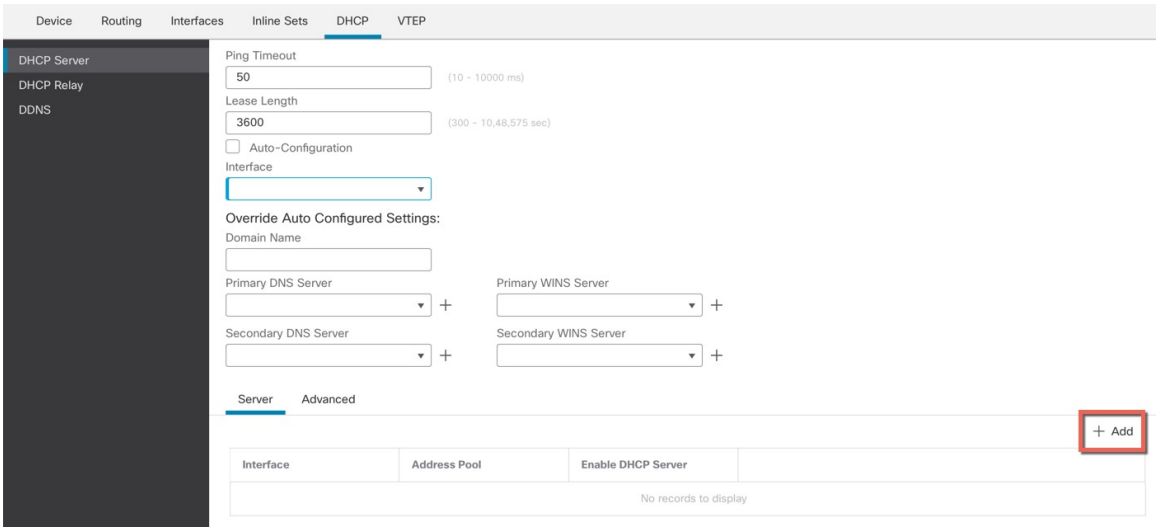
Enable the DHCP server if you want clients to use DHCP to obtain IP addresses from the threat defense.

Procedure

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

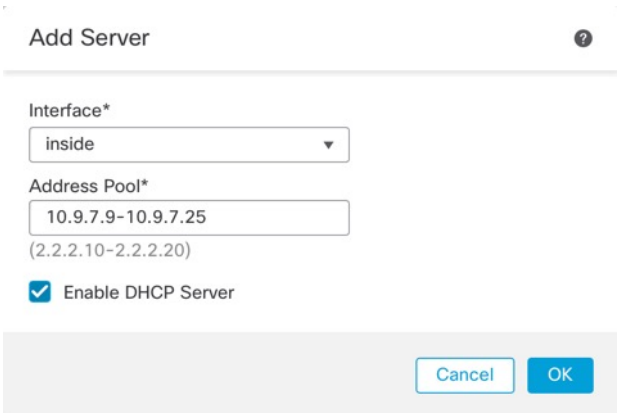
Step 2 Choose **DHCP** > **DHCP Server**.

Figure 17: DHCP Server



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

Figure 18: 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

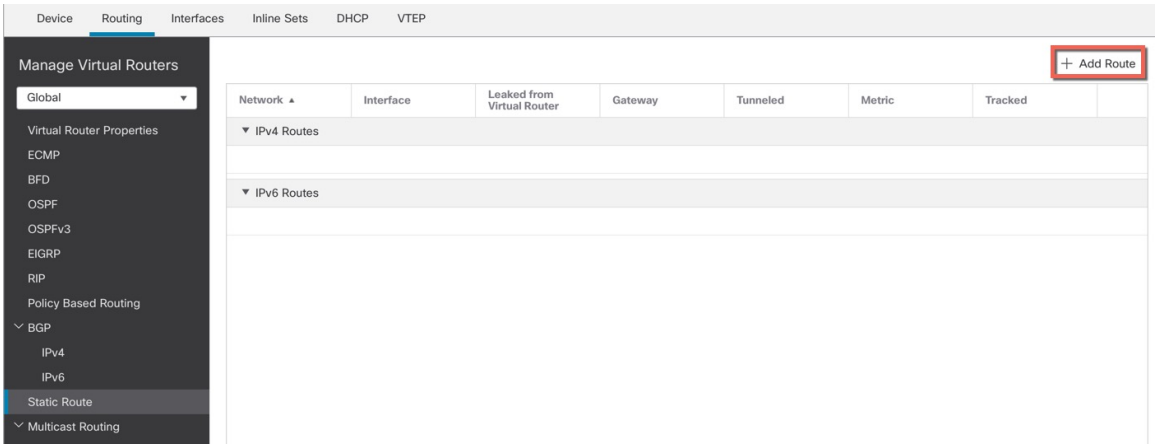
The default route normally points to the upstream router reachable from the outside interface. If you use DHCP for the outside interface, your device might have already received a default route. If you need to manually add the route, complete this procedure. If you received a default route from the DHCP 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 the **Edit** (✎) for the device.

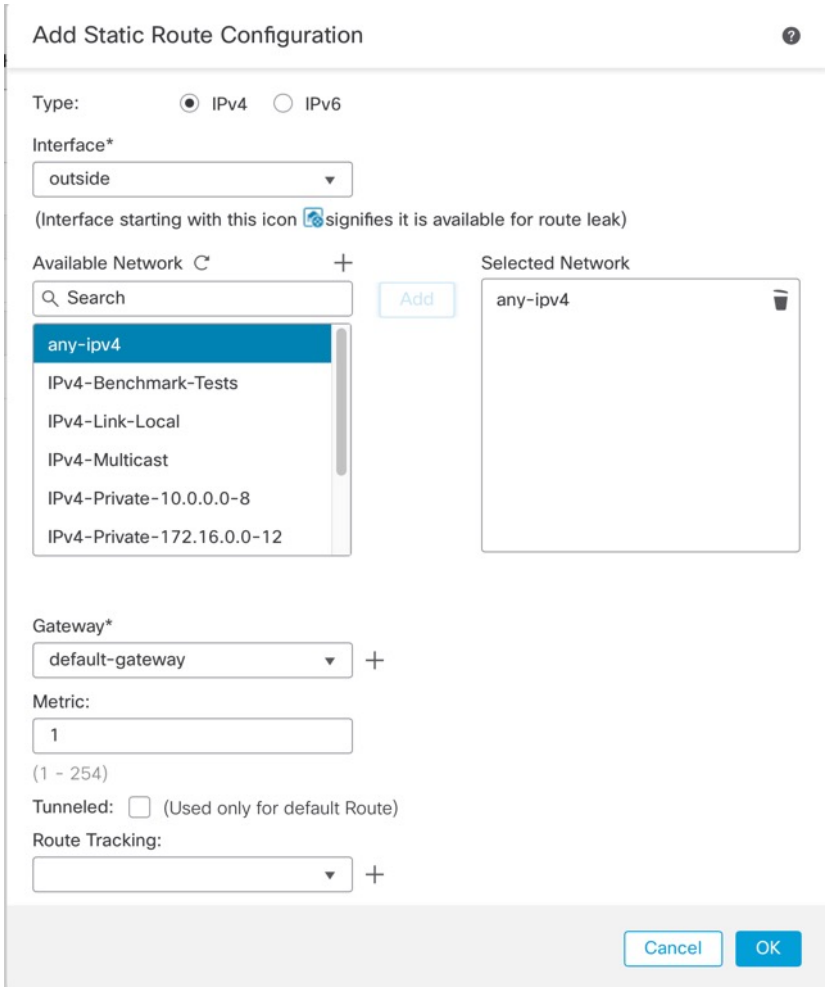
Step 2 Choose **Routing** > **Static Route**.

Figure 19: Static Route



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

Figure 20: 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

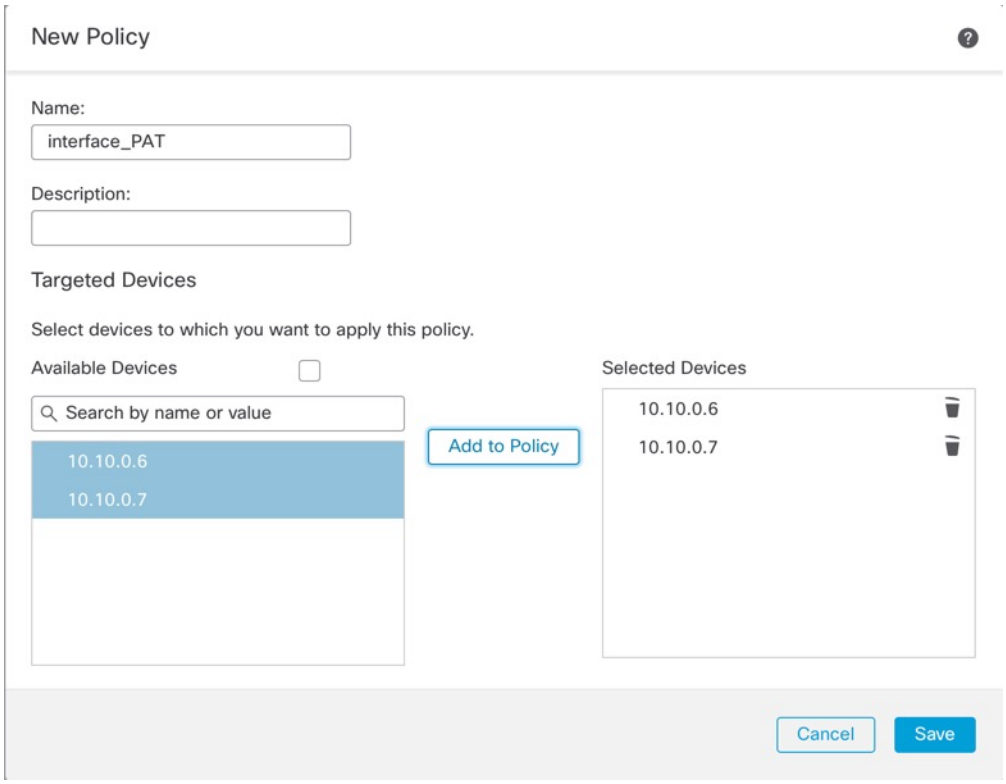
A typical NAT rule converts internal addresses to a port on the outside interface IP address. This type of NAT rule is called *interface Port Address Translation (PAT)*.

Procedure

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

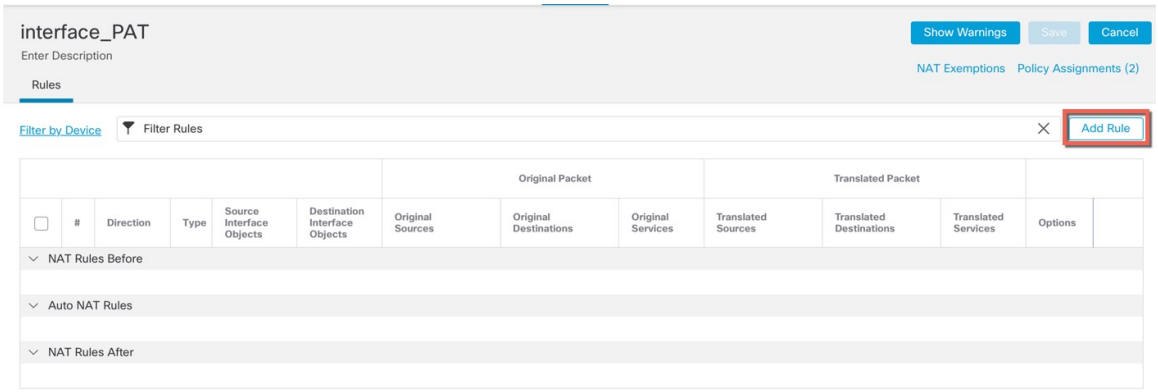
Step 2 Name the policy, select the device(s) that you want to use the policy, and click **Save**.

Figure 21: New Policy



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

Figure 22: NAT Policy

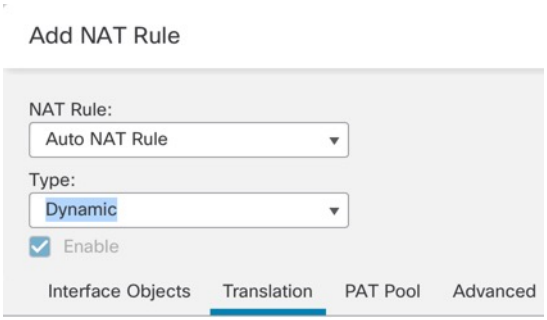


Step 3 Click **Add Rule**.

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

Step 4 Configure the basic rule options:

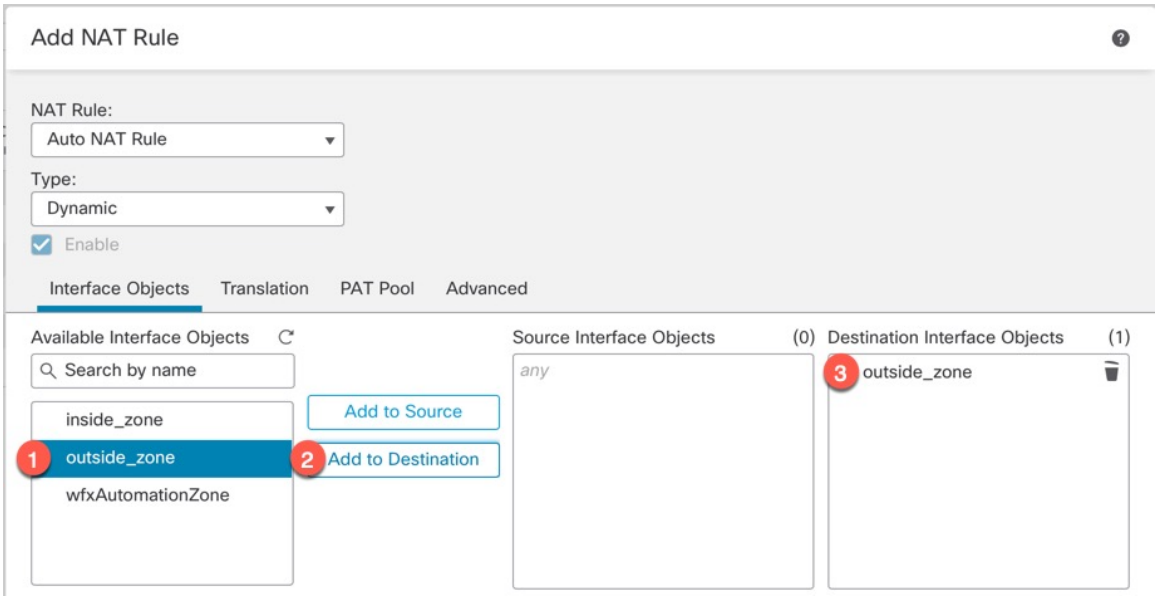
Figure 23: Basic Rule Options



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

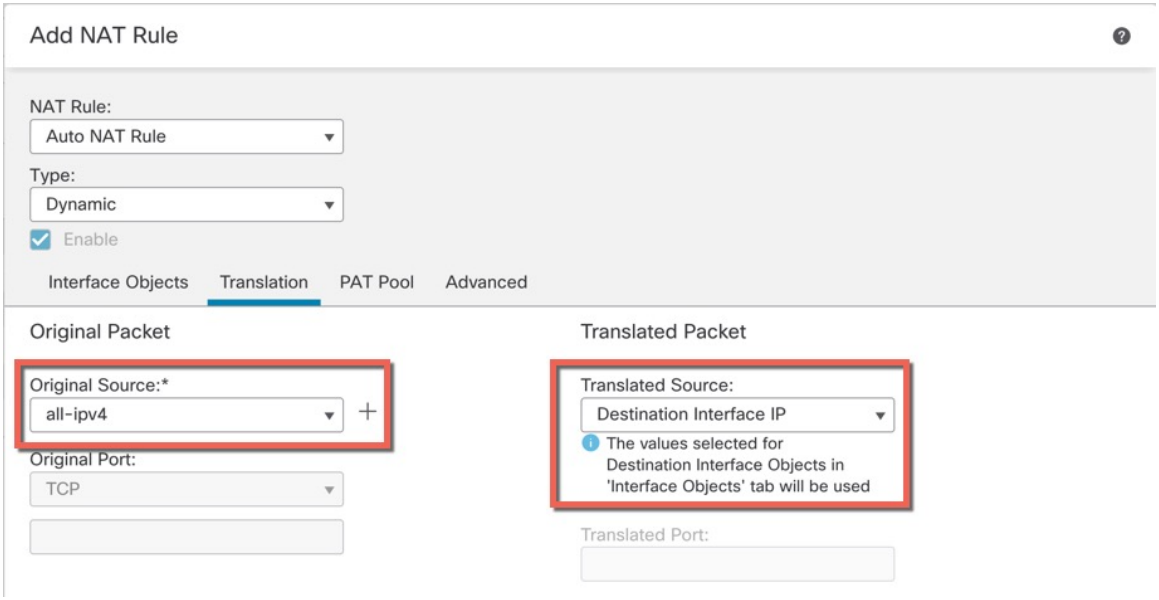
Step 5 On the **Interface Objects** page, add the outside zone from the **Available Interface Objects** area to the **Destination Interface Objects** area.

Figure 24: Interface Objects



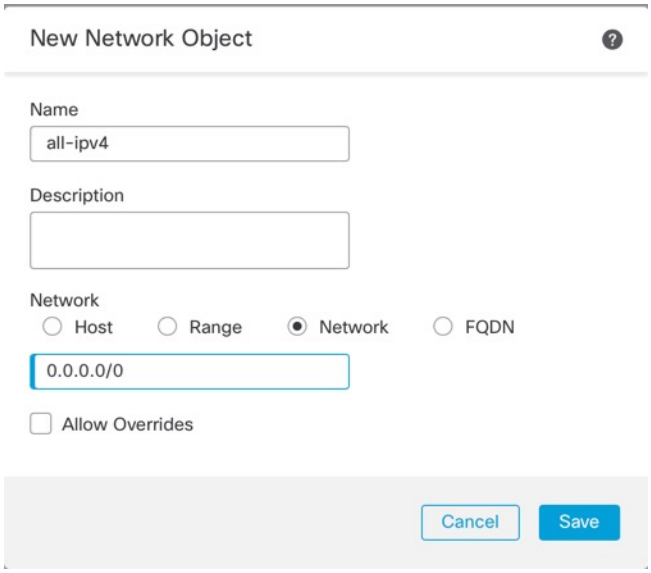
Step 6 On the **Translation** page, configure the following options:

Figure 25: Translation



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

Figure 26: New Network Object



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

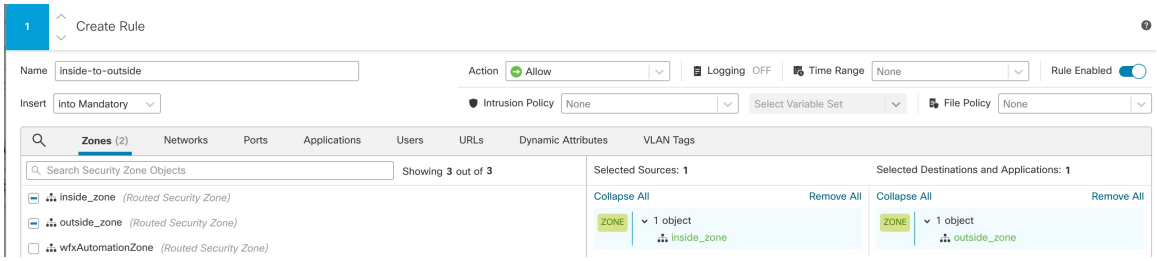
If you created a basic **Block all traffic** access control policy when you registered the threat defense, then you need to add rules to the policy to allow traffic through the device. The following procedure adds a rule to allow traffic from the inside zone to the outside zone. If you have other zones,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

Procedure

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

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

Figure 27: Add Rule



- **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**.

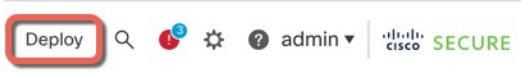
Deploy the Configuration

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 28: Deploy



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

Figure 29: Deploy All

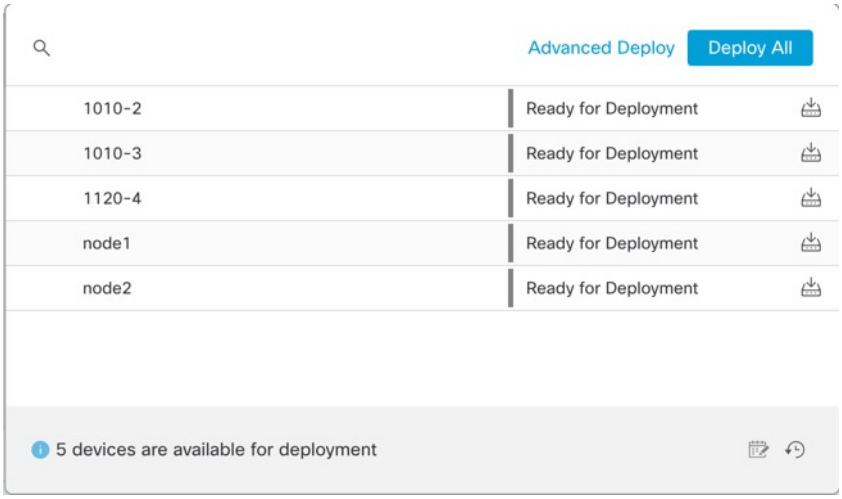
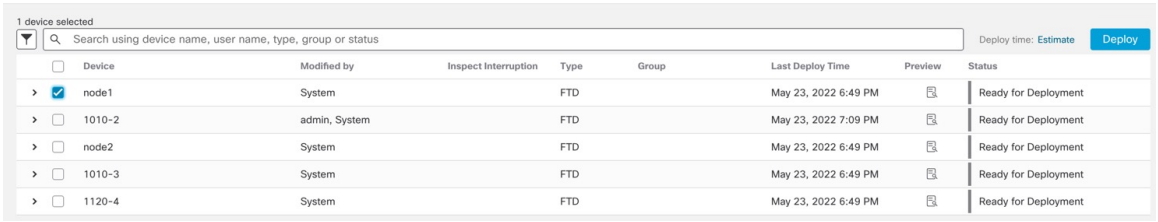
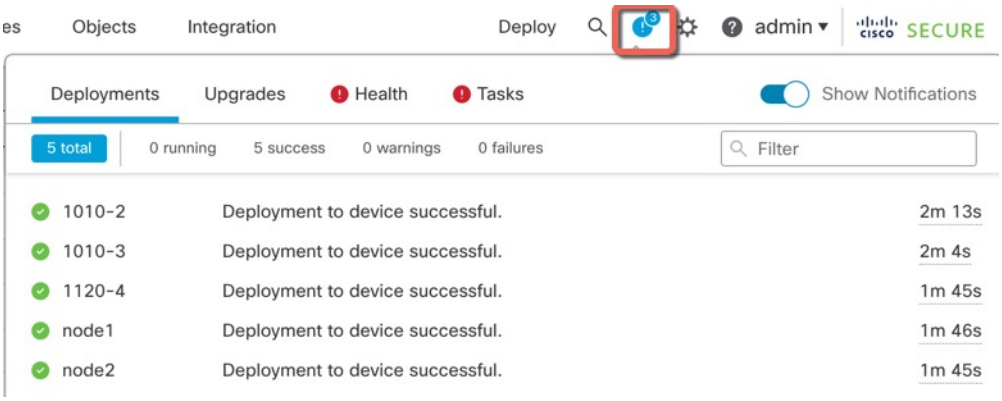


Figure 30: Advanced Deploy



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 31: 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 Firepower 2100 ships with a DB-9 to RJ-45 serial cable, so you may need 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 Device 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 43.

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:

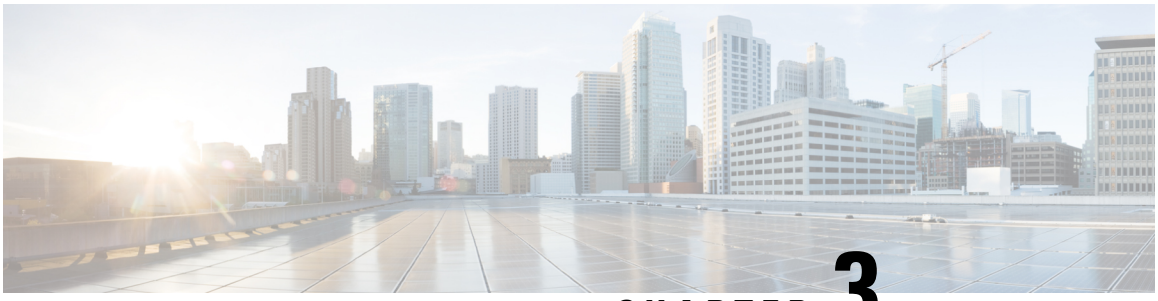
```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

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 Firepower Documentation.

For information related to using the management center, see the Firepower Management Center Configuration Guide.



CHAPTER 3

Threat Defense Deployment with a Remote Management Center

Is This Chapter for You?

To see all available applications and managers, see Which Application and Manager is Right for You?, on page 1. This chapter applies to the threat defense at a remote branch office using the management center at a central headquarters.

Each threat defense controls, inspects, monitors, and analyzes traffic, and then reports to a managing 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.

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.

How Remote Management Works

To allow the management center to manage the threat defense over the internet, you use the outside interface for management center manager access instead of the Management interface. Because most remote branch offices only have a single internet connection, outside management center access makes centralized management possible.

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.

Registration Methods

Use one of the following methods to provision your threat defense:

Low-Touch Provisioning (Management Center 7.4 and later, Threat Defense 7.2 and later)

- An administrator at the central headquarters sends the threat defense to the remote branch office. There is no pre-configuration required. In fact, you should not configure anything on the device, because low-touch provisioning may not work with pre-configured devices.

Note The central administrator can preregister the threat defense on the management center using the threat defense serial number before sending the device to the branch office. The management center integrates with SecureX and Cisco Defense Orchestrator (CDO) for this functionality.

- The branch office administrator cables and powers on the threat defense.
- The central administrator finishes registering the threat defense using CDO.

Manual Provisioning

- An administrator at the central headquarters pre-configures the threat defense at the CLI or using the device manager, and then sends the threat defense to the remote branch office.
- The branch office administrator cables and powers on the threat defense.
- The central administrator finishes registering the threat defense using the management center.

Threat Defense Manager Access Interface

This guide covers outside interface access, because it is the most likely scenario for remote branch offices. Although manager access occurs on the outside interface, the dedicated Management interface is still relevant. The Management interface is a special interface configured separately from the threat defense data interfaces, and it has its own network settings.

- The Management interface network settings are still used even though you are enabling manager access on a data interface.
- All management traffic continues to be sourced from or destined to the Management interface.
- When you enable manager access on a data interface, the threat defense forwards incoming management traffic over the backplane to the Management interface.
- For outgoing management traffic, the Management interface forwards the traffic over the backplane to the data interface.

Manager Access Requirements

Manager access from a data interface has the following limitations:

- You can only enable manager access on a physical, data interface. You cannot use a subinterface or EtherChannel. You can also use the management center to enable manager access on a single secondary interface for redundancy.
- This interface cannot be management-only.
- Routed firewall mode only, using a routed interface.
- PPPoE is not supported. If your ISP requires PPPoE, you will have to put a router with PPPoE support between the threat defense and the WAN modem.
- The interface must be in the global VRF only.
- SSH is not enabled by default for data interfaces, so you will have to enable SSH later using the management center. Because the Management interface gateway will be changed to be the data interfaces, you also cannot SSH to the Management interface from a remote network unless you add a static route for the Management interface using the **configure network static-routes** command.

High Availability Requirements

When using a data interface with device high availability, see the following requirements.

- Use the same data interface on both devices for manager access.
- Redundant manager access data interface is not supported.
- You cannot use DHCP; only a static IP address is supported. Features that rely on DHCP cannot be used, including DDNS and low-touch provisioning.
- Have different static IP addresses in the same subnet.
- Use either IPv4 or IPv6; you cannot set both.
- Use the same manager configuration (**configure manager add** command) to ensure that the connectivity is the same.
- You cannot use the data interface as the failover or state link.

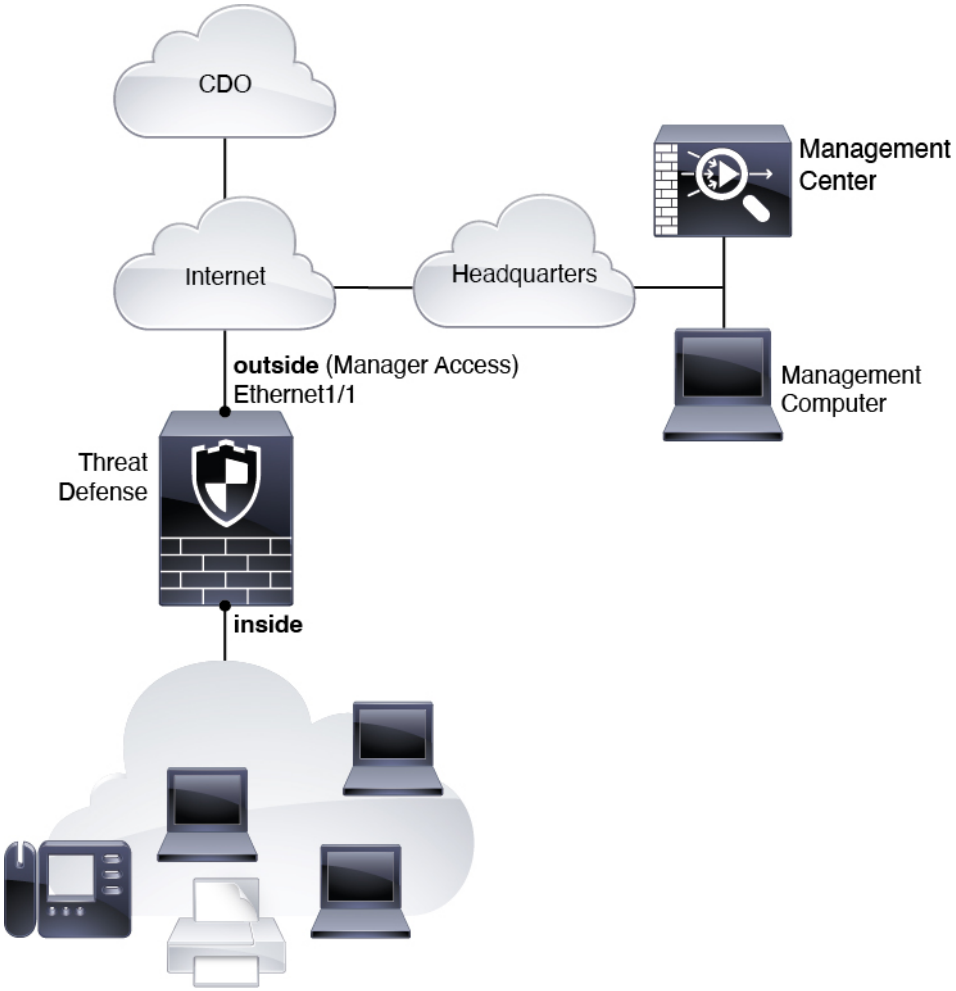
Low-Touch Provisioning Network

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

- The management center is at central headquarters.

- The threat defense uses the outside interface for manager access.
- Either the threat defense or management center needs a public IP address or hostname to allow the inbound management connection, although you do not need to know the IP address for registration. For pre-7.2(4) and 7.3 threat defense versions, the management center needs to be publicly reachable.
- Both the management center and threat defense initially communicate with CDO to establish the management connection
- After initial establishment, CDO is used to reestablish the management connection if it is disrupted; for example, if the threat defense IP address changes due to a new DHCP assignment, CDO will inform the management center of the change.

Figure 32: Low-Touch Provisioning Network



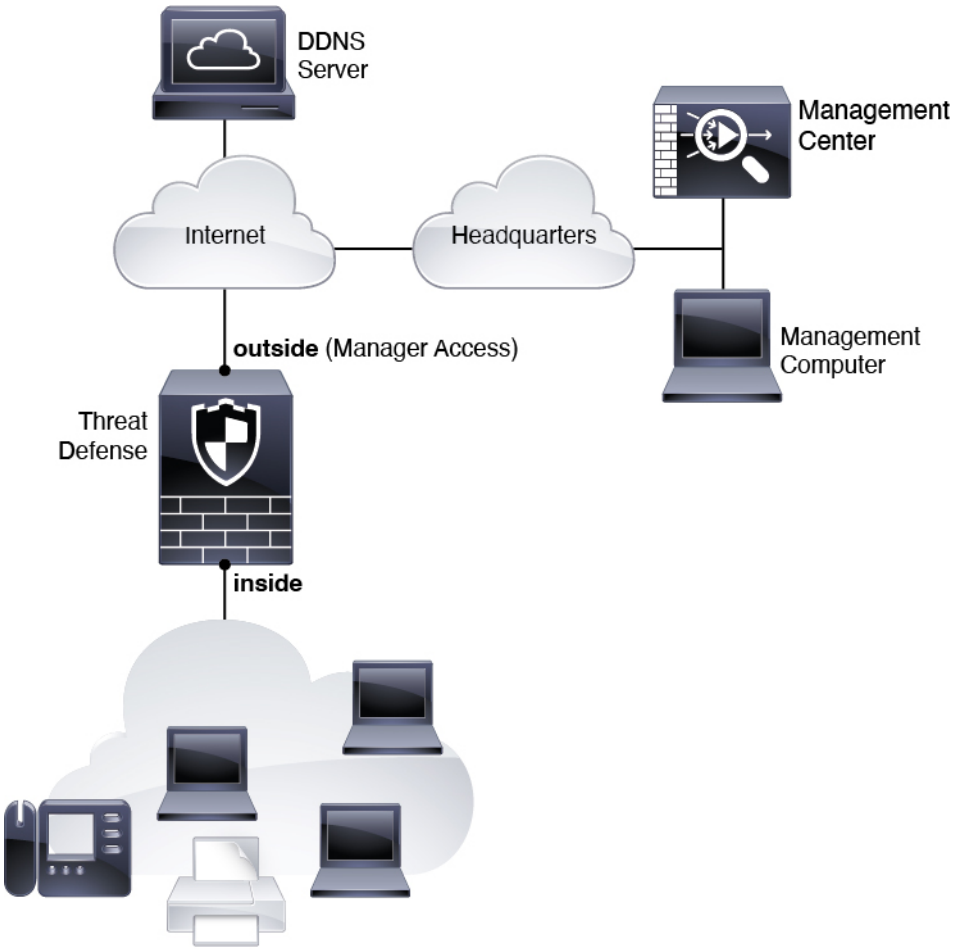
Manual Provisioning Network

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

- The management center is at central headquarters.

- The threat defense uses the outside interface for manager access.
- Either the threat defense or management center needs a public IP address or hostname to allow to allow the inbound management connection; you need to know this IP address for initial setup. You can also optionally configure Dynamic DNS (DDNS) for the outside interface to accommodate changing DHCP IP assignments.

Figure 33: Manual Provisioning Network



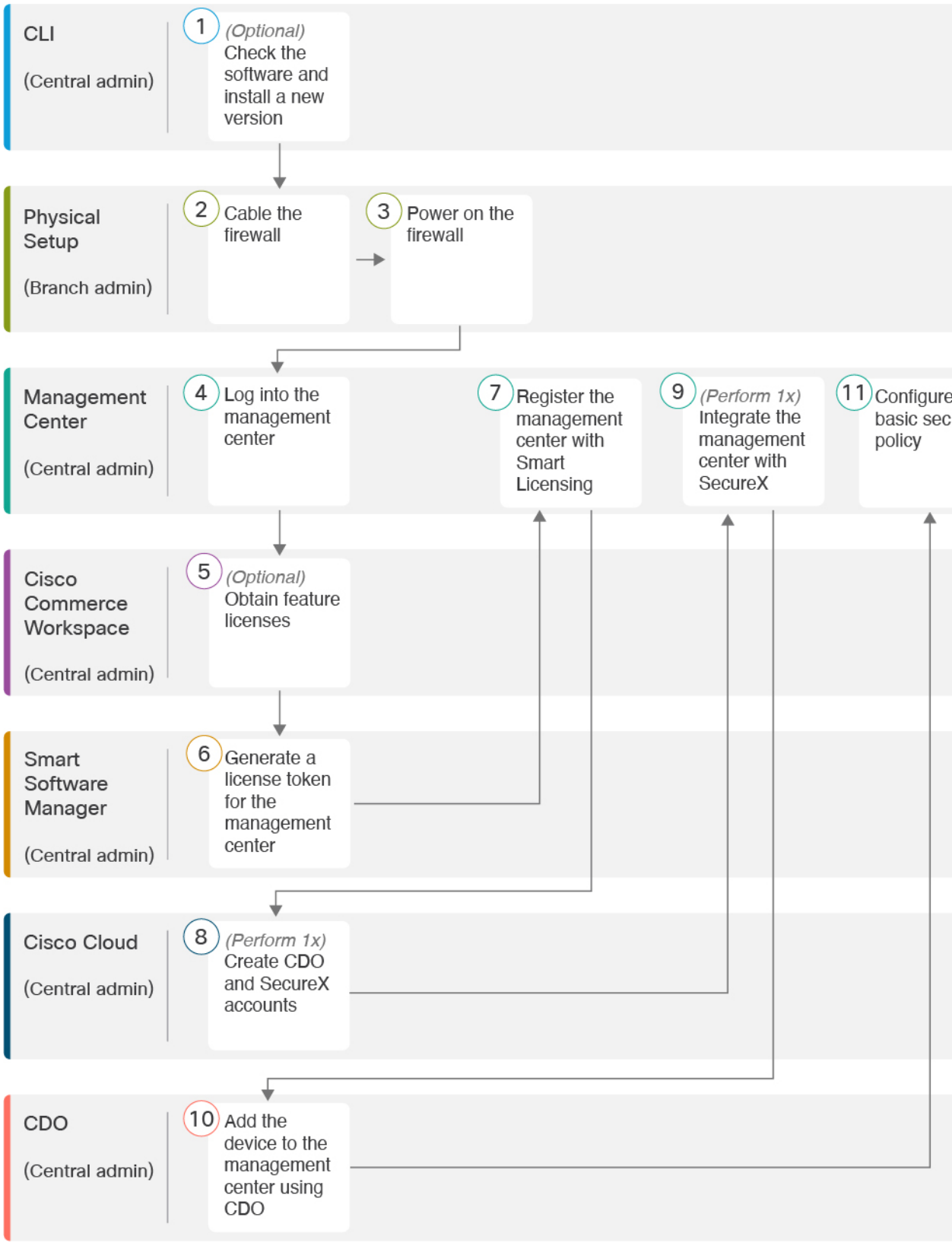
Before You Start

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

End-to-End Tasks: Low-Touch Provisioning

See the following tasks to deploy the threat defense with the management center using low-touch provisioning.

Figure 34: End-to-End Procedure: Low-Touch Provisioning

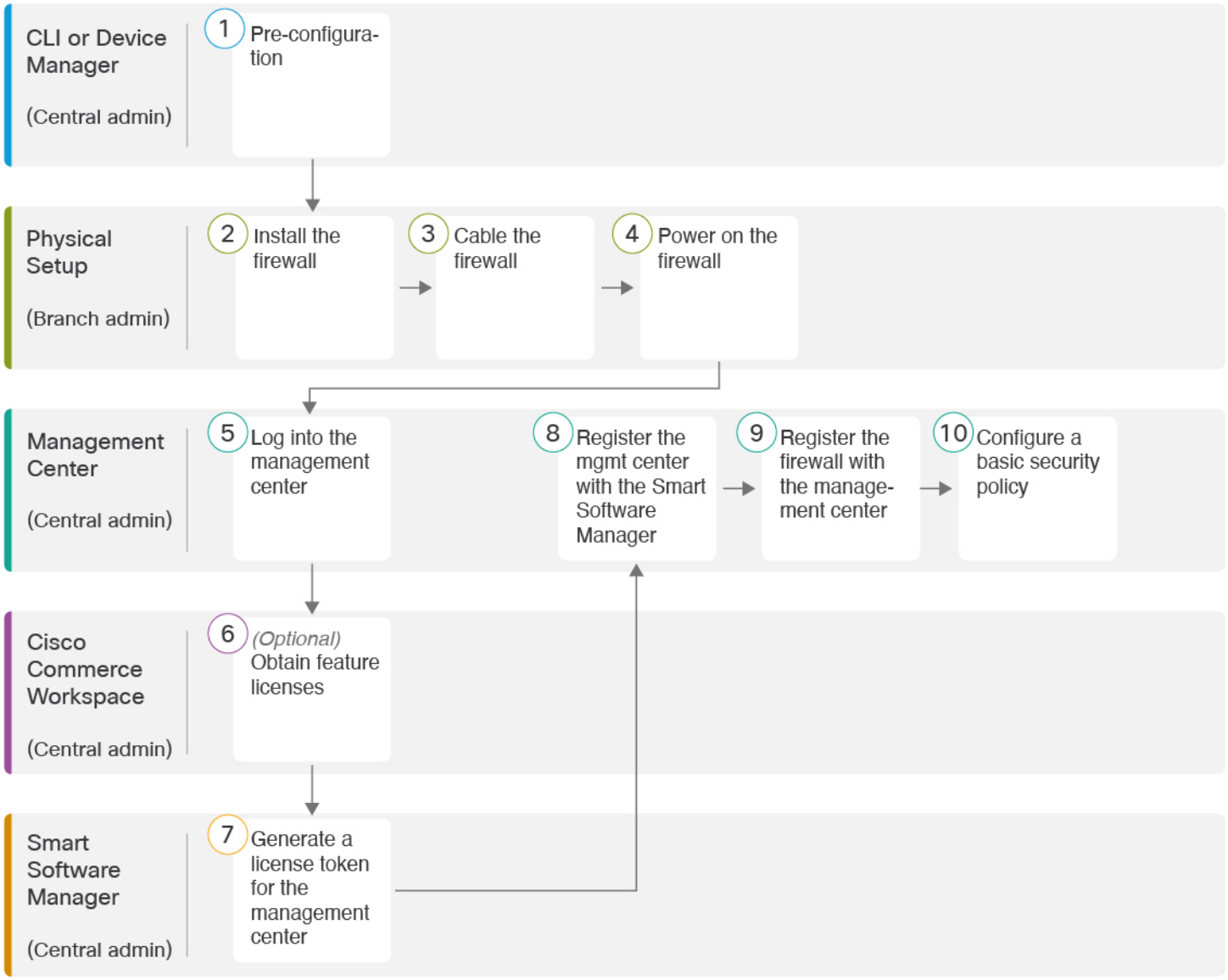

CLI
(Central admin)
1 (Optional) Check the software and install a new version
Physical Setup
(Branch admin)
2 Cable the firewall
3 Power on the firewall
Management Center
(Central admin)
4 Log into the management center
7 Register the management center with Smart Licensing
9 (Perform 1x) Integrate the management center with SecureX
11 Configure basic sec policy
Cisco Commerce Workspace
(Central admin)
5 (Optional) Obtain feature licenses
Smart Software Manager
(Central admin)
6 Generate a license token for the management center
Cisco Cloud
(Central admin)
8 (Perform 1x) Create CDO and SecureX accounts
CDO
(Central admin)
10 Add the device to the management center using CDO

1	CLI (Central administrator)	(Optional) Check the Software and Install a New Version, on page 56.
2	Physical Setup (Branch administrator)	Cable the Firewall, on page 69.
3	Physical Setup (Branch administrator)	Power on the Device, on page 70
4	Management Center (Central administrator)	Log Into the Management Center, on page 23.
5	Cisco Commerce Workspace (Central administrator)	Buy feature licenses (Obtain Licenses for the Management Center, on page 71).
6	Smart Software Manager (Central administrator)	Generate a license token for the management center (Obtain Licenses for the Management Center, on page 71).
7	Management Center (Central administrator)	Register the Management Center with the Smart Licensing server (Obtain Licenses for the Management Center, on page 71).
8	Cisco Cloud (Central administrator)	(Required one time for each management center) Add a Device to the Management Center Using Low-Touch Provisioning, on page 73: Create CDO and SecureX accounts.
9	Management Center (Central administrator)	(Required one time for each management center) Add a Device to the Management Center Using Low-Touch Provisioning, on page 73: Integrate the management center with SecureX.
10	CDO (Central administrator)	Add a Device to the Management Center Using Low-Touch Provisioning, on page 73.
11	Management Center (Central administrator)	Configure a Basic Security Policy, on page 82 .

End-to-End Tasks: Manual Provisioning

See the following tasks to deploy the threat defense with the management center using manual provisioning.

Figure 35: End-to-End Tasks: Manual Provisioning



1	CLI or Device Manager (Central admin)	• (Optional) Check the Software and Install a New Version, on page 56 • Pre-Configuration Using the Device Manager, on page 58 • Pre-Configuration Using the CLI, on page 63

2	Physical Setup (Branch admin)	Install the firewall. See the Cisco Firepower 2100 Series Hardware Installation Guide.
3	Physical Setup (Branch admin)	Cable the Firewall, on page 69.
4	Physical Setup (Branch admin)	Power on the Device, on page 70
5	Management Center (Central admin)	Log Into the Management Center, on page 23.
6	Cisco Commerce Workspace (Central admin)	Obtain Licenses for the Management Center, on page 71: Buy feature licenses.
7	Smart Software Manager (Central admin)	Obtain Licenses for the Management Center, on page 71: Generate a license token for the management center.
8	Management Center (Central admin)	Obtain Licenses for the Management Center, on page 71: Register the management center with the Smart Licensing server.
9	Management Center (Central admin)	Add a Device to the Management Center Manually, on page 79.
10	Management Center (Central admin)	Configure a Basic Security Policy, on page 28.

Central Administrator Pre-Configuration

You might need to manually pre-configure the threat defense before you send it to the branch office.

(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 CLI. See Access the Threat Defense and FXOS CLI, on page 94 for more information. This procedure shows using the console port, but you can use SSH instead.

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               7.4.0.65        7.4.0.65
        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 19. 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.

For low-touch provisioning, when you onboard the device, for the **Password Reset** area, be sure to choose **No...** because you already set the password.

d) Shut down the device. See Power Off the Device at the CLI, on page 102.

Perform Initial Configuration (Manual Provisioning)

For manual provisioning, perfom initial configuration of the threat defense using the CLI or using the device manager.

Pre-Configuration Using the Device Manager

Connect to the device manager to perform initial setup of the threat defense. 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 settings. Note that other default configuration settings, such as the access control policy or security zones, are not retained. 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).

Before you begin

Deploy and perform initial configuration of the management center. You will need to know the management center IP address or hostname before you set up the threat defense.

Procedure

Step 1 Connect your management computer to the Inside (Ethernet 1/2) interface.

Step 2 Power on the firewall.

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

Step 3 Log in to the device manager.

a) Enter the following URL in your browser: **https://192.168.95.1**

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

c) You are prompted to read and accept the End User License Agreement and change the admin password.

Step 4 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.

   The Management interface settings are used even though you are enabling the manager access on a data interface. For example, the management traffic that is routed over the backplane through the data interface will resolve FQDNs using the Management interface DNS servers, and not the data interface DNS servers.

   DNS Servers—The DNS server for the system's management address. 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 system's management address.

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 5 (Might be required) Configure the Management interface. See the Management interface on **Device** > **Interfaces**.

The Management interface must have the gateway set to data interfaces. By default, the Management interface receives an IP address and gateway from DHCP. If you do not receive a gateway from DHCP (for example, you did not connect this interface to a network), then the gateway will default to data interfaces, and you do not need to configure anything. If you did receive a gateway from DHCP, then you need to instead configure this interface with a static IP address and set the gateway to data interfaces.

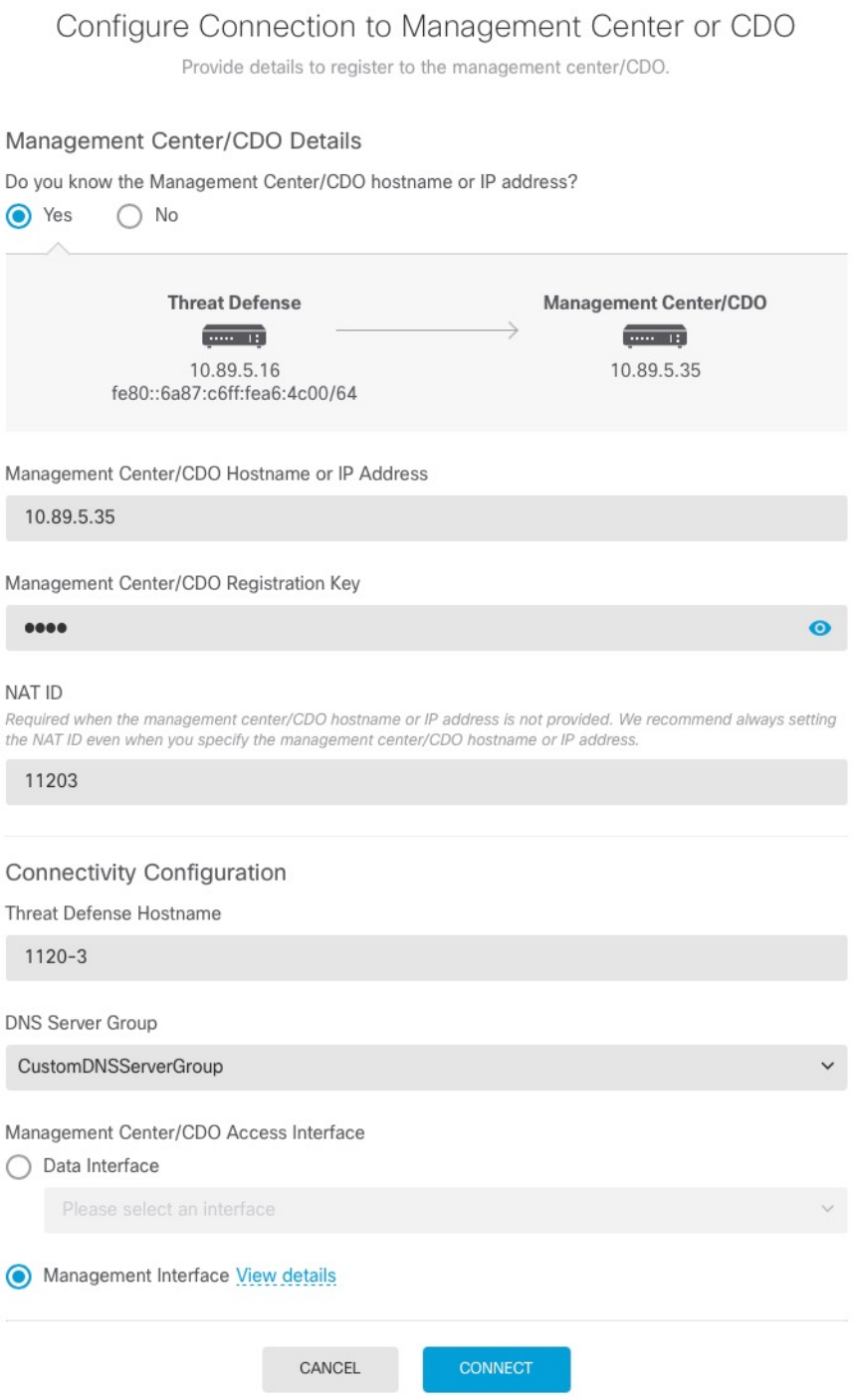
Step 6 If you want to configure additional interfaces, including an interface other than outside or inside that you want to use for the manager access, choose **Device**, and then click the link in the **Interfaces** summary.

See Configure the Firewall in the Device Manager, on page 124 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 7 Choose **Device** > **System Settings** > **Central Management**, and click **Proceed** to set up the management center management.

Step 8 Configure the **Management Center/CDO Details**.

Figure 36: Management Center/CDO Details



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, SSL-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 9 Configure the **Connectivity Configuration**.

a) Specify the **FTD Hostname**.

This FQDN will be used for the outside interface, or whichever interface you choose for the **Management Center/CDO Access Interface**.

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.

This setting sets the *data* interface DNS server. The Management DNS server that you set with the setup wizard is used for management traffic. The data DNS server is used for DDNS (if configured) or for security policies applied to this interface. You are likley to choose the same DNS server group that you used for Management, because both management and data traffic reach the DNS server through the outside interface.

On the management center, the data interface DNS servers are configured in the Platform Settings policy that you assign to this threat defense. When you add the threat defense to the management center, the local setting is maintained, and the DNS servers are *not* added to a Platform Settings policy. However, if you later assign a Platform Settings policy to the threat defense that includes a DNS configuration, then that configuration will overwrite the local setting. We suggest that you actively configure the DNS Platform Settings to match this setting to bring the management center and the threat defense into sync.

Also, local DNS servers are only retained by the management center if the DNS servers were discovered at initial registration.

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

You can choose any configured interface, but this guide assumes you are using outside.

Step 10 If you chose a different data interface from outside, then add a default route.

You will see a message telling you to check that you have a default route through the interface. If you chose outside, you already configured this route as part of the setup wizard. If you chose a different interface, then you need to manually configure a default route before you connect to the management center. See Configure

the Firewall in the Device Manager, on page 124 for more information about configuring static routes in the device manager.

Step 11 Click **Add a Dynamic DNS (DDNS) method**.

DDNS ensures the management center can reach the threat defense at its Fully-Qualified Domain Name (FQDN) if the threat defense's IP address changes. See **Device** > **System Settings** > **DDNS Service** to configure DDNS.

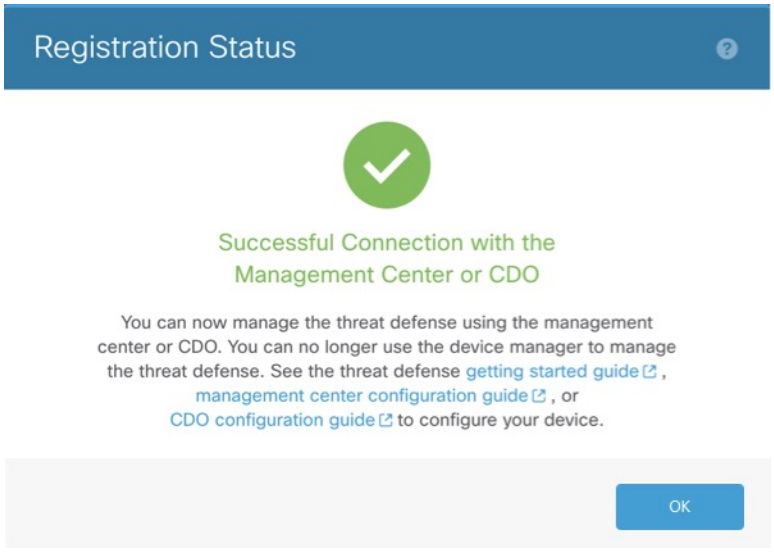
If you configure DDNS before you add the threat defense to the management center, the threat defense automatically adds certificates for all of the major CAs from the Cisco Trusted Root CA bundle so that the threat defense can validate the DDNS server certificate for the HTTPS connection. The threat defense supports any DDNS server that uses the DynDNS Remote API specification (https://help.dyn.com/remote-access-api/).

Step 12 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 37: Successful Connection



Pre-Configuration Using the CLI

Connect to the threat defense CLI to perform initial setup. When you use the CLI for initial configuration, only the Management interface and manager access interface settings are retained. When you perform initial setup using the device manager (7.1 and later), *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.

Before you begin

You will need to know the management center IP address or hostname before you set up the threat defense.

Procedure

Step 1 Power on the firewall.

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

Step 2 Connect to the threat defense CLI on the console port.

The console port connects to the FXOS CLI.

Step 3 Log in with the username **admin** and the password **Admin123**.

The first time you log in to the 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, then 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 4 Connect to the threat defense CLI.

connect ftd

Example:

```
firepower# connect ftd
>
```

Step 5 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 for the Management interface settings.

The Management interface settings are used even though you are enabling manager access on a data interface.

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. Although you do not plan to use the Management interface, you must set an IP address, for example, a private address.
- **Configure IPv4 via DHCP or manually?** and/or **Configure IPv6 via DHCP, router, or manually?**—Choose **manual**. You cannot configure a data interface for management if the management interface is set to DHCP, because the default route, which must be **data-interfaces** (see the next bullet), might be overwritten with one received from the DHCP server.
- **Enter the IPv4 default gateway for the management interface** and/or **Enter the IPv6 gateway for the management interface**—Set the gateway to be **data-interfaces**. This setting forwards management traffic over the backplane so it can be routed through the manager access data interface.
- **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?**—Enter **routed**. Outside manager access is only supported in routed firewall mode.

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 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 [192.168.45.61]: 10.89.5.17
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]:
Enter a fully qualified hostname for this system [firepower]: 1010-3
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 1010-3
```

```
Setting static IPv4: 10.89.5.17 netmask: 255.255.255.192 gateway: data 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 6 Configure the outside interface for manager access.

configure network management-data-interface

You are then prompted to configure basic network settings for the outside interface. See the following details for using this command:

- The Management interface cannot use DHCP if you want to use a data interface for management. If you did not set the IP address manually during initial setup, you can set it beforehand using the **configure network** {**ipv4** | **ipv6**} **manual** command. If you did not already set the Management interface gateway to **data-interfaces**, this command will set it now.
- When you add the threat defense to the management center, the management center discovers and maintains the interface configuration, including the following settings: interface name and IP address, static route to the gateway, DNS servers, and DDNS server. For more information about the DNS server configuration, see below. In the management center, you can later make changes to the manager access interface configuration, but make sure you don't make changes that can prevent the threat defense or the management center from re-establishing the management connection. If the management connection is disrupted, the threat defense includes the **configure policy rollback** command to restore the previous deployment.

- If you configure a DDNS server update URL, the threat defense automatically adds certificates for all of the major CAs from the Cisco Trusted Root CA bundle so that the threat defense can validate the DDNS server certificate for the HTTPS connection. The threat defense supports any DDNS server that uses the DynDNS Remote API specification (https://help.dyn.com/remote-access-api/).
- This command sets the *data* interface DNS server. The Management DNS server that you set with the setup script (or using the **configure network dns servers** command) is used for management traffic. The data DNS server is used for DDNS (if configured) or for security policies applied to this interface.

  On the management center, the data interface DNS servers are configured in the Platform Settings policy that you assign to this threat defense. When you add the threat defense to the management center, the local setting is maintained, and the DNS servers are *not* added to a Platform Settings policy. However, if you later assign a Platform Settings policy to the threat defense that includes a DNS configuration, then that configuration will overwrite the local setting. We suggest that you actively configure the DNS Platform Settings to match this setting to bring the management center and the threat defense into sync.

  Also, local DNS servers are only retained by the management center if the DNS servers were discovered at initial registration. For example, if you registered the device using the Management interface, but then later configure a data interface using the **configure network management-data-interface** command, then you must manually configure all of these settings in the management center, including the DNS servers, to match the threat defense configuration.
- You can change the management interface after you register the threat defense to the management center, to either the Management interface or another data interface.
- The FQDN that you set in the setup wizard will be used for this interface.
- You can clear the entire device configuration as part of the command; you might use this option in a recovery scenario, but we do not suggest you use it for initial setup or normal operation.
- To disable data managemement, enter the **configure network management-data-interface disable** command.

Example:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]:
IP address (manual / dhcp) [dhcp]:
DDNS server update URL [none]:
https://deanwinchester:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow manager access from any network, if you wish to
change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

Example:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
```

```
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow manager access from any network, if you wish to
change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

Step 7 (Optional) Limit data interface access to the management center on a specific network.

configure network management-data-interface client *ip_address netmask*

By default, all networks are allowed.

Step 8 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**. 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 use a data interface for management, then you must specify the NAT ID on *both* the threat defense and the management center for registration. 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 fmc-1.example.com regk3y78 natid56
Manager successfully configured.
```

Step 9 Shut down the threat defense so you can send the device to the remote branch office.

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 system.

a) Enter the **shutdown** command.
b) Observe the Power LED and Status LED to verify that the chassis is powered off (appear unlit).

c) After the chassis has successfully powered off, you can then unplug the power to physically remove power from the chassis if necessary.

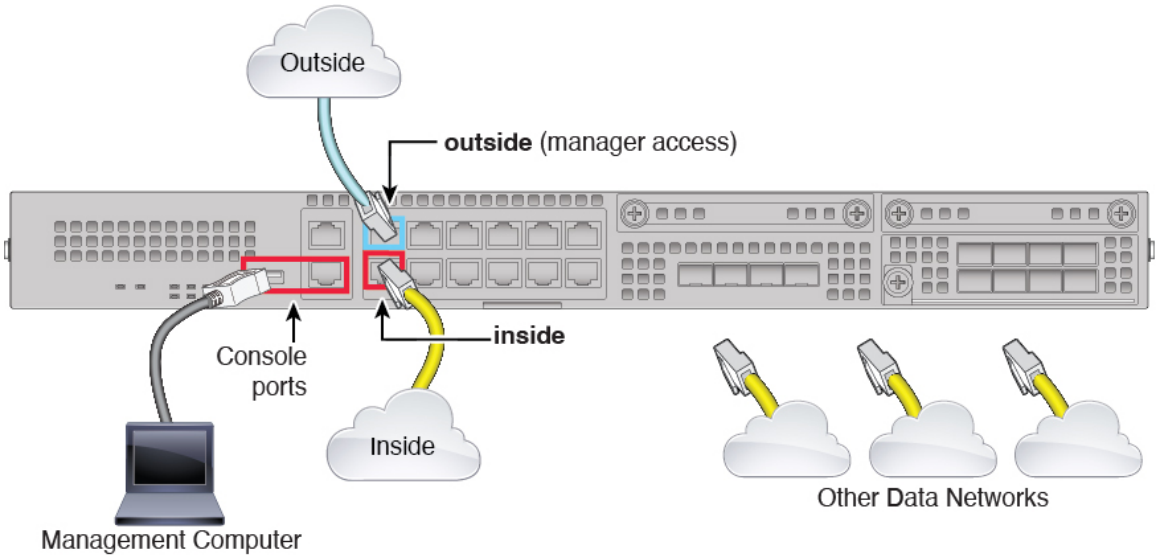
Branch Office Installation

After you receive the threat defense from central headquarters, you only need to cable and power on the firewall so that it has internet access from the outside interface. The central administrator can then complete the configuration.

Cable the Firewall

The management center and your management computer reside at a remote headquarters, and can reach the threat defense over the internet. To cable the Firepower 2100, see the following steps.

Figure 38: Cabling a Remote Management Deployment



Procedure

Step 1 Install the chassis. See the Cisco Firepower 2100 Series Hardware Installation Guide.

Step 2 Connect the outside interface (Ethernet 1/1) to your outside router.

Step 3 Connect the inside interface (for example, Ethernet 1/2) to your inside switch or router.

Step 4 Connect other networks to the remaining interfaces.

Step 5 (Optional) Connect the management computer to the console port.

At the branch office, the console connection is not required for everyday use; however, it may be required for troubleshooting purposes.

Power on the Device

The power switch is located to the left of power supply module 1 on the rear of the chassis. It is a toggle switch that controls power to the system. If the power switch is in standby position, only the 3.3-V standby power is enabled from the power supply module and the 12-V main power is OFF. When the switch is in the ON position, the 12-V main power is turned on and the system boots.

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

Before you begin

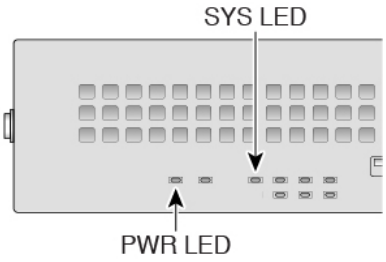
It's important that you provide reliable power for your device (for example, using an uninterruptable power supply (UPS)). Loss of power without first shutting down can cause serious file system damage. There are many processes running in the background all the time, and losing power does not allow the graceful shutdown of your system.

Procedure

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

Step 2 Press the power switch on the back of the device.

Step 3 Check the PWR LED on the front of the device; if it is solid green, the device is powered on.



Step 4 Check the SYS LED on the front of the device; after it is solid green, the system has passed power-on diagnostics.

Note Before you move the power switch to the OFF position, use the shutdown commands so that the system can perform a graceful shutdown. This may take several minutes to complete. After the graceful shutdown is complete, the console displays `It is safe to power off now`. The front panel blue locator beacon LED lights up indicating the system is ready to be powered off. You can now move the switch to the OFF position. The front panel PWR LED flashes momentarily and turns off. Do not remove the power until the PWR LED is completely off.

See the FXOS Configuration Guide for more information on using the shutdown commands.

Central Administrator Post-Configuration

After the remote branch administrator cables the threat defense so it has internet access from the outside interface, you can register the threat defense to the management center and complete configuration of the device.

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 optionally purchase the following feature licenses:

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

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.

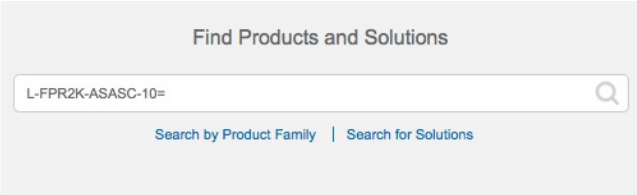
- Your Smart Software Licensing account must qualify for the Strong Encryption (3DES/AES) license to use some features (enabled using the export-compliance flag).

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 39: License Search



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

- IPS, Malware Defense, and URL license combination:
  - L-FPR2110T-TMC=
  - L-FPR2120T-TMC=
  - L-FPR2130T-TMC=
  - L-FPR2140T-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-FPR2110T-TMC-1Y
  - L-FPR2110T-TMC-3Y
  - L-FPR2110T-TMC-5Y
  - L-FPR2120T-TMC-1Y
  - L-FPR2120T-TMC-3Y
  - L-FPR2120T-TMC-5Y
  - L-FPR2130T-TMC-1Y
  - L-FPR2130T-TMC-3Y
  - L-FPR2130T-TMC-5Y
  - L-FPR2140T-TMC-1Y
  - L-FPR2140T-TMC-3Y
  - L-FPR2140T-TMC-5Y
- 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 Software Manager.

Registering requires you to generate a registration token in the Smart Software Manager. See the management center configuration guide for detailed instructions. For Low-Touch Provisioning, you must enable **Cloud Assistance for Low-Touch Provisioning** either when you register with the Smart Software Manager, or after you register. See the **System** > **Licenses** > **Smart Licenses** page.

Register the Threat Defense with the Management Center

Register the threat defense with the management center depending on which deployment method you are using.

Add a Device to the Management Center Using Low-Touch Provisioning

Low-touch provisioning lets you register devices to the management center by serial number without having to perform any initial setup on the device. The management center integrates with Cisco Defense Orchestrator (CDO) and SecureX for this functionality.

Use this procedure to add a single device to the management center. High availability is only supported when you use the Management interface, because DHCP is not supported for data interfaces and high availability. Clustering is not supported.

Note If the management center is configured for high availability, CDO automatically onboards the threat defense to the primary management center.

Low-touch provisioning is only supported on the following models:

- Firepower 1000
- Firepower 2100
- Secure Firewall 3100

Threat Defense Feature History:

- 7.2.4 (7.3 does not include this enhancement)—Outside and Management interface support. For the outside interface, the management center does not have to be publicly reachable if the device outside interface is reachable.
- 7.2, 7.3—Outside interface support only. The management center must be publicly reachable.

Before you begin

- Make sure the device is unconfigured or a fresh install. Low-touch provisioning is meant for new devices only. Pre-configuration can disable low-touch provisioning, depending on your settings.
- Cable the outside interface or Management interface so it can reach the internet. If you use the outside interface for low-touch provisioning, do not also cable the Management interface; if the Management interface gets an IP address from DHCP, the routing will be incorrect for the outside interface.

- Make sure you have at least one access control policy configured on the management center so you can assign it to new devices. You cannot add a policy using CDO.
- If the device does not have a public IP address or FQDN, or you use the Management interface, set a public IP address/FQDN for the management center (if different from the management center management interface IP address; for example, it is behind NAT) so the device can initiate the management connection. See . You can also configure the public IP address/FQDN in CDO during this procedure.

Procedure

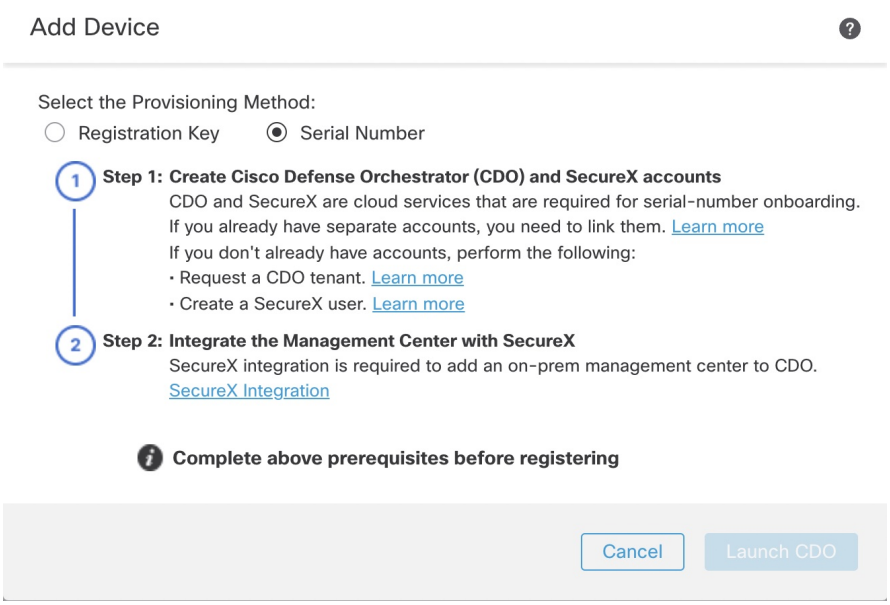
Step 1 The first time you add a device using a serial number, you need to complete the following prerequisites. After the first time, you can skip to adding the devices directly in CDO.

a) In the management center, choose **Devices** > **Device Management**.

b) From the **Add** drop-down menu, choose **Device**.

c) Click **Serial Number** for the provisioning method.

Figure 40: Add Device by Serial Number



d) Create CDO and SecureX accounts.

Note If you already have preexisting but separate SecureX and CDO accounts, you need to link them. See https://cisco.com/go/cdo-securex-link for more information about linking accounts.

If you don't already have accounts, perform the following:

- Request a CDO tenant. See the CDO documentation for information about requesting a new CDO tenant.
- Create a SecureX account. See the CDO documentation for information about how to create one.

e) Integrate the management center with SecureX. Click the link for step 2 to open the **SecureX Integration** page in the management center.

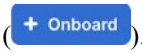
See . See also the SecureX integration guide.

By default, CDO onboards the on-prem management center after you integrate the management center with SecureX. CDO needs the management center in its inventory for low-touch provisioning to operate. CDO's management center support is limited to device onboarding, viewing its managed devices, viewing objects associated with the management center, and cross-launching the management center.

Note For a management center high-availability pair, you also need to integrate the secondary management center with SecureX.

f) Click **Launch CDO** if you do not already have it open, or log in here: https://www.defenseorchestrator.com/ .

Make sure CDO is not blocked by a pop-up blocker.

Step 2 On the CDO **Dashboard** (https://www.defenseorchestrator.com/), click **Onboard** (

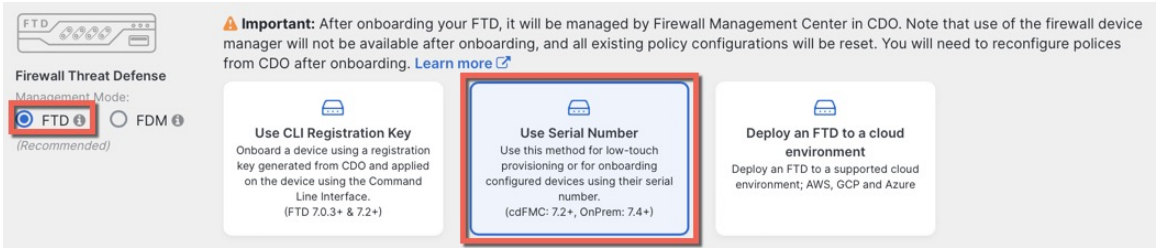
).

Step 3 Click the **FTD** tile.

Figure 41: FTD Tile

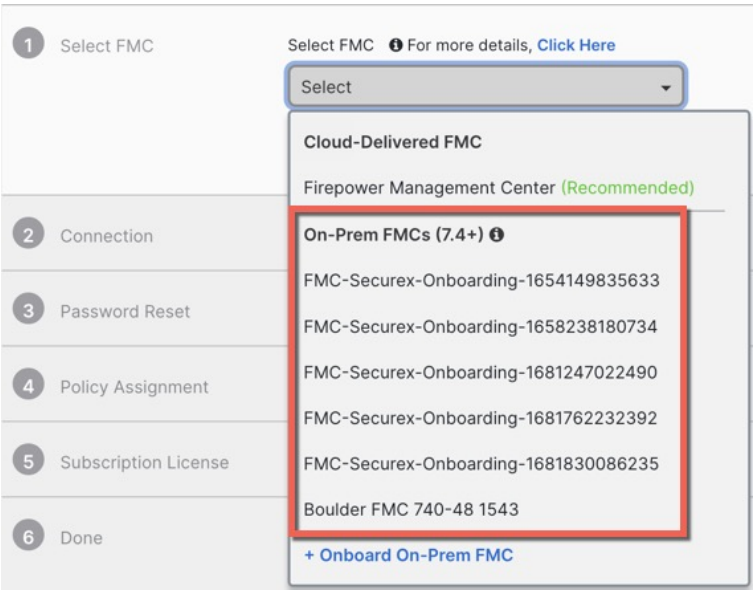
Step 4 On the **Onboard FTD Device** screen, click **Use Serial Number**.

Figure 42: Use Serial Number



Step 5 In **Select FMC**, choose an **On-Prem FMC** from the list, and click **Next**.

Figure 43: Select FMC

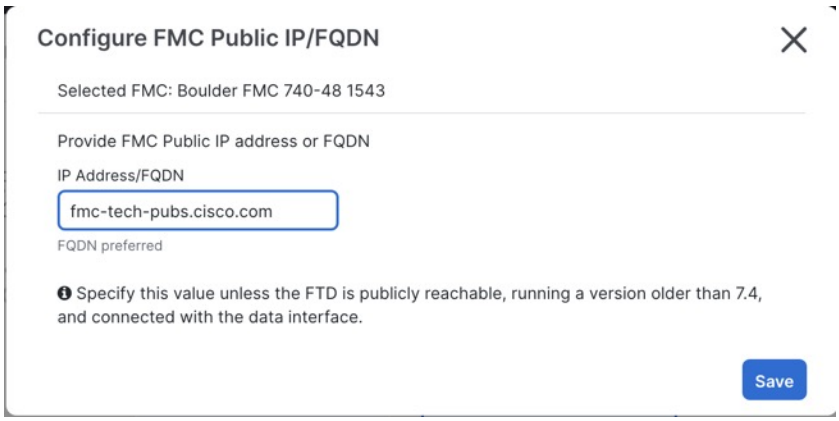


If the management center has a public IP address or FQDN set, it will show after you choose it.

Figure 44: Public IP Address/FQDN

The management center needs a public IP address/FQDN if the device does not have a public IP address/FQDN or if you use the Management interface for low-touch provisioning. You can set the management center public IP address/FQDN by clicking the **FMC Public IP** link. You see the following dialog box.

Figure 45: Configure FMC Public IP/FQDN



Note For a management center high-availability pair, you also need to set the public IP address/FQDN on the secondary management center. You can't set value this using CDO; you need to set it in the secondary management center. See .

Step 6 In **Connection**, enter the device's serial number and device name. Click **Next**.

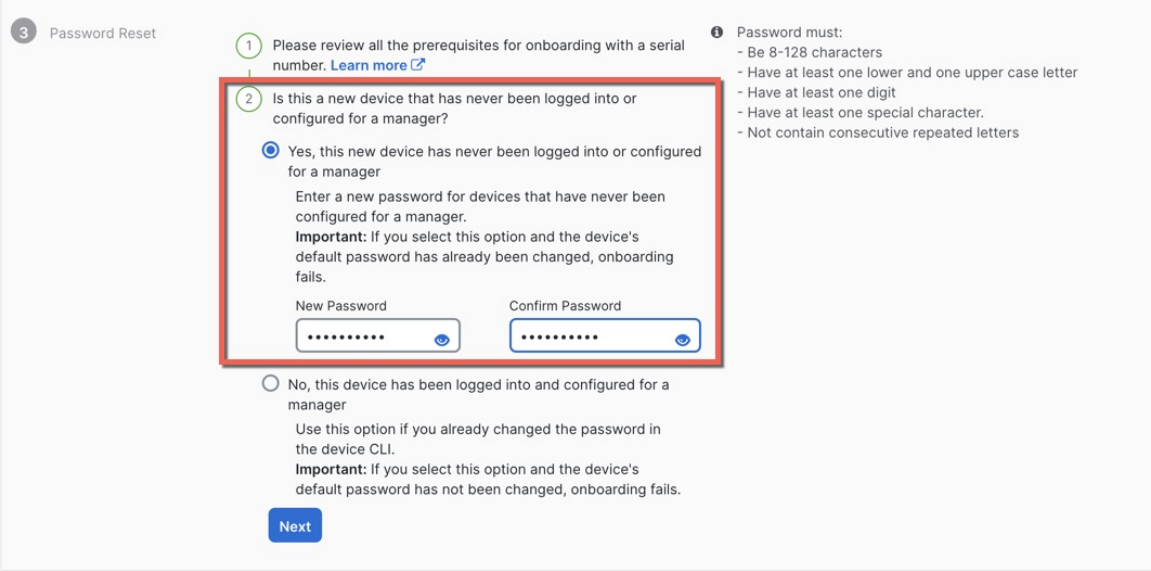
Figure 46: Connection

Step 7 In **Password Reset**, click **Yes...**. Enter a new password and confirm the new password for the device, then click **Next**.

For low-touch provisioning, the device must be brand new or has been reimaged.

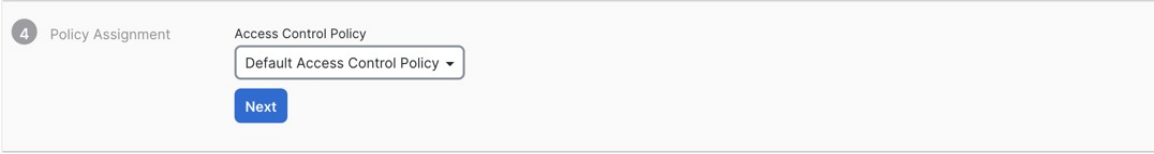
Note If you did log into the device and reset the password, and you did not change the configuration in a way that would disable low-touch provisioning, then you should choose the **No...** option. There are a number of configurations that disable low-touch provisioning, so we don't recommend logging into the device unless you need to, for example, to perform a reimage.

Figure 47: Password Reset



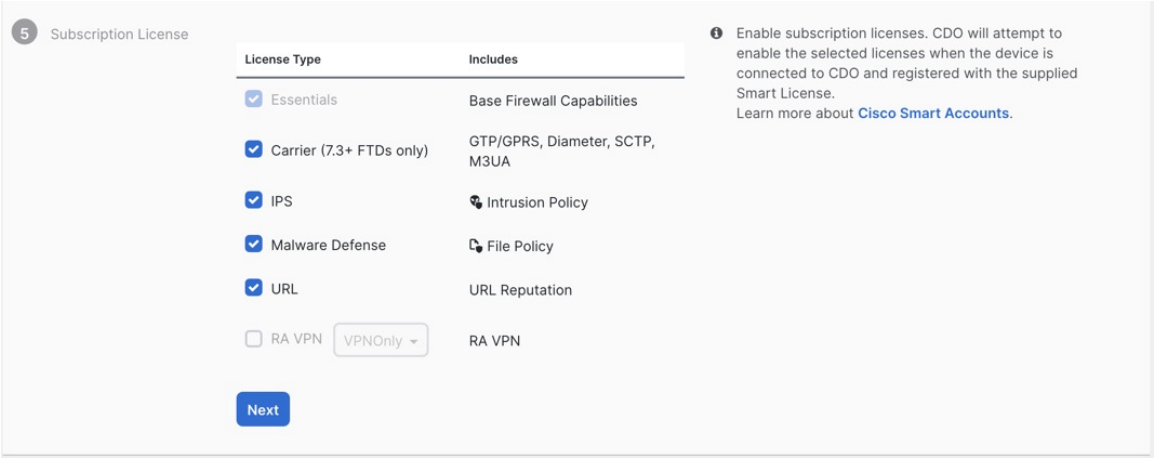
Step 8 In **Policy Assignment**, use the drop-down menu to select an access control policy for the device. If you have not added a policy on the management center, you should go to the management center and add one now. Click **Next**.

Figure 48: Policy Assignment



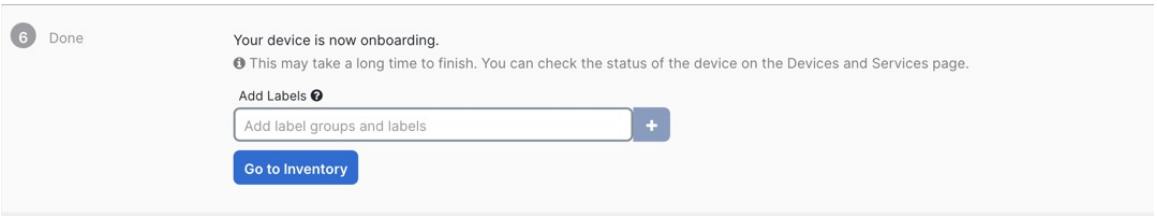
Step 9 In **Subscription License**, select the licenses for the device. Click **Next**.

Figure 49: Subscription License



Step 10 In **Done**, you can add labels to the device that show in CDO; they are not used on the management center.

Figure 50: Done



In the management center, the device is added to the **Device Management** page. You can also click **Go to Inventory** to see the devices in CDO. On-prem management center devices are viewable in CDO inventory for information purposes.

When using low-touch provisioning on the outside interface, CDO acts as a DDNS provider and does the following:

- Enables DDNS on outside using the "fmcOnly" method. This method is only supported for low-touch provisioning devices.
- Maps the outside IP address with the following hostname: *serial-number*.**local**.
- Provides the IP address/hostname mapping to the management center so it can resolve the hostname to the correct IP address.
- Informs the management center if the IP address ever changes, for example, if the DHCP lease renews.

If you use low-touch provisioning on the Management interface, DDNS is not supported. The management center must be publicly reachable so the device and initiate the management connection.

You can continue to use CDO as the DDNS provider, or you can later change the DDNS configuration in the management center to a different method.

Add a Device to the Management Center Manually

Register the threat defense to the management center.

Before you begin

- Gather the following information that you set in the threat defense initial configuration:
  - The threat defense management IP address or hostname, and NAT ID
  - The management center registration key

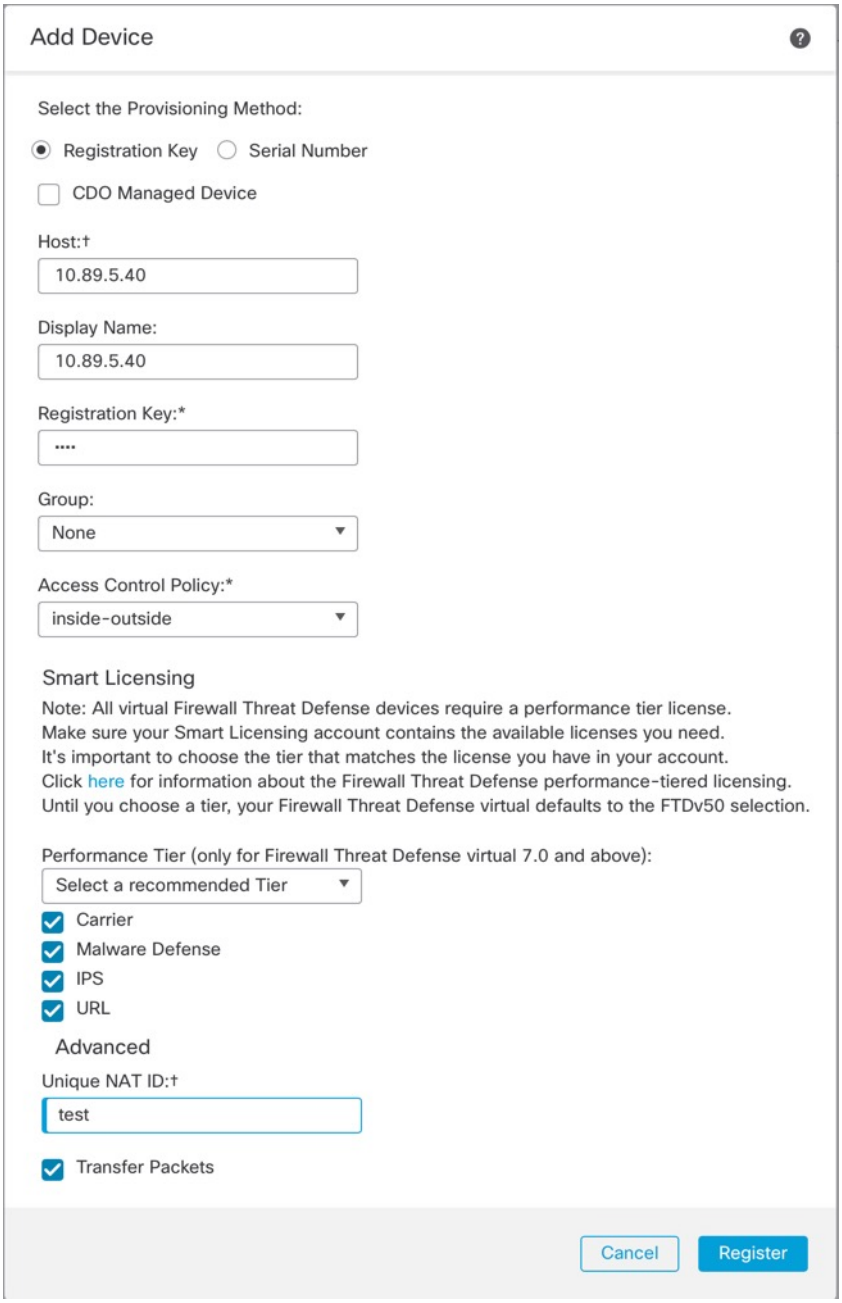
Procedure

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

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

The **Registration Key** method is selected by default.

Figure 51: Add Device Using a Registration Key



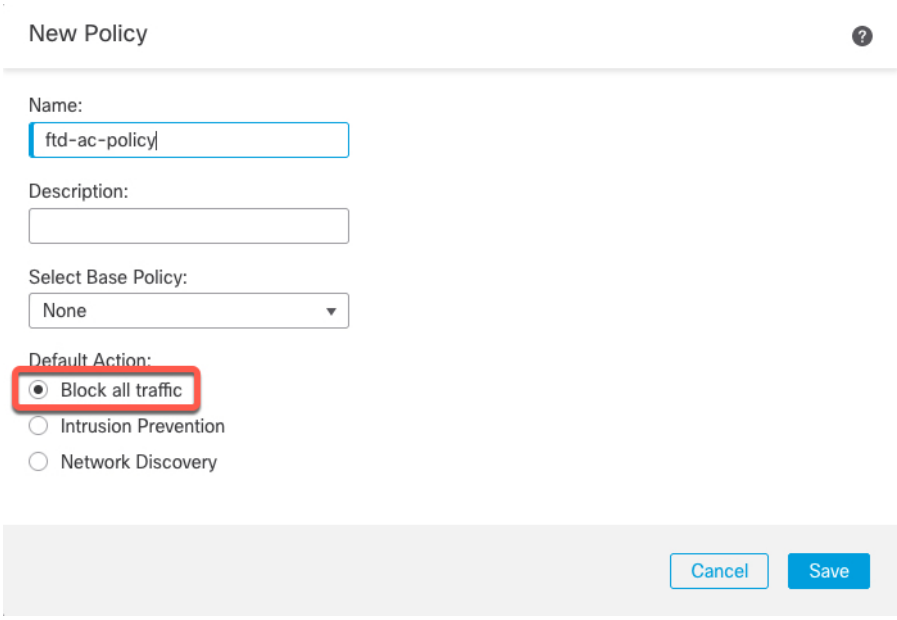
Set the following parameters:

- **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 40.

Figure 52: New Policy



- **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 management-data-interface** command.

- Registration key, NAT ID, and 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. You configured basic settings for the outside interface as part of the manager access setup, but you still need to assign it to a security zone.
- DHCP server—Use a DHCP server on the inside interface for clients.
- NAT—Use interface PAT on the outside interface.
- Access control—Allow traffic from inside to outside.
- SSH—Enable SSH on the manager access interface.

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.

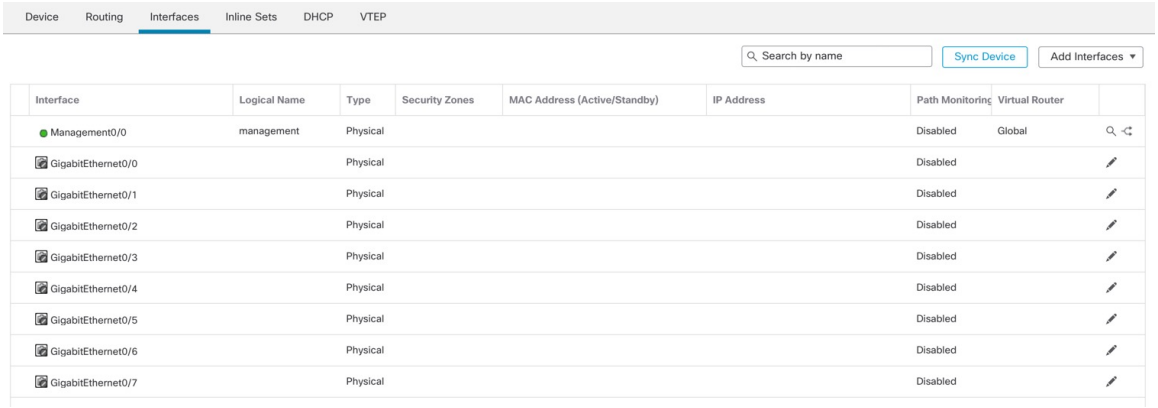
The following example configures a routed mode inside interface with a static address and a routed mode outside interface using DHCP.

Procedure

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

Step 2 Click **Interfaces**.

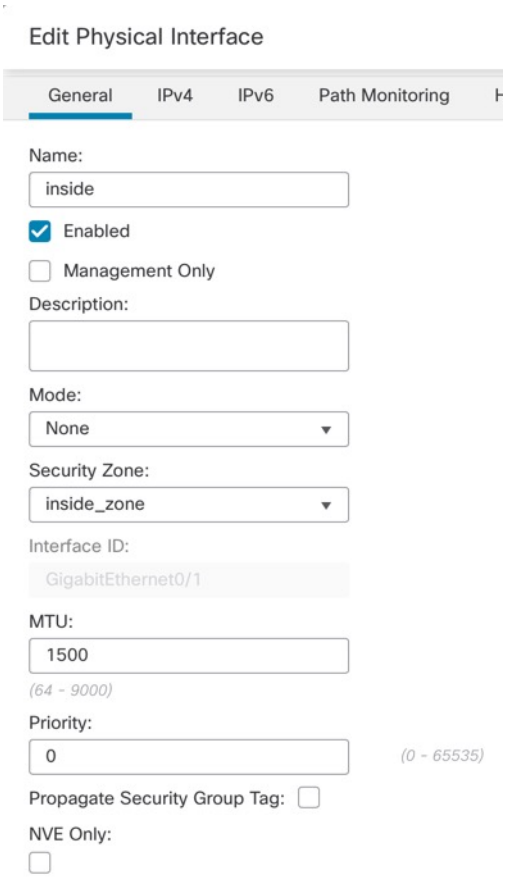
Figure 53: Interfaces



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

The **General** tab appears.

Figure 54: 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**.

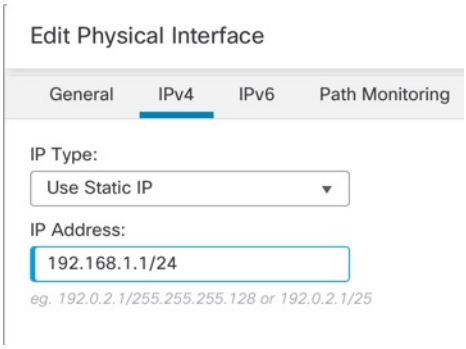
For example, add a zone called **inside_zone**. Each interface must be assigned to a security zone and/or interface group. An interface can belong to only one security zone, but can also belong to multiple interface groups. You apply your security policy based on zones or groups. For example, you can 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.

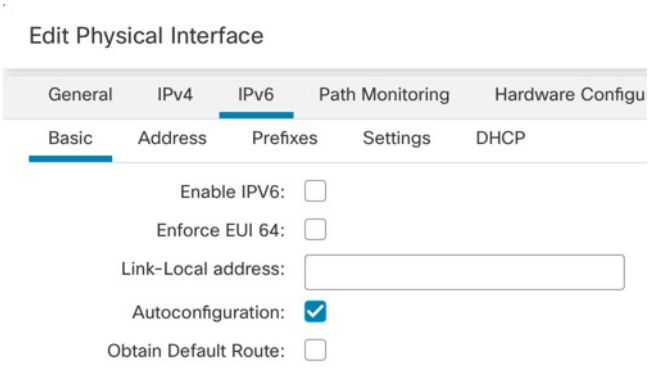
  For example, enter **192.168.1.1/24**

  Figure 55: IPv4 Tab



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

  Figure 56: IPv6 Tab

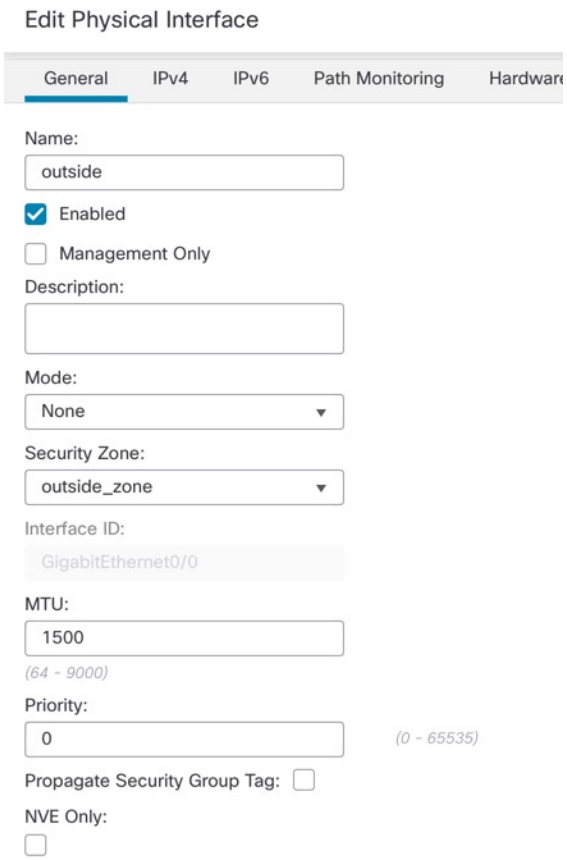


f) Click **OK**.

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

The **General** tab appears.

Figure 57: General Tab



You already pre-configured this interface for manager access, so 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 must still configure the Security Zone on this screen for through traffic policies.

a) 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**.

b) Click **OK**.

Step 5 Click **Save**.

Configure the DHCP Server

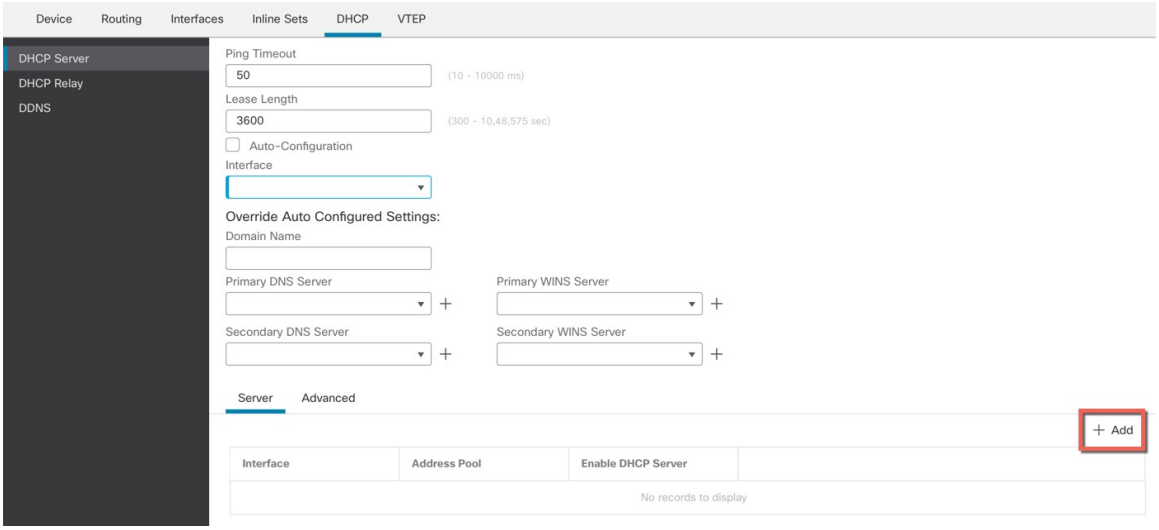
Enable the DHCP server if you want clients to use DHCP to obtain IP addresses from the threat defense.

Procedure

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

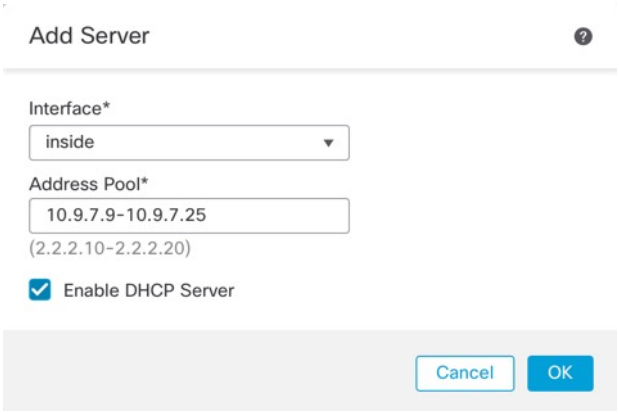
Step 2 Choose **DHCP** > **DHCP Server**.

Figure 58: DHCP Server



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

Figure 59: 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**.

Configure NAT

Configure NAT

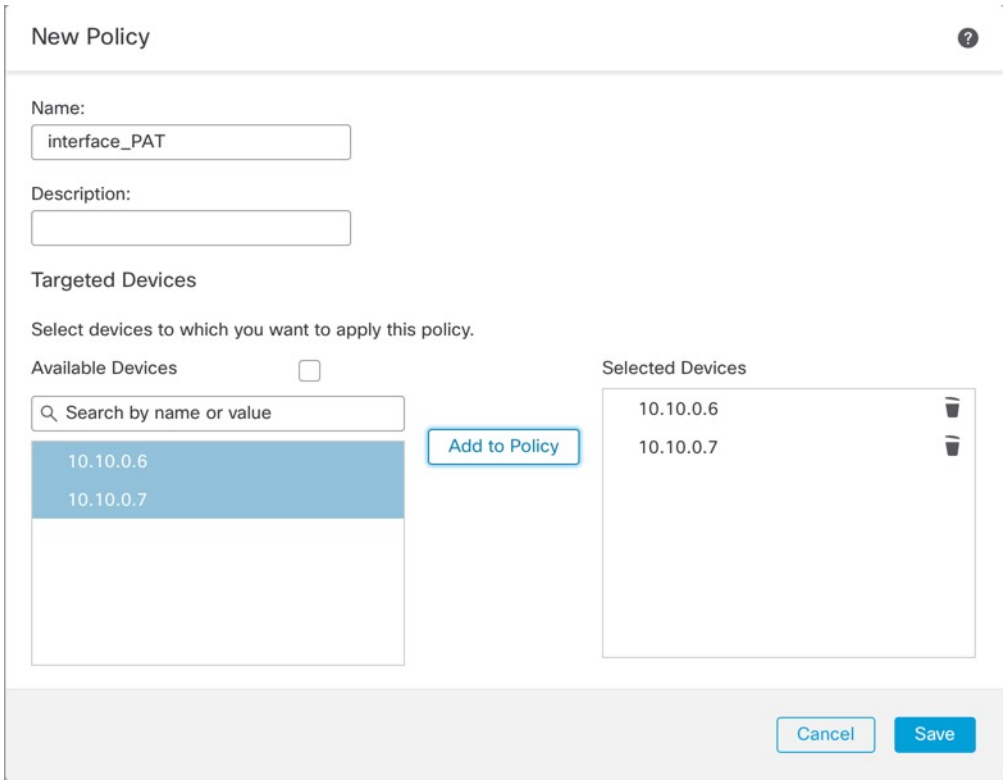
A typical NAT rule converts internal addresses to a port on the outside interface IP address. This type of NAT rule is called *interface Port Address Translation (PAT)*.

Procedure

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

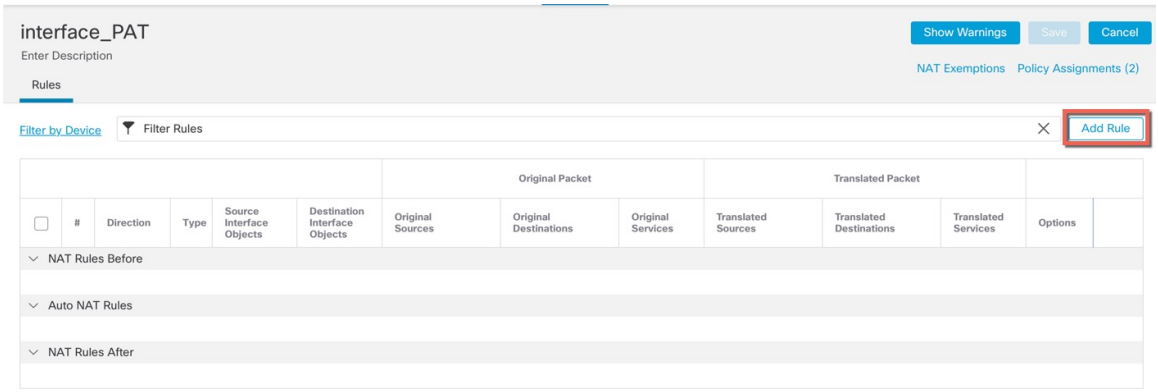
Step 2 Name the policy, select the device(s) that you want to use the policy, and click **Save**.

Figure 60: New Policy



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

Figure 61: NAT Policy

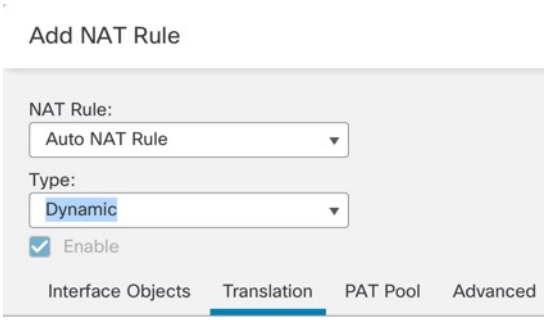


Step 3 Click **Add Rule**.

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

Step 4 Configure the basic rule options:

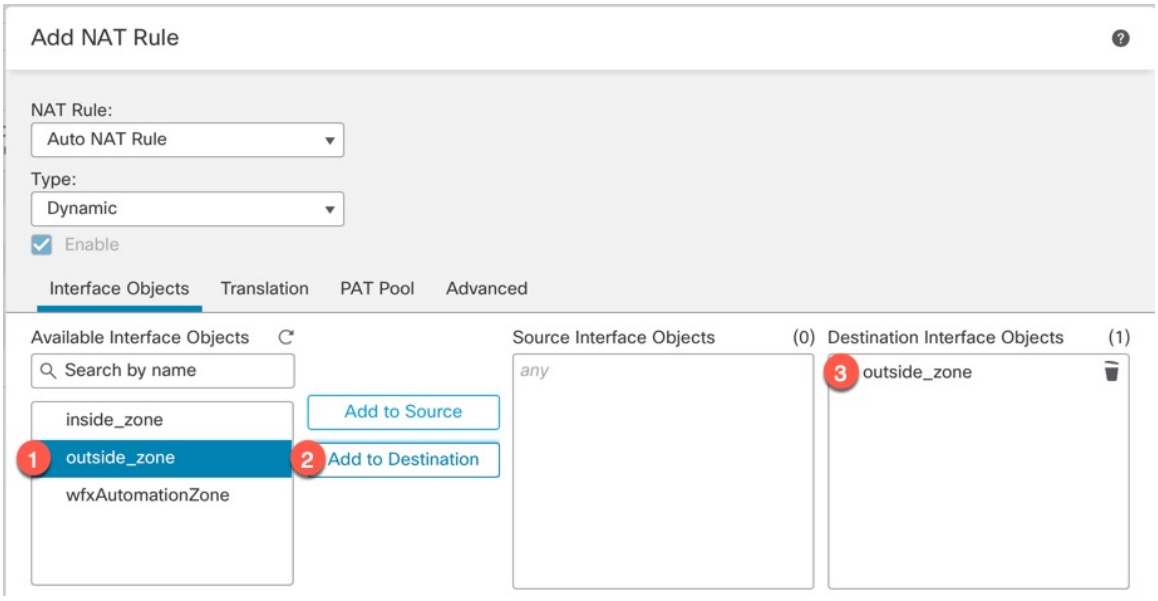
Figure 62: Basic Rule Options



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

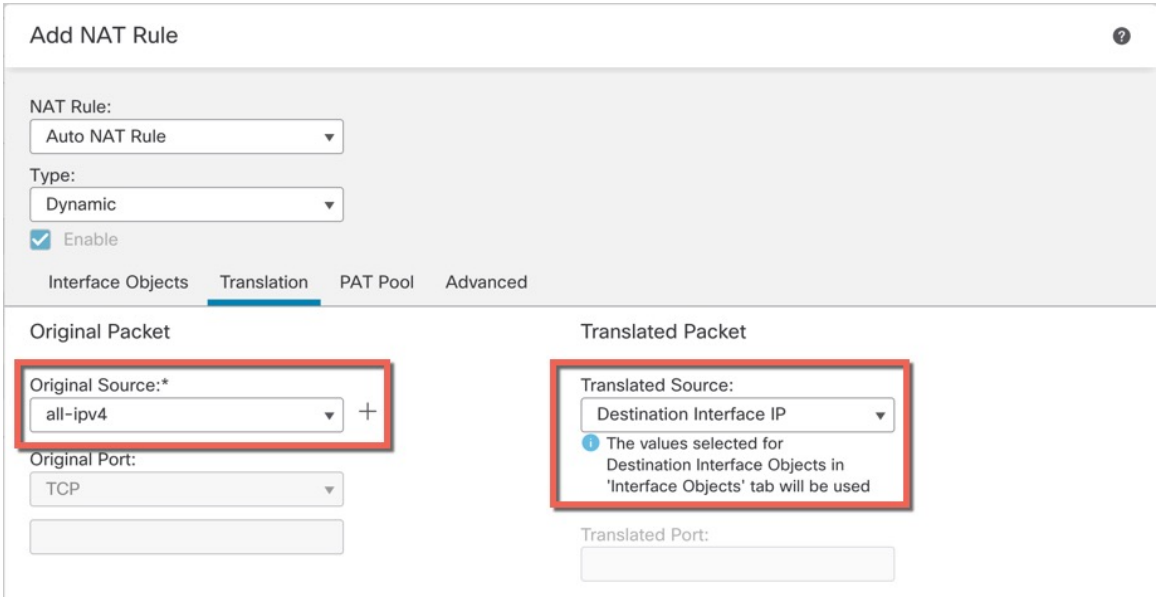
Step 5 On the **Interface Objects** page, add the outside zone from the **Available Interface Objects** area to the **Destination Interface Objects** area.

Figure 63: Interface Objects



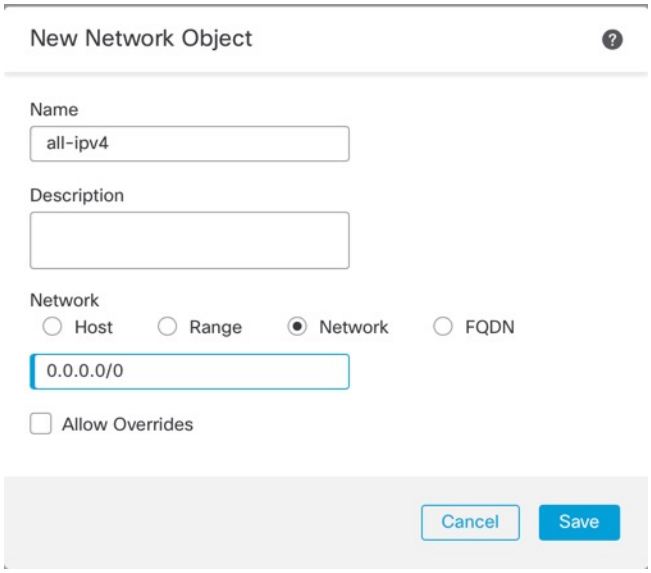
Step 6 On the **Translation** page, configure the following options:

Figure 64: Translation



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

Figure 65: New Network Object



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

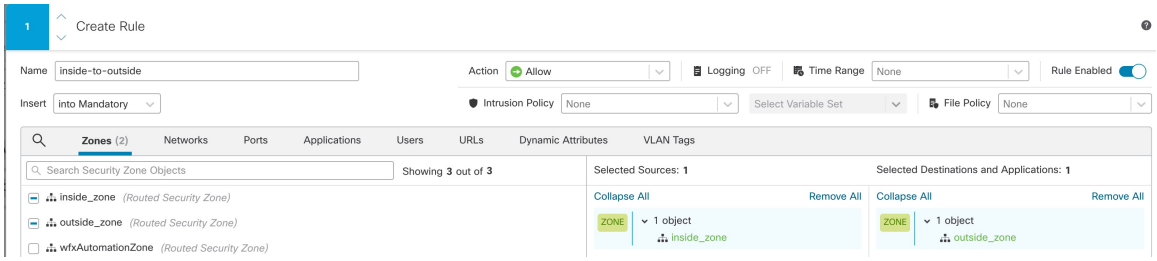
If you created a basic **Block all traffic** access control policy when you registered the threat defense, then you need to add rules to the policy to allow traffic through the device. The following procedure adds a rule to allow traffic from the inside zone to the outside zone. If you have other zones,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

Procedure

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

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

Figure 66: Add Rule



- **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**.

Configure SSH on the Manager Access Data Interface

If you enabled management center access on a data interface, such as outside, you should enable SSH on that interface using this procedure. This section describes how to enable SSH connections to one or more *data* interfaces on the threat defense.

Note SSH is enabled by default on the Management interface; however, this screen does not affect Management SSH access.

The Management interface is separate from the other interfaces on the device. It is used to set up and register the device to the management center. SSH for data interfaces shares the internal and external user list with SSH for the Management interface. Other settings are configured separately: for data interfaces, enable SSH and access lists using this screen; SSH traffic for data interfaces uses the regular routing configuration, and not any static routes configured at setup or at the CLI.

For the Management interface, to configure an SSH access list, see the **configure ssh-access-list** command in the Cisco Secure Firewall Threat Defense Command Reference. To configure a static route, see the **configure network static-routes** command. By default, you configure the default route through the Management interface at initial setup.

To use SSH, you do not also need an access rule allowing the host IP address. You only need to configure SSH access according to this section.

You can only SSH to a reachable interface; if your SSH host is located on the outside interface, you can only initiate a management connection directly to the outside interface.

Note After you make three consecutive failed attempts to log into the CLI using SSH, the device terminates the SSH connection.

Threat Defense Feature History

- 7.4—Loopback interface support for SSH.

Before you begin

- You can configure SSH internal users at the CLI using the **configure user add** command. By default, there is an **admin** user for which you configured the password during initial setup. You can also configure external users on LDAP or RADIUS by configuring **External Authentication** in platform settings.
- You need network objects that define the hosts or networks you will allow to make SSH connections to the device. You can add objects as part of the procedure, but if you want to use object groups to identify a group of IP addresses, ensure that the groups needed in the rules already exist. Select **Objects** > **Object Management** to configure objects.

Note You cannot use the system-provided **any** network object. Instead, use **any-ipv4** or **any-ipv6**.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the threat defense policy.

Step 2 Select **SSH Access**.

Step 3 Identify the interfaces and IP addresses that allow SSH connections.

Use this table to limit which interfaces will accept SSH connections, and the IP addresses of the clients who are allowed to make those connections. You can use network addresses rather than individual IP addresses.

a) Click **Add** to add a new rule, or click **Edit** to edit an existing rule.
b) Configure the rule properties:
   - **IP Address**—The network object or group that identifies the hosts or networks you are allowing to make SSH connections. Choose an object from the drop-down menu, or click + to add a new network object.
   - **Available Zones/Interfaces**—Add the zones that contain the interfaces to which you will allow SSH connections. For interfaces not in a zone, you can type the interface name into the field below the **Selected Zones/Interfaces** list and click **Add**. You can also add loopback interfaces. These rules will be applied to a device only if the device includes the selected interfaces or zones.
c) Click **OK**.

Step 4 Click **Save**.

You can now go to **Deploy** > **Deployment** and deploy the policy to assigned devices. The changes are not active until you deploy them.

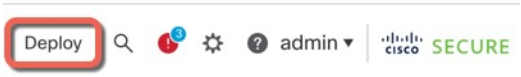
Deploy the Configuration

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 67: Deploy



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

Figure 68: Deploy All

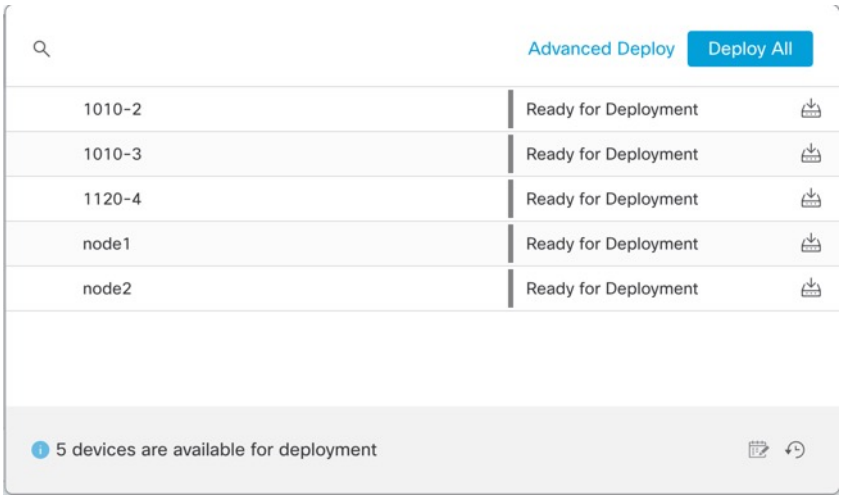
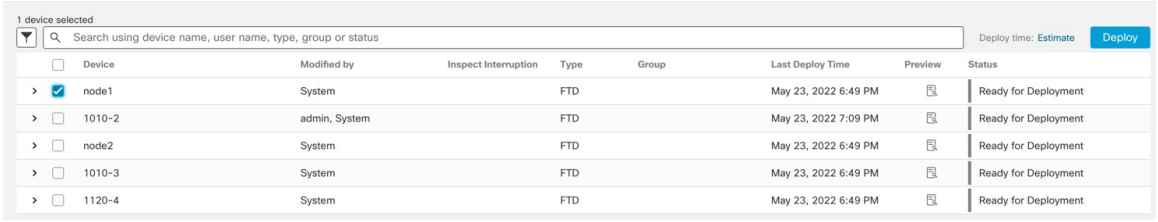
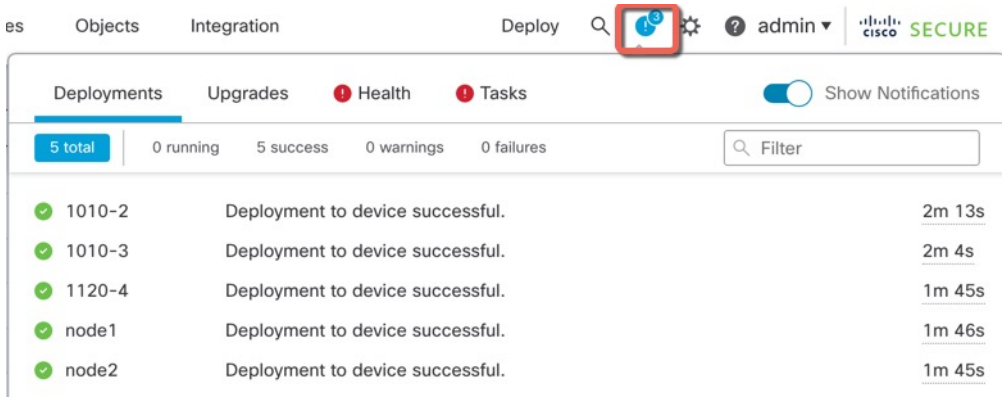


Figure 69: Advanced Deploy



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 70: 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 Firepower 2100 ships with a DB-9 to RJ-45 serial cable, so you may need 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#
```

Troubleshoot Management Connectivity on a Data Interface

Model Support—Threat Defense

When you use a data interface for the management center instead of using the dedicated Management interface, you must be careful about changing the interface and network settings for the threat defense in the management center so you do not disrupt the connection. If you change the management interface type after you add the threat defense to the management center (from data to Management, or from Management to data), if the interfaces and network settings are not configured correctly, you can lose management connectivity.

This topic helps you troubleshoot the loss of management connectivity.

View management connection status

In the management center, check the management connection status on the **Devices** > **Device Management** > **Device** > **Management** > **FMC Access Details** > **Connection Status** page.

At the threat defense CLI, enter the **sftunnel-status-brief** command to view the management connection status. You can also use **sftunnel-status** to view more complete information.

See the following sample output for a connection that is down; there is no peer channel "connected to" information, nor heartbeat information shown:

```
> sftunnel-status-brief
```

```
PEER:10.10.17.202
Registration: Completed.
Connection to peer '10.10.17.202' Attempted at Mon Jun 15 09:21:57 2020 UTC
Last disconnect time : Mon Jun 15 09:19:09 2020 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

See the following sample output for a connection that is up, with peer channel and heartbeat information shown:

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
 via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202'
 via '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

View the Threat Defense network information

At the threat defense CLI, view the Management and the management center access data interface network settings:

show network

```
> show network
===============[ System Information ]===============
Hostname                  : 5516X-4
DNS Servers               : 208.67.220.220,208.67.222.222
Management port           : 8305
IPv4 Default route
  Gateway                 : data-interfaces
IPv6 Default route
  Gateway                 : data-interfaces

=====================[ br1 ]======================
State                     : Enabled
Link                      : Up
Channels                  : Management & Events
Mode                      : Non-Autonegotiation
MDI/MDIX                  : Auto/MDIX
MTU                       : 1500
MAC Address               : 28:6F:7F:D3:CB:8D
---------------------[ IPv4 ]---------------------
Configuration             : Manual
Address                   : 10.99.10.4
Netmask                   : 255.255.255.0
Gateway                   : 10.99.10.1
---------------------[ IPv6 ]---------------------
Configuration             : Disabled

===============[ Proxy Information ]================
State                     : Disabled
Authentication            : Disabled

======[ System Information - Data Interfaces ]======
DNS Servers               :
Interfaces                : GigabitEthernet1/1
```

```
===============[ GigabitEthernet1/1 ]===============
State                        : Enabled
Link                         : Up
Name                         : outside
MTU                          : 1500
MAC Address                  : 28:6F:7F:D3:CB:8F
----------------------[ IPv4 ]----------------------
Configuration                : Manual
Address                      : 10.89.5.29
Netmask                      : 255.255.255.192
Gateway                      : 10.89.5.1
----------------------[ IPv6 ]----------------------
Configuration                : Disabled
```

Check that the Threat Defense registered with the Management Center

At the threat defense CLI, check that the management center registration was completed. Note that this command will not show the *current* status of the management connection.

show managers

```
> show managers
Type                         : Manager
Host                         : 10.89.5.35
Registration                 : Completed

>
```

Ping the Management Center

At the threat defense CLI, use the following command to ping the management center from the data interfaces:

ping *fmc_ip*

At the threat defense CLI, use the following command to ping the management center from the Management interface, which should route over the backplane to the data interfaces:

ping system *fmc_ip*

Capture packets on the Threat Defense internal interface

At the threat defense CLI, capture packets on the internal backplane interface (nlp_int_tap) to see if management packets are being sent:

capture *name* **interface nlp_int_tap trace detail match ip any any**

show capture*name* **trace detail**

Check the internal interface status, statistics, and packet count

At the threat defense CLI, see information about the internal backplane interface, nlp_int_tap:

show interace detail

```
> show interface detail
[...]
Interface Internal-Data0/1 "nlp_int_tap", is up, line protocol is up
  Hardware is en_vtun rev00, BW Unknown Speed-Capability, DLY 1000 usec
 (Full-duplex), (1000 Mbps)
 Input flow control is unsupported, output flow control is unsupported
```

```
MAC address 0000.0100.0001, MTU 1500
IP address 169.254.1.1, subnet mask 255.255.255.248
37 packets input, 2822 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 pause input, 0 resume input
0 L2 decode drops
5 packets output, 370 bytes, 0 underruns
0 pause output, 0 resume output
0 output errors, 0 collisions, 0 interface resets
0 late collisions, 0 deferred
0 input reset drops, 0 output reset drops
input queue (blocks free curr/low): hardware (0/0)
output queue (blocks free curr/low): hardware (0/0)
 Traffic Statistics for "nlp_int_tap":
37 packets input, 2304 bytes
5 packets output, 300 bytes
37 packets dropped
     1 minute input rate 0 pkts/sec,  0 bytes/sec
     1 minute output rate 0 pkts/sec,  0 bytes/sec
     1 minute drop rate, 0 pkts/sec
     5 minute input rate 0 pkts/sec,  0 bytes/sec
     5 minute output rate 0 pkts/sec,  0 bytes/sec
     5 minute drop rate, 0 pkts/sec
 Control Point Interface States:
Interface number is 14
Interface config status is active
Interface state is active
```

Check routing and NAT

At the threat defense CLI, check that the default route (S*) was added and that internal NAT rules exist for the Management interface (nlp_int_tap).

show route

```
> show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF
Gateway of last resort is 10.89.5.1 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 10.89.5.1, outside
C        10.89.5.0 255.255.255.192 is directly connected, outside
L        10.89.5.29 255.255.255.255 is directly connected, outside

>
```

show nat

```
> show nat

Auto NAT Policies (Section 2)
1 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_intf3 interface  service
```

```
 tcp 8305 8305
    translate_hits = 0, untranslate_hits = 6
2 (nlp_int_tap) to (outside) source static nlp_server_0_ssh_intf3 interface  service
tcp ssh ssh
    translate_hits = 0, untranslate_hits = 73
3 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_ipv6_intf3 interface
ipv6  service tcp 8305 8305
    translate_hits = 0, untranslate_hits = 0
4 (nlp_int_tap) to (outside) source dynamic nlp_client_0_intf3 interface
    translate_hits = 174, untranslate_hits = 0
5 (nlp_int_tap) to (outside) source dynamic nlp_client_0_ipv6_intf3 interface ipv6
    translate_hits = 0, untranslate_hits = 0
>
```

Check other settings

See the following commands to check that all other settings are present. You can also see many of these commands on the management center's **Devices** > **Device Management** > **Device** > **Management** > **FMC Access Details** > **CLI Output** page.

show running-config sftunnel

```
> show running-config sftunnel
sftunnel interface outside
sftunnel port 8305
```

show running-config ip-client

```
> show running-config ip-client
ip-client outside
```

show conn address *fmc_ip*

```
> show conn address 10.89.5.35
5 in use, 16 most used
Inspect Snort:
        preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect

TCP nlp_int_tap  10.89.5.29(169.254.1.2):51231 outside  10.89.5.35:8305, idle 0:00:04,
 bytes 86684, flags UxIO
TCP nlp_int_tap  10.89.5.29(169.254.1.2):8305 outside  10.89.5.35:52019, idle 0:00:02,
 bytes 1630834, flags UIO
>
```

Check for a successful DDNS update

At the threat defense CLI, check for a successful DDNS update:

debug ddns

```
> debug ddns
DDNS update request = /v3/update?hostname=domain.example.org&myip=209.165.200.225
Successfuly updated the DDNS sever with current IP addresses
DDNS: Another update completed, outstanding = 0
DDNS: IDB SB total = 0
```

If the update failed, use the **debug http** and **debug ssl** commands. For certificate validation failures, check that the root certificates are installed on the device:

show crypto ca certificates *trustpoint_name*

To check the DDNS operation:

show ddns update interface *fmc_access_ifc_name*

```
> show ddns update interface outside

Dynamic DNS Update on outside:
    Update Method Name Update Destination
    RBD_DDNS not available

Last Update attempted on 04:11:58.083 UTC Thu Jun 11 2020
Status : Success
FQDN : domain.example.org
IP addresses : 209.165.200.225
```

Check Management Center log files

See https://cisco.com/go/fmc-reg-error.

Roll Back the Configuration if the Management Center Loses Connectivity

If you use a data interface on the threat defense for the management center, and you deploy a configuration change from the management center that affects the network connectivity, you can roll back the configuration on the threat defense to the last-deployed configuration so you can restore management connectivity. You can then adjust the configuration settings in the management center so that the network connectivity is maintained, and re-deploy. You can use the rollback feature even if you do not lose connectivity; it is not limited to this troubleshooting situation.

See the following guidelines:

- Only the previous deployment is available locally on the threat defense; you cannot roll back to any earlier deployments.
- Rollback is not supported for High Availability or Clustering deployments.
- The rollback only affects configurations that you can set in the management center. For example, the rollback does not affect any local configuration related to the dedicated Management interface, which you can only configure at the threat defense CLI. Note that if you changed data interface settings after the last management center deployment using the **configure network management-data-interface** command, and then you use the rollback command, those settings will not be preserved; they will roll back to the last-deployed management center settings.
- UCAPL/CC mode cannot be rolled back.
- Out-of-band SCEP certificate data that was updated during the previous deployment cannot be rolled back.
- During the rollback, connections will drop because the current configuration will be cleared.

Before you begin

Model Support—Threat Defense

Procedure

Step 1 At the threat defense CLI, roll back to the previous configuration.

configure policy rollback

After the rollback, the threat defense notifies the management center that the rollback was completed successfully. In the management center, the deployment screen will show a banner stating that the configuration was rolled back.

If the rollback failed, refer to https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw-virtual/215258-troubleshooting-firepower-threat-defense.html for common deployment problems. In some cases, the rollback can fail after the management center access is restored; in this case, you can resolve the management center configuration issues, and redeploy from the management center.

Example:

```
> configure policy rollback

The last deployment to this FTD was on June 1, 2020 and its status was Successful.
Do you want to continue [Y/N]?

Y

Rolling back complete configuration on the FTD. This will take time.
.....................
Policy rollback was successful on the FTD.
Configuration has been reverted back to transaction id:
Following is the rollback summary:
...................
.....................
>
```

Step 2 Check that the management connection was reestablished.

In the management center, check the management connection status on the **Devices** > **Device Management** > **Device** > **Management** > **FMC Access Details** > **Connection Status** page.

At the threat defense CLI, enter the **sftunnel-status-brief** command to view the management connection status.

If it takes more than 10 minutes to reestablish the connection, you should troubleshoot the connection. See Troubleshoot Management Connectivity on a Data Interface, on page 95.

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 Device 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 94.

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:

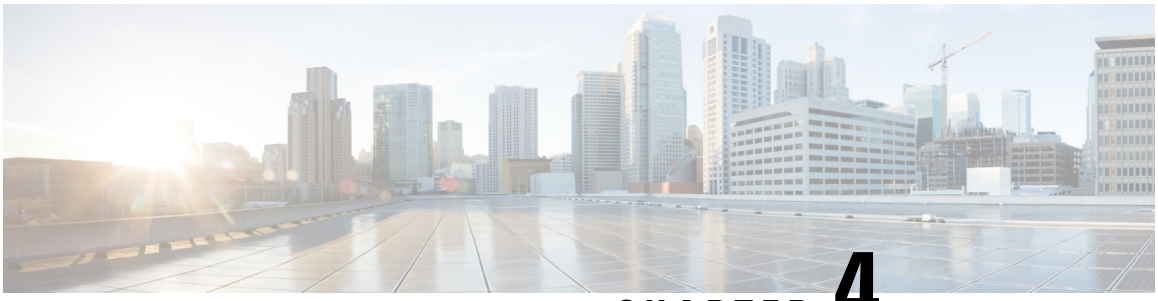
```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

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 Firepower Documentation.

For information related to using the management center, see the Firepower Management Center Configuration Guide.



CHAPTER 4

Threat Defense Deployment with the Device Manager

Is This Chapter for You?

To see all available applications and managers, see Which Application and Manager is Right for You?, on page 1. This chapter applies to the threat defense with the device manager.

This chapter explains how to complete the initial set up and configuration of your threat defense using the web-based device setup wizard.

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

About the Firewall

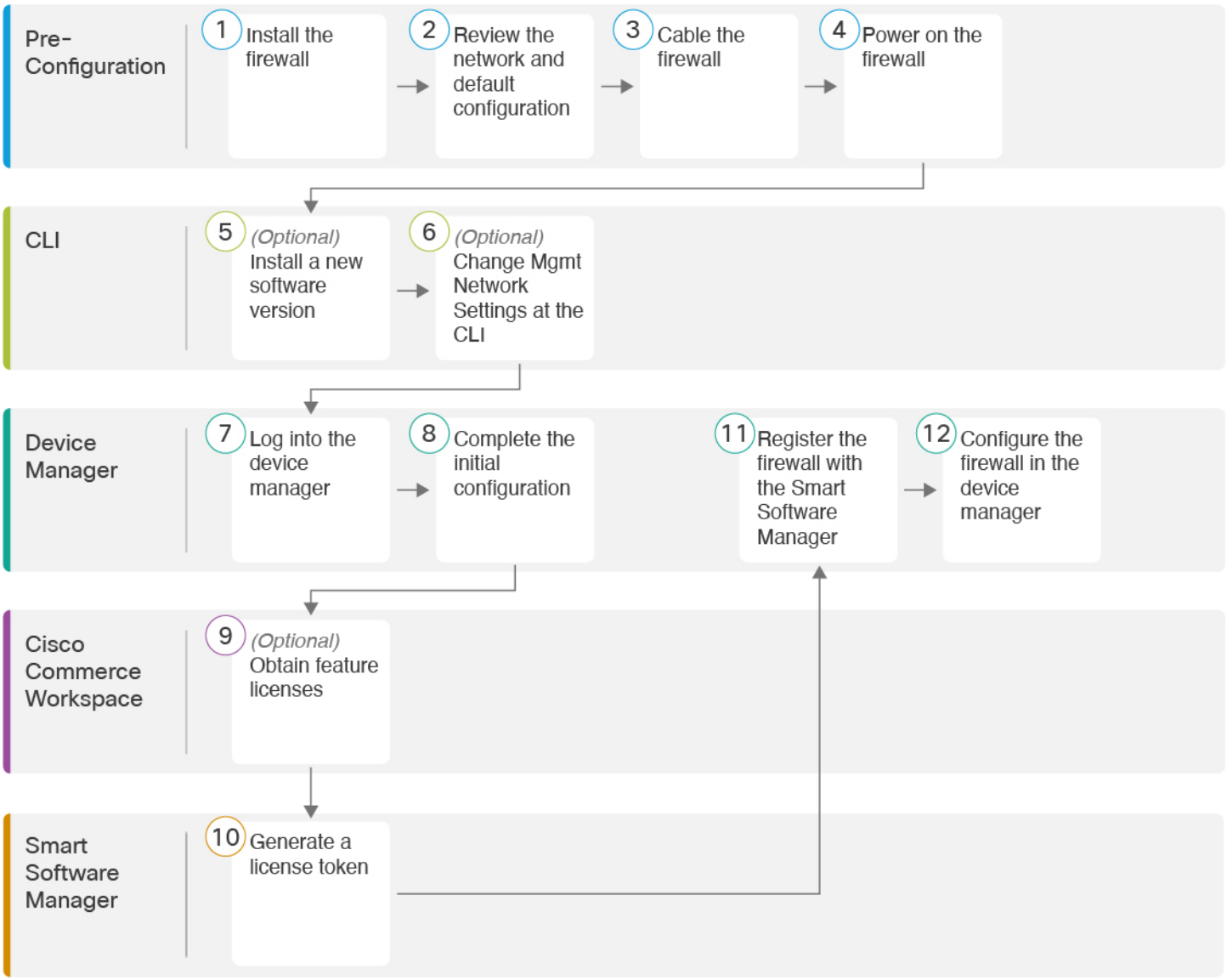
The hardware can run either threat defense software or ASA software. Switching between threat defense and ASA requires you to reimage the device. You should also reimage if you need a different software version than is currently installed. See Cisco Secure Firewall ASA and Secure Firewall Threat Defense 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.

End-to-End Tasks

See the following tasks to deploy the threat defense with the device manager.



1	Pre-Configuration	Install the firewall. See the hardware installation guide.

2	Pre-Configuration	Review the Network Deployment and Default Configuration, on page 107
3	Pre-Configuration	Cable the Device, on page 110.
4	Pre-Configuration	Power on the Device, on page 111.
5	CLI	(Optional) Check the Software and Install a New Version, on page 112
6	CLI	(Optional) Change Management Network Settings at the CLI, on page 113.
7	Device Manager	Log Into the Device Manager, on page 115.
8	Device Manager	Complete the Initial Configuration, on page 116.
9	Cisco Commerce Workspace	(Optional) Obtain feature licenses (Configure Licensing, on page 118).
10	Smart Software Manager	Generate a license token (Configure Licensing, on page 118).
11	Device Manager	Register the device with the Smart Licensing Server (Configure Licensing, on page 118).
12	Device Manager	Configure the Firewall in the Device Manager, on page 124.

Review the Network Deployment and Default Configuration

You can manage the threat defense using the device manager from either the Management 1/1 interface or the inside interface. The dedicated Management interface is a special interface with its own network settings.

The following figure shows the recommended network deployment. If you connect the outside interface directly to a cable modem or DSL modem, we recommend that you put the modem into bridge mode so the threat defense performs all routing and NAT for your inside networks. If you need to configure PPPoE for the outside interface to connect to your ISP, you can do so after you complete initial setup in device manager.

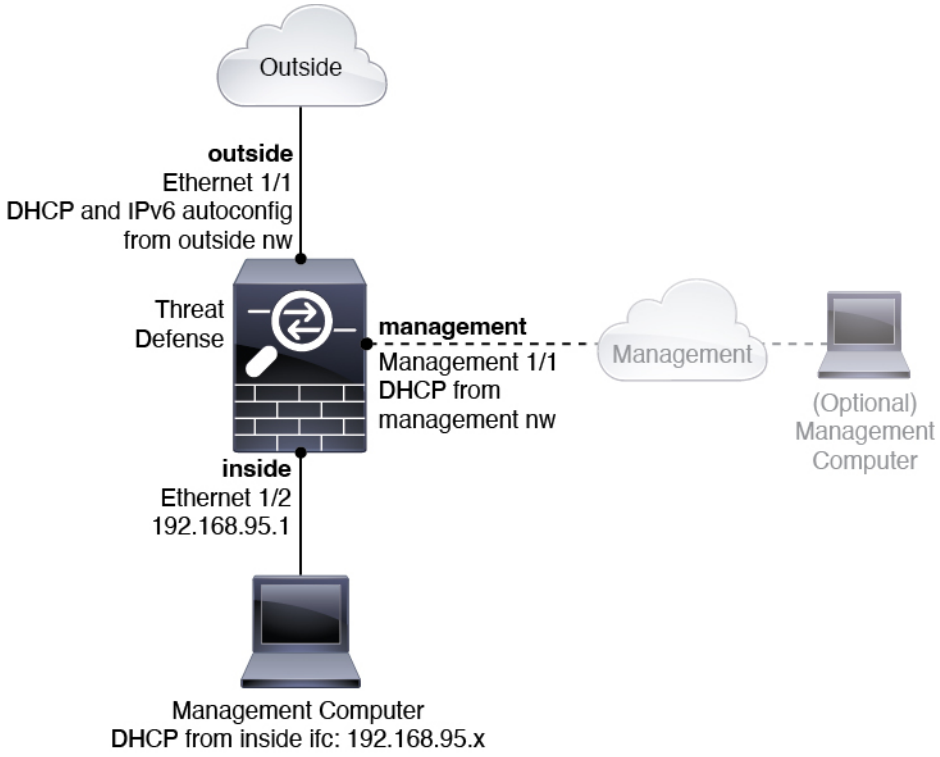
Note If you cannot use the default management IP address (for example, your management network does not include a DHCP server), then you can connect to the console port and perform initial setup at the CLI, including setting the Management IP address, gateway, and other basic networking settings.

If you need to change the inside IP address, you can do so after you complete initial setup in the device manager. For example, you may need to change the inside IP address in the following circumstances:

- (7.0 and later) The inside IP address is 192.168.95.1. (6.7 and earlier) The inside IP address is 192.168.1.1. If the outside interface tries to obtain an IP address on the 192.168.1.0 network, which is a common default network, the DHCP lease will fail, and the outside interface will not obtain an IP address. This problem occurs because the threat defense cannot have two interfaces on the same network. In this case you must change the inside IP address to be on a new network.
- If you add the threat defense to an existing inside network, you will need to change the inside IP address to be on the existing network.

The following figure shows the default network deployment for the threat defense using the device manager with the default configuration.

Figure 71: Suggested Network Deployment



Note For 6.7 and earlier, the Ethernet 1/2 inside IP address is 192.168.1.1.

For 6.5 and earlier, the Management 1/1 default IP address is 192.168.45.45.

Default Configuration

The configuration for the firewall after initial setup includes the following:

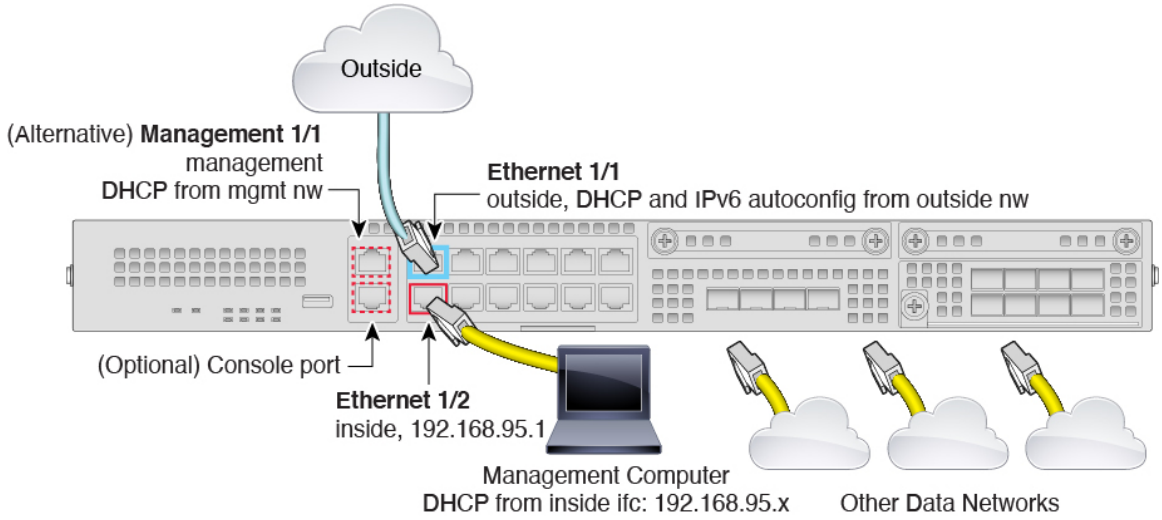
- **inside**—Ethernet 1/2, IP address (7.0 and later) 192.168.95.1; (pre-7.0) 192.168.1.1.
- **outside**—Ethernet 1/1, IP address from IPv4 DHCP and IPv6 autoconfiguration
- **inside→outside** traffic flow
- **management**—Management 1/1 (management)
  - (6.6 and later) IP address from DHCP
  - (6.5 and earlier) IP address 192.168.45.45

Note The Management 1/1 interface is a special interface separate from data interfaces that is used for management, Smart Licensing, and database updates. The physical interface is shared with a second logical interface, the Diagnostic interface. Diagnostic is a data interface, but is limited to other types of management traffic (to-the-device and from-the-device), such as syslog or SNMP. The Diagnostic interface is not typically used. See the Cisco Secure Firewall Device Manager Configuration Guide for more information.

- **DNS server for management**—OpenDNS: (IPv4) 208.67.222.222, 208.67.220.220; (IPv6) 2620:119:35::35, or servers you specify during setup. DNS servers obtained from DHCP are never used.
- **NTP**—Cisco NTP servers: 0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org, 2.sourcefire.pool.ntp.org, or servers you specify during setup
- **Default routes**
  - **Data interfaces**—Obtained from outside DHCP, or a gateway IP address you specify during setup
  - **Management interface**—(6.6 and later) Obtained from management DHCP. If you do not receive a gateway, then the default route is over the backplane and through the data interfaces. (6.5 and earlier) Over the backplane and through the data interfaces

    Note that the Management interface requires internet access for licensing and updates, either over the backplane or using a separate internet gateway. Note that only traffic originating on the Management interface can go over the backplane; otherwise, Management does not allow through traffic for traffic entering Management from the network.
- **DHCP server**—Enabled on the inside interface and (6.5 and earlier only) management interface
- **Device Manager access**—All hosts allowed on Management and the inside interface.
- **NAT**—Interface PAT for all traffic from inside to outside

Cable the Device



Note For 6.7 and earlier, the Ethernet 1/2 inside IP address is 192.168.1.1.

For 6.5 and earlier, the Management 1/1 default IP address is 192.168.45.45.

Manage the Firepower 2100 on either Management 1/1 or Ethernet 1/2. The default configuration also configures Ethernet1/1 as outside.

Procedure

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

Step 2 Connect your management computer to either of the following interfaces:

- Ethernet 1/2—Connect your management computer directly to Ethernet 1/2 for initial configuration, or connect Ethernet 1/2 to your inside network. Ethernet 1/2 has a default IP address (192.168.95.1) and also runs a DHCP server to provide IP addresses to clients (including the management computer), so make sure these settings do not conflict with any existing inside network settings (see Default Configuration, on page 109).
- Management 1/1 (labeled MGMT)—Connect Management 1/1 to your management network, and make sure your management computer is on—or has access to—the management network. Management 1/1 obtains an IP address from a DHCP server on your management network; if you use this interface, you must determine the IP address assigned to the threat defense so that you can connect to the IP address from your management computer.

  If you need to change the Management 1/1 IP address from the default to configure a static IP address, you must also cable your management computer to the console port. See (Optional) Change Management Network Settings at the CLI, on page 113.

You can later configure the device manager management access from other interfaces; see the FDM configuration guide.

Step 3 Connect the outside network to the Ethernet1/1 interface (labeled WAN).

By default, the IP address is obtained using IPv4 DHCP and IPv6 autoconfiguration, but you can set a static address during initial configuration.

Step 4 Connect other networks to the remaining interfaces.

Power on the Device

The power switch is located to the left of power supply module 1 on the rear of the chassis. It is a toggle switch that controls power to the system. If the power switch is in standby position, only the 3.3-V standby power is enabled from the power supply module and the 12-V main power is OFF. When the switch is in the ON position, the 12-V main power is turned on and the system boots.

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

Before you begin

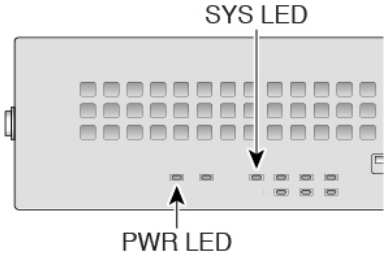
It's important that you provide reliable power for your device (for example, using an uninterruptable power supply (UPS)). Loss of power without first shutting down can cause serious file system damage. There are many processes running in the background all the time, and losing power does not allow the graceful shutdown of your system.

Procedure

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

Step 2 Press the power switch on the back of the device.

Step 3 Check the PWR LED on the front of the device; if it is solid green, the device is powered on.



Step 4 Check the SYS LED on the front of the device; after it is solid green, the system has passed power-on diagnostics.

Note Before you move the power switch to the OFF position, use the shutdown commands so that the system can perform a graceful shutdown. This may take several minutes to complete. After the graceful shutdown is complete, the console displays `It is safe to power off now`. The front panel blue locator beacon LED lights up indicating the system is ready to be powered off. You can now move the switch to the OFF position. The front panel PWR LED flashes momentarily and turns off. Do not remove the power until the PWR LED is completely off.

See the FXOS Configuration Guide for more information on using the shutdown commands.

(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 CLI. See Access the Threat Defense and FXOS CLI, on page 127 for more information. This procedure shows using the console port, but you can use SSH instead.

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               7.4.0.65        7.4.0.65
        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 (Optional) Change Management Network Settings at the CLI, on page 113. 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.

(Optional) Change Management Network Settings at the CLI

If you cannot use the default management IP address, then you can connect to the console port and perform initial setup at the CLI, including setting the Management IP address, gateway, and other basic networking settings. You can only configure the Management interface settings; you cannot configure inside or outside interfaces, which you can later configure in the GUI.

Note You cannot repeat the CLI setup script 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.

Procedure

Step 1 Connect to the threat defense console port. See Access the Threat Defense and FXOS CLI, on page 127 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 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 2 Connect to the threat defense CLI.

connect ftd

Example:

```
firepower# connect ftd
>
```

Step 3 The first time you log into the threat defense, you are prompted to accept the End User License Agreement (EULA). You are then presented with the CLI setup script.

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

See the following guidelines:

- **Enter the IPv4 default gateway for the management interface**—If you set a manual IP address, enter either **data-interfaces** or the IP address of the gateway router. The **data-interfaces** setting sends outbound management traffic over the backplane to exit a data interface. This setting is useful if you do not have a separate Management network that can access the internet. Traffic originating on the Management interface includes license registration and database updates that require internet access. If you use **data-interfaces**, you can still use the device manager (or SSH) on the Management interface if you are directly-connected to the Management network, but for remote management for specific networks or hosts, you should add a static route using the **configure network static-routes** command. Note that the device manager management on data interfaces is not affected by this setting. If you use DHCP, the

system uses the gateway provided by DHCP and uses the **data-interfaces** as a fallback method if DHCP doesn't provide a gateway.

- **If your networking information has changed, you will need to reconnect**—If you are connected with SSH to the default IP address 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 **yes** to use the device manager. A **no** answer means you intend to use the on-premises or cloud-delivered management center to manage the device.

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 configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [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]:
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: yes

>
```

Step 4 Log into the device manager on the new Management IP address.

Log Into the Device Manager

Log into the device manager to configure your threat defense.

Before you begin

- Use a current version of Firefox, Chrome, Safari, Edge, or Internet Explorer.

Procedure

Step 1 Enter the following URL in your browser.

- (7.0 and later) Inside (Ethernet 1/2)—**https://192.168.95.1**.

- (6.7 and earlier) Inside (Ethernet 1/2)—**https://192.168.1.1**.
- (6.6 and later) Management—**https://***management_ip*. The Management interface is a DHCP client, so the IP address depends on your DHCP server. If you changed the Management IP address at the CLI setup, then enter that address.
- (6.5 and earlier) Management—**https://192.168.45.45**. If you changed the Management IP address at the CLI setup, then enter that address.

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

What to do next

- Run through the device manager setup wizard; see Complete the Initial Configuration, on page 116.

Complete the Initial Configuration

Use the setup wizard when you first log into the device manager to complete the initial configuration. After you complete the setup wizard, you should have a functioning device with a few basic policies in place:

- An outside (Ethernet1/1) and an inside interface (Ethernet1/2).
- Security zones for the inside and outside interfaces.
- An access rule trusting all inside to outside traffic.
- An interface NAT rule that translates all inside to outside traffic to unique ports on the IP address of the outside interface.
- A DHCP server running on the inside interface.

Note If you performed the (Optional) Change Management Network Settings at the CLI, on page 113 procedure, then some of these tasks, specifically changing the admin password and configuring the outside and management interfaces, should have already been completed.

Procedure

Step 1 You are prompted to read and accept the End User License Agreement and change the admin password.

You must complete these steps to continue.

Step 2 Configure the following options for the outside and management interfaces and click **Next**.

Note Your settings are deployed to the device when you click **Next**. The interface will be named "outside" and it will be added to the "outside_zone" security zone. Ensure that your settings are correct.

a) **Outside Interface**—This is the data port that you connected to your gateway router. You cannot select an alternative outside interface during initial device setup. The first data interface is the default outside interface.

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.

b) **Management Interface**

DNS Servers—The DNS server for the system's management address. 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 system's management address.

Step 3 Configure the system time settings and click **Next**.

a) **Time Zone**—Select the time zone for the system.
b) **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.

Step 4 (Optional) Configure the smart licenses for the system.

Your purchase of the threat defense device automatically includes a Base license. All additional licenses are optional.

You must have a smart license account to obtain and apply the licenses that the system requires. Initially, you can use the 90-day evaluation license and set up smart licensing later.

To register the device now, click the link to log into your Smart Software Manager account, and see Configure Licensing, on page 118.

To use the evaluation license, select **Start 90 day evaluation period without registration**.

Step 5 Click **Finish**.

What to do next

- Although you can continue using the evaluation license, we recommend that you register and license your device; see Configure Licensing, on page 118.
- You can also choose to configure the device using the device manager; see Configure the Firewall in the Device Manager, on page 124.

Configure Licensing

The threat defense uses Smart Software Licensing, which lets you purchase and manage a pool of licenses centrally.

When you register the chassis, the Smart Software Manager issues an ID certificate for communication between the chassis and the Smart Software Manager. It also assigns the chassis to the appropriate virtual account.

For a more detailed overview on Cisco Licensing, go to cisco.com/go/licensingguide

The Essentials license is included automatically. Smart Licensing does not prevent you from using product features that you have not yet purchased. You can start using a license immediately, as long as you are registered with the Smart Software Manager, and purchase the license later. This allows you to deploy and use a feature, and avoid delays due to purchase order approval. See the following licenses:

- **Essentials**—(Required) Essentials license.
- **IPS**—Security Intelligence and Next-Generation IPS
- **Malware Defense**—Malware defense
- **URL**—URL Filtering
- **Cisco Secure Client**—Secure Client Advantage, Secure Client Premier, or Secure Client VPN Only

Before you begin

- Have a master account on the Smart Software Manager.

  If you do not yet have an account, click the link to set up a new account. The Smart Software Manager lets you create a master account for your organization.

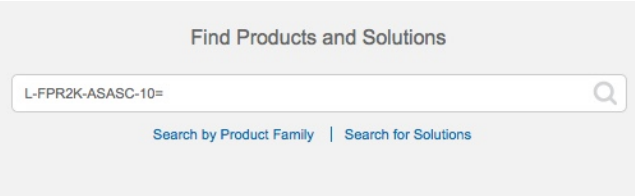
- Your Smart Software Licensing account must qualify for the Strong Encryption (3DES/AES) license to use some features (enabled using the export-compliance flag).

Procedure

Step 1 Make sure your Smart Licensing account contains the available licenses you need.

When you bought your device from Cisco or a reseller, your licenses should have been linked to your Smart Software License account. However, if you need to add licenses yourself, use the **Find Products and Solutions** search field on the Cisco Commerce Workspace. Search for the following license PIDs:

Figure 72: License Search



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

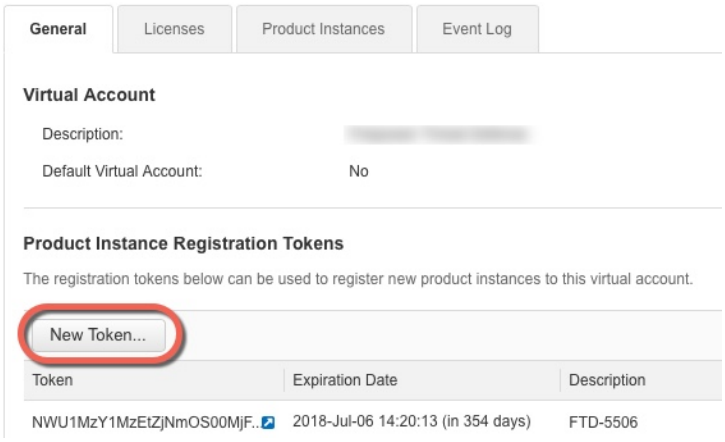
- IPS, Malware Defense, and URL license combination:
  - L-FPR2110T-TMC=
  - L-FPR2120T-TMC=
  - L-FPR2130T-TMC=
  - L-FPR2140T-TMC=

  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-FPR2110T-TMC-1Y
  - L-FPR2110T-TMC-3Y
  - L-FPR2110T-TMC-5Y
  - L-FPR2120T-TMC-1Y
  - L-FPR2120T-TMC-3Y
  - L-FPR2120T-TMC-5Y
  - L-FPR2130T-TMC-1Y
  - L-FPR2130T-TMC-3Y
  - L-FPR2130T-TMC-5Y
  - L-FPR2140T-TMC-1Y
  - L-FPR2140T-TMC-3Y
  - L-FPR2140T-TMC-5Y
- Cisco Secure Client—See the Cisco Secure Client Ordering Guide.

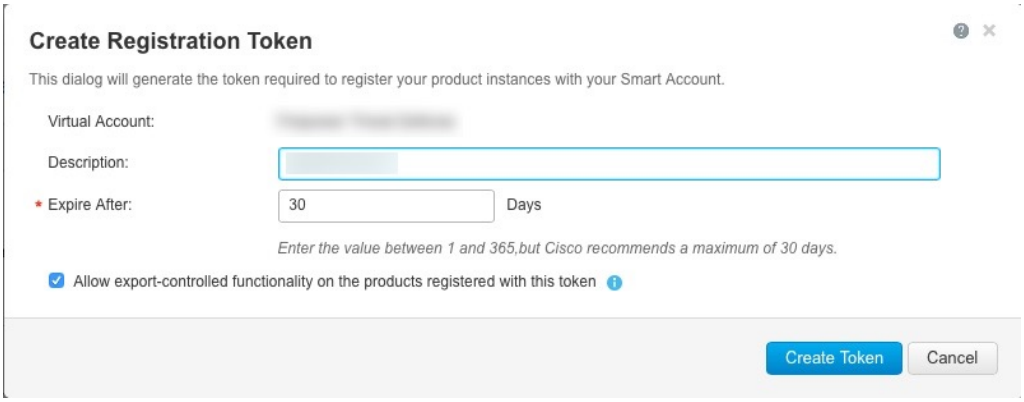
Step 2 In the Smart Software Manager, request and copy a registration token for the virtual account to which you want to add this device.

a) Click **Inventory**.

b) On the **General** tab, click **New Token**.



c) On the **Create Registration Token** dialog box enter the following settings, and then click **Create Token**:



- **Description**
- **Expire After**—Cisco recommends 30 days.
- **Allow export-controlled functionality on the products registered with this token**—Enables the export-compliance flag if you are in a country that allows for strong encryption. You must select this option now if you plan to use this functionality. If you enable this functionality later, you will need to re-register your device with a new product key and reload the device. If you do not see this option, your account does not support export-controlled functionality.

The token is added to your inventory.

d) Click the arrow icon to the right of the token to open the **Token** dialog box so you can copy the token ID to your clipboard. Keep this token ready for later in the procedure when you need to register the threat defense.

Figure 73: View Token

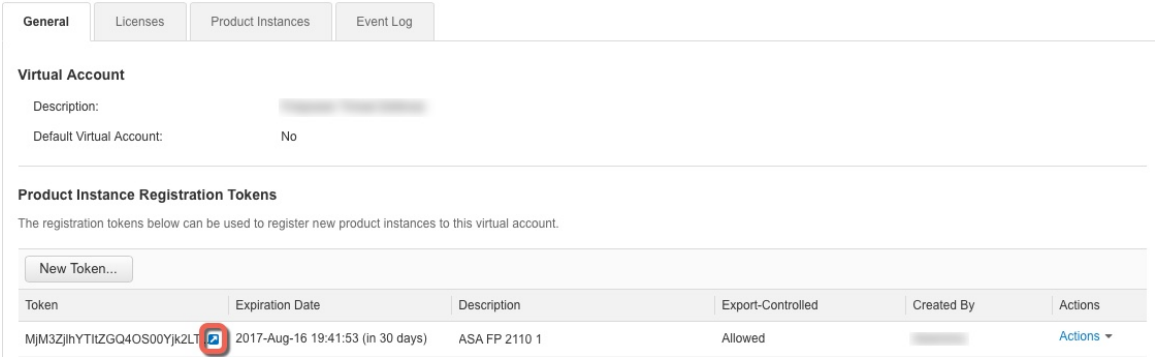
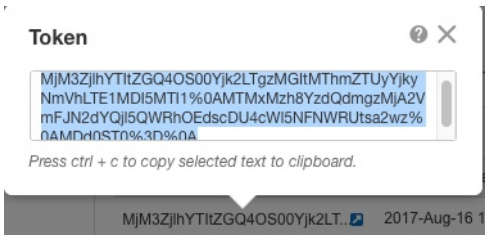


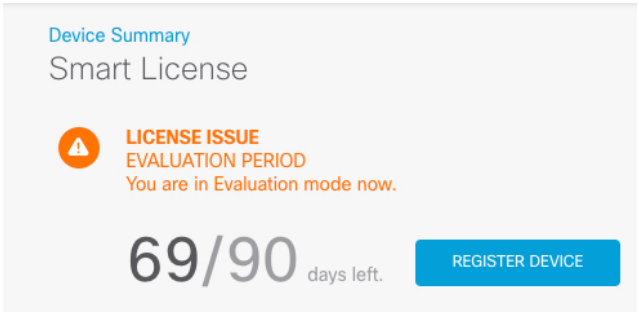
Figure 74: Copy Token



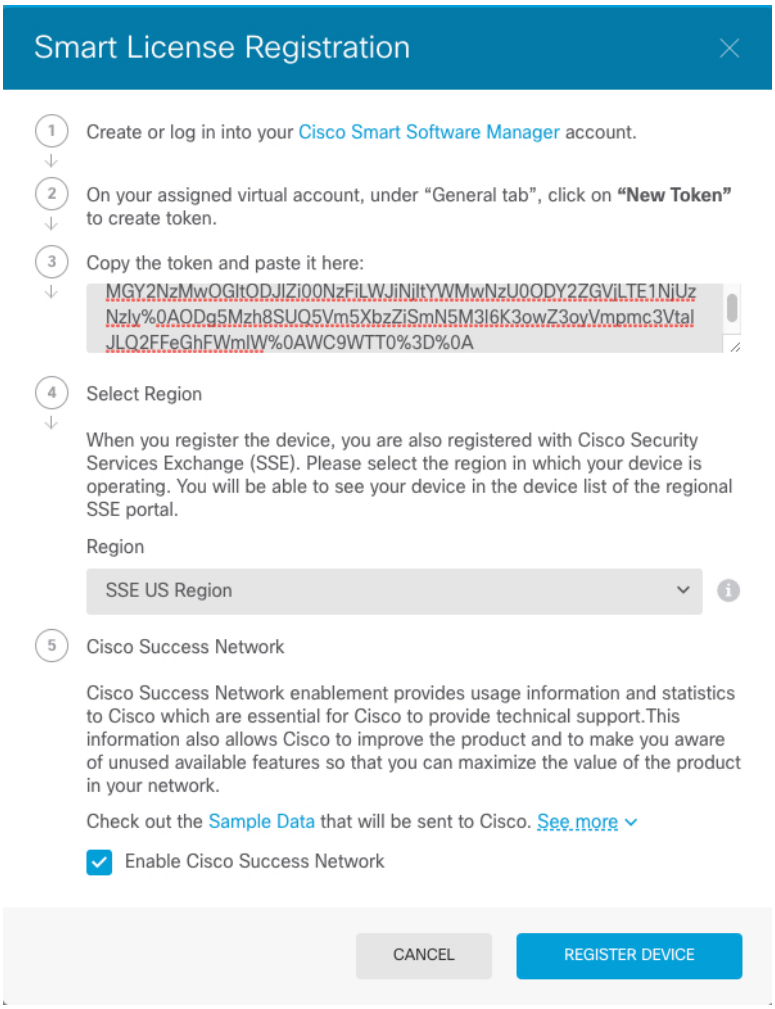
Step 3 In the device manager, click **Device**, and then in the **Smart License** summary, click **View Configuration**.

You see the **Smart License** page.

Step 4 Click **Register Device**.

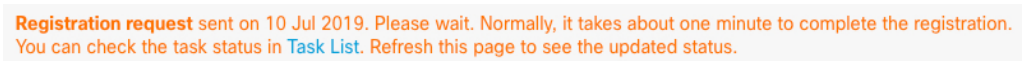


Then follow the instructions on the **Smart License Registration** dialog box to paste in your token:

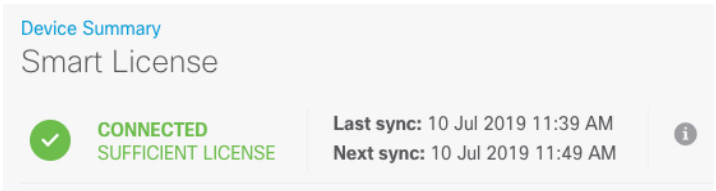


Step 5 Click **Register Device**.

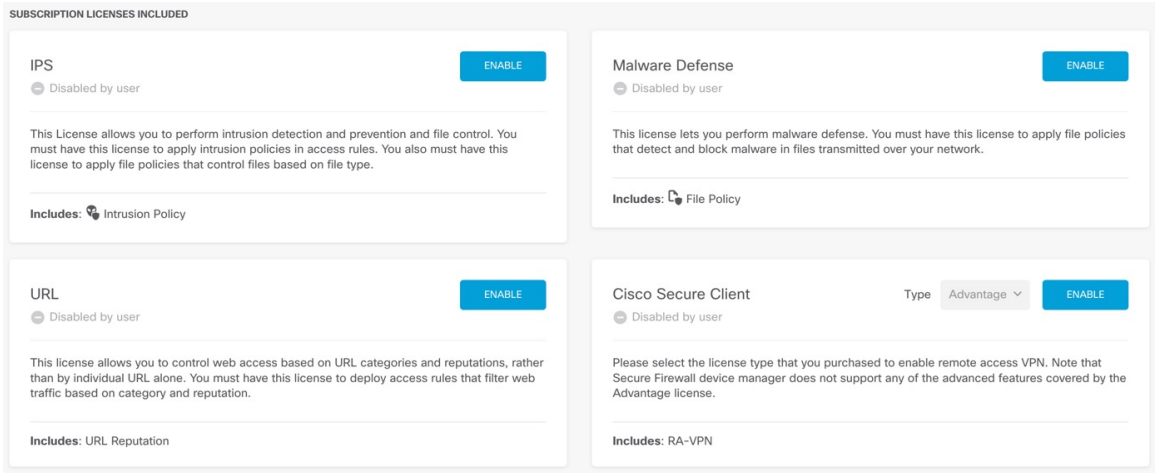
You return to the **Smart License** page. While the device registers, you see the following message:



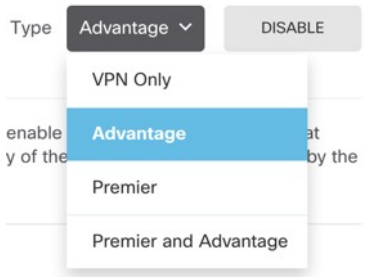
After the device successfully registers and you refresh the page, you see the following:



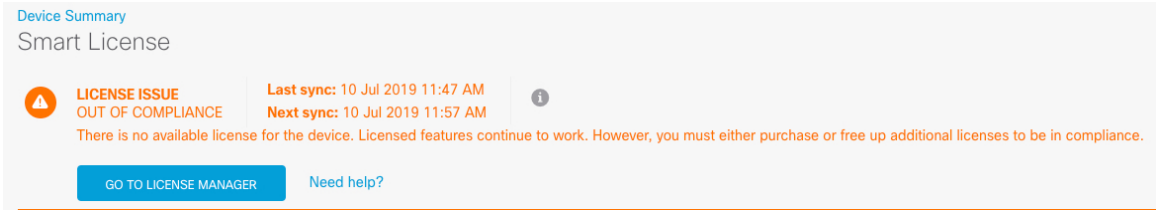
Step 6 Click the **Enable/Disable** control for each optional license as desired.



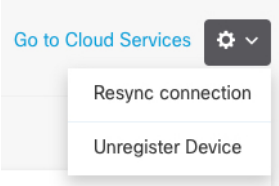
- **Enable**—Registers the license with your Cisco Smart Software Manager account and enables the controlled features. You can now configure and deploy policies controlled by the license.
- **Disable**—Unregisters the license with your Cisco Smart Software Manager account and disables the controlled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



After you enable features, if you do not have the licenses in your account, you will see the following non-compliance message after you refresh the page:



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



Configure the Firewall in the Device Manager

The following steps provide an overview of additional features you might want to configure. Please click the help button (**?**) on a page to get detailed information about each step.

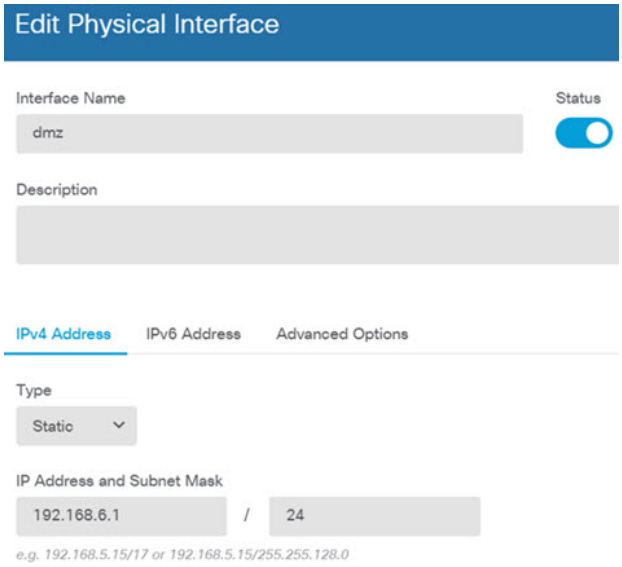
Procedure

Step 1 If you wired other interfaces, choose **Device**, and then click the link in the **Interfaces** summary.

Click the edit icon ( ) for each interface to set the mode and define the IP address and other settings.

The following example configures an interface to be used as a "demilitarized zone" (DMZ), where you place publicly-accessible assets such as your web server. Click **Save** when you are finished.

Figure 75: Edit Interface



Step 2 If you configured new interfaces, choose **Objects**, then select **Security Zones** from the table of contents.

Edit or create new zones as appropriate. Each interface must belong to a zone, because you configure policies based on security zones, not interfaces. You cannot put the interfaces in zones when configuring them, so you must always edit the zone objects after creating new interfaces or changing the purpose of existing interfaces.

The following example shows how to create a new dmz-zone for the dmz interface.

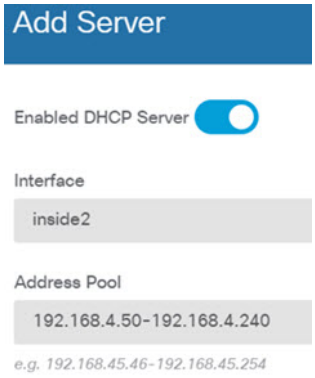
Figure 76: Security Zone Object

Step 3 If you want internal clients to use DHCP to obtain an IP address from the device, choose **Device** > **System Settings** > **DHCP Server**, then select the **DHCP Servers** tab.

There is already a DHCP server configured for the inside interface, but you can edit the address pool or even delete it. If you configured other inside interfaces, it is very typical to set up a DHCP server on those interfaces. Click + to configure the server and address pool for each inside interface.

You can also fine-tune the WINS and DNS list supplied to clients on the **Configuration** tab. The following example shows how to set up a DHCP server on the inside2 interface with the address pool 192.168.4.50-192.168.4.240.

Figure 77: DHCP Server



Step 4 Choose **Device**, then click **View Configuration** (or **Create First Static Route**) in the **Routing** group and configure a default route.

The default route normally points to the upstream or ISP router that resides off the outside interface. A default IPv4 route is for any-ipv4 (0.0.0.0/0), whereas a default IPv6 route is for any-ipv6 (::0/0). Create routes for each IP version you use. If you use DHCP to obtain an address for the outside interface, you might already have the default routes that you need.

Note The routes you define on this page are for the data interfaces only. They do not impact the management interface. Set the management gateway on **Device** > **System Settings** > **Management Interface**.

The following example shows a default route for IPv4. In this example, isp-gateway is a network object that identifies the IP address of the ISP gateway (you must obtain the address from your ISP). You can create this object by clicking **Create New Network** at the bottom of the **Gateway** drop-down list.

Figure 78: Default Route

Step 5 Choose **Policies** and configure the security policies for the network.

The device setup wizard enables traffic flow between the inside-zone and outside-zone, and interface NAT for all interfaces when going to the outside interface. Even if you configure new interfaces, if you add them to the inside-zone object, the access control rule automatically applies to them.

However, if you have multiple inside interfaces, you need an access control rule to allow traffic flow from inside-zone to inside-zone. If you add other security zones, you need rules to allow traffic to and from those zones. These would be your minimum changes.

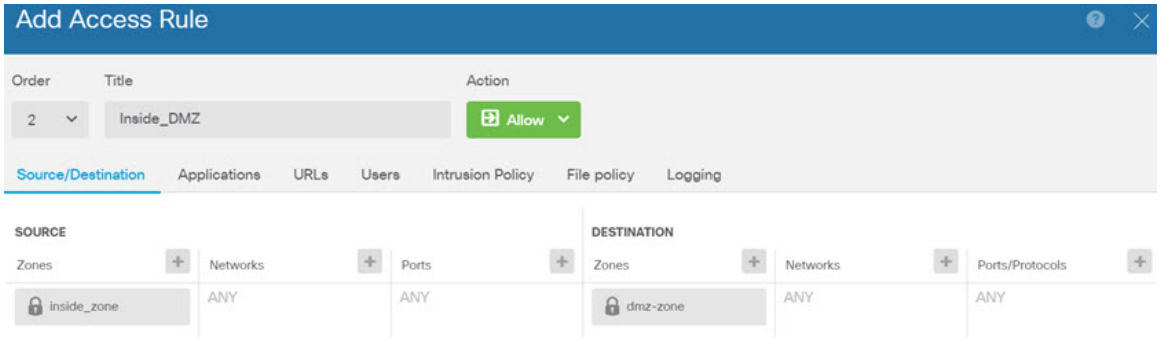
In addition, you can configure other policies to provide additional services, and fine-tune NAT and access rules to get the results that your organization requires. You can configure the following policies:

- **SSL Decryption**—If you want to inspect encrypted connections (such as HTTPS) for intrusions, malware, and so forth, you must decrypt the connections. Use the SSL decryption policy to determine which connections need to be decrypted. The system re-encrypts the connection after inspecting it.
- **Identity**—If you want to correlate network activity to individual users, or control network access based on user or user group membership, use the identity policy to determine the user associated with a given source IP address.
- **Security Intelligence**—Use the Security Intelligence policy to quickly drop connections from or to blacklisted IP addresses or URLs. By blacklisting known bad sites, you do not need to account for them in your access control policy. Cisco provides regularly updated feeds of known bad addresses and URLs so that the Security Intelligence blacklist updates dynamically. Using feeds, you do not need to edit the policy to add or remove items in the blacklist.
- **NAT (Network Address Translation)**—Use the NAT policy to convert internal IP addresses to externally routeable addresses.

- **Access Control**—Use the access control policy to determine which connections are allowed on the network. You can filter by security zone, IP address, protocol, port, application, URL, user or user group. You also apply intrusion and file (malware) policies using access control rules. Use this policy to implement URL filtering.
- **Intrusion**—Use the intrusion policies to inspect for known threats. Although you apply intrusion policies using access control rules, you can edit the intrusion policies to selectively enable or disable specific intrusion rules.

The following example shows how to allow traffic between the inside-zone and dmz-zone in the access control policy. In this example, no options are set on any of the other tabs except for **Logging**, where **At End of Connection** is selected.

Figure 79: Access Control Policy



Step 6 Choose **Device**, then click **View Configuration** in the **Updates** group and configure the update schedules for the system databases.

If you are using intrusion policies, set up regular updates for the Rules and VDB databases. If you use Security Intelligence feeds, set an update schedule for them. If you use geolocation in any security policies as matching criteria, set an update schedule for that database.

Step 7 Click the **Deploy** button in the menu, then click the Deploy Now button ( ), to deploy your changes to the device.

Changes are not active on the device until you deploy them.

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 Firepower 2100 ships with a DB-9 to RJ-45 serial cable, so you may need 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 Using the Device Manager

You can shut down your system properly using the device manager.

Procedure

Step 1 Use the device manager to shut down the firewall.

Note For 6.4 and earlier, enter the **shutdown** command at the device manager CLI.

a) Click **Device**, then click the **System Settings** > **Reboot/Shutdown** link.
b) Click **Shut Down**.

Step 2 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]
```

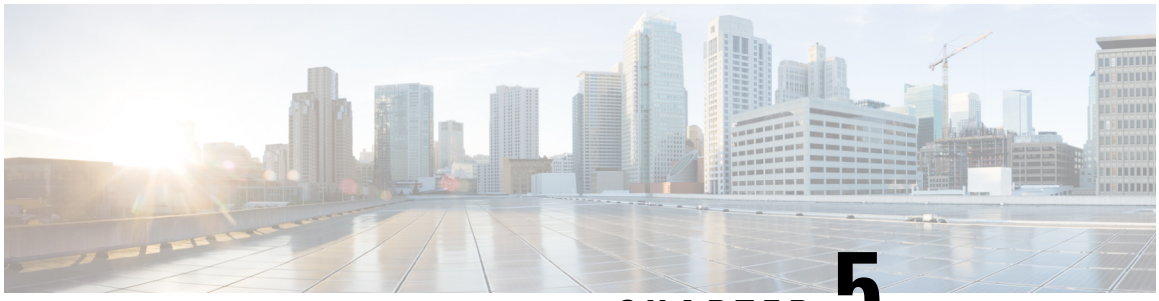
If you do not have a console connection, wait approximately 3 minutes to ensure the system has shut down.

Step 3 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 Firepower Documentation.

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



CHAPTER 5

Threat Defense Deployment with CDO

Is This Chapter for You?

To see all available applications and managers, see Which Application and Manager is Right for You?, on page 1. This chapter applies to the threat defense using Cisco Defense Orchestrator (CDO)'s cloud-delivered Firewall Management Center.

Note The cloud-delivered Firewall Management Center supports threat defense 7.2 and later.

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

About the Firewall

The hardware can run either threat defense software or ASA software. Switching between threat defense and ASA requires you to reimage the device. You should also reimage if you need a different software version than is currently installed. See 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.

• What's Next, on page 184

About Threat Defense Management by CDO

About the Cloud-delivered Firewall Management Center

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

CDO Onboarding Methods

Use one of the following methods to onboard a device.

Low-Touch Provisioning

- An administrator at the central headquarters sends the threat defense to the remote branch office. There is no pre-configuration required. In fact, you should not configure anything on the device, because low-touch provisioning might not work with pre-configured devices.

Note The central administrator can preregister the threat defense on CDO using the threat defense serial number before sending the device to the branch office.

- The branch office administrator cables and powers on the threat defense.
- The central administrator onboards the threat defense using CDO.

Manual Provisioning

Use the manual onboarding wizard and CLI registration if you need to perform any pre-configuration or if you are using a manager interface that low-touch provisioning does not support.

Threat Defense Manager Access Interface

This guide covers outside interface access, because it is the most likely scenario for remote branch offices. Although manager access occurs on the outside interface, the dedicated Management interface is still relevant. The Management interface is a special interface configured separately from the threat defense data interfaces, and it has its own network settings.

- The Management interface network settings are still used even though you are enabling manager access on a data interface.
- All management traffic continues to be sourced from or destined to the Management interface.
- When you enable manager access on a data interface, the threat defense forwards incoming management traffic over the backplane to the Management interface.
- For outgoing management traffic, the Management interface forwards the traffic over the backplane to the data interface.

Manager Access Requirements

Manager access from a data interface has the following limitations:

- You can only enable manager access on a physical, data interface. You cannot use a subinterface or EtherChannel. You can also use the management center to enable manager access on a single secondary interface for redundancy.
- This interface cannot be management-only.
- Routed firewall mode only, using a routed interface.
- PPPoE is not supported. If your ISP requires PPPoE, you will have to put a router with PPPoE support between the threat defense and the WAN modem.
- The interface must be in the global VRF only.
- SSH is not enabled by default for data interfaces, so you will have to enable SSH later using the management center. Because the Management interface gateway will be changed to be the data interfaces, you also cannot SSH to the Management interface from a remote network unless you add a static route for the Management interface using the **configure network static-routes** command.

High Availability Requirements

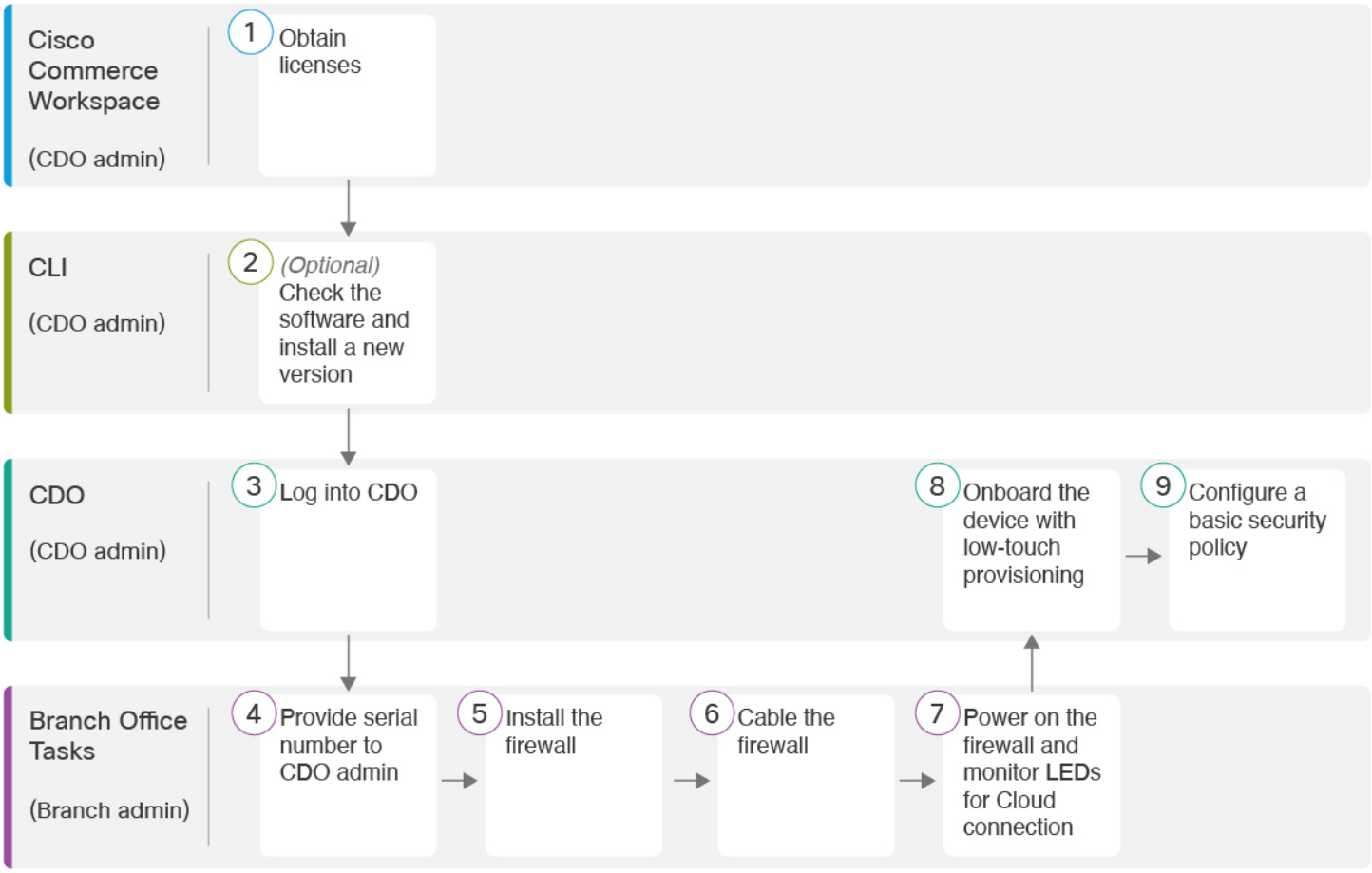
When using a data interface with device high availability, see the following requirements.

- Use the same data interface on both devices for manager access.
- Redundant manager access data interface is not supported.
- You cannot use DHCP; only a static IP address is supported. Features that rely on DHCP cannot be used, including DDNS and low-touch provisioning.
- Have different static IP addresses in the same subnet.
- Use either IPv4 or IPv6; you cannot set both.
- Use the same manager configuration (**configure manager add** command) to ensure that the connectivity is the same.
- You cannot use the data interface as the failover or state link.

End-to-End Tasks: Low-Touch Provisioning

See the following tasks to deploy the threat defense with CDO using low-touch provisioning.

Figure 80: End-to-End Tasks: Low-Touch Provisioning



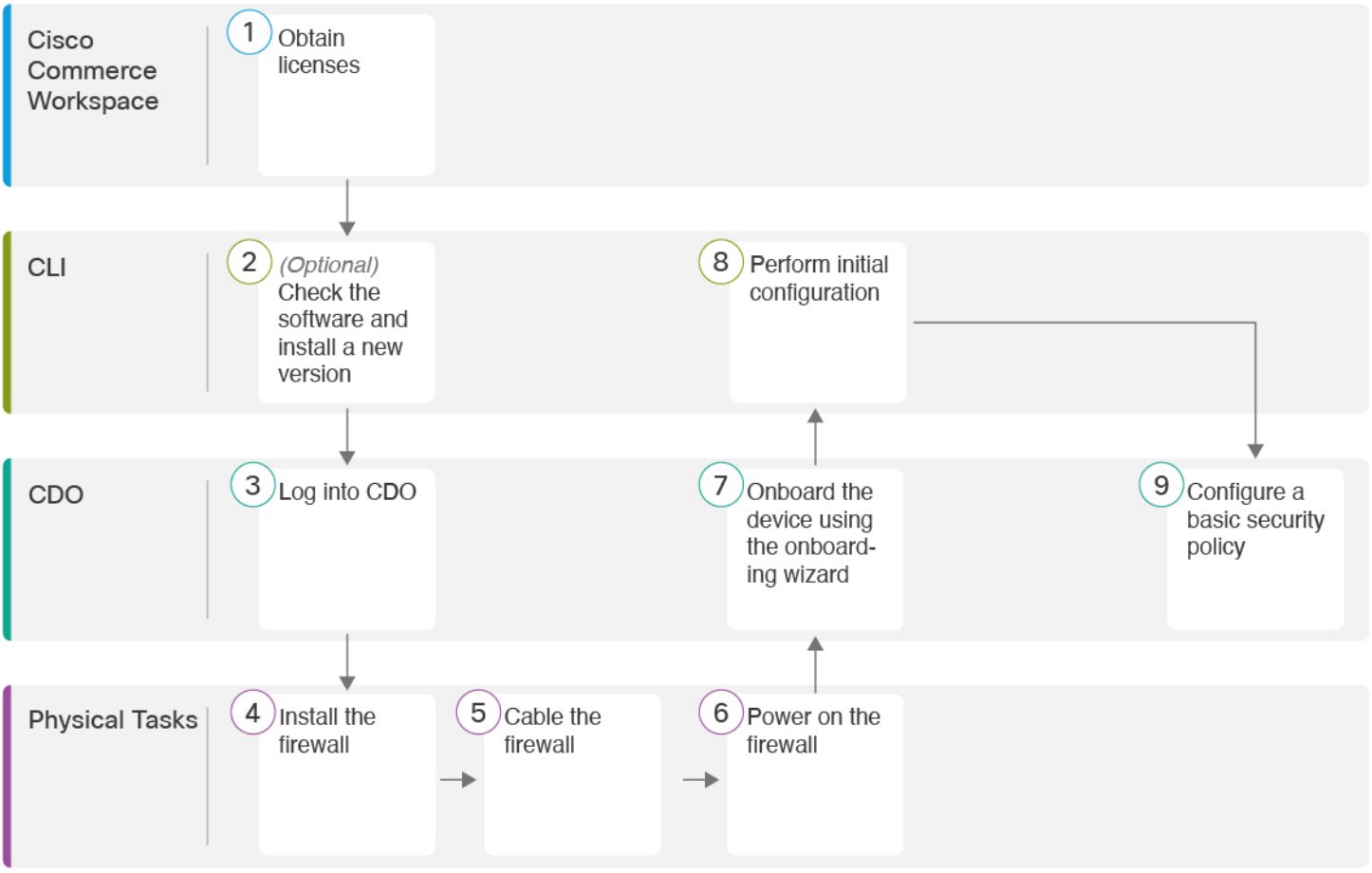
1	Cisco Commerce Workspace (CDO admin)	Obtain Licenses, on page 136.
2	CLI (CDO admin)	(Optional) Check the Software and Install a New Version, on page 138.
3	CDO (CDO admin)	Log Into CDO, on page 139.
4	Branch Office Tasks (Branch admin)	Provide the Firewall Serial Number to the Central Administrator, on page 143.
5	Branch Office Tasks (Branch admin)	Install the firewall. See the hardware installation guide.
6	Branch Office Tasks (Branch admin)	Cable the Firewall, on page 144.

7	Branch Office Tasks (Branch admin)	Power On the Firewall, on page 145.
8	CDO (CDO admin)	Onboard a Device with Low-Touch Provisioning, on page 146.
9	CDO (CDO admin)	Configure a Basic Security Policy, on page 162.

End-to-End Tasks: Onboarding Wizard

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

Figure 81: End-to-End Tasks: Onboarding Wizard



1	Cisco Commerce Workspace	Obtain Licenses, on page 136.

2	CLI	(Optional) Check the Software and Install a New Version, on page 138.
3	CDO	Log Into CDO, on page 139.
4	Physical Tasks	Install the firewall. See the hardware installation guide.
5	Physical Tasks	Cable the Firewall, on page 149.
6	Physical Tasks	Power on the Firewall, on page 150.
7	CDO	Onboard a Device with the Onboarding Wizard, on page 151.
8	CLI or Device Manager	• Perform Initial Configuration Using the CLI, on page 154. • Perform Initial Configuration Using the Device Manager, on page 158.
9	CDO	Configure a Basic Security Policy, on page 162.

Central Administrator Pre-Configuration

This section describes how to obtain feature licenses for your firewall; how to install a new software version before you deploy; and how to log into CDO.

Obtain Licenses

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

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

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.

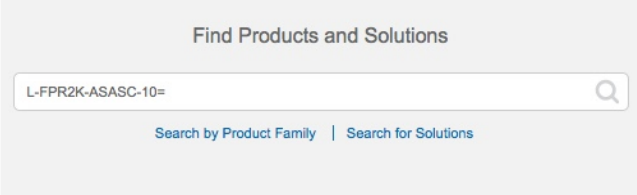
- Your Smart Software Licensing account must qualify for the Strong Encryption (3DES/AES) license to use some features (enabled using the export-compliance flag).

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 82: License Search



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

- IPS, Malware Defense, and URL license combination:
  - L-FPR2110T-TMC=
  - L-FPR2120T-TMC=
  - L-FPR2130T-TMC=
  - L-FPR2140T-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-FPR2110T-TMC-1Y
  - L-FPR2110T-TMC-3Y
  - L-FPR2110T-TMC-5Y
  - L-FPR2120T-TMC-1Y
  - L-FPR2120T-TMC-3Y
  - L-FPR2120T-TMC-5Y
  - L-FPR2130T-TMC-1Y
  - L-FPR2130T-TMC-3Y
  - L-FPR2130T-TMC-5Y
  - L-FPR2140T-TMC-1Y

- L-FPR2140T-TMC-3Y
- L-FPR2140T-TMC-5Y

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

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

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

(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 Power on the firewall and connect to the console port. See Power on the Firewall, on page 150 and Access the Threat Defense and FXOS CLI, on page 175 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               7.4.0.65        7.4.0.65
        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 Perform Initial Configuration Using the CLI, on page 154. 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.

For low-touch provisioning, when you onboard the device, for the **Password Reset** area, be sure to choose **No...** because you already set the password.

d) Shut down the device. See Power Off the Device at the CLI, on page 183.

Log Into CDO

CDO uses Cisco Secure Sign-On as its identity provider and Duo Security for multi-factor authentication (MFA). CDO requires MFA which provides an added layer of security in protecting your user identity. Two-factor authentication, a type of MFA, requires two components, or factors, to ensure the identity of the user logging into CDO.

The first factor is a username and password, and the second is a one-time password (OTP), which is generated on demand from Duo Security.

After you establish your Cisco Secure Sign-On credentials, you can log into CDO from your Cisco Secure Sign-On dashboard. From the Cisco Secure Sign-On dashboard, you can also log into any other supported Cisco products.

- If you have a Cisco Secure Sign-On account, skip ahead to Log Into CDO with Cisco Secure Sign-On, on page 142.
- If you don't have a Cisco Secure Sign-On account, continue to Create a New Cisco Secure Sign-On Account, on page 140.

Create a New Cisco Secure Sign-On Account

The initial sign-on workflow is a four-step process. You need to complete all four steps.

Before you begin

- **Install DUO Security—**We recommend that you install the Duo Security app on a mobile phone. Review Duo Guide to Two Factor Authentication: Enrollment Guide if you have questions about installing Duo.
- **Time Synchronization—**You are going to use your mobile device to generate a one-time password. It is important that your device clock is synchronized with real time as the OTP is time-based. Make sure your device clock is set to the correct time.
- Use a current version of Firefox or Chrome.

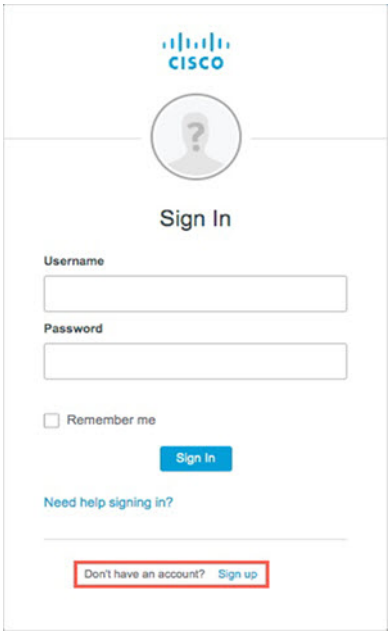
Procedure

Step 1 **Sign Up for a New Cisco Secure Sign-On Account.**

a) Browse to https://sign-on.security.cisco.com.

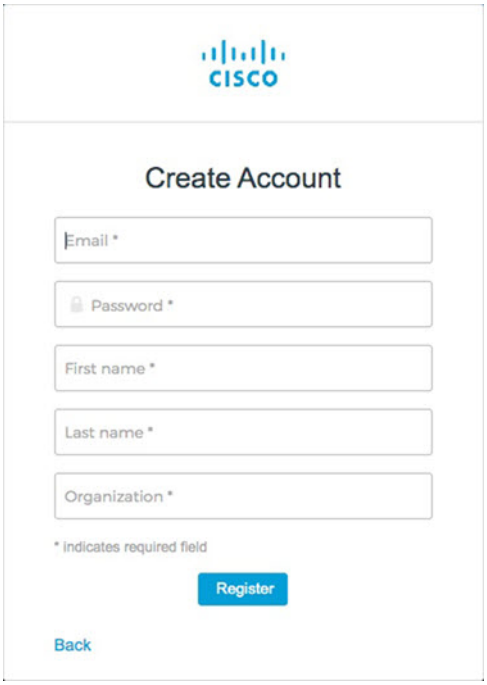
b) At the bottom of the Sign In screen, click **Sign up**.

Figure 83: Cisco SSO Sign Up



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

Figure 84: Create Account



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

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

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

a) In the **Set up multi-factor authentication** screen, click **Configure**.

b) Click **Start setup** and follow the prompts to choose a device and verify the pairing of that device with your account.

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

c) At the end of the wizard click **Continue to Login**.

d) Log in to Cisco Secure Sign-On with the two-factor authentication.

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

a) Choose the mobile device you are pairing with Google Authenticator and click **Next**.

b) Follow the prompts in the setup wizard to setup Google Authenticator.

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

a) Choose a "forgot password" question and answer.

b) Choose a recovery phone number for resetting your account using SMS.

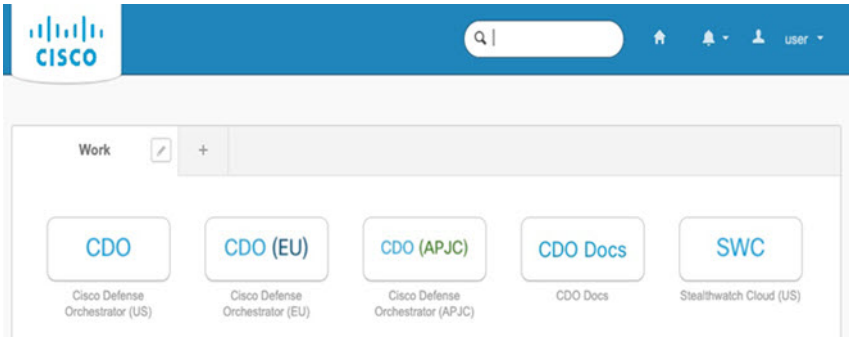
c) Choose a security image.

d) Click **Create My Account**.

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

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

Figure 85: Cisco SSO Dashboard



Log Into CDO with Cisco Secure Sign-On

Log into CDO to onboard and manage your device.

Before you begin

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

- To log into CDO, you must first create your account in Cisco Secure Sign-On and configure MFA using Duo; see Create a New Cisco Secure Sign-On Account, on page 140.
- Use a current version of Firefox or Chrome.

Procedure

Step 1 In a web browser, navigate to https://sign-on.security.cisco.com/.

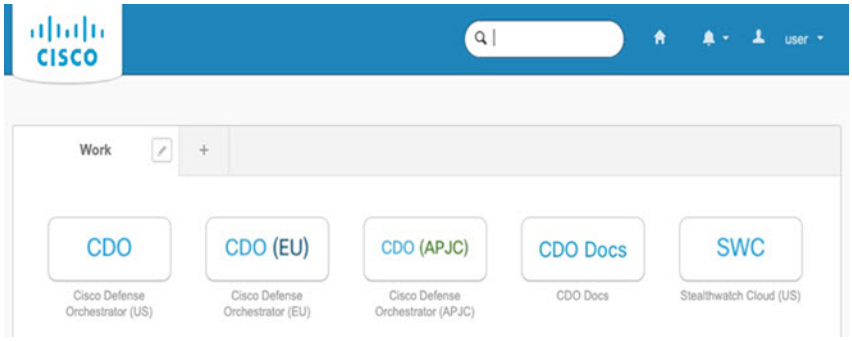
Step 2 Enter your **Username** and **Password**.

Step 3 Click **Log in**.

Step 4 Receive another authentication factor using Duo Security, and confirm your login. The system confirms your login and displays the Cisco Secure Sign-On dashboard.

Step 5 Click the appropriate CDO tile on the Cisco Secure Sign-on dashboard. The **CDO** tile directs you to https://defenseorchestrator.com, the **CDO (EU)** tile directs you to https://defenseorchestrator.eu, and the **CDO (APJC)** tile directs you to to https://www.apj.cdo.cisco.com.

Figure 86: Cisco SSO Dashboard



Step 6 Click the authenticator logo to choose **Duo Security** or **Google Authenticator**, if you have set up both authenticators.

- If you already have a user record on an existing tenant, you are logged into that tenant.
- If you already have a user record on several tenants, you will be able to choose which CDO tenant to connect to.
- If you do not already have a user record on an existing tenant, you will be able to learn more about CDO or request a trial account.

Deploy the Firewall With Low-Touch Provisioning

After you receive the threat defense from central headquarters, you only need to cable and power on the firewall so that it has internet access from the outside interface. The central administrator can then complete the configuration.

Provide the Firewall Serial Number to the Central Administrator

Before you rack the firewall or discard the shipping box, record the serial number so you can coordinate with the central adminstrator.

Procedure

Step 1 Unpack the chassis and chassis components.

Take inventory of your firewall and packaging before you connect any cables or power on the firewall. You should also familiarize yourself with the chassis layout, components, and LEDs.

Step 2 Record the firewall's serial number.

The serial number of the firewall can be found on the shipping box. It can also be found on a sticker on a pull-out tab on the front of the firewall.

Step 3 Send the firewall serial number to the CDO network administrator at your IT department/central headquarters.

Your network administrator needs your firewall serial number to facilitate low-touch provisioning, connect to the firewall, and configure it remotely.

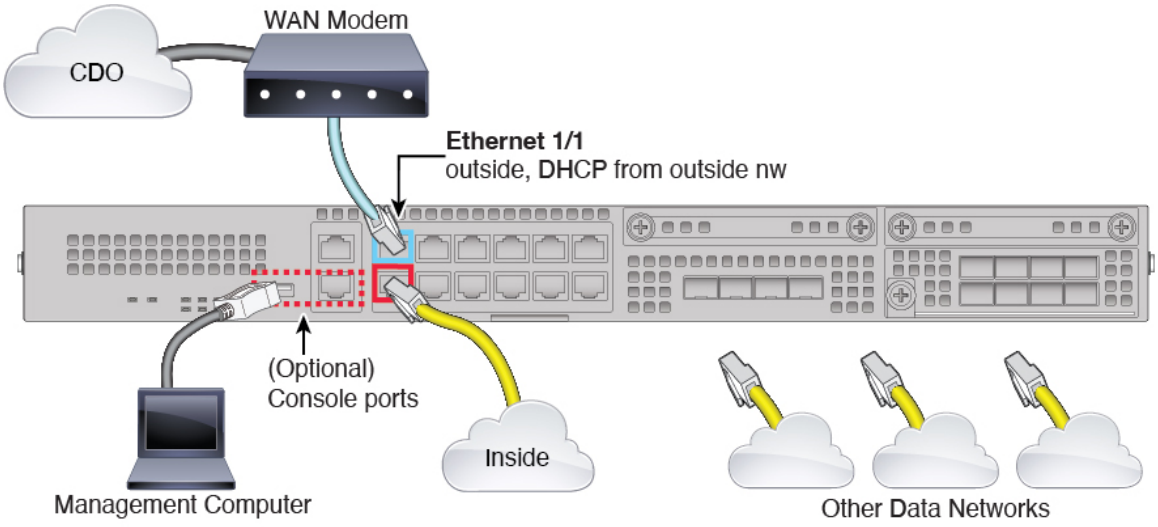
Communicate with the CDO administrator to develop an onboarding timeline.

Cable the Firewall

This topic describes how to connect the Firepower 2100 to your network so that it can be managed by CDO.

If you received a firewall at your branch office, and your job is to plug it in to your network, watch this video. The video describes your firewall and the LED sequences on the firewall that indicate the firewall's status. If you need to, you'll be able to confirm the firewall's status with your IT department just by looking at the LEDs.

Figure 87: Cabling the Firepower 2100



Low-touch provisioning supports connecting to CDO on Ethernet 1/1 (outside).

Procedure

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

Step 2 Connect the network cable from the Ethernet 1/1 interface to your wide area network (WAN) modem. Your WAN modem is your branch's connection to the internet and will be your firewall's route to the internet as well.

Step 3 Connect the inside interface (for example, Ethernet 1/2) to your inside switch or router.

You can choose any interface for inside.

Step 4 Connect other networks to the remaining interfaces.

Step 5 (Optional) Connect the management computer to the console port.

At the branch office, the console connection is not required for everyday use; however, it may be required for troubleshooting purposes.

Power On the Firewall

The power switch is located to the left of power supply module 1 on the rear of the chassis. It is a toggle switch that controls power to the system. If the power switch is in standby position, only the 3.3-V standby power is enabled from the power supply module and the 12-V main power is OFF. When the switch is in the ON position, the 12-V main power is turned on and the system boots.

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

Before you begin

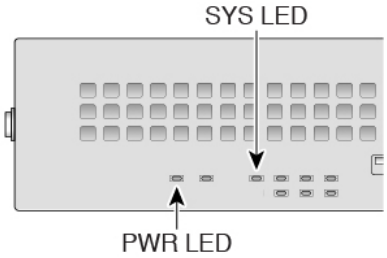
It's important that you provide reliable power for your device (for example, using an uninterruptable power supply (UPS)). Loss of power without first shutting down can cause serious file system damage. There are many processes running in the background all the time, and losing power does not allow the graceful shutdown of your system.

Procedure

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

Step 2 Press the power switch on the back of the device.

Step 3 Check the PWR LED on the front of the device; if it is solid green, the device is powered on.



Step 4 Observe the SYS LED on the front the device; when the device is booting correctly, the SYS LED flashes fast green.

If there is a problem, the SYS LED flashes fast amber. If this happens, call your IT department.

Step 5 Observe the SYS LED on the front; when the device connects to the Cisco cloud, the SYS LED slowly flashes green.

If there is a problem, the SYS LED flashes amber and green, and the device did not reach the Cisco Cloud. If this happens, make sure that your network cable is connected to the Ethernet 1/1 interface and to your WAN

modem. If after adjusting the network cable, the device does not reach the Cisco cloud after about 10 more minutes, call your IT department.

What to do next

- Communicate with your IT department to confirm your onboarding timeline and activities. You should have a communication plan in place with the CDO administrator at your central headquarters.
- After you complete this task, your CDO administrator will be able to configure and manage the Firepower device remotely. You're done.

Onboard a Device with Low-Touch Provisioning

Onboard the threat defense using low-touch provisioning and the device serial number.

Procedure

Step 1 In the CDO navigation pane, click **Inventory**, then click the blue plus button ( ) to **Onboard** a device.

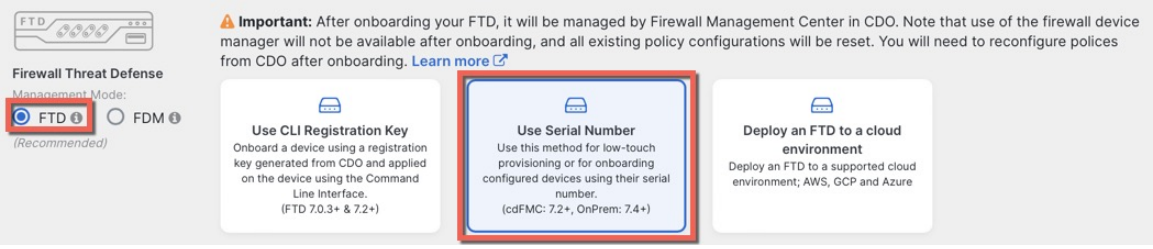
Step 2 Select the **FTD** tile.

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

At any point after selecting **FTD** as the management mode, you can click **Manage Smart License** to enroll in or modify the existing smart licenses available for your device. See Obtain Licenses, on page 136 to see which licenses are available.

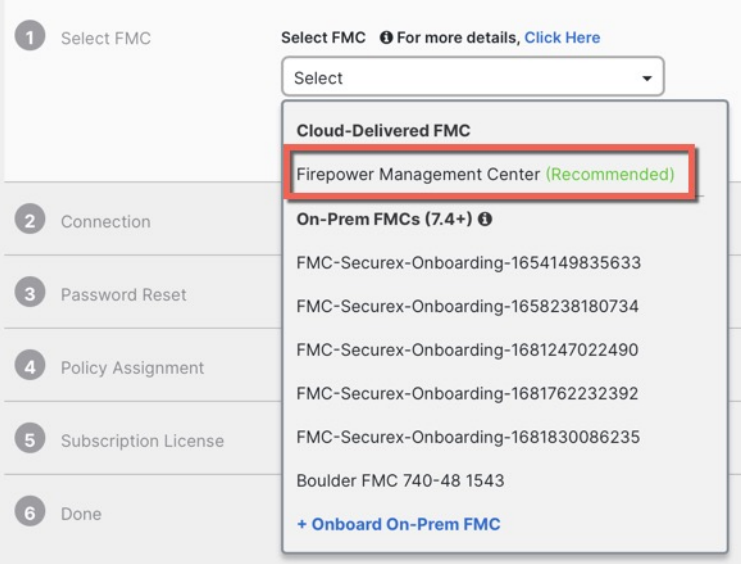
Step 4 Select **Use Serial Number** as the onboarding method.

Figure 88: Use Serial Number



Step 5 In **Select FMC**, choose the **Cloud-Delivered FMC** > **Firewall Management Center** from the list, and click **Next**.

Figure 89: Select FMC



Step 6 In the **Connection** area, enter the **Device Serial Number** and the **Device Name** and then click **Next**.

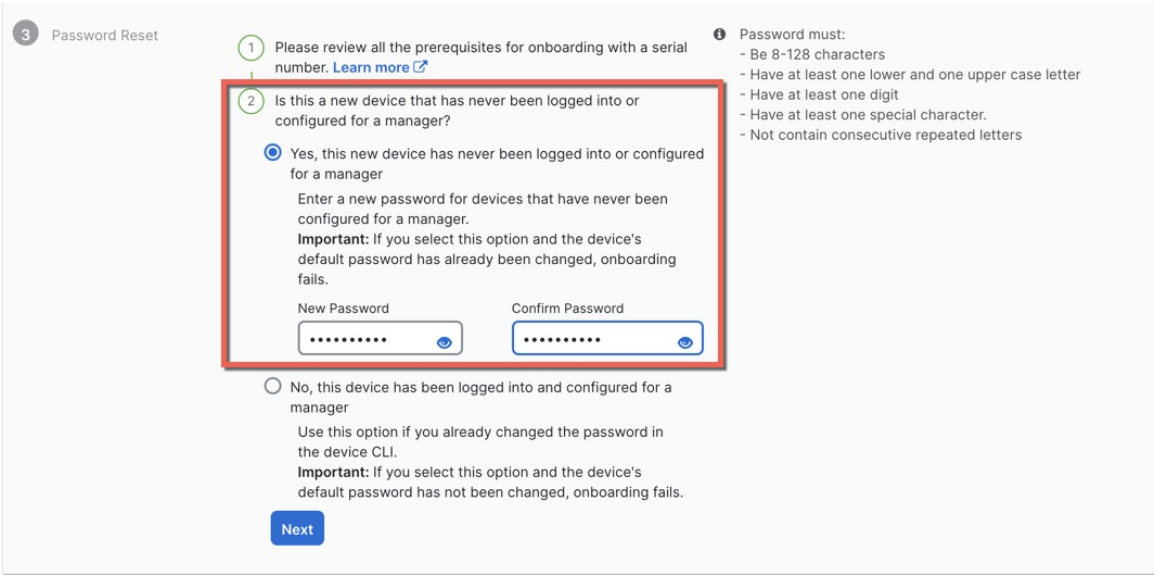
Figure 90: Connection

Step 7 In **Password Reset**, click **Yes...**. Enter a new password and confirm the new password for the device, then click **Next**.

For low-touch provisioning, the device must be brand new or has been reimaged.

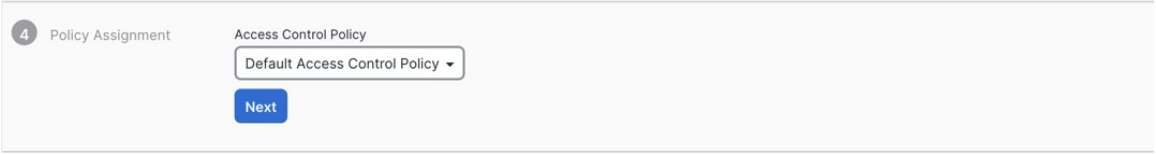
Note If you did log into the device and reset the password, and you did not change the configuration in a way that would disable low-touch provisioning, then you should choose the **No...** option. There are a number of configurations that disable low-touch provisioning, so we don't recommend logging into the device unless you need to, for example, to perform a reimage.

Figure 91: Password Reset



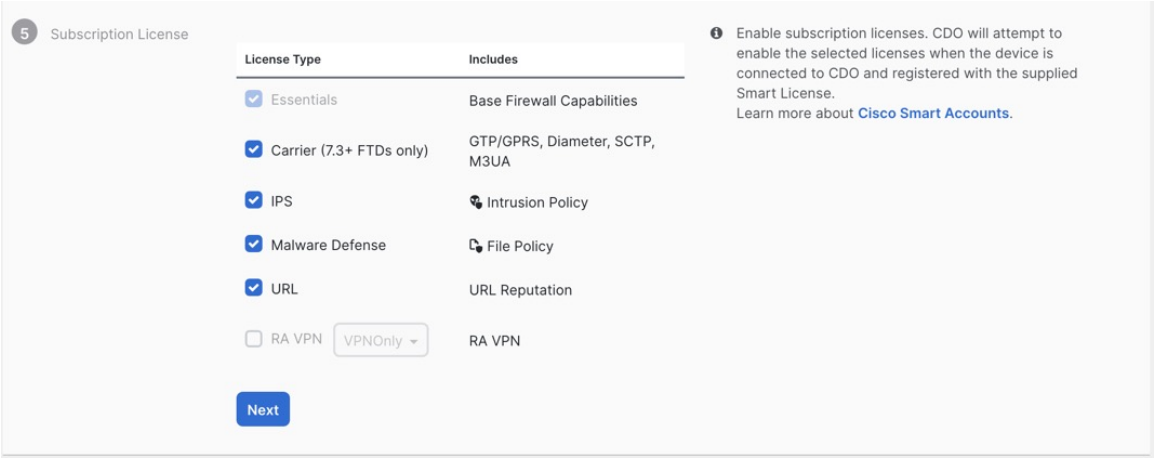
Step 8 For the **Policy Assignment**, use the drop-down menu to choose an access control policy for the device. If you have no policies configured, choose the **Default Access Control Policy**.

Figure 92: Policy Assignment



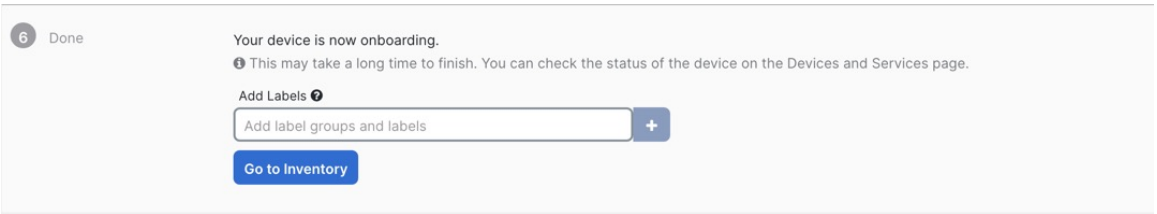
Step 9 For the **Subscription License**, check each of the feature licenses you want to enable. Click **Next**.

Figure 93: Subscription License



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

Figure 94: Done



What to do next

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

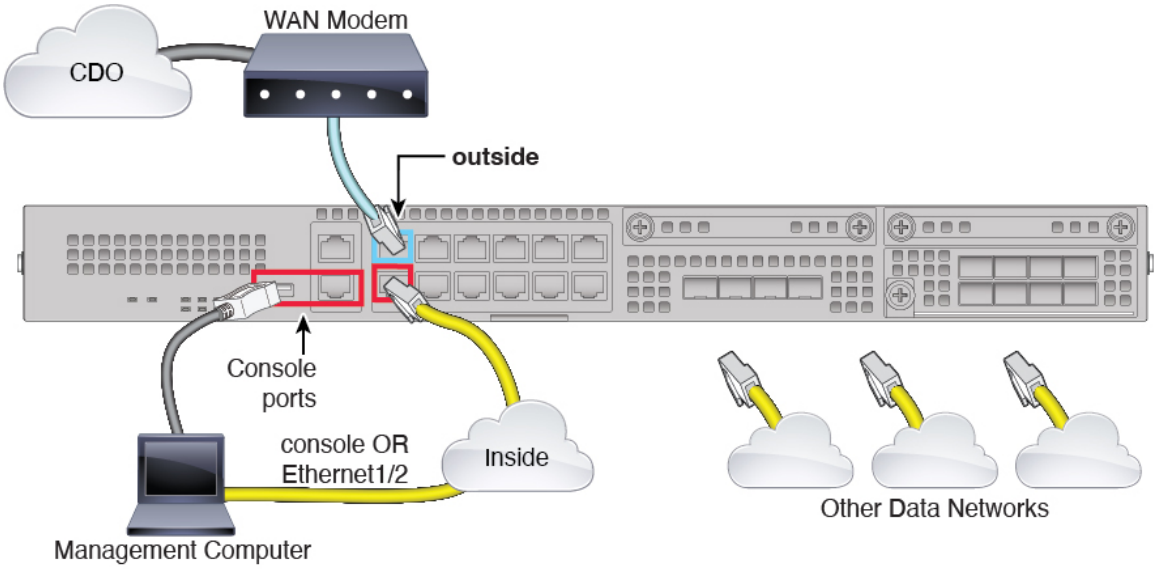
Deploy the Firewall With the Onboarding Wizard

This section describes how to configure the firewall for onboarding using the CDO onboarding wizard.

Cable the Firewall

This topic describes how to connect the Firepower 2100 to your network so that it can be managed by CDO.

Figure 95: Cabling the Firepower 2100



You can connect to CDO on any data interface or the Management interface, depending on which interface you set for manager access during initial setup. This guide shows the outside interface.

Procedure

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

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

Step 3 Connect the inside interface (for example, Ethernet 1/2) to your inside switch or router.

Step 4 Connect other networks to the remaining interfaces.

Step 5 Connect the management computer to the console port or the Ethernet 1/2 interface.

If you perform intial setup using the CLI, you will need to connect to the console port. The console port may also be required for troubleshooting purposes. If you perform initial setup using the device manager, connect to the Ethernet 1/2 interface.

Power on the Firewall

The power switch is located to the left of power supply module 1 on the rear of the chassis. It is a toggle switch that controls power to the system. If the power switch is in standby position, only the 3.3-V standby power is enabled from the power supply module and the 12-V main power is OFF. When the switch is in the ON position, the 12-V main power is turned on and the system boots.

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

Before you begin

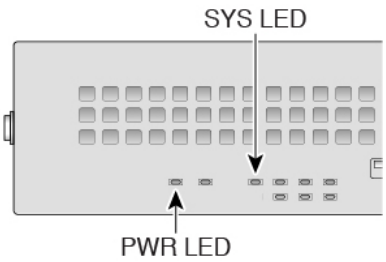
It's important that you provide reliable power for your device (for example, using an uninterruptable power supply (UPS)). Loss of power without first shutting down can cause serious file system damage. There are many processes running in the background all the time, and losing power does not allow the graceful shutdown of your system.

Procedure

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

Step 2 Press the power switch on the back of the device.

Step 3 Check the PWR LED on the front of the device; if it is solid green, the device is powered on.



Step 4 Check the SYS LED on the front of the device; after it is solid green, the system has passed power-on diagnostics.

Note Before you move the power switch to the OFF position, use the shutdown commands so that the system can perform a graceful shutdown. This may take several minutes to complete. After the graceful shutdown is complete, the console displays `It is safe to power off now`. The front panel blue locator beacon LED lights up indicating the system is ready to be powered off. You can now move the switch to the OFF position. The front panel PWR LED flashes momentarily and turns off. Do not remove the power until the PWR LED is completely off.

See the FXOS Configuration Guide for more information on using the shutdown commands.

Onboard a Device with the Onboarding Wizard

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

Procedure

Step 1 In the CDO navigation pane, click **Inventory**, then click the blue plus button ( ) to **Onboard** a device.

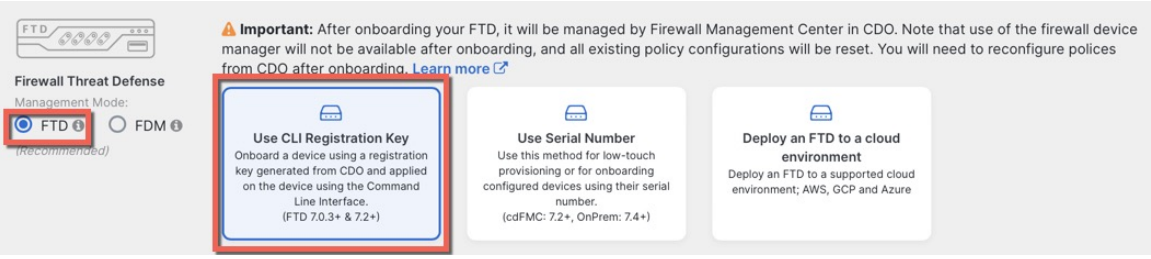
Step 2 Select the **FTD** tile.

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

At any point after selecting **FTD** as the management mode, you can click **Manage Smart License** to enroll in or modify the existing smart licenses available for your device. See Obtain Licenses, on page 136 to see which licenses are available.

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

Figure 96: Use CLI Registration Key

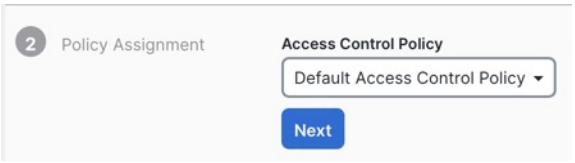


Step 5 Enter the **Device Name** and click **Next**.

Figure 97: Device Name

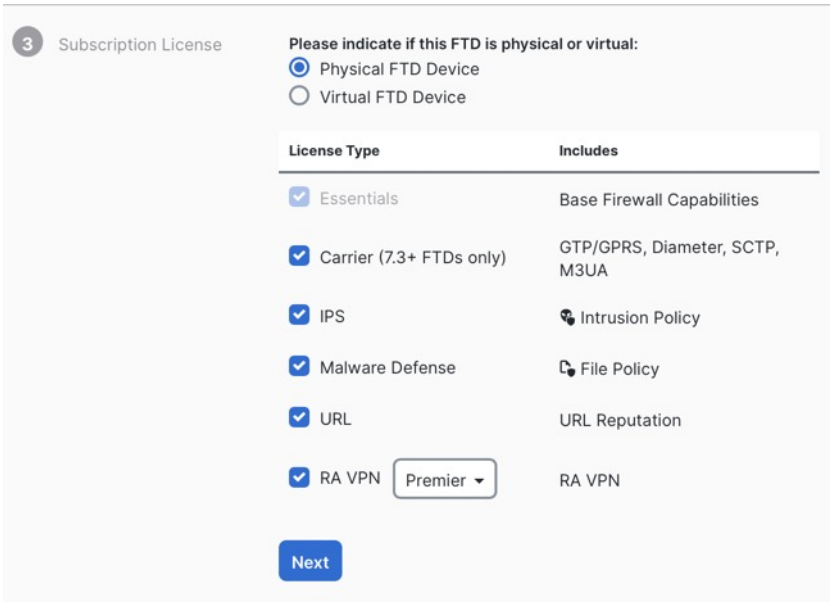
Step 6 For the **Policy Assignment**, use the drop-down menu to choose an access control policy for the device. If you have no policies configured, choose the **Default Access Control Policy**.

Figure 98: Access Control Policy



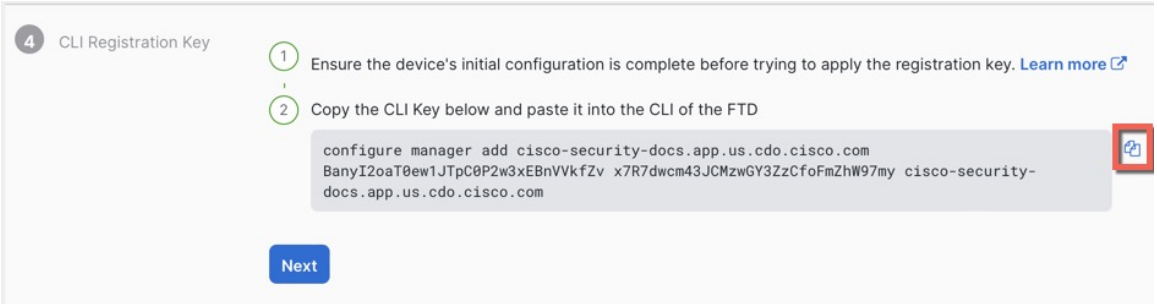
Step 7 For the **Subscription License**, click the **Physical FTD Device** radio button, and then check each of the feature licenses you want to enable. Click **Next**.

Figure 99: Subscription License



Step 8 For the **CLI Registration Key**, CDO generates a command with the registration key and other parameters. You must copy this command and use it in the intial configuration of the threat defense.

Figure 100: CLI Registration Key



configure manager add *cdo_hostname registration_key nat_id display_name*

Complete initial configuration at the CLI or using the device manager:

- Perform Initial Configuration Using the CLI, on page 154—Copy this command at the threat defense CLI after you complete the startup script.
- Perform Initial Configuration Using the Device Manager, on page 158—Copy the *cdo_hostname*, *registration_key*, and *nat_id* parts of the command into the **Management Center/CDO Hostname/IP Address**, **Management Center/CDO Registration Key**, and **NAT ID** fields.

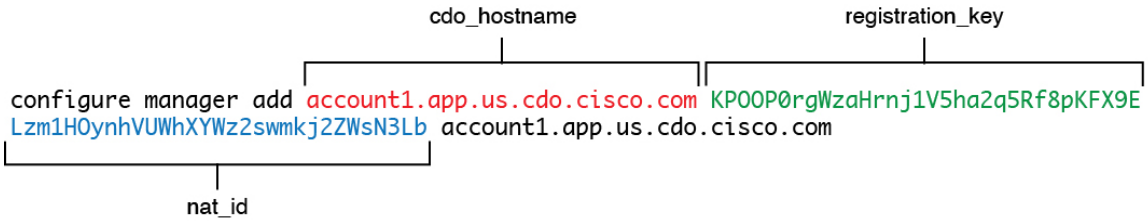
Example:

Sample command for CLI setup:

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

Sample command components for GUI setup:

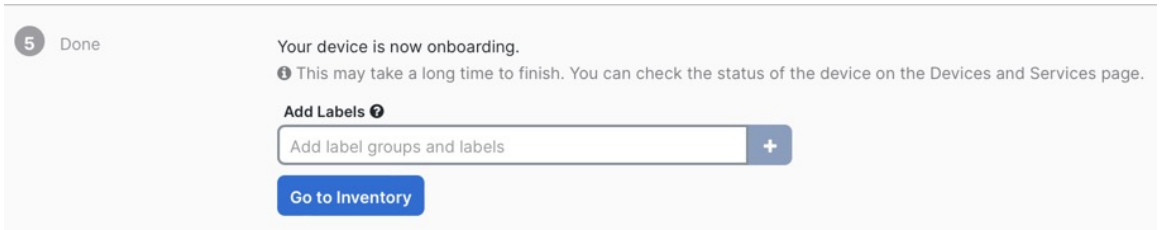
Figure 101: configure manager add command components



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

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

Figure 102: Done



What to do next

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

Perform Initial Configuration

Perfom initial configuration of the threat defense using the CLI or using the device manager.

Perform Initial Configuration Using the CLI

Connect to the threat defense CLI to perform initial setup. When you use the CLI for initial configuration, only the Management interface and manager access interface settings are retained.When you perform initial setup using the device manager, *all* interface configuration completed in the device manager is retained when you switch to CDO 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 on the console port.

The console port connects to the FXOS CLI.

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

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, then 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 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). You are then presented with the CLI setup script for the Management interface settings.

The Management interface settings are used even though you are enabling manager access on a data interface.

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. Although you do not plan to use the Management interface, you must set an IP address, for example, a private address.
- **Configure IPv4 via DHCP or manually?** and/or **Configure IPv6 via DHCP, router, or manually?**—Choose **manual**. You cannot configure a data interface for management if the management interface is set to DHCP, because the default route, which must be **data-interfaces** (see the next bullet), might be overwritten with one received from the DHCP server.
- **Enter the IPv4 default gateway for the management interface** and/or **Enter the IPv6 gateway for the management interface**—Set the gateway to be **data-interfaces**. This setting forwards management traffic over the backplane so it can be routed through the manager access data interface.
- **Manage the device locally?**—Enter **no** to use CDO. A **yes** answer means you will use the device manager instead.
- **Configure firewall mode?**—Enter **routed**. Outside manager access is only supported in routed firewall mode.

Example:

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

System initialization in progress.  Please stand by.
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 [192.168.45.61]: 10.89.5.17
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]:
Enter a fully qualified hostname for this system [firepower]: 1010-3
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 1010-3
Setting static IPv4: 10.89.5.17 netmask: 255.255.255.192 gateway: data 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 Configure the outside interface for manager access.

configure network management-data-interface

You are then prompted to configure basic network settings for the outside interface. See the following details for using this command:

- The Management interface cannot use DHCP if you want to use a data interface for management. If you did not set the IP address manually during initial setup, you can set it now using the **configure network** {**ipv4** | **ipv6**} **manual** command. If you did not already set the Management interface gateway to **data-interfaces**, this command will set it now.
- When you add the threat defense to CDO, CDO discovers and maintains the interface configuration, including the following settings: interface name and IP address, static route to the gateway, DNS servers, and DDNS server. For more information about the DNS server configuration, see below. In CDO, you can later make changes to the manager access interface configuration, but make sure you don't make changes that can prevent the threat defense or CDO from re-establishing the management connection. If the management connection is disrupted, the threat defense includes the **configure policy rollback** command to restore the previous deployment.
- If you configure a DDNS server update URL, the threat defense automatically adds certificates for all of the major CAs from the Cisco Trusted Root CA bundle so that the threat defense can validate the DDNS server certificate for the HTTPS connection. The threat defense supports any DDNS server that uses the DynDNS Remote API specification (https://help.dyn.com/remote-access-api/).
- This command sets the *data* interface DNS server. The Management DNS server that you set with the setup script (or using the **configure network dns servers** command) is used for management traffic. The data DNS server is used for DDNS (if configured) or for security policies applied to this interface.

  On CDO, the data interface DNS servers are configured in the Platform Settings policy that you assign to this threat defense. When you add the threat defense to CDO, the local setting is maintained, and the DNS servers are *not* added to a Platform Settings policy. However, if you later assign a Platform Settings policy to the threat defense that includes a DNS configuration, then that configuration will overwrite the

local setting. We suggest that you actively configure the DNS Platform Settings to match this setting to bring CDO and the threat defense into sync.

Also, local DNS servers are only retained by CDO if the DNS servers were discovered at initial registration. For example, if you registered the device using the Management interface, but then later configure a data interface using the **configure network management-data-interface** command, then you must manually configure all of these settings in CDO, including the DNS servers, to match the threat defense configuration.

- You can change the management interface after you register the threat defense to CDO, to either the Management interface or another data interface.
- The FQDN that you set in the setup wizard will be used for this interface.
- You can clear the entire device configuration as part of the command; you might use this option in a recovery scenario, but we do not suggest you use it for initial setup or normal operation.
- To disable data managemement, enter the **configure network management-data-interface disable** command.

Example:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]:
IP address (manual / dhcp) [dhcp]:
DDNS server update URL [none]:
https://deanwinchester:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow manager access from any network, if you wish to
change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

Example:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow manager access from any network, if you wish to
change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

Step 6 Identify the CDO that will manage this threat defense using the **configure manager add** command that CDO generated. See Onboard a Device with the Onboarding Wizard, on page 151 to generate the command.

Example:

```
> configure manager add account1.app.us.cdo.cisco.com KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
Lzm1HOynhVUWhXYWz2swmkj2ZWsN3Lb account1.app.us.cdo.cisco.com
Manager successfully configured.
```

Perform Initial Configuration Using the Device Manager

Connect to the device manager to perform initial setup of the threat defense. When you perform initial setup using the device manager, *all* interface configuration completed in the device manager is retained when you switch to CDO for management, in addition to the Management interface and manager access settings. Note that other default configuration settings, such as the access control policy or security zones, are not retained. 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 Connect your management computer to the Ethernet1/2 interface.

Step 2 Log in to the device manager.

a) Enter the following URL in your browser: **https://192.168.95.1**

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

c) You are prompted to read and accept the End User License Agreement and change the admin password.

Step 3 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 CDO 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.

   The Management interface settings are used even though you are enabling the manager access on a data interface. For example, the management traffic that is routed over the backplane through the data interface will resolve FQDNs using the Management interface DNS servers, and not the data interface DNS servers.

   DNS Servers—The DNS server for the system's management address. 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 system's management address.

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 in CDO.

d) Click **Finish**.

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

   The **Cloud Management** option is for legacy CDO/FDM functionality.

Step 4 (Might be required) Configure the Management interface. See the Management interface on **Device** > **Interfaces**.

The Management interface must have the gateway set to data interfaces. By default, the Management interface receives an IP address and gateway from DHCP. If you do not receive a gateway from DHCP (for example, you did not connect this interface to a network), then the gateway will default to data interfaces, and you do not need to configure anything. If you did receive a gateway from DHCP, then you need to instead configure this interface with a static IP address and set the gateway to data interfaces.

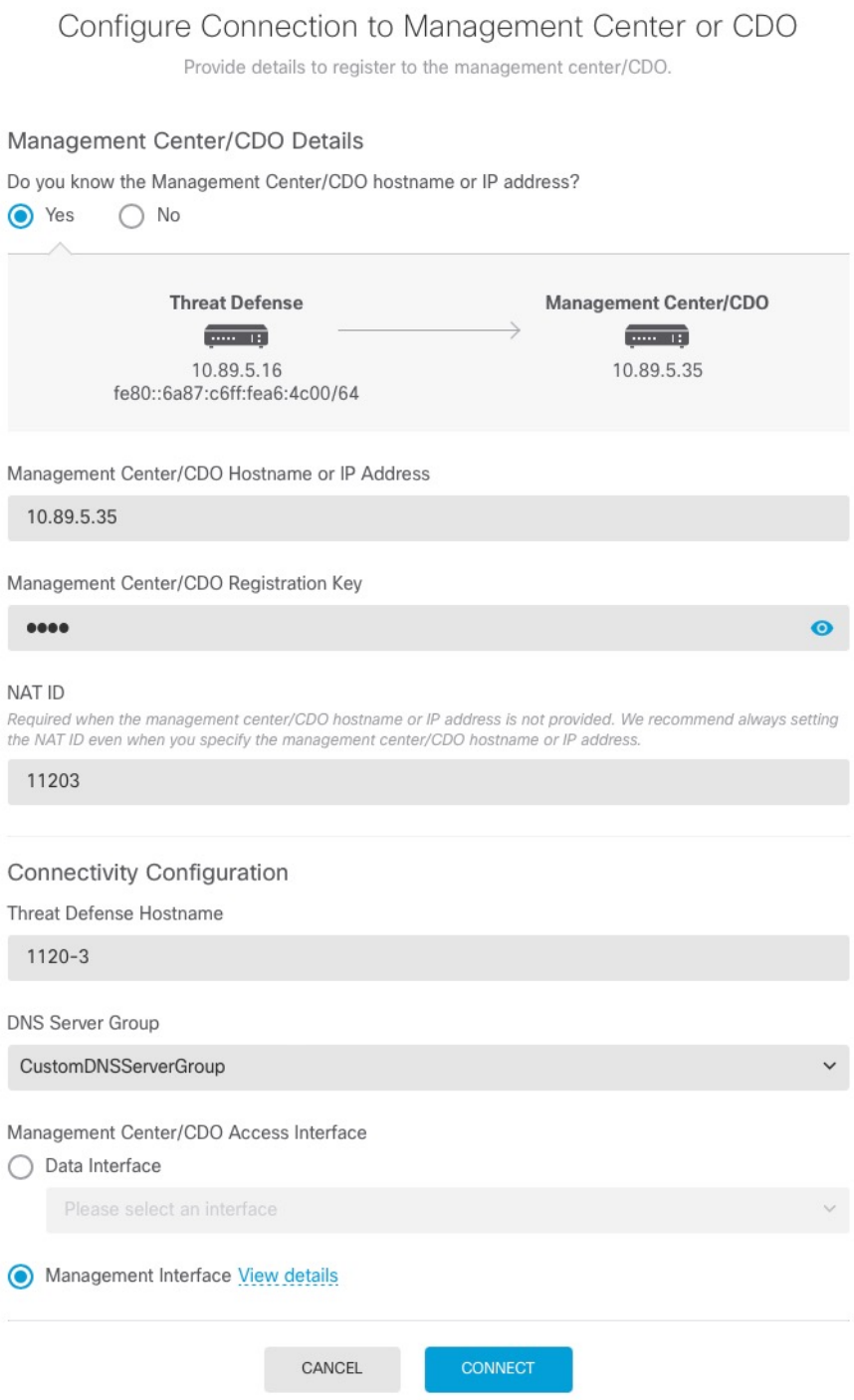
Step 5 If you want to configure additional interfaces, including an interface other than outside or inside that you want to use for the manager access, choose **Device**, and then click the link in the **Interfaces** summary.

See Configure the Firewall in the Device Manager, on page 124 for more information about configuring interfaces in the device manager. Other device manager configuration will not be retained when you register the device to CDO.

Step 6 Choose **Device** > **System Settings** > **Central Management**, and click **Proceed** to set up the management center management.

Step 7 Configure the **Management Center/CDO Details**.

Figure 103: Management Center/CDO Details



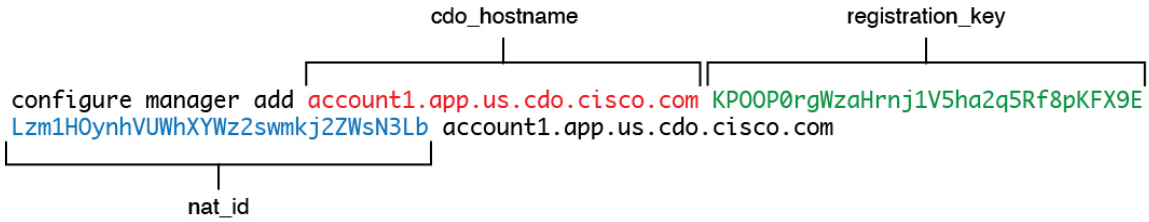
a) For **Do you know the Management Center/CDO hostname or IP address**, click **Yes**.

CDO generates the **configure manager add** command. See Onboard a Device with the Onboarding Wizard, on page 151 to generate the command.

configure manager add *cdo_hostname registration_key nat_id display_name*

Example:

Figure 104: configure manager add command components



b) Copy the *cdo_hostname*, *registration_key*, and *nat_id* parts of the command into the **Management Center/CDO Hostname/IP Address**, **Management Center/CDO Registration Key**, and **NAT ID** fields.

Step 8 Configure the **Connectivity Configuration**.

a) Specify the **FTD Hostname**.

This FQDN will be used for the outside interface, or whichever interface you choose for the **Management Center/CDO Access Interface**.

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.

This setting sets the *data* interface DNS server. The Management DNS server that you set with the setup wizard is used for management traffic. The data DNS server is used for DDNS (if configured) or for security policies applied to this interface. You are likley to choose the same DNS server group that you used for Management, because both management and data traffic reach the DNS server through the outside interface.

On CDO, the data interface DNS servers are configured in the Platform Settings policy that you assign to this threat defense. When you add the threat defense to CDO, the local setting is maintained, and the DNS servers are *not* added to a Platform Settings policy. However, if you later assign a Platform Settings policy to the threat defense that includes a DNS configuration, then that configuration will overwrite the local setting. We suggest that you actively configure the DNS Platform Settings to match this setting to bring CDO and the threat defense into sync.

Also, local DNS servers are only retained by CDO if the DNS servers were discovered at initial registration.

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

You can choose any configured interface, but this guide assumes you are using outside.

Step 9 If you chose a different data interface from outside, then add a default route.

You will see a message telling you to check that you have a default route through the interface. If you chose outside, you already configured this route as part of the setup wizard. If you chose a different interface, then you need to manually configure a default route before you connect to CDO. See Configure the Firewall in the Device Manager, on page 124 for more information about configuring static routes in the device manager.

Step 10 Click **Add a Dynamic DNS (DDNS) method**.

DDNS ensures CDO can reach the threat defense at its Fully-Qualified Domain Name (FQDN) if the threat defense's IP address changes. See **Device** > **System Settings** > **DDNS Service** to configure DDNS.

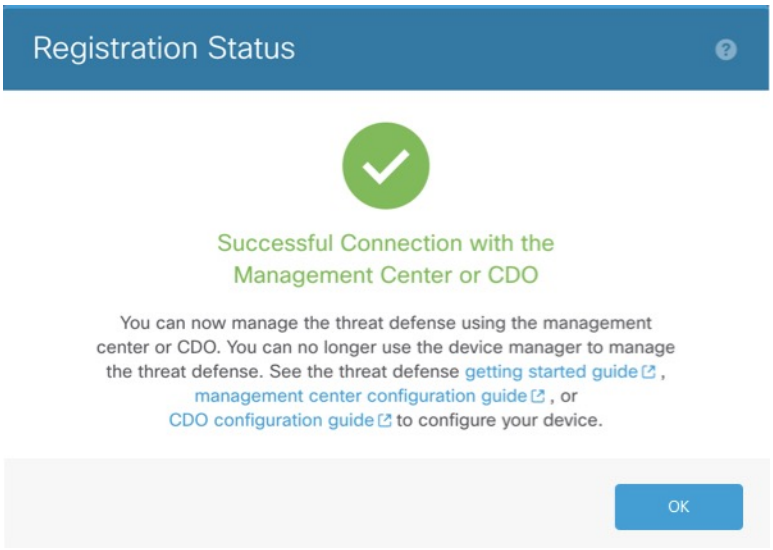
If you configure DDNS before you add the threat defense to CDO, the threat defense automatically adds certificates for all of the major CAs from the Cisco Trusted Root CA bundle so that the threat defense can validate the DDNS server certificate for the HTTPS connection. The threat defense supports any DDNS server that uses the DynDNS Remote API specification (https://help.dyn.com/remote-access-api/).

Step 11 Click **Connect**. The **Registration Status** dialog box shows the current status of the switch to CDO. After the **Saving Management Center/CDO Registration Settings** step, go to CDO, and add the firewall.

If you want to cancel the switch to CDO, 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 105: Successful Connection



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. You configured basic settings for the outside interface as part of the manager access setup, but you still need to assign it to a security zone.
- DHCP server—Use a DHCP server on the inside interface for clients.
- NAT—Use interface PAT on the outside interface.
- Access control—Allow traffic from inside to outside.
- SSH—Enable SSH on the manager access interface.

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.

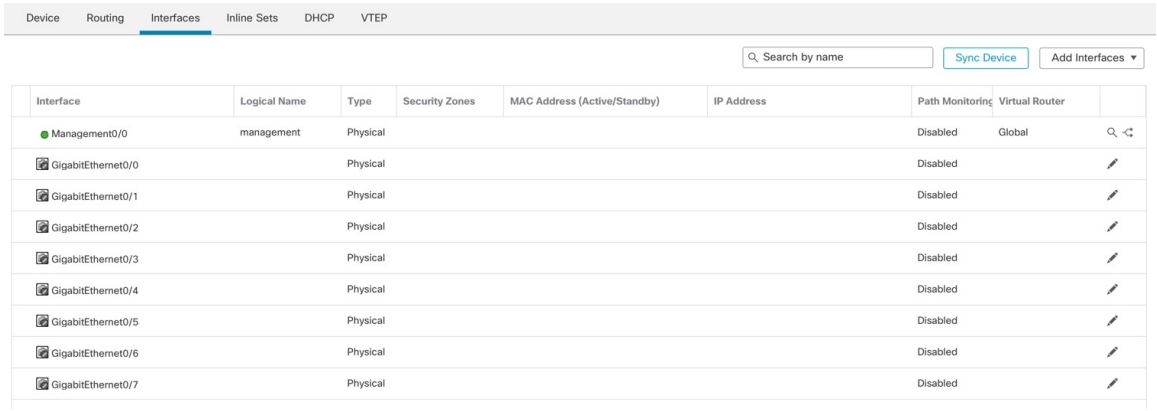
The following example configures a routed mode inside interface with a static address and a routed mode outside interface using DHCP.

Procedure

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

Step 2 Click **Interfaces**.

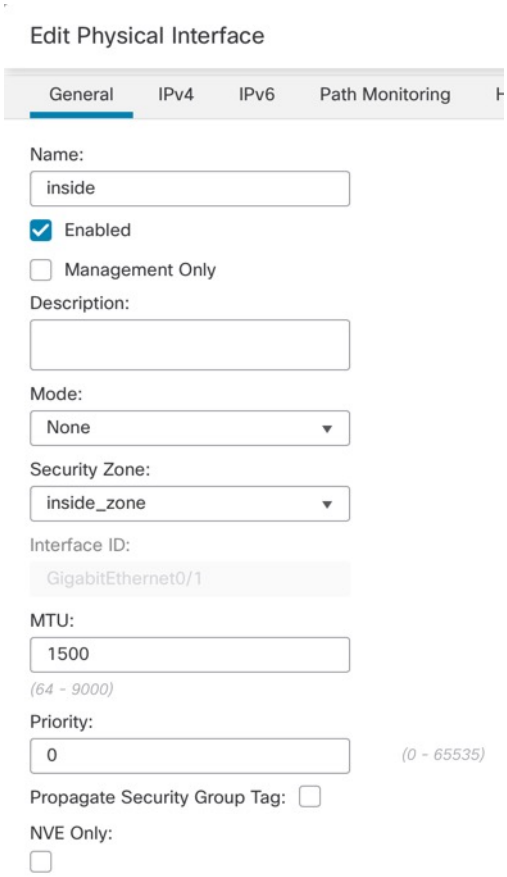
Figure 106: Interfaces



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

The **General** tab appears.

Figure 107: 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**.

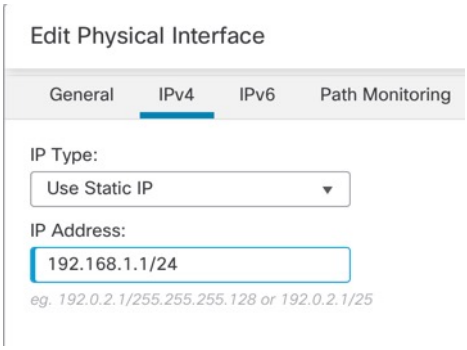
   For example, add a zone called **inside_zone**. Each interface must be assigned to a security zone and/or interface group. An interface can belong to only one security zone, but can also belong to multiple interface groups. You apply your security policy based on zones or groups. For example, you can 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.

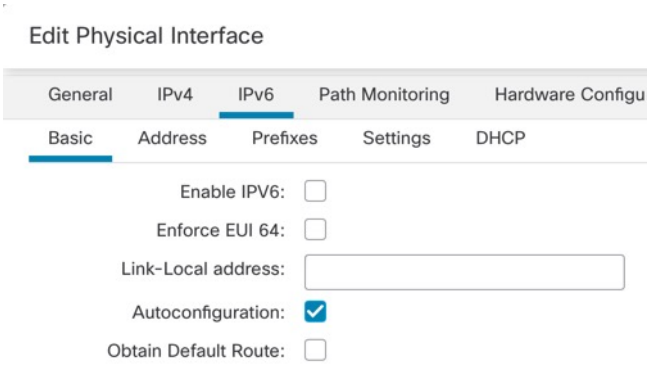
     For example, enter **192.168.1.1/24**

Figure 108: IPv4 Tab



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

Figure 109: IPv6 Tab

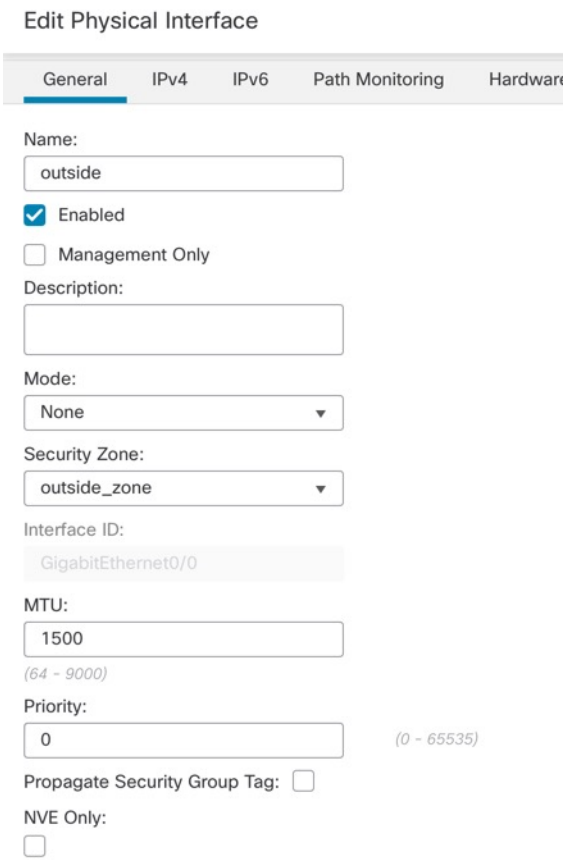


f) Click **OK**.

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

The **General** tab appears.

Figure 110: General Tab



You already pre-configured this interface for manager access, so 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 must still configure the Security Zone on this screen for through traffic policies.

a) 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**.

b) Click **OK**.

Step 5 Click **Save**.

Configure the DHCP Server

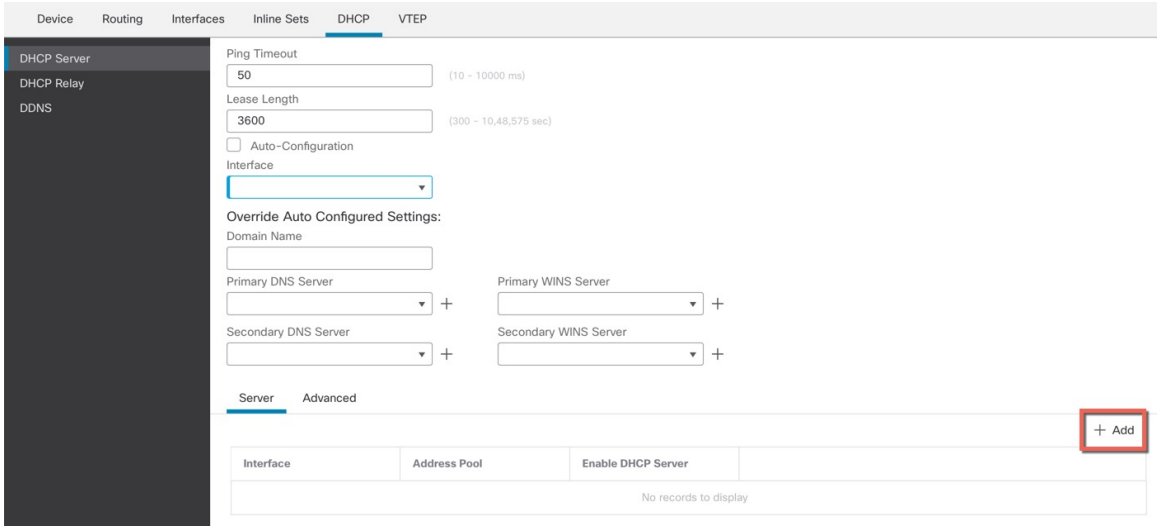
Enable the DHCP server if you want clients to use DHCP to obtain IP addresses from the threat defense.

Procedure

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

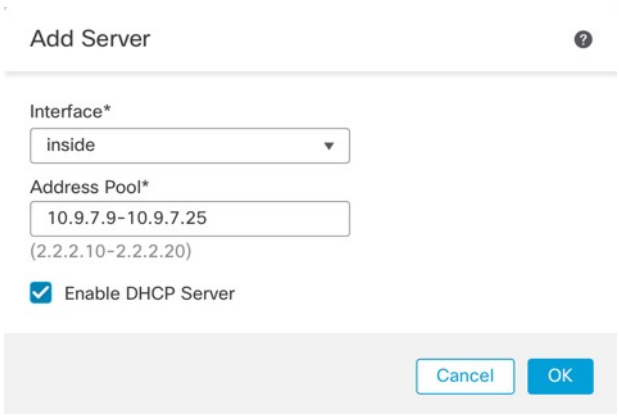
Step 2 Choose **DHCP** > **DHCP Server**.

Figure 111: DHCP Server



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

Figure 112: 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**.

Configure NAT

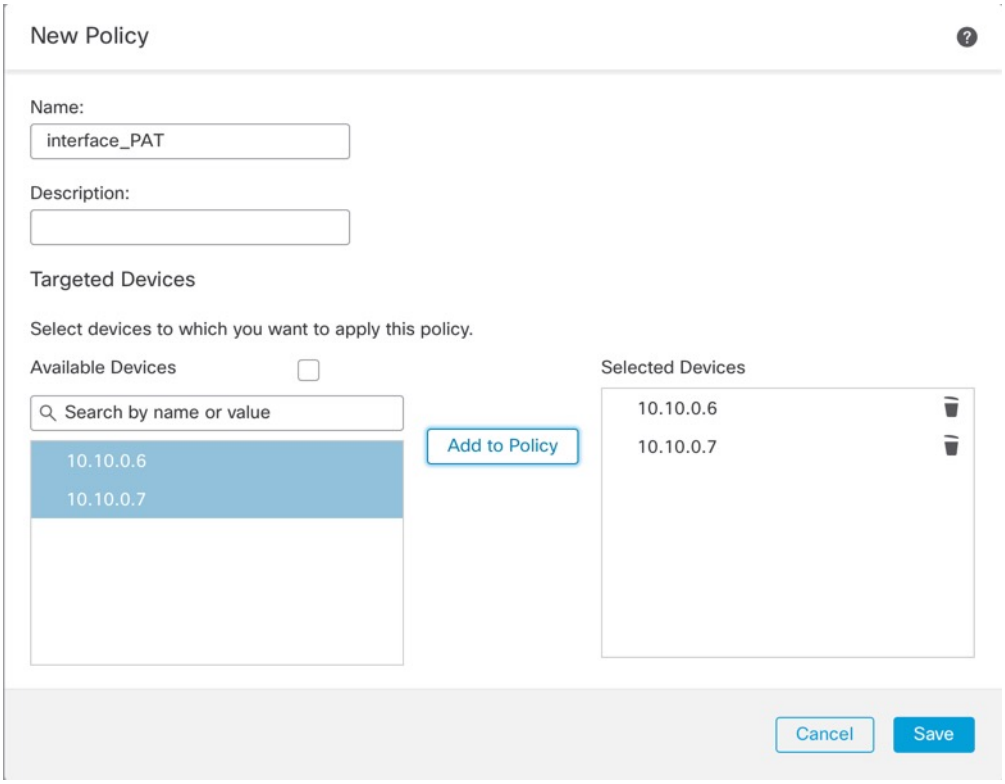
A typical NAT rule converts internal addresses to a port on the outside interface IP address. This type of NAT rule is called *interface Port Address Translation (PAT)*.

Procedure

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

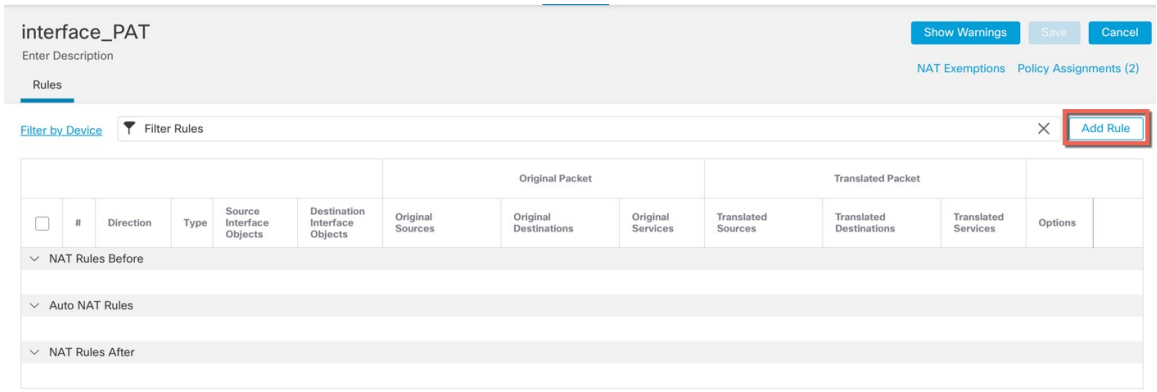
Step 2 Name the policy, select the device(s) that you want to use the policy, and click **Save**.

Figure 113: New Policy



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

Figure 114: NAT Policy

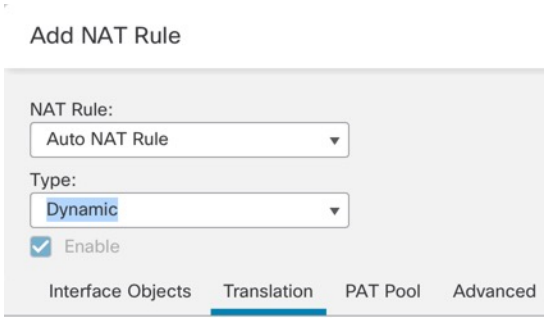


Step 3 Click **Add Rule**.

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

Step 4 Configure the basic rule options:

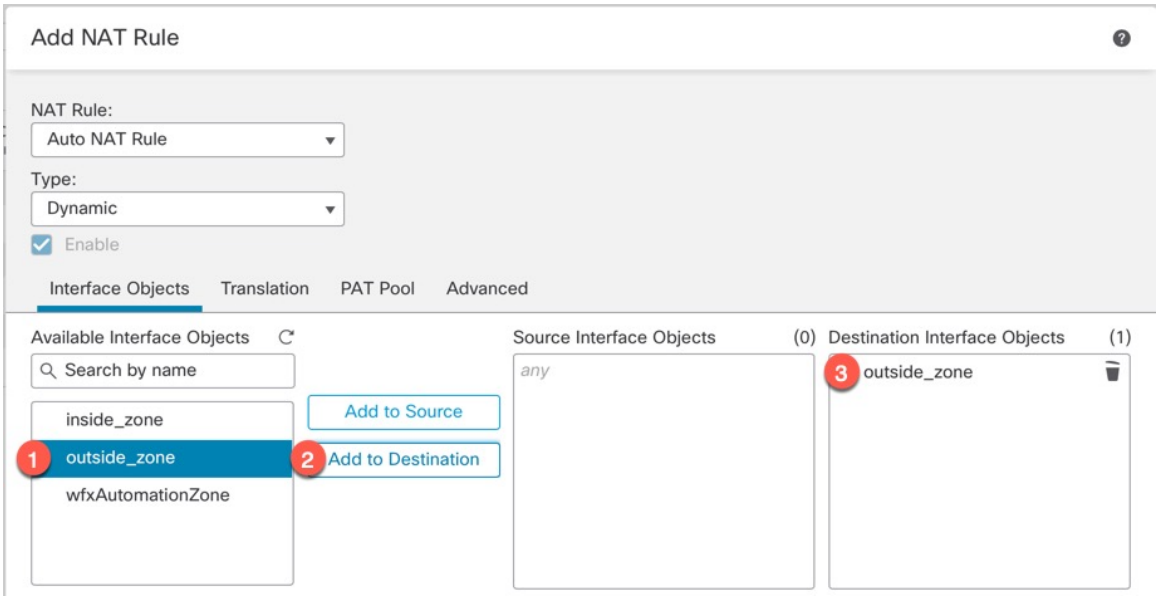
Figure 115: Basic Rule Options



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

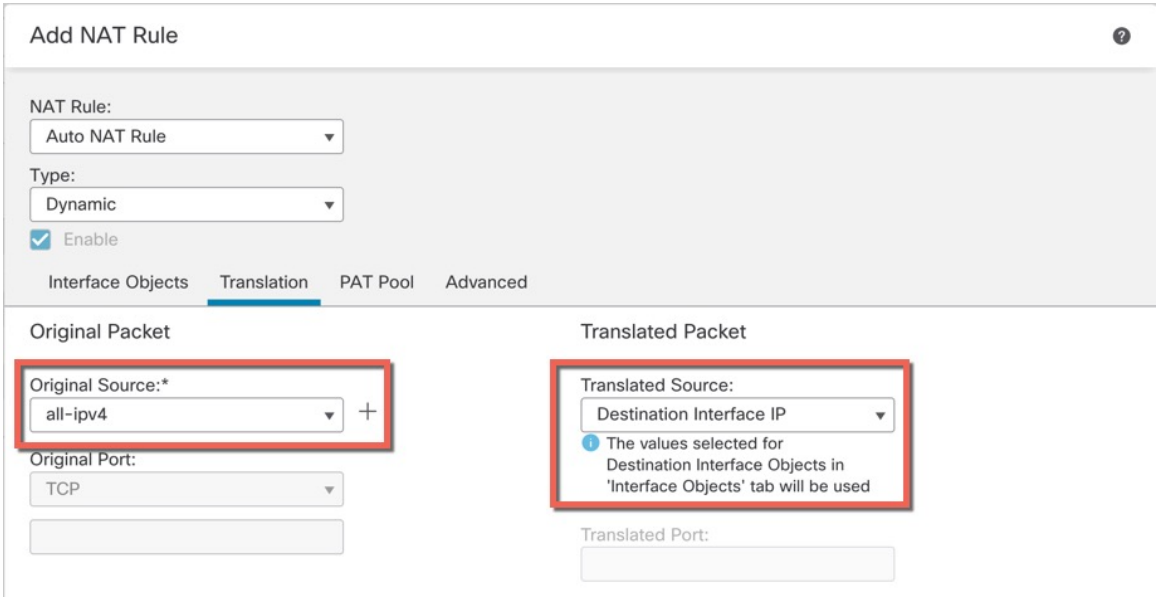
Step 5 On the **Interface Objects** page, add the outside zone from the **Available Interface Objects** area to the **Destination Interface Objects** area.

Figure 116: Interface Objects



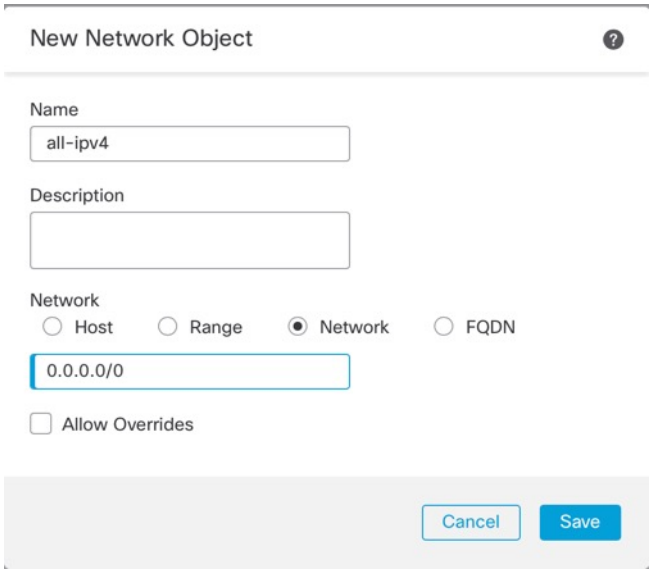
Step 6 On the **Translation** page, configure the following options:

Figure 117: Translation



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

Figure 118: New Network Object



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

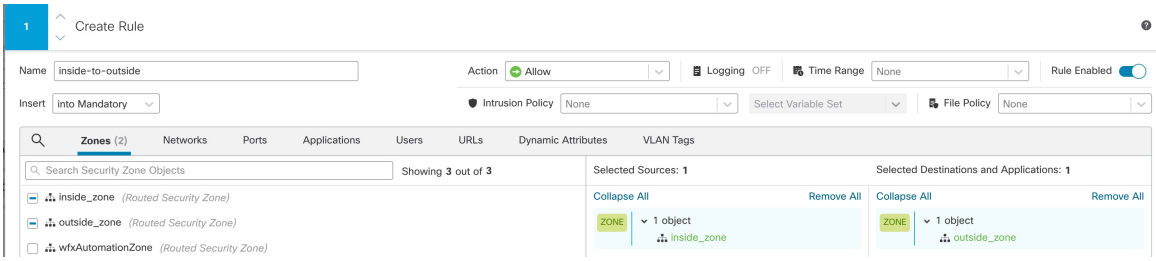
If you created a basic **Block all traffic** access control policy when you registered the threat defense, then you need to add rules to the policy to allow traffic through the device. The following procedure adds a rule to allow traffic from the inside zone to the outside zone. If you have other zones,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

Procedure

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

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

Figure 119: Add Rule



- **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**.

Configure SSH on the Manager Access Data Interface

If you enabled management center access on a data interface, such as outside, you should enable SSH on that interface using this procedure. This section describes how to enable SSH connections to one or more *data* interfaces on the threat defense.

Note SSH is enabled by default on the Management interface; however, this screen does not affect Management SSH access.

The Management interface is separate from the other interfaces on the device. It is used to set up and register the device to the management center. SSH for data interfaces shares the internal and external user list with SSH for the Management interface. Other settings are configured separately: for data interfaces, enable SSH and access lists using this screen; SSH traffic for data interfaces uses the regular routing configuration, and not any static routes configured at setup or at the CLI.

For the Management interface, to configure an SSH access list, see the **configure ssh-access-list** command in the Cisco Secure Firewall Threat Defense Command Reference. To configure a static route, see the **configure network static-routes** command. By default, you configure the default route through the Management interface at initial setup.

To use SSH, you do not also need an access rule allowing the host IP address. You only need to configure SSH access according to this section.

You can only SSH to a reachable interface; if your SSH host is located on the outside interface, you can only initiate a management connection directly to the outside interface.

Note After you make three consecutive failed attempts to log into the CLI using SSH, the device terminates the SSH connection.

Threat Defense Feature History

- 7.4—Loopback interface support for SSH.

Before you begin

- You can configure SSH internal users at the CLI using the **configure user add** command. By default, there is an **admin** user for which you configured the password during initial setup. You can also configure external users on LDAP or RADIUS by configuring **External Authentication** in platform settings.
- You need network objects that define the hosts or networks you will allow to make SSH connections to the device. You can add objects as part of the procedure, but if you want to use object groups to identify a group of IP addresses, ensure that the groups needed in the rules already exist. Select **Objects** > **Object Management** to configure objects.

Note You cannot use the system-provided **any** network object. Instead, use **any-ipv4** or **any-ipv6**.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the threat defense policy.

Step 2 Select **SSH Access**.

Step 3 Identify the interfaces and IP addresses that allow SSH connections.

Use this table to limit which interfaces will accept SSH connections, and the IP addresses of the clients who are allowed to make those connections. You can use network addresses rather than individual IP addresses.

a) Click **Add** to add a new rule, or click **Edit** to edit an existing rule.
b) Configure the rule properties:
   - **IP Address**—The network object or group that identifies the hosts or networks you are allowing to make SSH connections. Choose an object from the drop-down menu, or click + to add a new network object.
   - **Available Zones/Interfaces**—Add the zones that contain the interfaces to which you will allow SSH connections. For interfaces not in a zone, you can type the interface name into the field below the **Selected Zones/Interfaces** list and click **Add**. You can also add loopback interfaces. These rules will be applied to a device only if the device includes the selected interfaces or zones.
c) Click **OK**.

Step 4 Click **Save**.

You can now go to **Deploy** > **Deployment** and deploy the policy to assigned devices. The changes are not active until you deploy them.

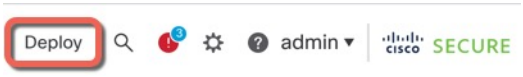
Deploy the Configuration

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 120: Deploy



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

Figure 121: Deploy All

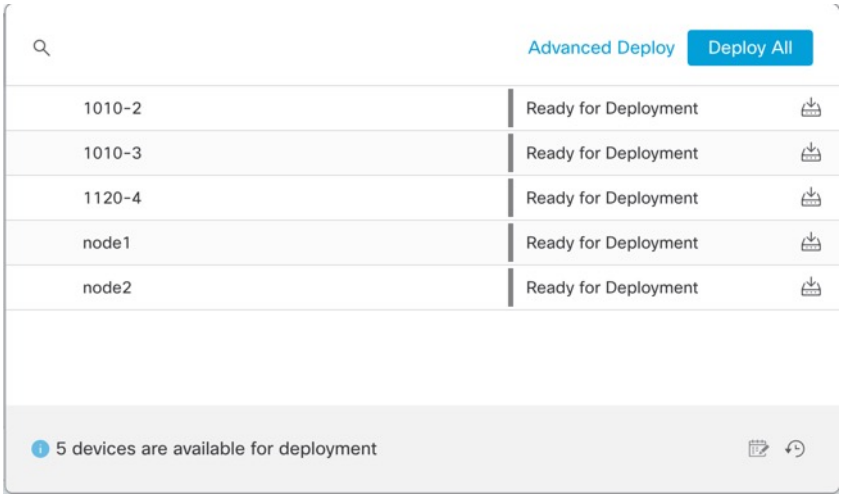
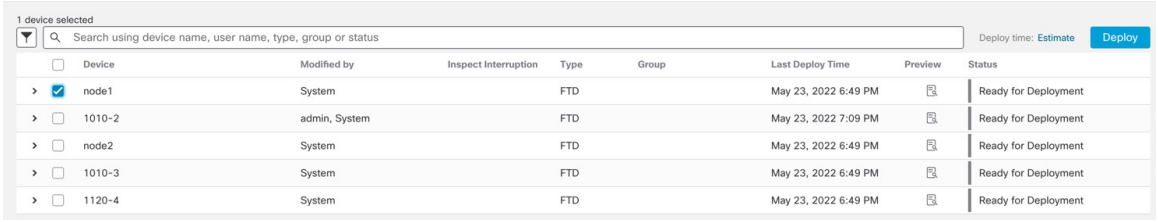
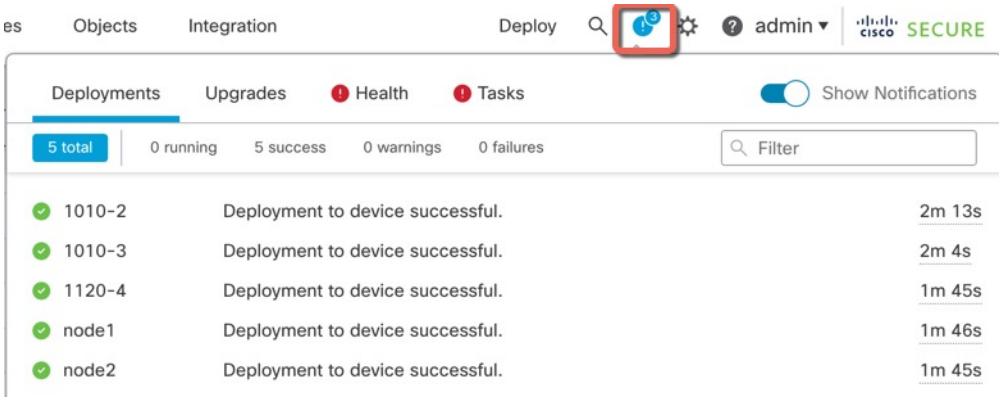


Figure 122: Advanced Deploy



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 123: Deployment Status



Troubleshooting and Maintenance

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 Firepower 2100 ships with a DB-9 to RJ-45 serial cable, so you may need 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#
```

Troubleshoot Management Connectivity on a Data Interface

When you use a data interface for manager access instead of using the dedicated Management interface, you must be careful about changing the interface and network settings for the threat defense in CDO so you do not disrupt the connection. If you change the management interface type after you add the threat defense to CDO (from data to Management, or from Management to data), if the interfaces and network settings are not configured correctly, you can lose management connectivity.

This topic helps you troubleshoot the loss of management connectivity.

View management connection status

In CDO, check the management connection status on the **Devices** > **Device Management** > **Device** > **Management** > **Manager Access - Configuration Details** > **Connection Status** page.

At the threat defense CLI, enter the **sftunnel-status-brief** command to view the management connection status. You can also use **sftunnel-status** to view more complete information.

See the following sample output for a connection that is down; there is no peer channel "connected to" information, nor heartbeat information shown:

```
> sftunnel-status-brief
PEER:10.10.17.202
Registration: Completed.
Connection to peer '10.10.17.202' Attempted at Mon Jun 15 09:21:57 2020 UTC
Last disconnect time : Mon Jun 15 09:19:09 2020 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

See the following sample output for a connection that is up, with peer channel and heartbeat information shown:

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
 via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202'
 via '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

View the threat defense network information

At the threat defense CLI, view the Management and manager access data interface network settings:

show network

```
> show network
===============[ System Information ]===============
Hostname                  : ftd-1
DNS Servers               : 208.67.220.220,208.67.222.222
Management port           : 8305
IPv4 Default route
  Gateway                 : data-interfaces
IPv6 Default route
  Gateway                 : data-interfaces

======================[ management0 ]=======================
State                     : Enabled
Link                      : Up
Channels                  : Management & Events
Mode                      : Non-Autonegotiation
MDI/MDIX                  : Auto/MDIX
MTU                       : 1500
MAC Address               : 28:6F:7F:D3:CB:8D
----------------------[ IPv4 ]----------------------
Configuration             : Manual
Address                   : 10.99.10.4
Netmask                   : 255.255.255.0
Gateway                   : 10.99.10.1
----------------------[ IPv6 ]----------------------
Configuration             : Disabled

===============[ Proxy Information ]================
State                     : Disabled
Authentication            : Disabled

======[ System Information - Data Interfaces ]======
DNS Servers               :
```

```
Interfaces               : Ethernet1/1

===============[ Ethernet1/1 ]===============
State                    : Enabled
Link                     : Up
Name                     : outside
MTU                      : 1500
MAC Address              : 28:6F:7F:D3:CB:8F
----------------------[ IPv4 ]----------------------
Configuration            : Manual
Address                  : 10.89.5.29
Netmask                  : 255.255.255.192
Gateway                  : 10.89.5.1
----------------------[ IPv6 ]----------------------
Configuration            : Disabled
```

Check that the threat defense registered with CDO

At the threat defense CLI, check that CDO registration was completed. Note that this command will not show the *current* status of the management connection.

show managers

```
> show managers
Type                     : Manager
Host                     : account1.app.us.cdo.cisco.com
Display name             : account1.app.us.cdo.cisco.com
Identifier               : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration             : Completed
Management type          : Configuration
```

Ping CDO

At the threat defense CLI, use the following command to ping CDO from the data interfaces:

ping *cdo_hostname*

At the threat defense CLI, use the following command to ping CDO from the Management interface, which should route over the backplane to the data interfaces:

ping system *cdo_hostname*

Capture packets on the threat defense internal interface

At the threat defense CLI, capture packets on the internal backplane interface (nlp_int_tap) to see if management packets are being sent:

capture *name* **interface nlp_int_tap trace detail match ip any any**

show capture*name* **trace detail**

Check the internal interface status, statistics, and packet count

At the threat defense CLI, see information about the internal backplane interface, nlp_int_tap:

show interace detail

```
> show interface detail
[...]
Interface Internal-Data0/1 "nlp_int_tap", is up, line protocol is up
  Hardware is en_vtun rev00, BW Unknown Speed-Capability, DLY 1000 usec
 (Full-duplex), (1000 Mbps)
```

```
 Input flow control is unsupported, output flow control is unsupported
 MAC address 0000.0100.0001, MTU 1500
 IP address 169.254.1.1, subnet mask 255.255.255.248
 37 packets input, 2822 bytes, 0 no buffer
 Received 0 broadcasts, 0 runts, 0 giants
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
 0 pause input, 0 resume input
 0 L2 decode drops
 5 packets output, 370 bytes, 0 underruns
 0 pause output, 0 resume output
 0 output errors, 0 collisions, 0 interface resets
 0 late collisions, 0 deferred
 0 input reset drops, 0 output reset drops
 input queue (blocks free curr/low): hardware (0/0)
 output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "nlp_int_tap":
 37 packets input, 2304 bytes
 5 packets output, 300 bytes
 37 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Control Point Interface States:
 Interface number is 14
 Interface config status is active
 Interface state is active
```

Check routing and NAT

At the threat defense CLI, check that the default route (S*) was added and that internal NAT rules exist for the Management interface (nlp_int_tap).

show route

```
> show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-ISinter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF
Gateway of last resort is 10.89.5.1 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 10.89.5.1, outside
C        10.89.5.0 255.255.255.192 is directly connected, outside
L        10.89.5.29 255.255.255.255 is directly connected, outside

>
```

show nat

```
> show nat

Auto NAT Policies (Section 2)
```

```
1 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_intf3 interface  service
 tcp 8305 8305
    translate_hits = 0, untranslate_hits = 6
2 (nlp_int_tap) to (outside) source static nlp_server_0_ssh_intf3 interface  service
tcp ssh ssh
    translate_hits = 0, untranslate_hits = 73
3 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_ipv6_intf3 interface
ipv6  service tcp 8305 8305
    translate_hits = 0, untranslate_hits = 0
4 (nlp_int_tap) to (outside) source dynamic nlp_client_0_intf3 interface
    translate_hits = 174, untranslate_hits = 0
5 (nlp_int_tap) to (outside) source dynamic nlp_client_0_ipv6_intf3 interface ipv6
    translate_hits = 0, untranslate_hits = 0
>
```

Check other settings

See the following commands to check that all other settings are present. You can also see many of these commands on CDO's **Devices** > **Device Management** > **Device** > **Management** > **Manager Access - Configuration Details** > **CLI Output** page.

show running-config sftunnel

```
> show running-config sftunnel
sftunnel interface outside
sftunnel port 8305
```

show running-config ip-client

```
> show running-config ip-client
ip-client outside
```

show conn address *fmc_ip*

```
> show conn address 10.89.5.35
5 in use, 16 most used
Inspect Snort:
        preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect

TCP nlp_int_tap  10.89.5.29(169.254.1.2):51231 outside  10.89.5.35:8305, idle 0:00:04,
 bytes 86684, flags UxIO
TCP nlp_int_tap  10.89.5.29(169.254.1.2):8305 outside  10.89.5.35:52019, idle 0:00:02,
 bytes 1630834, flags UIO
>
```

Check for a successful DDNS update

At the threat defense CLI, check for a successful DDNS update:

debug ddns

```
> debug ddns
DDNS update request = /v3/update?hostname=domain.example.org&myip=209.165.200.225
Successfuly updated the DDNS sever with current IP addresses
DDNS: Another update completed, outstanding = 0
DDNS: IDB SB total = 0
```

If the update failed, use the **debug http** and **debug ssl** commands. For certificate validation failures, check that the root certificates are installed on the device:

show crypto ca certificates *trustpoint_name*

To check the DDNS operation:

show ddns update interface *fmc_access_ifc_name*

```
> show ddns update interface outside

Dynamic DNS Update on outside:
    Update Method Name Update Destination
    RBD_DDNS not available

Last Update attempted on 04:11:58.083 UTC Thu Jun 11 2020
Status : Success
FQDN : domain.example.org
IP addresses : 209.165.200.225
```

Check CDO log files

See https://cisco.com/go/fmc-reg-error.

Roll Back the Configuration if CDO Loses Connectivity

If you use a data interface on the threat defense for manager access, and you deploy a configuration change from CDO that affects the network connectivity, you can roll back the configuration on the threat defense to the last-deployed configuration so you can restore management connectivity. You can then adjust the configuration settings in CDO so that the network connectivity is maintained, and re-deploy. You can use the rollback feature even if you do not lose connectivity; it is not limited to this troubleshooting situation.

See the following guidelines:

- Only the previous deployment is available locally on the threat defense; you cannot roll back to any earlier deployments.
- The rollback only affects configurations that you can set in CDO. For example, the rollback does not affect any local configuration related to the dedicated Management interface, which you can only configure at the threat defense CLI. Note that if you changed data interface settings after the last CDO deployment using the **configure network management-data-interface** command, and then you use the rollback command, those settings will not be preserved; they will roll back to the last-deployed CDO settings.
- Out-of-band SCEP certificate data that was updated during the previous deployment cannot be rolled back.
- During the rollback, connections will drop because the current configuration will be cleared.

Procedure

Step 1 At the threat defense CLI, roll back to the previous configuration.

configure policy rollback

After the rollback, the threat defense notifies CDO that the rollback was completed successfully. In CDO, the deployment screen will show a banner stating that the configuration was rolled back.

Note If the rollback failed and CDO management is restored, refer to https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw-virtual/215258-troubleshooting-firepower-threat-defense.html for common deployment problems. In some cases, the rollback can fail after CDO management access is restored; in this case, you can resolve the CDO configuration issues, and redeploy from CDO.

Example:

For the threat defense that uses a data interface for manager access:

```
> configure policy rollback

The last deployment to this FTD was on June 1, 2022 and its status was Successful.
Do you want to continue [Y/N]?

Y

Rolling back complete configuration on the FTD. This will take time.
.....................
Policy rollback was successful on the FTD.
Configuration has been reverted back to transaction id:
Following is the rollback summary:
...................
.....................
>
```

Step 2 Check that the management connection was reestablished.

In CDO, check the management connection status on the **Devices** > **Device Management** > **Device** > **Management** > **Manager Access - Configuration Details** > **Connection Status** page.

At the threat defense CLI, enter the **sftunnel-status-brief** command to view the management connection status.

If it takes more than 10 minutes to reestablish the connection, you should troubleshoot the connection. See Troubleshoot Management Connectivity on a Data Interface, on page 176.

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 CDO

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 Device 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 175.

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]
```

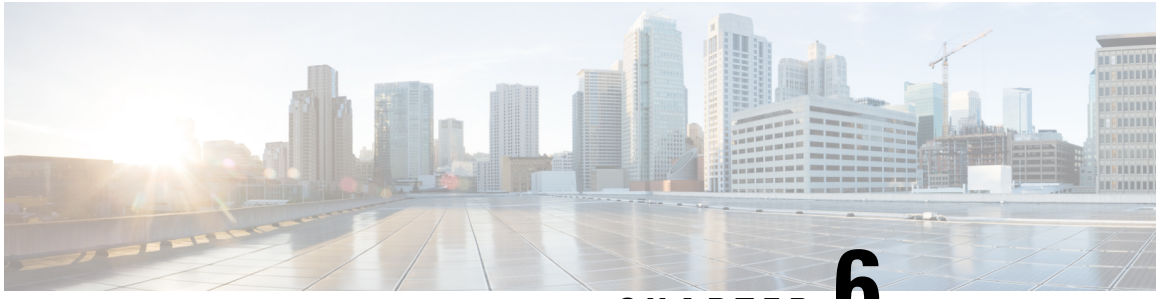
Step 4 You can now turn off the power switch and unplug the power to physically remove power from the chassis if necessary.

What's Next

To continue configuring your threat defense using CDO, see the Cisco Defense Orchestrator home page.

PART I

ASA Deployment with ASDM



CHAPTER 6

ASA Appliance Mode Deployment with ASDM

Is This Chapter for You?

The Firepower 2100 runs an underlying operating system called the FXOS. You can run the Firepower 2100 for ASA in the following modes:

- Appliance mode (the default)—Appliance mode lets you configure all settings in the ASA. Only advanced troubleshooting commands are available from the FXOS CLI. See the FXOS troubleshooting guide for more information. The chassis manager is not supported.
- Platform mode—When in Platform mode, you must configure basic operating parameters and hardware interface settings in FXOS. These settings include enabling interfaces, establishing EtherChannels, NTP, image management, and more. You can use the chassis manager web interface or FXOS CLI. You can then configure your security policy in the ASA operating system using ASDM or the ASA CLI.

This chapter describes how to deploy the Firepower 2100 in your network in ASA Appliance mode. By default, the Firepower 2100 runs in Appliance mode; to use Platform mode, see ASA Platform Mode Deployment with ASDM and Chassis Manager, on page 207. This chapter does not cover the following deployments, for which you should refer to the ASA configuration guide:

- Failover
- CLI configuration

This chapter also walks you through configuring a basic security policy; if you have more advanced requirements, refer to the configuration guide.

The Firepower 2100 hardware can run either ASA software or threat defense software. Switching between ASA and threat defense requires you to reimage the device. See Reimage the Cisco ASA or Firepower Threat Defense Device.

Privacy Collection Statement—The Firepower 2100 does not require or actively collect personally-identifiable information. However, you can use personally-identifiable information in the configuration, for example for usernames. In this case, an administrator might be able to see this information when working with the configuration or when using SNMP.

About the ASA

The ASA provides advanced stateful firewall and VPN concentrator functionality in one device.

Unsupported Features

The following ASA features are not supported on the Firepower 2100:

- Integrated Routing and Bridging
- Redundant interfaces
- Clustering
- Clientless SSL VPN with KCD
- ASA REST API
- ASA FirePOWER module
- Botnet Traffic Filter
- The following inspections:
  - SCTP inspection maps (SCTP stateful inspection using ACLs is supported)
  - Diameter
  - GTP/GPRS

Migrating an ASA 5500-X Configuration

You can copy and paste an ASA 5500-X configuration into the Firepower 2100 in Appliance Mode. However, you will need to modify your configuration. Also note some behavioral differences between the platforms.

1. To copy the configuration, enter the **more system:running-config** command on the ASA 5500-X.
2. Edit the configuration as necessary (see below).
3. Connect to the console port of the Firepower 2100 in Appliance Mode, and enter global configuration mode:

```
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
```

```
ciscoasa# configure terminal
ciscoasa(config)#
```

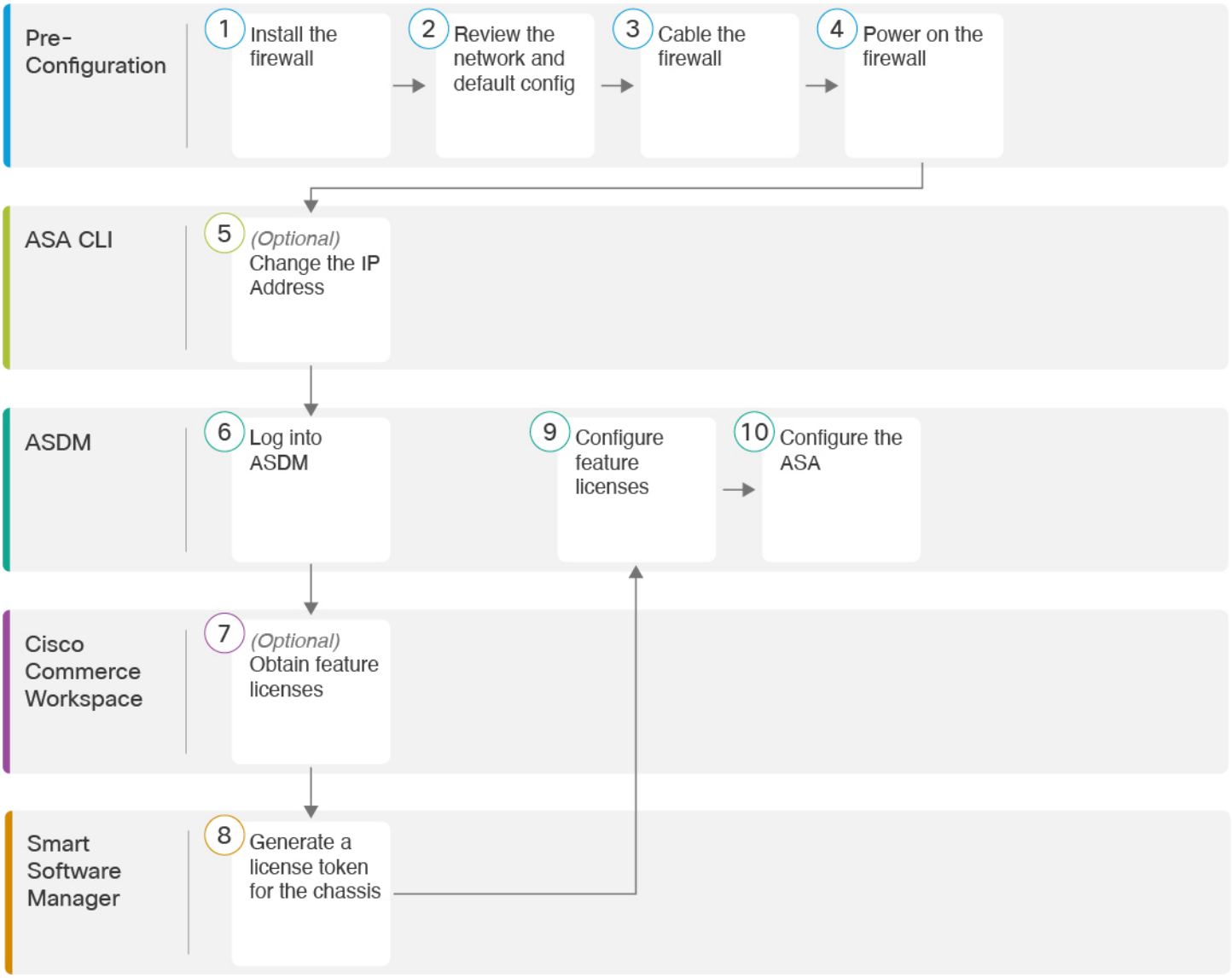
4. Clear the current configuration using the **clear configure all** command.
5. Paste the modified configuration at the ASA CLI.

This guide assumes a factory default configuration, so if you paste in an existing configuration, some of the procedures in this guide will not apply to your ASA.

ASA 5500-X Configuration	Firepower 2100 in Appliance Mode Configuration
PAK License	Smart License PAK licensing is not applied when you copy and paste your configuration. There are no licenses installed by default. Smart Licensing requires that you connect to the Smart Licensing server to obtain your licenses. Smart Licensing also affects ASDM or SSH access (see below).
Initial ASDM access	Remove any VPN or other strong encryption feature configuration—even if you only configured weak encryption—if you cannot connect to ASDM or register with the Smart Licensing server. You can reenable these features after you obtain the Strong Encryption (3DES) license. The reason for this issue is that the ASA includes 3DES capability by default for management access only. If you enable a strong encryption feature, then ASDM and HTTPS traffic (like that to and from the Smart Licensing server) are blocked. The exception to this rule is if you are connected to a management-only interface, such as Management 1/1. SSH is not affected.
Interface IDs	Make sure you change the interface IDs to match the new hardware IDs. For example, the ASA 5525-X includes Management 0/0, and GigabitEthernet 0/0 through 0/5. The Firepower 1120 includes Management 1/1 and Ethernet 1/1 through 1/8.
boot system commands The ASA 5500-X allows up to four **boot system** commands to specify the booting image to use.	The Firepower 2100 in Appliance Mode only allows a single **boot system** command, so you should remove all but one command before you paste. You actually do not need to have *any* **boot system** commands present in your configuration, as it is not read at startup to determine the booting image. The last-loaded boot image will always run upon reload. The **boot system** command performs an action when you enter it: the system validates and unpacks the image and copies it to the boot location (an internal location on disk0 managed by FXOS). The new image will load when you reload the ASA.

End-to-End Tasks

See the following tasks to deploy and configure the ASA.



1	Pre-Configuration	Install the firewall. See the hardware installation guide.
2	Pre-Configuration	Review the Network Deployment and Default Configuration, on page 191.
3	Pre-Configuration	Cable the Device, on page 193.

4	Pre-Configuration	Power on the Firewall, on page 194.
5	ASA CLI	(Optional) Change the IP Address, on page 195.
6	ASDM	Log Into ASDM, on page 196.
7	Cisco Commerce Workspace	Configure Licensing, on page 197: Obtain feature licenses.
8	Smart Software Manager	Configure Licensing, on page 197: Generate a license token for the chassis.
9	ASDM	Configure Licensing, on page 197: Configure feature licenses.
10	ASDM	Configure the ASA, on page 203.

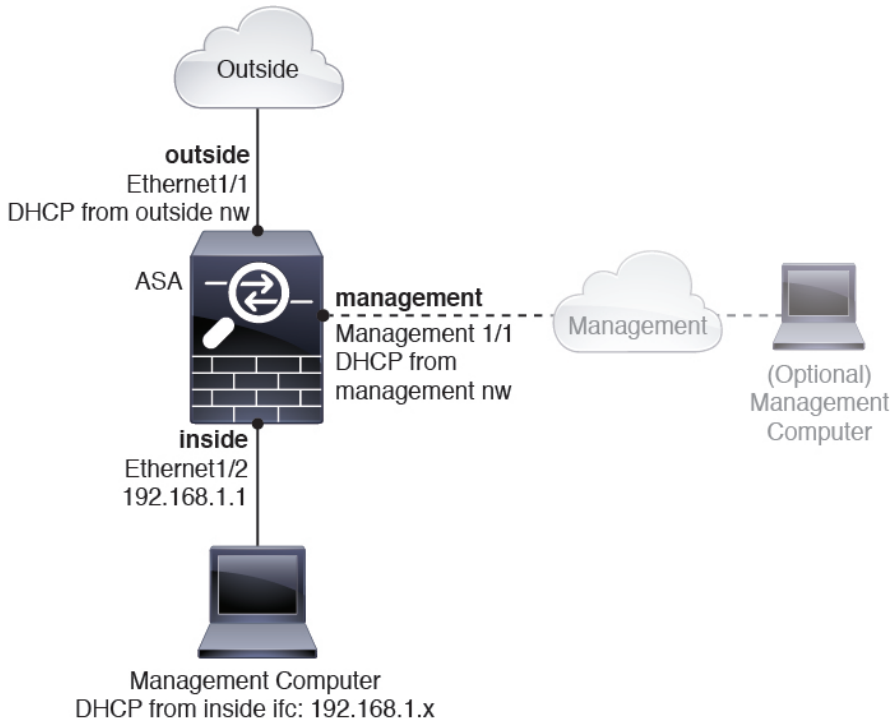
Review the Network Deployment and Default Configuration

The following figure shows the default network deployment for the Firepower 2100 using the default configuration in ASA Appliance mode.

If you connect the outside interface directly to a cable modem or DSL modem, we recommend that you put the modem into bridge mode so the ASA performs all routing and NAT for your inside networks. If you need to configure PPPoE for the outside interface to connect to your ISP, you can do so as part of the ASDM Startup Wizard.

Note If you cannot use the default inside IP address for ASDM access, you can set the inside IP address at the ASA CLI. See (Optional) Change the IP Address, on page 195. For example, you may need to change the inside IP address in the following circumstances:

- If the outside interface tries to obtain an IP address on the 192.168.1.0 network, which is a common default network, the DHCP lease will fail, and the outside interface will not obtain an IP address. This problem occurs because the ASA cannot have two interfaces on the same network. In this case you must change the inside IP address to be on a new network.
- If you add the ASA to an existing inside network, you will need to change the inside IP address to be on the existing network.



Firepower 2100 Appliance Mode Default Configuration

The Firepower 2100 runs in Appliance mode by default.

Note For pre-9.13(1) versions, Platform mode was the default and only option. If you upgrade from Platform mode, Platform mode is maintained.

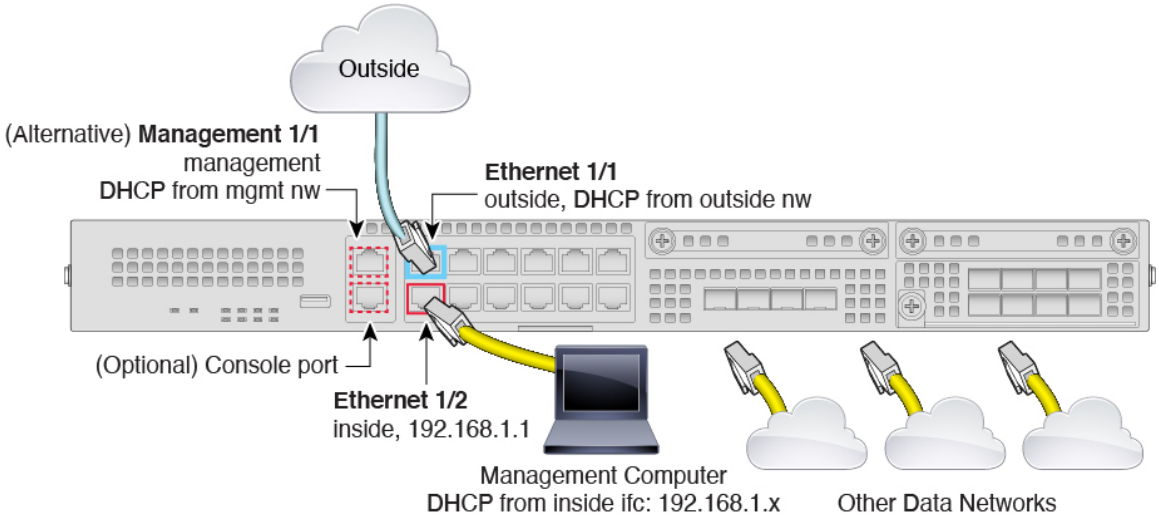
The default factory configuration for the Firepower 2100 in Appliance mode configures the following:

- **inside→outside traffic flow**—Ethernet 1/1 (outside), Ethernet 1/2 (inside)
- **outside IP address** from DHCP, **inside IP address**—192.168.1.1
- **management IP address** from DHCP—Management 1/1 (management)
- **DHCP server** on inside interface
- **Default routes** from outside DHCP, management DHCP
- **ASDM** access—Management and inside hosts allowed. Inside hosts are limited to the 192.168.1.0/24 network.
- **NAT**—Interface PAT for all traffic from inside to outside.
- **DNS** servers—OpenDNS servers are pre-configured.

The configuration consists of the following commands:

```
interface Management1/1
  management-only
  nameif management
  security-level 100
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/2
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
  no shutdown
!
object network obj_any
  subnet 0.0.0.0 0.0.0.0
  nat (any,outside) dynamic interface
!
http server enable
http 0.0.0.0 0.0.0.0 management
http 192.168.1.0 255.255.255.0 management
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd enable inside
!
dns domain-lookup outside
dns server-group DefaultDNS
   name-server 208.67.222.222 outside
   name-server 208.67.220.220 outside
!
```

Cable the Device



Manage the Firepower 2100 on either Management 1/1 or Ethernet 1/2. The default configuration also configures Ethernet1/1 as outside.

Procedure

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

Step 2 Connect your management computer to either of the following interfaces:

- Management 1/1 (labeled MGMT)—Connect Management 1/1 to your management network, and make sure your management computer is on—or has access to—the management network. Management 1/1 obtains an IP address from a DHCP server on your management network; if you use this interface, you must determine the IP address assigned to the ASA so that you can connect to the IP address from your management computer.
- Ethernet 1/2—Connect your management computer directly to Ethernet 1/2 for initial configuration. Or connect Ethernet 1/2 to your inside network; make sure your management computer is on the inside network, because only clients on that network can access the ASA. Ethernet 1/2 has a default IP address (192.168.1.1) and also runs a DHCP server to provide IP addresses to clients (including the management computer), so make sure these settings do not conflict with any existing inside network settings (see Firepower 2100 Appliance Mode Default Configuration, on page 192).

  If you need to change the Ethernet 1/2 IP address from the default, you must also cable your management computer to the console port. See (Optional) Change the IP Address, on page 195.

You can later configure ASA management access from other interfaces; see the ASA general operations configuration guide.

Step 3 Connect the outside network to the Ethernet1/1 interface (labeled WAN).

For Smart Software Licensing, the ASA needs internet access so that it can access the License Authority.

Step 4 Connect other networks to the remaining interfaces.

Power on the Firewall

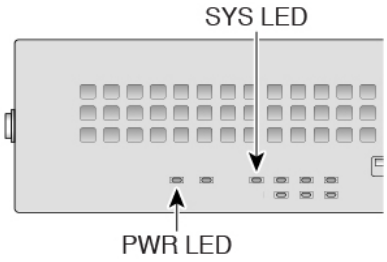
The power switch is located to the left of power supply module 1 on the rear of the chassis. It is a toggle switch that controls power to the system. If the power switch is in standby position, only the 3.3-V standby power is enabled from the power supply module and the 12-V main power is OFF. When the switch is in the ON position, the 12-V main power is turned on and the system boots.

Procedure

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

Step 2 Press the power switch on the back of the device.

Step 3 Check the PWR LED on the front of the device; if it is solid green, the device is powered on.



Step 4 Check the SYS LED on the front of the device; after it is solid green, the system has passed power-on diagnostics.

Note Before you move the power switch to the OFF position, use the shutdown commands so that the system can perform a graceful shutdown. This may take several minutes to complete. After the graceful shutdown is complete, the console displays `It is safe to power off now`. The front panel blue locator beacon LED lights up indicating the system is ready to be powered off. You can now move the switch to the OFF position. The front panel PWR LED flashes momentarily and turns off. Do not remove the power until the PWR LED is completely off.

See the FXOS Configuration Guide for more information on using the shutdown commands.

(Optional) Change the IP Address

If you cannot use the default IP address for ASDM access, you can set the IP address of the inside interface at the ASA CLI.

Note This procedure restores the default configuration and also sets your chosen IP address, so if you made any changes to the ASA configuration that you want to preserve, do not use this procedure.

Procedure

Step 1 Connect to the ASA console port, and enter global configuration mode. See Access the ASA and FXOS CLI, on page 204 for more information.

Step 2 Restore the default configuration with your chosen IP address.

configure factory-default [*ip_address* [*mask*]]

Note This command does not clear the currently-set mode, Appliance or Platform, for the Firepower 2100.

Example:

```
ciscoasa(config)# configure factory-default 10.1.1.151 255.255.255.0
Based on the management IP address and mask, the DHCP address
pool size is reduced to 103 from the platform limit 256
```

```
WARNING: The boot system configuration will be cleared.
The first image found in disk0:/ will be used to boot the
system on the next reload.
Verify there is a valid image on disk0:/ or the system will
not boot.

Begin to apply factory-default configuration:
Clear all configuration
Executing command: interface ethernet1/2
Executing command: nameif inside
INFO: Security level for "inside" set to 100 by default.
Executing command: ip address 10.1.1.151 255.255.255.0
Executing command: security-level 100
Executing command: no shutdown
Executing command: exit
Executing command: http server enable
Executing command: http 10.1.1.0 255.255.255.0 management
Executing command: dhcpd address 10.1.1.152-10.1.1.254 management
Executing command: dhcpd enable management
Executing command: logging asdm informational
Factory-default configuration is completed
ciscoasa(config)#
```

Step 3 Save the default configuration to flash memory.

write memory

Log Into ASDM

Launch ASDM so you can configure the ASA.

The ASA includes 3DES capability by default for management access only, so you can connect to the Smart Software Manager and also use ASDM immediately. You can also use SSH and SCP if you later configure SSH access on the ASA. Other features that require strong encryption (such as VPN) must have Strong Encryption enabled, which requires you to first register to the Smart Software Manager.

Note If you attempt to configure any features that can use strong encryption before you register—even if you only configure weak encryption—then your HTTPS connection will be dropped on that interface, and you cannot reconnect. The exception to this rule is if you are connected to a management-only interface, such as Management 1/1. SSH is not affected. If you lose your HTTPS connection, you can connect to the console port to reconfigure the ASA, connect to a management-only interface, or connect to an interface not configured for a strong encryption feature.

Before you begin

- See the ASDM release notes on Cisco.com for the requirements to run ASDM.

Procedure

Step 1 Enter the following URL in your browser.

- **https://192.168.1.1**—Inside (Ethernet 1/2) interface IP address.
- **https://***management_ip*—Management interface IP address assigned from DHCP.

Note Be sure to specify **https://**, and not **http://** or just the IP address (which defaults to HTTP); the ASA does not automatically forward an HTTP request to HTTPS.

The **Cisco ASDM** web page appears. You may see browser security warnings because the ASA does not have a certificate installed; you can safely ignore these warnings and visit the web page.

Step 2 Click **Install ASDM Launcher**.

Step 3 Follow the onscreen instructions to launch ASDM.

The **Cisco ASDM-IDM Launcher** appears.

Step 4 Leave the username and password fields empty, and click **OK**.

The main ASDM window appears.

Configure Licensing

The ASA uses Smart Licensing. You can use regular Smart Licensing, which requires internet access; or for offline management, you can configure Permanent License Reservation or a Smart Software Manager On-Prem (formerly known as a Satellite server). For more information about these offline licensing methods, see Cisco ASA Series Feature Licenses; this guide applies to regular Smart Licensing.

For a more detailed overview on Cisco Licensing, go to cisco.com/go/licensingguide

When you register the chassis, the Smart Software Manager issues an ID certificate for communication between the firewall and the Smart Software Manager. It also assigns the firewall to the appropriate virtual account. Until you register with the Smart Software Manager, you will not be able to make configuration changes to features requiring special licenses, but operation is otherwise unaffected. Licensed features include:

- Essentials
- Security Contexts
- Strong Encryption (3DES/AES)—If your Smart Account is not authorized for strong encryption, but Cisco has determined that you are allowed to use strong encryption, you can manually add a stong encryption license to your account.
- Cisco Secure Client—Secure Client Advantage, Secure Client Premier, or Secure Client VPN Only.

The ASA includes 3DES capability by default for management access only, so you can connect to the Smart Software Manager and also use ASDM immediately. You can also use SSH and SCP if you later configure SSH access on the ASA. Other features that require strong encryption (such as VPN) must have Strong Encryption enabled, which requires you to first register to the Smart Software Manager.

Note If you attempt to configure any features that can use strong encryption before you register—even if you only configure weak encryption—then your HTTPS connection will be dropped on that interface, and you cannot reconnect. The exception to this rule is if you are connected to a management-only interface, such as Management 1/1. SSH is not affected. If you lose your HTTPS connection, you can connect to the console port to reconfigure the ASA, connect to a management-only interface, or connect to an interface not configured for a strong encryption feature.

When you request the registration token for the ASA from the Smart Software Manager, check the **Allow export-controlled functionality on the products registered with this token** check box so that the full Strong Encryption license is applied (your account must be qualified for its use). The Strong Encryption license is automatically enabled for qualified customers when you apply the registration token on the chassis, so no additional action is required. If your Smart Account is not authorized for strong encryption, but Cisco has determined that you are allowed to use strong encryption, you can manually add a strong encryption license to your account.

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.

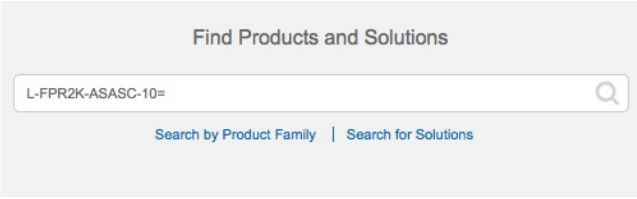
- Your Smart Software Manager account must qualify for the Strong Encryption (3DES/AES) license to use some features (enabled using the export-compliance flag).

Procedure

Step 1 Make sure your Smart Licensing account contains the available licenses you need, including at a minimum the Essentials license.

When you bought your device from Cisco or a reseller, your licenses should have been linked to your Smart Software Manager 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 124: License Search



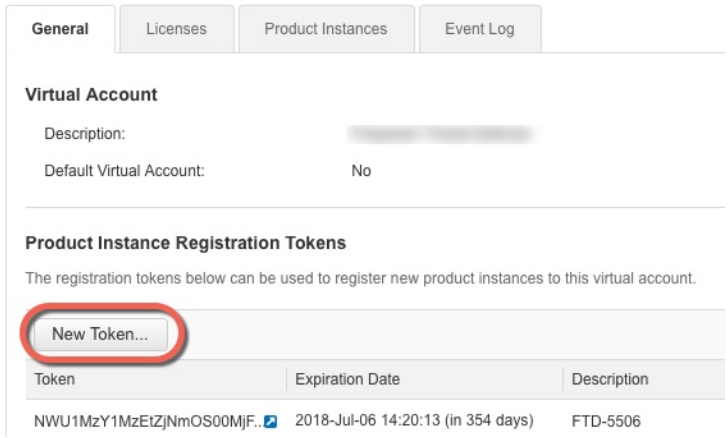
- Essentials license—L-FPR2100-ASA=. The Essentials license is free, but you still need to add it to your Smart Software Licensing account.
- 5 context license—L-FPR2K-ASASC-5=. Context licenses are additive; buy multiple licenses to meet your needs.

- 10 context license—L-FPR2K-ASASC-10=. Context licenses are additive; buy multiple licenses to meet your needs.
- Strong Encryption (3DES/AES) license—L-FPR2K-ENC-K9=. Only required if your account is not authorized for strong encryption.
- Cisco Secure Client—See the Cisco Secure Client Ordering Guide. You do not enable this license directly in the ASA.

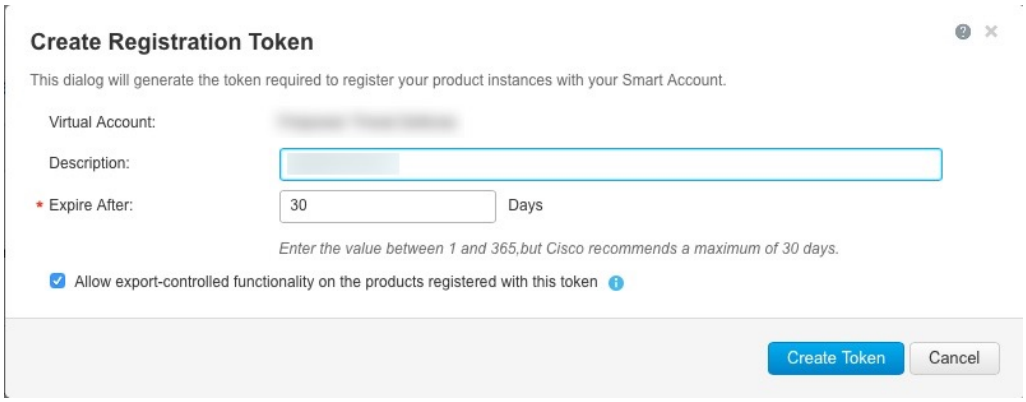
Step 2 In the Cisco Smart Software Manager, request and copy a registration token for the virtual account to which you want to add this device.

a) Click **Inventory**.

b) On the **General** tab, click **New Token**.



c) On the **Create Registration Token** dialog box enter the following settings, and then click **Create Token**:



- **Description**

- **Expire After**—Cisco recommends 30 days.
- **Allow export-controlled functionaility on the products registered with this token**—Enables the export-compliance flag.

The token is added to your inventory.

d) Click the arrow icon to the right of the token to open the **Token** dialog box so you can copy the token ID to your clipboard. Keep this token ready for later in the procedure when you need to register the ASA.

Figure 125: View Token

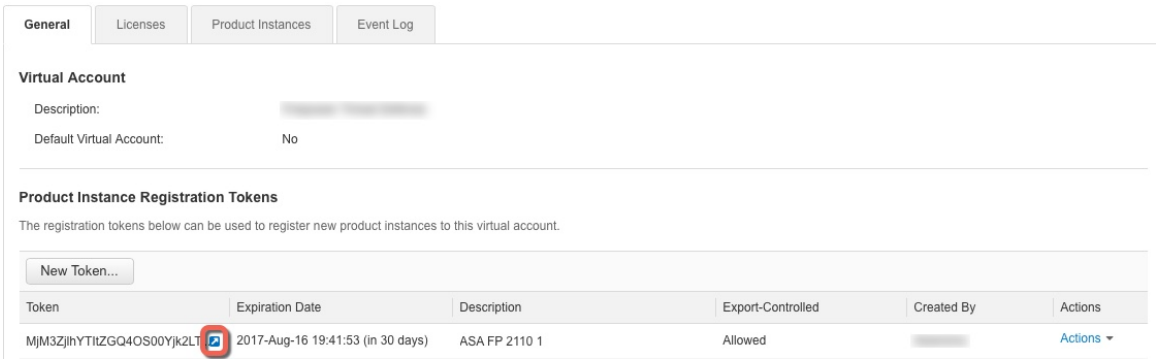
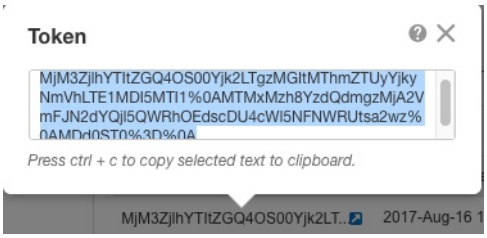
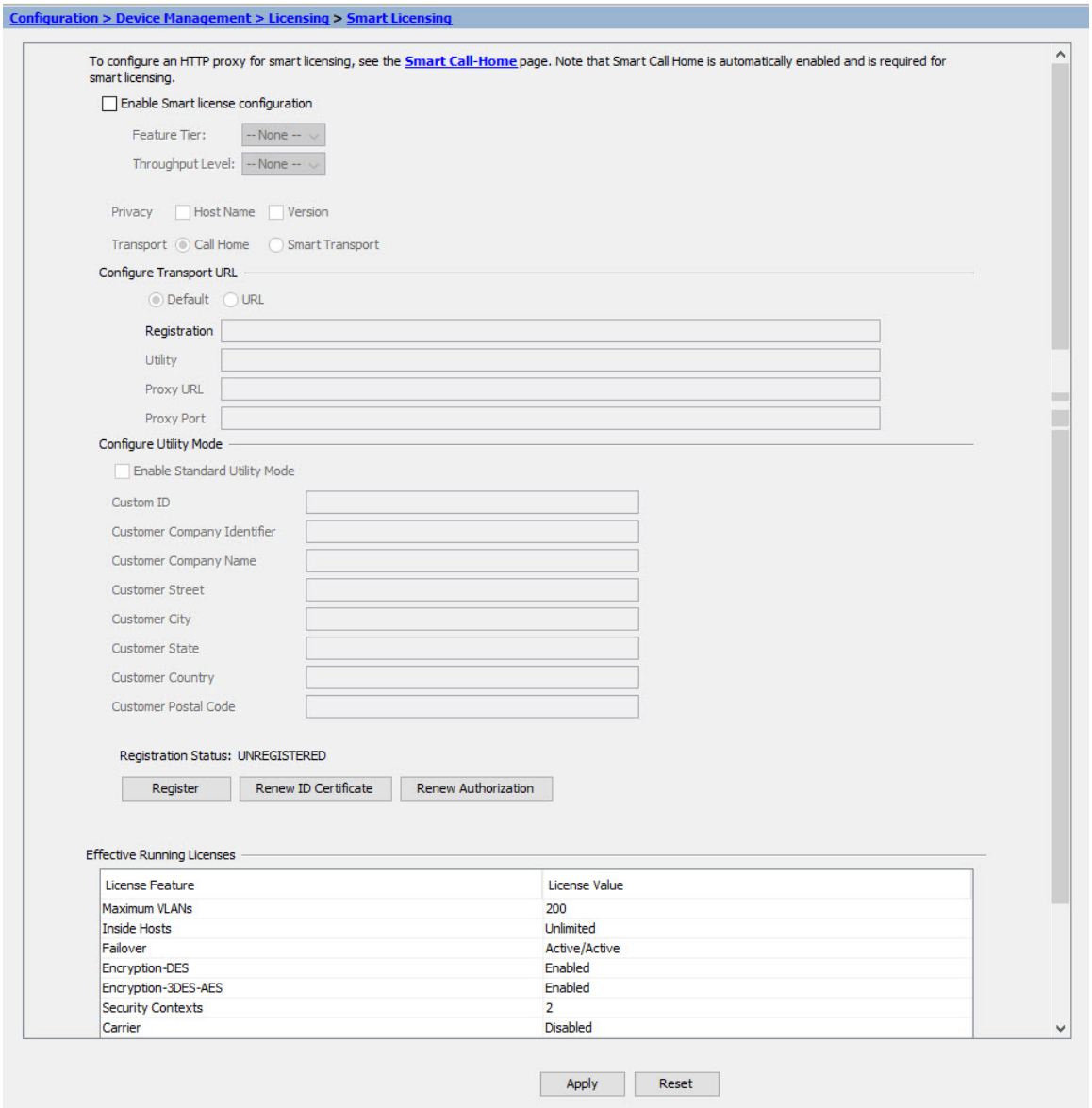


Figure 126: Copy Token

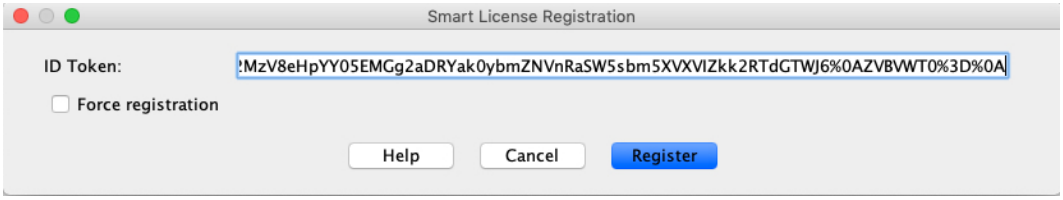


Step 3 In ASDM, choose **Configuration** > **Device Management** > **Licensing** > **Smart Licensing**.

Step 4 Click **Register**.



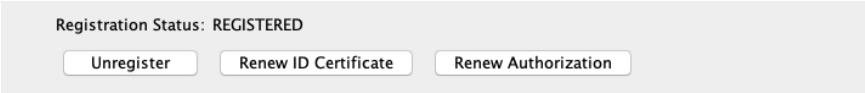
Step 5 Enter the registration token in the **ID Token** field.



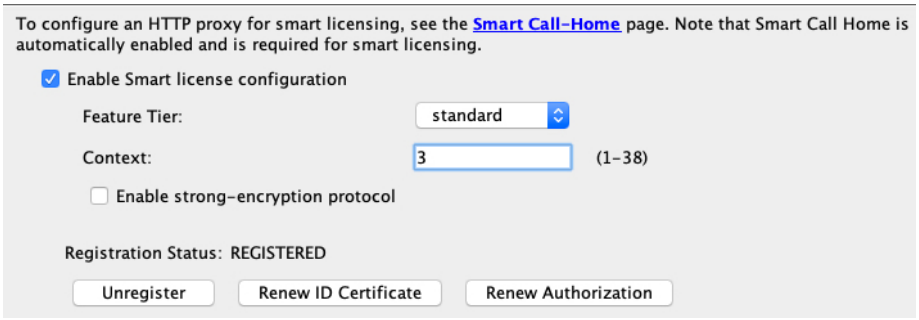
You can optionally check the **Force registration** check box to register the ASA that is already registered, but that might be out of sync with the Smart Software Manager. For example, use **Force registration** if the ASA was accidentally removed from the Smart Software Manager.

Step 6 Click **Register**.

The ASA registers with the Smart Software Manager using the pre-configured outside interface, and requests authorization for the configured license entitlements. The Smart Software Manager also applies the Strong Encryption (3DES/AES) license if your account allows. ASDM refreshes the page when the license status is updated. You can also choose **Monitoring** > **Properties** > **Smart License** to check the license status, particularly if the registration fails.



Step 7 Set the following parameters:



a) Check **Enable Smart license configuration**.

b) From the **Feature Tier** drop-down list, choose **Essentials**.

Only the Essentials tier is available.

c) (Optional) For the **Context** license, enter the number of contexts.

You can use 2 contexts without a license. The maximum number of contexts depends on your model:

- Firepower 2110—25 contexts
- Firepower 2120—25 contexts
- Firepower 2130—30 contexts
- Firepower 2140—40 contexts

For example, to use the maximum of 25 contexts on the Firepower 2110, enter 23 for the number of contexts; this value is added to the default of 2.

Step 8 Click **Apply**.

Step 9 Click the **Save** icon in the toolbar.

Step 10 Quit ASDM and relaunch it.

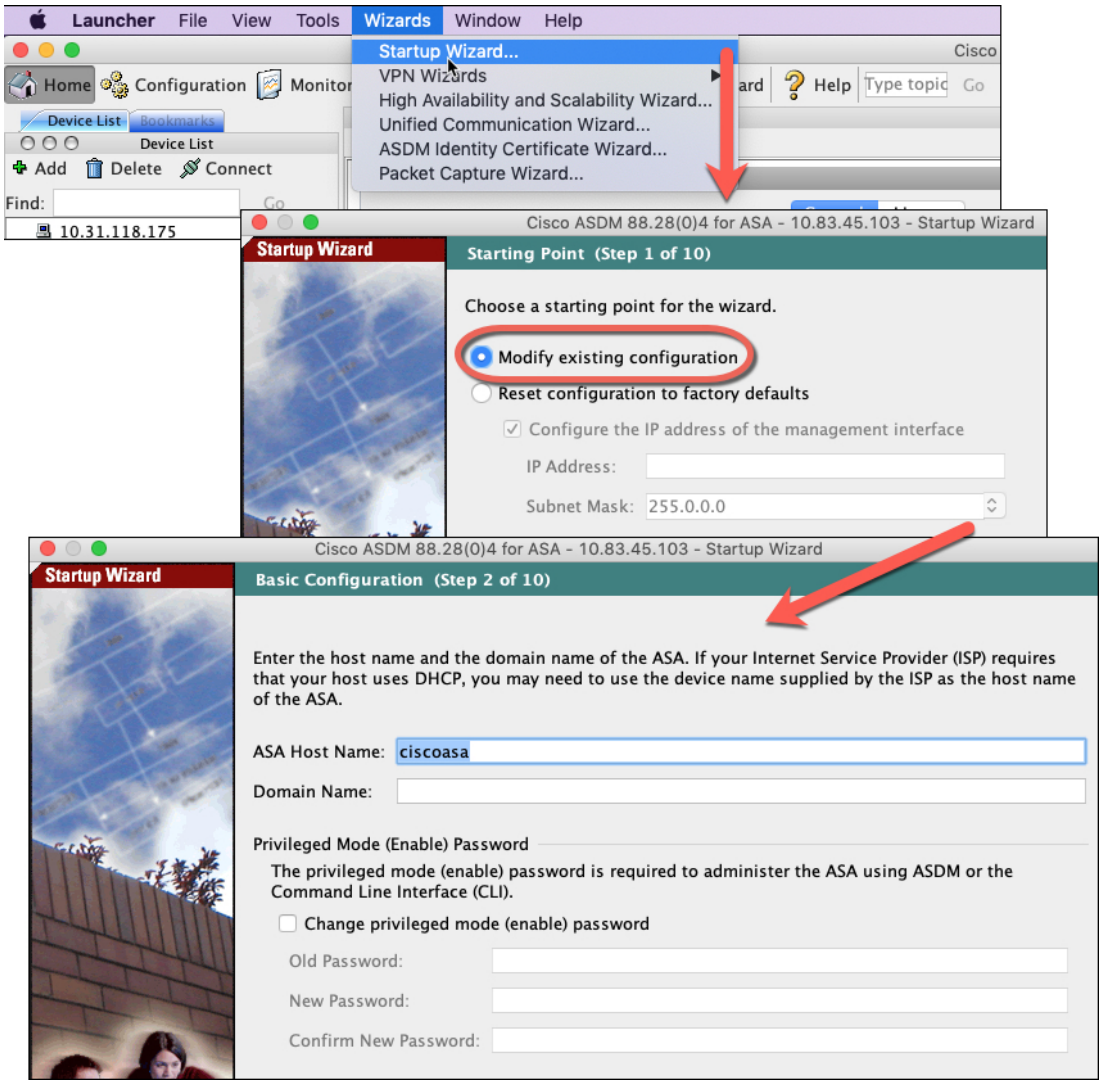
When you change licenses, you need to relaunch ASDM to show updated screens.

Configure the ASA

Using ASDM, you can use wizards to configure basic and advanced features. You can also manually configure features not included in wizards.

Procedure

Step 1 Choose **Wizards** > **Startup Wizard**, and click the **Modify existing configuration** radio button.



Step 2 The **Startup Wizard** walks you through configuring:

- The enable password
- Interfaces, including setting the inside and outside interface IP addresses and enabling interfaces.
- Static routes

- The DHCP server
- And more...

Step 3 (Optional) From the **Wizards** menu, run other wizards.

Step 4 To continue configuring your ASA, see the documents available for your software version at Navigating the Cisco ASA Series Documentation.

Access the ASA and FXOS CLI

You can use the ASA CLI to troubleshoot or configure the ASA instead of using ASDM. You can access the CLI by connecting to the console port. You can later configure SSH access to the ASA on any interface; SSH access is disabled by default. See the ASA general operations configuration guide for more information.

You can also access the FXOS CLI from the ASA CLI for troubleshooting purposes.

Procedure

Step 1 Connect your management computer to the console port. Be sure to install any necessary serial drivers for your operating system. Use the following serial settings:

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

You connect to the ASA CLI. There are no user credentials required for console access by default.

Step 2 Access privileged EXEC mode.

enable

You are prompted to change the password the first time you enter the **enable** command.

Example:

```
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
ciscoasa#
```

The enable password that you set on the ASA is also the FXOS **admin** user password if the ASA fails to boot up, and you enter FXOS failsafe mode.

All non-configuration commands are available in privileged EXEC mode. You can also enter configuration mode from privileged EXEC mode.

To exit privileged EXEC mode, enter the **disable**, **exit**, or **quit** command.

Step 3 Access global configuration mode.

configure terminal

Example:

```
ciscoasa# configure terminal
ciscoasa(config)#
```

You can begin to configure the ASA from global configuration mode. To exit global configuration mode, enter the **exit**, **quit**, or **end** command.

Step 4 (Optional) Connect to the FXOS CLI.

connect fxos [**admin**]

- **admin**—Provides admin-level access. Without this option, users have read-only access. Note that no configuration commands are available even in admin mode.

You are not prompted for user credentials. The current ASA username is passed through to FXOS, and no additional login is required. To return to the ASA CLI, enter **exit** or type **Ctrl-Shift-6**, **x**.

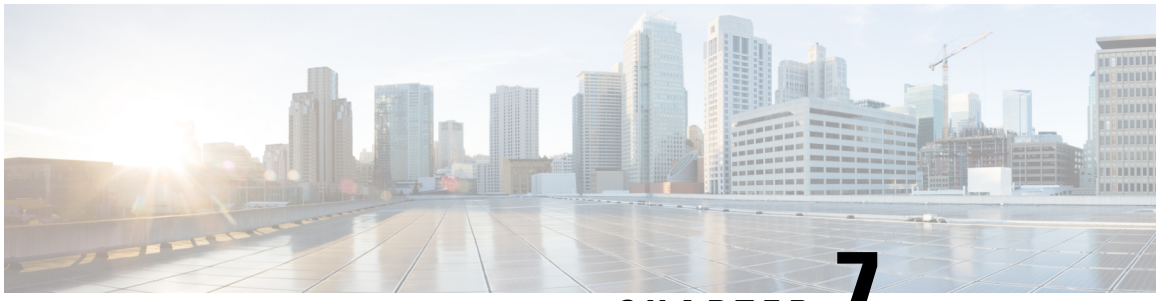
Within FXOS, you can view user activity using the **scope security/show audit-logs** command.

Example:

```
ciscoasa# connect fxos admin
Connecting to fxos.
Connected to fxos. Escape character sequence is 'CTRL-^X'.
firepower#
firepower# exit
Connection with FXOS terminated.
Type help or '?' for a list of available commands.
ciscoasa#
```

What's Next?

- To continue configuring your ASA, see the documents available for your software version at Navigating the Cisco ASA Series Documentation.
- For troubleshooting, see the FXOS troubleshooting guide.



CHAPTER 7

ASA Platform Mode Deployment with ASDM and Chassis Manager

Is This Chapter for You?

The Firepower 2100 runs an underlying operating system called the FXOS. You can run the Firepower 2100 for ASA in the following modes:

- Platform mode—When in Platform mode, you must configure basic operating parameters and hardware interface settings in FXOS. These settings include enabling interfaces, establishing EtherChannels, NTP, image management, and more. You can use the chassis manager web interface or FXOS CLI. You can then configure your security policy in the ASA operating system using ASDM or the ASA CLI. For the full FXOS configuration guide, see the FXOS ASA configuration guide. For FXOS troubleshooting commands, see the FXOS troubleshooting guide.

Note For many interface **show** commands, you either cannot use the ASA commands or the commands lack the full statistics. You must view more detailed interface information using FXOS commands. See the FXOS troubleshooting guide for more information.

- Appliance mode (the default)—Appliance mode lets you configure all settings in the ASA. Only advanced troubleshooting commands are available from the FXOS CLI.

This chapter describes how to deploy the Firepower 2100 in your network in ASA Platform mode. By default, the Firepower 2100 runs in Appliance mode, so this chapter tells you how to set the mode to Platform mode. This chapter does not cover the following deployments, for which you should refer to the ASA configuration guide:

- Failover
- CLI configuration

This chapter also walks you through configuring a basic security policy; if you have more advanced requirements, refer to the configuration guide.

The Firepower 2100 hardware can run either ASA software or threat defense software. Switching between ASA and threat defense requires you to reimage the device. See Reimage the Cisco ASA or Firepower Threat Defense Device.

Privacy Collection Statement—The Firepower 2100 does not require or actively collect personally-identifiable information. However, you can use personally-identifiable information in the configuration, for example for usernames. In this case, an administrator might be able to see this information when working with the configuration or when using SNMP.

About the ASA

The ASA provides advanced stateful firewall and VPN concentrator functionality in one device.

The Firepower 2100 is a single-application appliance for the ASA. You can run the ASA in either Platform mode or Appliance mode (the default). The Firepower 2100 runs an underlying operating system called the FXOS. When in Platform mode, you must configure basic operating parameters and hardware interface settings in FXOS. These settings include enabling interfaces, establishing EtherChannels, NTP, image management, and more. You can use the chassis manager web interface or FXOS CLI. You can then configure your security policy in the ASA operating system using one of the following managers:

- ASDM—A single device manager included on the device. This guide describes how to manage the ASA using ASDM.
- CLI
- Cisco Security Manager—A multi-device manager on a separate server.

Appliance mode lets you configure all settings in the ASA. Only advanced troubleshooting commands are available from the FXOS CLI.

ASA and FXOS Management

The ASA and FXOS operating systems share the Management 1/1 interface. This interface has separate IP addresses for connecting to ASA and to FXOS.

Note This interface is called Management 1/1 in the ASA; in FXOS, you might see it displayed as MGMT, management0, or other similar names. This guide refers to this interface as Management 1/1 for consistency and simplicity.

Some functions must be monitored on FXOS and others on the ASA, so you need to make use of both operating systems for ongoing maintenance. For initial configuration on FXOS, you can connect to the default 192.168.45.45 IP address using SSH or your browser (https://192.168.45.45).

For initial configuration of the ASA, you can connect using ASDM to https://192.168.45.1/admin. In ASDM, you can later configure SSH access from any interface.

Both operating systems are available from the console port. Initial connection accesses the FXOS CLI. You can access the ASA CLI using the **connect asa** command.

You can also allow FXOS management from ASA data interfaces; configure SSH, HTTPS, and SNMP access. This feature is useful for remote management.

Unsupported Features

Unsupported ASA Features

The following ASA features are not supported on the Firepower 2100:

- Integrated Routing and Bridging
- Redundant interfaces
- Clustering
- Clientless SSL VPN with KCD
- ASA REST API
- ASA FirePOWER module
- Botnet Traffic Filter
- The following inspections:
  - SCTP inspection maps (SCTP stateful inspection using ACLs is supported)
  - Diameter
  - GTP/GPRS

Unsupported FXOS Features

The following FXOS features are not supported on the Firepower 2100:

- Backup and restore FXOS configuration

  You can instead show all or parts of the configuration by using the **show configuration** command.

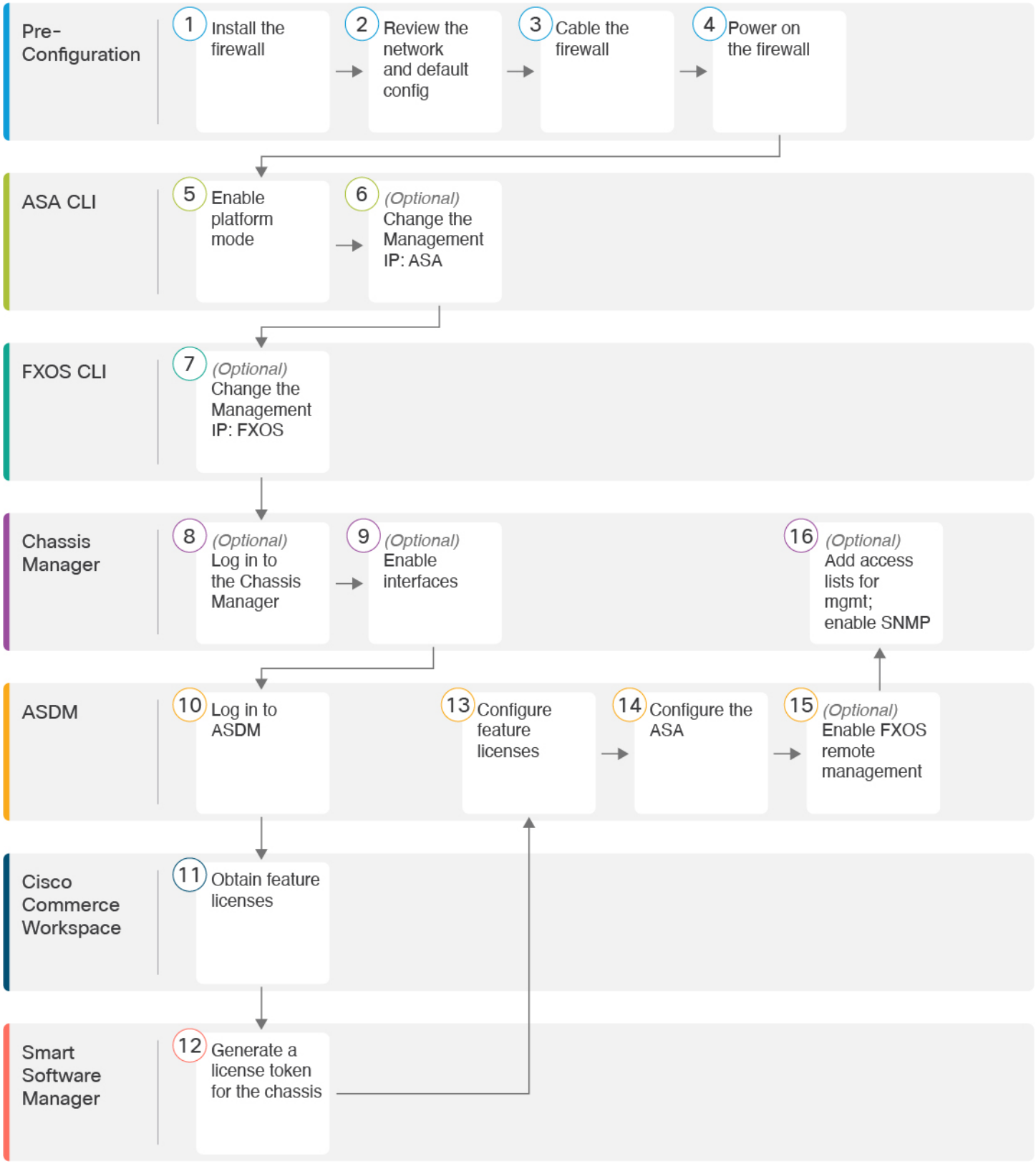
Note Show commands do not show the secrets (password fields), so if you want to paste a configuration into a new device, you will have to modify the show output to include the actual passwords.

- External AAA Authentication for FXOS

  Note that when you connect to the ASA console from FXOS (**connect asa**), then ASA AAA configuration for console access applies (**aaa authentication serial console**).

End-to-End Procedure

See the following tasks to deploy and configure the ASA.


Pre-Configuration
1 Install the firewall
2 Review the network and default config
3 Cable the firewall
4 Power on the firewall
ASA CLI
5 Enable platform mode
6 (Optional) Change the Management IP: ASA
FXOS CLI
7 (Optional) Change the Management IP: FXOS
Chassis Manager
8 (Optional) Log in to the Chassis Manager
9 (Optional) Enable interfaces
16 (Optional) Add access lists for mgmt; enable SNMP
ASDM
10 Log in to ASDM
13 Configure feature licenses
14 Configure the ASA
15 (Optional) Enable FXOS remote management
Cisco Commerce Workspace
11 Obtain feature licenses
Smart Software Manager
12 Generate a license token for the chassis

1	Pre-Configuration	Install the firewall. See the hardware installation guide.
2	Pre-Configuration	Review the Network Deployment and Default Configuration, on page 213.
3	Pre-Configuration	Cable the Device, on page 216.
4	Pre-Configuration	Power on the Firewall, on page 217.
5	ASA CLI	Enable Platform Mode, on page 217.
6	ASA CLI	(Optional) Change the FXOS and ASA Management IP Addresses or Gateway, on page 220: Change the Management IP: ASA.
7	FXOS CLI	(Optional) Change the FXOS and ASA Management IP Addresses or Gateway, on page 220: Change the Management IP: FXOS.
8	Chassis Manager	(Optional) Log Into the Chassis Manager, on page 225.
9	Chassis Manager	(Optional) Enable Additional Interfaces in the Chassis Manager, on page 226.
10	ASDM	Log Into ASDM, on page 228.
11	Cisco Commerce Workspace	Configure Licensing, on page 229: Obtain feature licenses.
12	Smart Software Manager	Configure Licensing, on page 229: Generate a license token for the chassis.
13	ASDM	Configure Licensing, on page 229: Configure feature licenses.
14	ASDM	Configure the ASA, on page 235.
15	ASDM	(Optional) Configure Management Access for FXOS on Data Interfaces, on page 236: Enable FXOS remote management; allow FXOS to initiate management connections from an ASA interface.
16	Chassis Manager	(Optional) Configure Management Access for FXOS on Data Interfaces, on page 236: Configure access lists to allow your management addresses; enable SNMP (HTTPS and SSH are enabled by default).

Review the Network Deployment and Default Configuration

The following figure shows the default network deployment for the Firepower 2100 using the default configuration in ASA Platform mode.

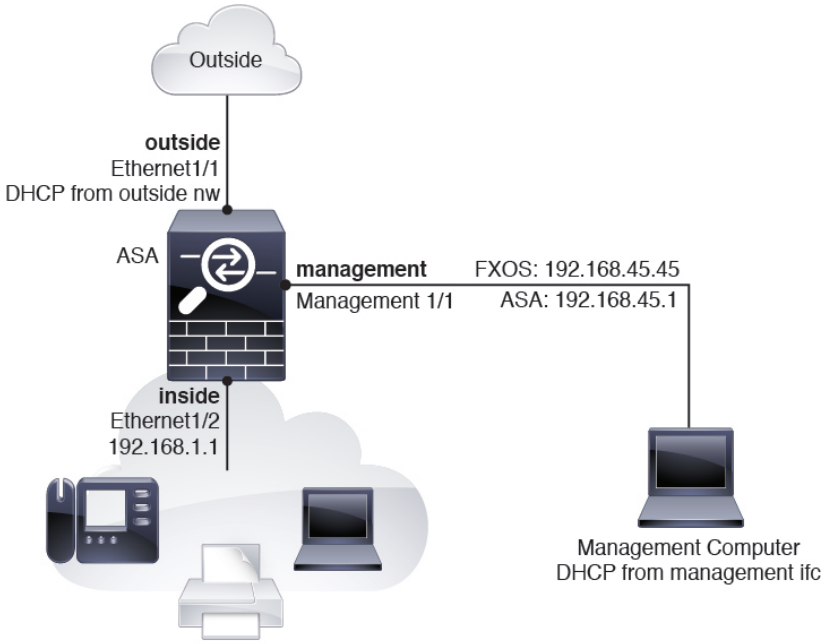
If you connect the outside interface directly to a cable modem or DSL modem, we recommend that you put the modem into bridge mode so the ASA performs all routing and NAT for your inside networks. If you need to configure PPPoE for the outside interface to connect to your ISP, you can do so as part of the ASDM Startup Wizard.

Note If you cannot use the default FXOS and ASA Management IP addresses, see (Optional) Change the FXOS and ASA Management IP Addresses or Gateway, on page 220.

If you need to change the inside IP address, you can do so using the ASDM Startup Wizard. For example, you may need to change the inside IP address in the following circumstances:

- If the outside interface tries to obtain an IP address on the 192.168.1.0 network, which is a common default network, the DHCP lease will fail, and the outside interface will not obtain an IP address. This problem occurs because the ASA cannot have two interfaces on the same network. In this case you must change the inside IP address to be on a new network.
- If you add the ASA to an existing inside network, you will need to change the inside IP address to be on the existing network.

Figure 127: Firepower 2100 in Your Network



Firepower 2100 Platform Mode Default Configuration

You can set the Firepower 2100 to run in Platform mode; Appliance mode is the default.

Note For pre-9.13(1) versions, Platform mode was the default and only option. If you upgrade from Platform mode, this mode is maintained.

ASA Configuration

The default factory configuration for the ASA on the Firepower 2100 configures the following:

- **inside→outside traffic flow**—Ethernet 1/1 (outside), Ethernet 1/2 (inside)
- **outside IP address** from DHCP, inside IP address—192.168.1.1
- **DHCP server** on inside interface
- **Default route** from outside DHCP
- **management**—Management 1/1 (management), IP address 192.168.45.1
- **ASDM** access—Management hosts allowed.
- **NAT**—Interface PAT for all traffic from inside to outside.
- **FXOS management** traffic initiation—The FXOS chassis can initiate management traffic on the ASA outside interface.
- **DNS** servers—OpenDNS servers are pre-configured.

The configuration consists of the following commands:

```
interface Management1/1
  management-only
  nameif management
  security-level 100
  ip address 192.168.45.1 255.255.255.0
  no shutdown
!
interface Ethernet1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/2
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
  no shutdown
!
object network obj_any
  subnet 0.0.0.0 0.0.0.0
  nat (any,outside) dynamic interface
!
http server enable
http 192.168.45.0 255.255.255.0 management
```

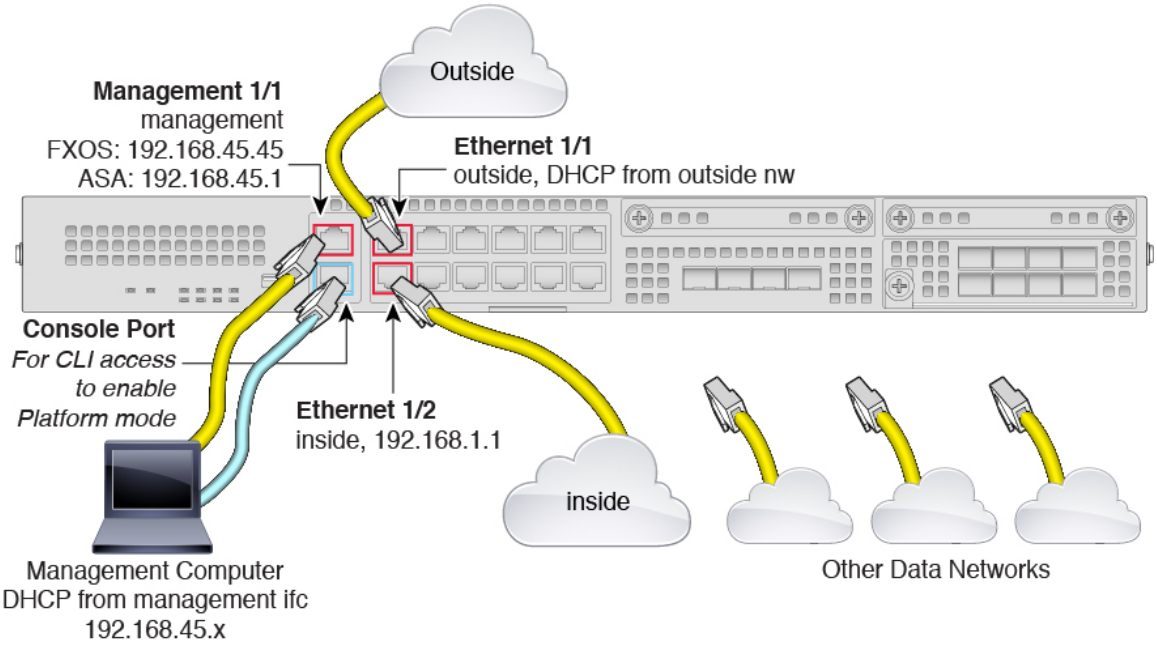
```
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd enable inside
!
ip-client outside
!
dns domain-lookup outside
dns server-group DefaultDNS
   name-server 208.67.222.222 outside
   name-server 208.67.220.220 outside
```

FXOS Configuration

The default factory configuration for FXOS on the Firepower 2100 configures the following:

- **Management 1/1**—IP address 192.168.45.45
- **Default gateway**—ASA data interfaces
- **Chassis Manager and SSH access**—From the management network only.
- **Default Username**—**admin**, with the default password **Admin123**
- **DHCP server**—Client IP address range 192.168.45.10-192.168.45.12
- **NTP** server—Cisco NTP servers: 0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org, 2.sourcefire.pool.ntp.org
- **DNS** Servers—OpenDNS: 208.67.222.222, 208.67.220.220
- **Ethernet 1/1 and Ethernet 1/2**—Enabled

Cable the Device



Manage the Firepower 2100 on the Management 1/1 interface. You can use the same management computer for FXOS and ASA. The default configuration also configures Ethernet1/1 as outside.

Procedure

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

Step 2 Connect your management computer directly to Management 1/1 (labeled MGMT), or connect Management 1/1 to your management network.

Make sure your management computer is on the management network, because only clients on that network can access the ASA or FXOS. Management 1/1 has a default FXOS IP address (192.168.45.45) and ASA default IP address (192.168.45.1). FXOS also runs a DHCP server to provide IP addresses to clients (including the management computer), so make sure these settings do not conflict with any existing management network settings (see Firepower 2100 Platform Mode Default Configuration, on page 214).

If you need to change the FXOS and ASA Management IP address from the defaults, see (Optional) Change the FXOS and ASA Management IP Addresses or Gateway, on page 220.

You can later configure FXOS and ASA management access from data interfaces. For FXOS access, see (Optional) Configure Management Access for FXOS on Data Interfaces, on page 236. For ASA access, see the ASA general operations configuration guide.

Step 3 Connect your management computer to the console port.

You need to access the ASA CLI to change from Appliance mode to Platform mode. The Firepower 2100 ships with a DB-9 to RJ-45 serial cable, so you will need a third party serial-to-USB cable to make the connection. Be sure to install any necessary USB serial drivers for your operating system.

Step 4 Connect the outside network to the Ethernet1/1 interface (labeled WAN).

For Smart Software Licensing, the ASA needs internet access so that it can access the License Authority.

Step 5 Connect the inside network to Ethernet1/2.

Step 6 Connect other networks to the remaining interfaces.

Power on the Firewall

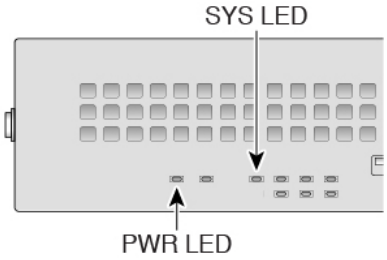
The power switch is located to the left of power supply module 1 on the rear of the chassis. It is a toggle switch that controls power to the system. If the power switch is in standby position, only the 3.3-V standby power is enabled from the power supply module and the 12-V main power is OFF. When the switch is in the ON position, the 12-V main power is turned on and the system boots.

Procedure

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

Step 2 Press the power switch on the back of the device.

Step 3 Check the PWR LED on the front of the device; if it is solid green, the device is powered on.



Step 4 Check the SYS LED on the front of the device; after it is solid green, the system has passed power-on diagnostics.

Note Before you move the power switch to the OFF position, use the shutdown commands so that the system can perform a graceful shutdown. This may take several minutes to complete. After the graceful shutdown is complete, the console displays `It is safe to power off now`. The front panel blue locator beacon LED lights up indicating the system is ready to be powered off. You can now move the switch to the OFF position. The front panel PWR LED flashes momentarily and turns off. Do not remove the power until the PWR LED is completely off.

See the FXOS Configuration Guide for more information on using the shutdown commands.

Enable Platform Mode

The Firepower 2100 runs in Appliance mode by default. This procedure tells you how to change the mode to Platform mode, and optionally how to change it back to Appliance mode.

When you change the mode, the configuration is cleared and you need to reload the system. The default configuration is applied upon reload.

Procedure

Step 1 Connect your management computer to the console port. The Firepower 2100 ships with a DB-9 to RJ-45 serial cable, so you will need a third party serial-to-USB cable to make the connection. Be sure to install any necessary USB serial drivers for your operating system. Use the following serial settings:

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

You connect to the ASA CLI. There are no user credentials required for console access by default.

Note After you change to Platform mode, the console connection will access the FXOS CLI, not the ASA CLI. But you can access the ASA CLI from the console in Platform mode; see Connect to the Console Port to Access FXOS and ASA CLI, on page 237.

Step 2 Access privileged EXEC mode.

enable

You are prompted to change the password the first time you enter the **enable** command.

Example:

```
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
ciscoasa#
```

All non-configuration commands are available in privileged EXEC mode. You can also enter configuration mode from privileged EXEC mode.

To exit privileged mode, enter the **disable**, **exit**, or **quit** command.

Step 3 Access global configuration mode.

configure terminal

Example:

```
ciscoasa# configure terminal
ciscoasa(config)#
```

Step 4 Set the mode to Platform mode.

no fxos mode appliance

write memory

reload

After you set the mode, you need to save the configuration and reload the device. Prior to reloading, you can set the mode back to the original value without any disruption.

Example:

```
ciscoasa(config)# no fxos mode appliance
Mode set to platform mode
WARNING: This command will take effect after the running-config is saved and the system has
 been rebooted. Command accepted.
ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: c0532471 648dc7c2 4f2b4175 1f162684

23736 bytes copied in 1.520 secs (23736 bytes/sec)
[OK]
ciscoasa(config)# reload
Proceed with reload? [confirm]
```

Step 5 After restart, view the current mode to confirm the change.

show fxos mode

Example:

```
ciscoasa(config)# show fxos mode
Mode is currently set to platform
```

Step 6 (Optional) Set the mode back to Appliance mode.

fxos mode appliance

write memory

reload

After you set the mode, you need to save the configuration and reload the device. Prior to reloading, you can set the mode back to the original value without any disruption.

Example:

```
ciscoasa(config)# fxos mode appliance
Mode set to appliance mode
WARNING: This command will take effect after the running-config is saved and the system has
 been rebooted. Command accepted.
ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: c0532471 648dc7c2 4f2b4175 1f162684

23736 bytes copied in 1.520 secs (23736 bytes/sec)
[OK]
ciscoasa(config)# reload
Proceed with reload? [confirm]
```

(Optional) Change the FXOS and ASA Management IP Addresses or Gateway

You can change the FXOS management IP address on the Firepower 2100 chassis from the FXOS CLI. The default address is 192.168.45.45. You can also change the default gateway for FXOS management traffic. The default gateway is set to 0.0.0.0, which sends FXOS traffic over the backplane to be routed through the ASA data interfaces. If you want to route traffic to a router on the Management 1/1 network instead, then you can change the gateway IP address. You must also change the access list for management connections to match your new network. If you change the gateway from the default 0.0.0.0 (the ASA data interfaces), then you will not be able to access FXOS on a data interface nor will FXOS be able to initiate traffic on a data interface (see (Optional) Configure Management Access for FXOS on Data Interfaces, on page 236).

Typically, the FXOS Management 1/1 IP address will be on the same network as the ASA Management 1/1 IP address, so this procedure also shows how to change the ASA IP address on the ASA.

Before you begin

- After you change the FXOS management IP address, you need to reestablish any chassis manager and SSH connections using the new address.
- Because the DHCP server is enabled by default on Management 1/1, you must disable DHCP before you change the management IP address.

Procedure

Step 1 Connect to the console port (see Connect to the Console Port to Access FXOS and ASA CLI, on page 237). We recommend that you connect to the console port to avoid losing your connection.

Step 2 Disable the DHCP server.

scope system

scope services

disable dhcp-server

commit-buffer

You can reenable DHCP using new client IP addresses after you change the management IP address. You can also enable and disable the DHCP server in the chassis manager at **Platform Settings** > **DHCP**.

Example:

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # disable dhcp-server
firepower-2110 /system/services* # commit-buffer
```

Step 3 Configure an IPv4 management IP address, and optionally the gateway.

a) Set the scope for fabric-interconnect a.

scope fabric-interconnect a

Example:

```
firepower-2110# scope fabric-interconnect a
firepower-2110 /fabric-interconnect #
```

b) View the current management IP address.

show

Example:

```
firepower-2110 /fabric-interconnect # show

Fabric Interconnect:
    ID   OOB IP Addr     OOB Gateway     OOB Netmask     OOB IPv6 Address OOB IPv6 Gateway
 Prefix Operability
    ---- --------------- --------------- --------------- ---------------- ----------------
 ------ -----------
    A    192.168.45.45    0.0.0.0        0.0.0.0          ::               ::
     64     Operable
```

c) Configure a new management IP address, and optionally a new default gateway.

set out-of-band static ip *ip_address* **netmask** *network_mask* **gw** *gateway_ip_address*

To keep the currently-set gateway, omit the **gw** keyword. Similarly, to keep the existing management IP address while changing the gateway, omit the **ip** and **netmask** keywords.

To set the gateway to the ASA data interfaces, set the **gw** to 0.0.0.0. This is the default setting.

Example:

```
firepower-2110 /fabric-interconnect # set out-of-band static ip 192.168.4.1 netmask
255.255.255.0
Warning: When committed, this change may disconnect the current CLI session
firepower-2110 /fabric-interconnect* #
```

Step 4 Configure an IPv6 management IP address and gateway.

a) Set the scope for fabric-interconnect a, and then the IPv6 configuration.

scope fabric-interconnect a

scope ipv6-config

Example:

```
firepower-2110# scope fabric-interconnect a
firepower-2110 /fabric-interconnect # scope ipv6-config
firepower-2110 /fabric-interconnect/ipv6-config #
```

b) View the current management IPv6 address.

show ipv6-if

Example:

```
firepower-2110 /fabric-interconnect/ipv6-config # show ipv6-if
```

```
Management IPv6 Interface:
    IPv6 Address                          Prefix     IPv6 Gateway
    ------------------------------------ ---------- ------------
    ::                                    ::         ::
```

c) Configure a new management IPv6 address and gateway:

Firepower-chassis /fabric-interconnect/ipv6-config # **set out-of-band static ipv6** *ipv6_address* **ipv6-prefix** *prefix_length* **ipv6-gw** *gateway_address*

To keep the currently-set gateway, omit the **ipv6-gw** keyword. Similarly, to keep the existing management IP address while changing the gateway, omit the **ipv6** and **ipv6-prefix** keywords.

To set the gateway to the ASA data interfaces, set the **gw** to ::. This is the default setting.

Example:

```
firepower-2110 /fabric-interconnect/ipv6-config # set out-of-band static ipv6 2001:DB8::34
 ipv6-prefix 64 ipv6-gw 2001:DB8::1
firepower-2110 /fabric-interconnect/ipv6-config* #
```

Step 5 Delete and add new access lists for HTTPS, SSH, and SNMP to allow management connections from the new network.

a) Set the scope for system/services.

scope system

scope services

Example:

```
firepower-2110# scope system
firepower-2110 /system # scope services
```

b) View the current access lists.

show ip-block

Example:

```
firepower-2110 /system/services # show ip-block

Permitted IP Block:
    IP Address      Prefix Length Protocol
    --------------- ------------- --------
    192.168.45.0               24 https
    192.168.45.0               24 ssh
firepower-2140 /system/services #
```

c) Add new access lists.

For IPv4:

enter ip-block *ip_address prefix* [**http** | **snmp** | **ssh**]

For IPv6:

enter ipv6-block *ipv6_address prefix* [**https** | **snmp** | **ssh**]

For IPv4, enter **0.0.0.0** and a prefix of **0** to allow all networks. For IPv6, enter **::** and a prefix of **0** to allow all networks. You can also add access lists in the chassis manager at **Platform Settings** > **Access List**.

Example:

```
firepower-2110 /system/services # enter ip-block 192.168.4.0 24 https
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* # enter ip-block 192.168.4.0 24 ssh
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* # enter ip-block 192.168.4.0 24 snmp
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* # enter ipv6-block 2001:DB8:: 64 https
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* # enter ipv6-block 2001:DB8:: 64 ssh
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* # enter ipv6-block 2001:DB8:: 64 snmp
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* #
```

a) Delete the old access lists.

For IPv4:

delete ip-block *ip_address prefix* [**http** | **snmp** | **ssh**]

For IPv6:

delete ipv6-block *ipv6_address prefix* [**https** | **snmp** | **ssh**]

Example:

```
firepower-2110 /system/services # delete ip-block 192.168.45.0 24 https
firepower-2110 /system/services* # delete ip-block 192.168.45.0 24 ssh
firepower-2110 /system/services* #
```

Step 6 (Optional) Reenable the IPv4 DHCP server.

scope system

scope services

enable dhcp-server *start_ip_address end_ip_address*

You can also enable and disable the DHCP server in the chassis manager at **Platform Settings** > **DHCP**.

Example:

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # enable dhcp-server 192.168.4.10 192.168.4.20
```

Step 7 Save the configuration.

commit-buffer

Example:

```
firepower-2110 /system/services* # commit-buffer
```

Step 8 Change the ASA address to be on the correct network. The default ASA Management 1/1 interface IP address is 192.168.45.1.

a) From the console, connect to the ASA CLI and access global configuration mode.

connect asa

enable

configure terminal

In ASA version 9.12(1) and later, you are prompted to set an enable password. In previous versions, the default enable password is blank.

Example:

```
firepower-2110# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
ciscoasa# configure terminal
ciscoasa(config)#
```

b) Change the Management 1/1 IP address.

interface management1/1

ip address *ip_address mask*

Example:

```
ciscoasa(config)# interface management1/1
ciscoasa(config-ifc)# ip address 10.86.118.4 255.255.255.0
```

c) Change the network that can access ASDM.

no http 192.168.45.0 255.255.255.0 management

http *ip_address mask* **management**

Example:

```
ciscoasa(config)# no http 192.168.45.0 255.255.255.0 management
ciscoasa(config)# http 10.86.118.0 255.255.255.0 management
```

d) Save the configuration.

write memory

e) To return to the FXOS console, enter **Ctrl+a**, **d**.

Example

The following example configures an IPv4 management interface and gateway:

```
firepower-2110# scope fabric-interconnect a
firepower-2110 /fabric-interconnect # show

Fabric Interconnect:
    ID   OOB IP Addr     OOB Gateway     OOB Netmask     OOB IPv6 Address OOB IPv6 Gateway
 Prefix Operability
    ---- --------------- --------------- --------------- ---------------- ----------------
 ------ -----------
    A    192.168.2.112    192.168.2.1     255.255.255.0   2001:DB8::2     2001:DB8::1
  64     Operable
firepower-2110 /fabric-interconnect # set out-of-band static ip 192.168.2.111 netmask
255.255.255.0 gw 192.168.2.1
Warning: When committed, this change may disconnect the current CLI session
firepower-2110 /fabric-interconnect* # commit-buffer
firepower-2110 /fabric-interconnect #
```

The following example configures an IPv6 management interface and gateway:

```
firepower-2110# scope fabric-interconnect a
firepower-2110 /fabric-interconnect # scope ipv6-config
firepower-2110 /fabric-interconnect/ipv6-config # show ipv6-if

Management IPv6 Interface:
    IPv6 Address                          Prefix     IPv6 Gateway
    ------------------------------------ ---------- ------------
    2001:DB8::2                           64         2001:DB8::1
firepower-2110 /fabric-interconnect/ipv6-config # set out-of-band static ipv6 2001:DB8::2
ipv6-prefix 64 ipv6-gw 2001:DB8::1
firepower-2110 /fabric-interconnect/ipv6-config* # commit-buffer
firepower-2110 /fabric-interconnect/ipv6-config #
```

(Optional) Log Into the Chassis Manager

Use the chassis manager to configure chassis settings, including enabling interfaces and creating EtherChannels.

Before you begin

- For information on supported browsers, refer to the release notes for the version you are using (see http://www.cisco.com/c/en/us/support/security/firepower-9000-series/products-release-notes-list.html).
- If you need to change the FXOS and ASA management IP addresses, see (Optional) Change the FXOS and ASA Management IP Addresses or Gateway, on page 220.

Procedure

Step 1 On your management computer connected to the Management 1/1 interface, launch the chassis manager by going to the following URL.

https://192.168.45.45

Step 2 Enter the default username: **admin**. You are prompted to set a password.

(Optional) Enable Additional Interfaces in the Chassis Manager

By default, the Management 1/1, Ethernet 1/1, and Ethernet 1/2 interfaces are physically enabled for the chassis and logically enabled in the ASA configuration. To use any additional interfaces, you must enable it for the chassis using this procedure, and then later enable it in the ASA configuration. You can also add EtherChannels (known as port-channels).

Note If you change the interfaces in FXOS after you enable failover (by adding or removing a network module, or by changing the EtherChannel configuration, for example), make the interface changes in FXOS on the standby unit, and then make the same changes on the active unit.

If you remove an interface in FXOS (for example, if you remove a network module, remove an EtherChannel, or reassign an interface to an EtherChannel), then the ASA configuration retains the original commands so that you can make any necessary adjustments; removing an interface from the configuration can have wide effects. You can manually remove the old interface configuration in the ASA OS.

Note For many interface **show** commands, you either cannot use the ASA commands or the commands lack the full statistics. You must view more detailed interface information using FXOS commands:

- /eth-uplink/fabric# **show interface**
- /eth-uplink/fabric# **show port-channel**
- /eth-uplink/fabric/interface# **show stats**
- (local-mgmt)# **show portmanager counters**
- (local-mgmt)# **show lacp**
- (local-mgmt)# **show portchannel**

See the FXOS troubleshooting guide for more information.

Before you begin

- Log into the chassis manager. See (Optional) Log Into the Chassis Manager, on page 225.
- The Firepower 2100 supports EtherChannels in Link Aggregation Control Protocol (LACP) Active or On mode. By default, the LACP mode is set to Active; you can change the mode to On at the CLI. We suggest setting the connecting switch ports to Active mode for the best compatibility.
- To change the management IP address from the default, see (Optional) Change the FXOS and ASA Management IP Addresses or Gateway, on page 220.

Procedure

Step 1 In the chassis manager, click **Interfaces**.

The **All Interfaces** page shows a visual representation of the currently-installed interfaces at the top of the page and provides a listing of the installed interfaces in the table below.

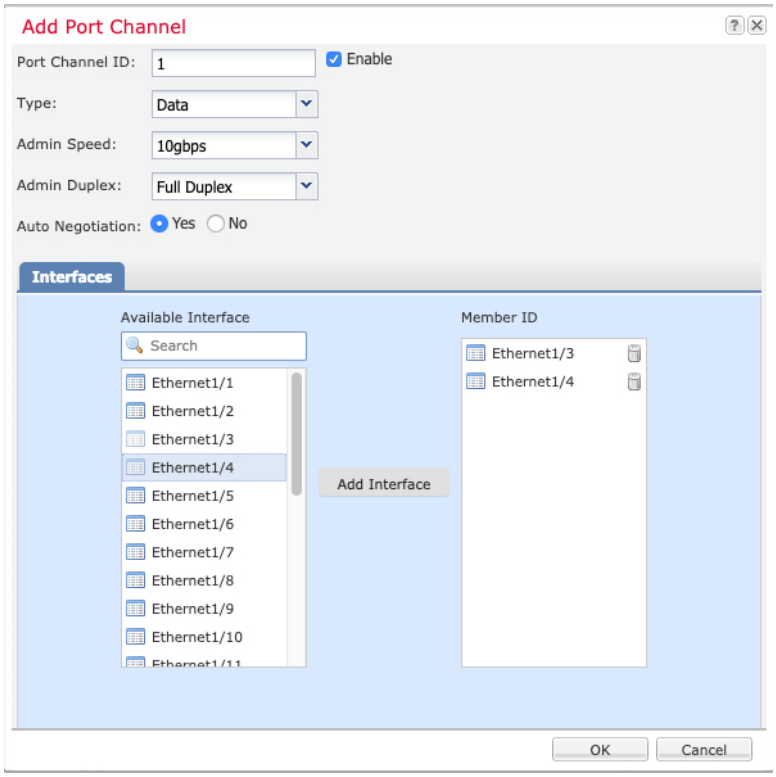
Step 2 To enable or disable an interface, click Enable slider ( ) or Disable slider ( ).

Note The Management 1/1 interface shows as **MGMT** in this table.

Step 3 (Optional) Add an EtherChannel.

Note EtherChannel member ports are visible on the ASA, but you can only configure EtherChannels and port membership in FXOS.

a) Click **Add Port Channel** above the interfaces table.



b) In the **Port Channel ID** field, enter an ID for the port channel. Valid values are between 1 and 47.

c) Check the **Enable** check box to enable the port channel.

Ignore the **Type** drop-down list; the only available type is **Data**.

d) From the **Admin Speed** drop-down list, choose the speed for all member interfaces.

If you choose interfaces that are not capable of the speed (and other settings that you choose), the fastest possible speed is automatically applied.

e) Click the **Auto Negotiation Yes** or **No** radio button for all member interfaces.

f) **Admin Duplex** drop-down list, choose the duplex for all member interfaces.
g) In the **Available Interface** list, select the interface you want to add, and click **Add Interface**.

You can add up to 16 interfaces of the same type and speed. The first interface added to the channel group determines the correct type and speed.

Tip You can add multiple interfaces at one time. To select multiple individual interfaces, click on the desired interfaces while holding down the **Ctrl** key. To select a range of interfaces, select the first interface in the range, and then, while holding down the **Shift** key, click to select the last interface in the range.

h) Click **OK**.

Log Into ASDM

Launch ASDM so you can configure the ASA.

Strong Encryption (3DES/AES) is available for management connections before you connect to the License Authority or Satellite server so you can launch ASDM. Note that ASDM access is only available on management-only interfaces with the default encryption. Through the box traffic is not allowed until you connect and obtain the Strong Encryption license.

Before you begin

See the ASDM release notes on Cisco.com for the requirements to run ASDM.

Procedure

Step 1 Using a supported browser, enter the following URL.

https://*management_ip***/admin**

- *management_ip*—Identifies the IP address or host name of the ASA management interface (192.168.45.1).

The **Cisco ASDM** web page appears. You may see browser security warnings because the ASA does not have a certificate installed; you can safely ignore these warnings and visit the web page.

Step 2 Click one of these available options: **Install ASDM Launcher** or **Run ASDM**.

Step 3 Follow the onscreen instructions to launch ASDM according to the option you chose.

The **Cisco ASDM-IDM Launcher** appears.

Step 4 Leave the username empty, enter the enable password that you set when you deployed the ASA, and click **OK**.

The main ASDM window appears.

Configure Licensing

The ASA uses Smart Licensing. You can use regular Smart Licensing, which requires internet access; or for offline management, you can configure Permanent License Reservation or a Smart Software Manager On-Prem (formerly known as a Satellite server). For more information about these offline licensing methods, see Cisco ASA Series Feature Licenses; this guide applies to regular Smart Licensing.

For a more detailed overview on Cisco Licensing, go to cisco.com/go/licensingguide

When you register the chassis, the Smart Software Manager issues an ID certificate for communication between the firewall and the Smart Software Manager. It also assigns the firewall to the appropriate virtual account. Until you register with the Smart Software Manager, you will not be able to make configuration changes to features requiring special licenses, but operation is otherwise unaffected. Licensed features include:

- Essentials
- Security Contexts
- Strong Encryption (3DES/AES)—If your Smart Account is not authorized for strong encryption, but Cisco has determined that you are allowed to use strong encryption, you can manually add a stong encryption license to your account.
- Cisco Secure Client—Secure Client Advantage, Secure Client Premier, or Secure Client VPN Only.

Strong Encryption (3DES/AES) is available for management connections before you connect to the License Authority or Satellite server so you can launch ASDM. Note that ASDM access is only available on management-only interfaces with the default encryption. Through the box traffic is not allowed until you connect and obtain the Strong Encryption license.

When you request the registration token for the ASA from the Smart Software Manager, check the **Allow export-controlled functionality on the products registered with this token** check box so that the full Strong Encryption license is applied (your account must be qualified for its use). The Strong Encryption license is automatically enabled for qualified customers when you apply the registration token on the chassis, so no additional action is required. If your Smart Account is not authorized for strong encryption, but Cisco has determined that you are allowed to use strong encryption, you can manually add a strong encryption license to your account.

Note Unlike the Firepower 4100/9300 chassis, you perform all licensing configuration on the ASA, and not in the FXOS configuration.

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.

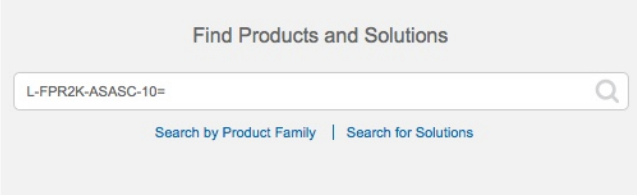
- Your Smart Software Manager account must qualify for the Strong Encryption (3DES/AES) license to use some features (enabled using the export-compliance flag).

Procedure

Step 1 Make sure your Smart Licensing account contains the available licenses you need, including at a minimum the Essentials license.

When you bought your device from Cisco or a reseller, your licenses should have been linked to your Smart Software Manager 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 128: License Search

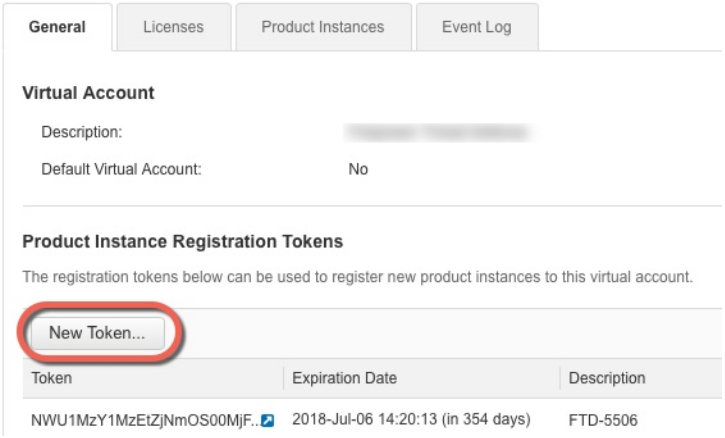


- Essentials license—L-FPR2100-ASA=. The Essentials license is free, but you still need to add it to your Smart Software Licensing account.
- 5 context license—L-FPR2K-ASASC-5=. Context licenses are additive; buy multiple licenses to meet your needs.
- 10 context license—L-FPR2K-ASASC-10=. Context licenses are additive; buy multiple licenses to meet your needs.
- Strong Encryption (3DES/AES) license—L-FPR2K-ENC-K9=. Only required if your account is not authorized for strong encryption.
- Cisco Secure Client—See the Cisco Secure Client Ordering Guide. You do not enable this license directly in the ASA.

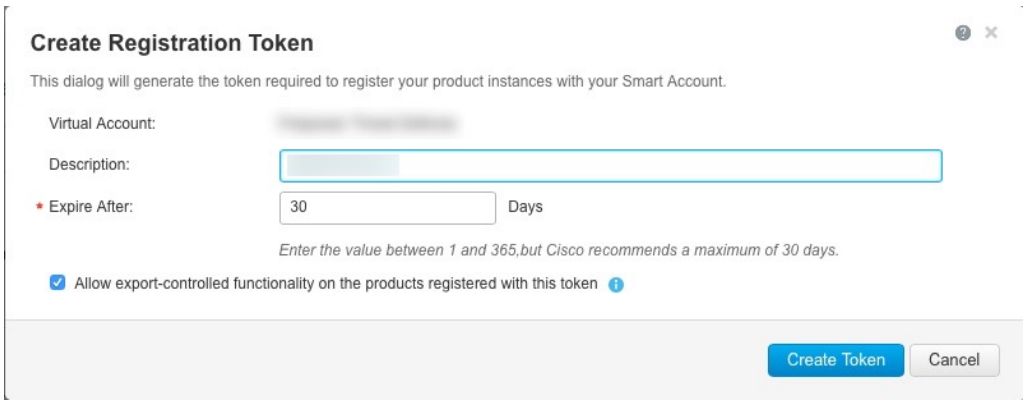
Step 2 In the Cisco Smart Software Manager, request and copy a registration token for the virtual account to which you want to add this device.

a) Click **Inventory**.

b) On the **General** tab, click **New Token**.



c) On the **Create Registration Token** dialog box enter the following settings, and then click **Create Token**:



- **Description**
- **Expire After**—Cisco recommends 30 days.
- **Allow export-controlled functionaility on the products registered with this token**—Enables the export-compliance flag.

The token is added to your inventory.

d) Click the arrow icon to the right of the token to open the **Token** dialog box so you can copy the token ID to your clipboard. Keep this token ready for later in the procedure when you need to register the ASA.

Figure 129: View Token

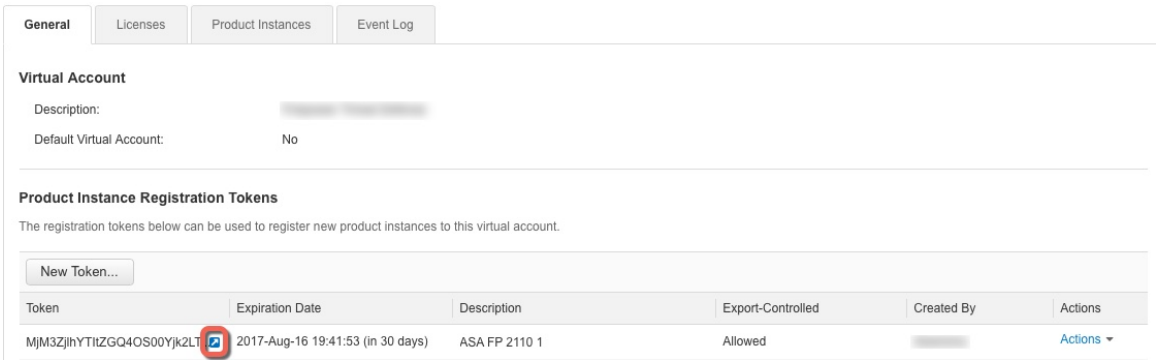
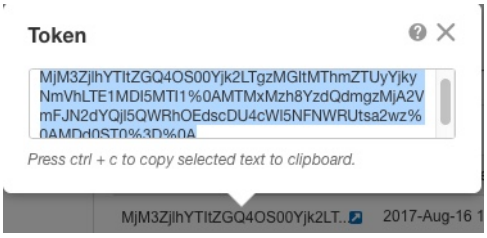
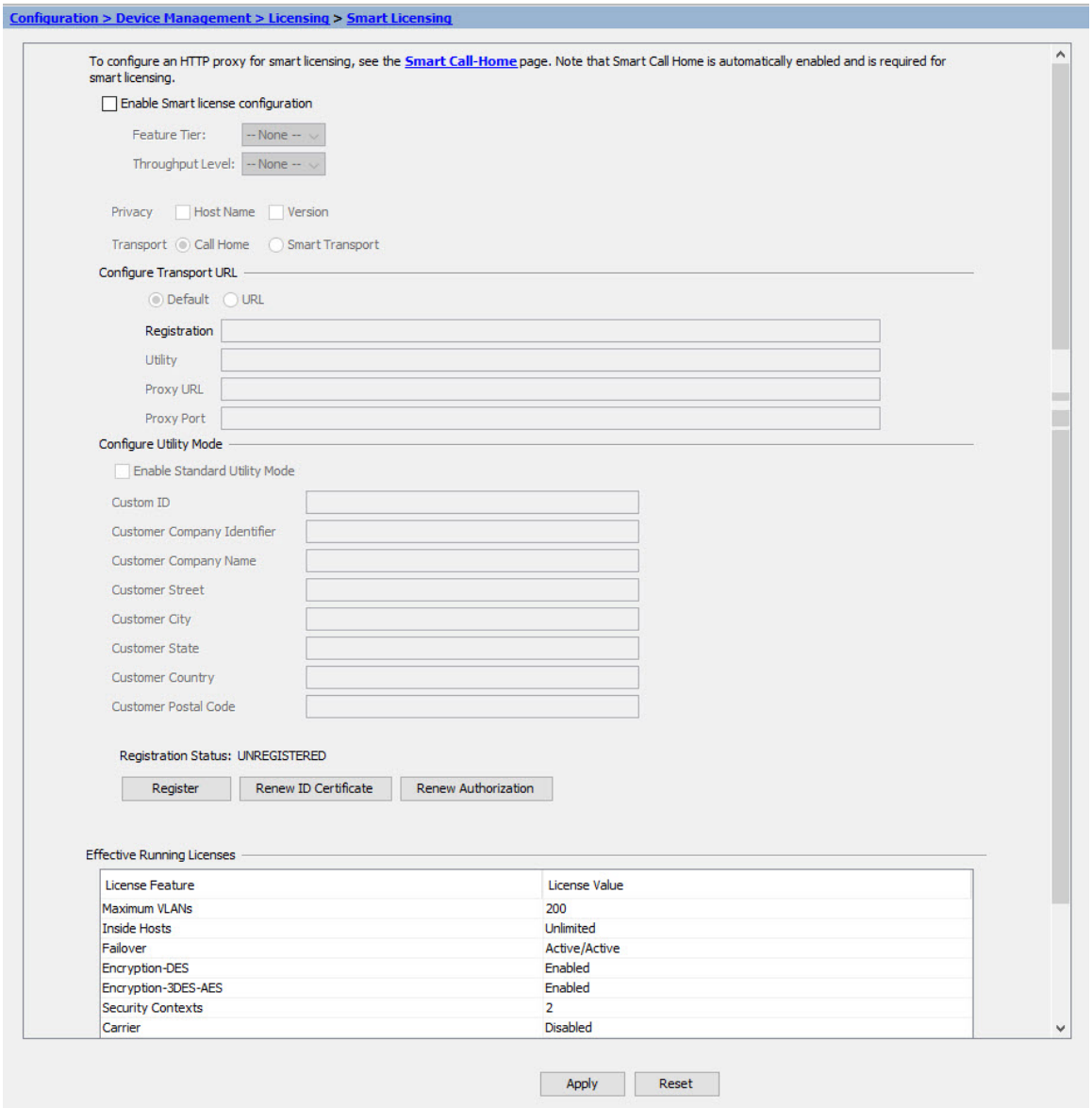


Figure 130: Copy Token

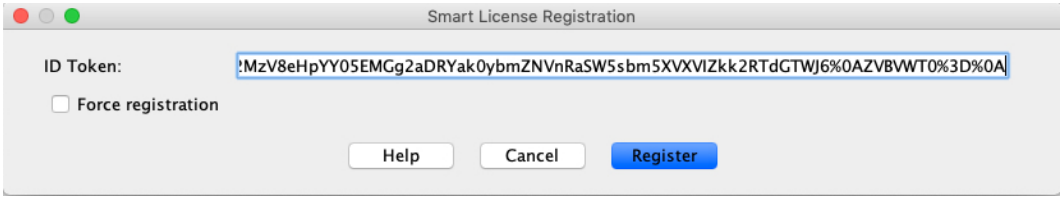


Step 3 In ASDM, choose **Configuration** > **Device Management** > **Licensing** > **Smart Licensing**.

Step 4 Click **Register**.



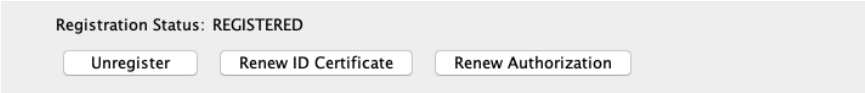
Step 5 Enter the registration token in the **ID Token** field.



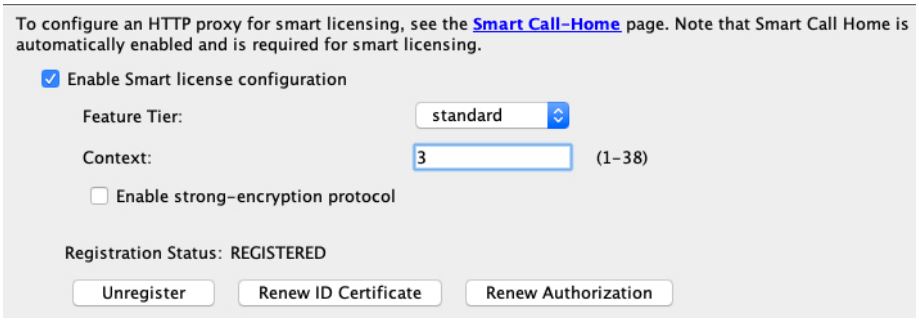
You can optionally check the **Force registration** check box to register the ASA that is already registered, but that might be out of sync with the Smart Software Manager. For example, use **Force registration** if the ASA was accidentally removed from the Smart Software Manager.

Step 6 Click **Register**.

The ASA registers with the Smart Software Manager using the pre-configured outside interface, and requests authorization for the configured license entitlements. The Smart Software Manager also applies the Strong Encryption (3DES/AES) license if your account allows. ASDM refreshes the page when the license status is updated. You can also choose **Monitoring** > **Properties** > **Smart License** to check the license status, particularly if the registration fails.



Step 7 Set the following parameters:



a) Check **Enable Smart license configuration**.

b) From the **Feature Tier** drop-down list, choose **Essentials**.

Only the Essentials tier is available.

c) (Optional) For the **Context** license, enter the number of contexts.

You can use 2 contexts without a license. The maximum number of contexts depends on your model:

- Firepower 2110—25 contexts
- Firepower 2120—25 contexts
- Firepower 2130—30 contexts
- Firepower 2140—40 contexts

For example, to use the maximum of 25 contexts on the Firepower 2110, enter 23 for the number of contexts; this value is added to the default of 2.

Step 8 Click **Apply**.

Step 9 Click the **Save** icon in the toolbar.

Step 10 Quit ASDM and relaunch it.

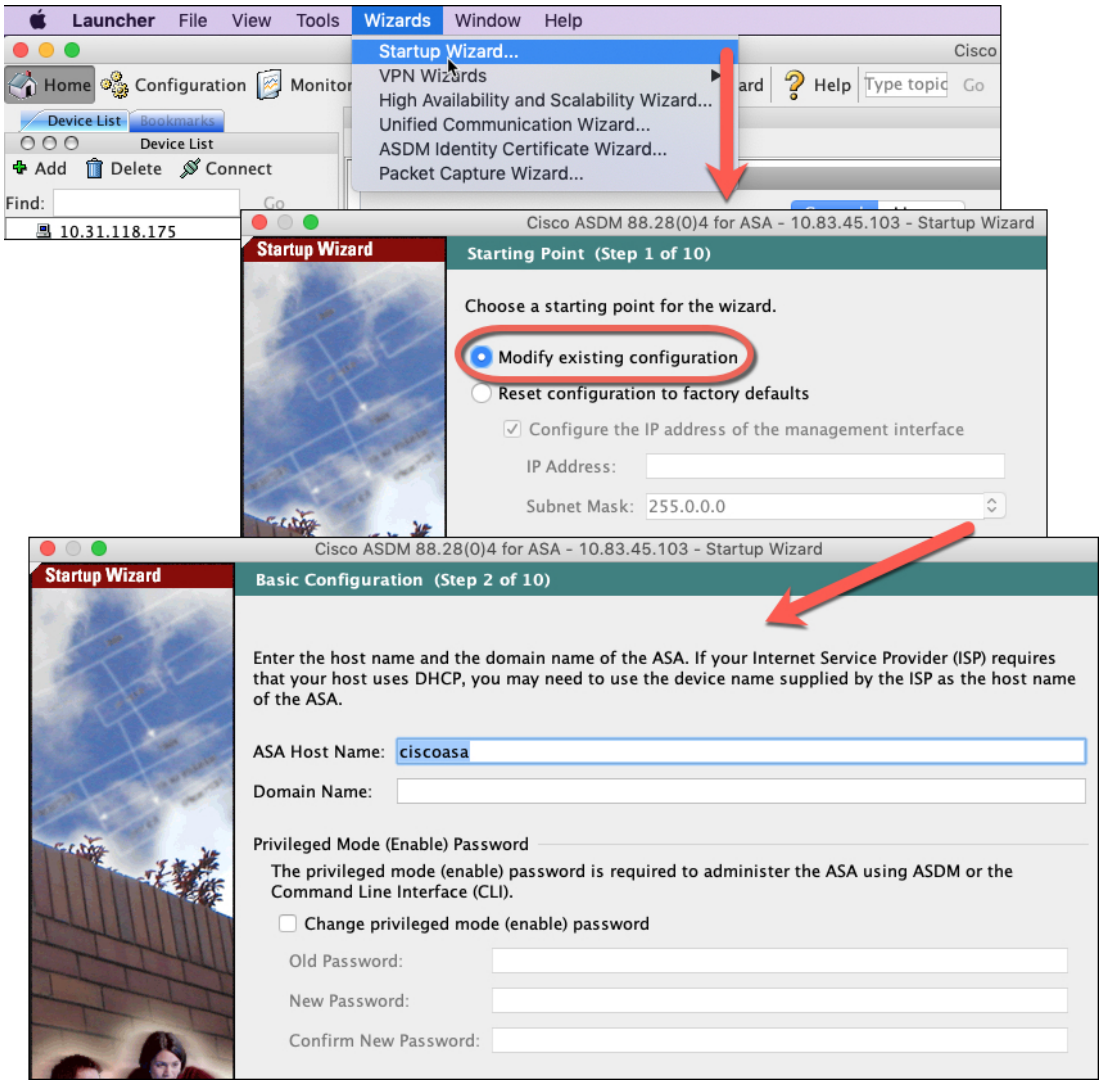
When you change licenses, you need to relaunch ASDM to show updated screens.

Configure the ASA

Using ASDM, you can use wizards to configure basic and advanced features. You can also manually configure features not included in wizards.

Procedure

Step 1 Choose **Wizards** > **Startup Wizard**, and click the **Modify existing configuration** radio button.



Step 2 The **Startup Wizard** walks you through configuring:

- The enable password
- Interfaces, including setting the inside and outside interface IP addresses and enabling interfaces.
- Static routes

- The DHCP server
- And more...

Step 3 (Optional) From the **Wizards** menu, run other wizards.

Step 4 To continue configuring your ASA, see the documents available for your software version at Navigating the Cisco ASA Series Documentation.

(Optional) Configure Management Access for FXOS on Data Interfaces

If you want to manage FXOS on the Firepower 2100 from a data interface, then you can configure SSH, HTTPS, and SNMP access. This feature is useful if you want to manage the device remotely, but you want to keep Management 1/1, which is the native way to access FXOS, on an isolated network. If you enable this feature, you can continue to use Management 1/1 for local access only. However, you cannot allow *remote* access to or from Management 1/1 for FXOS at the same time as using this feature. This feature requires forwarding traffic to the ASA data interfaces over the backplane (the default), and you can only specify one FXOS management gateway.

The ASA uses non-standard ports for FXOS access; the standard port is reserved for use by the ASA on the same interface. When the ASA forwards traffic to FXOS, it translates the non-standard destination port to the FXOS port for each protocol (do not change the HTTPS port in FXOS). The packet destination IP address (which is the ASA interface IP address) is also translated to an internal address for use by FXOS. The source address remains unchanged. For returning traffic, the ASA uses its data routing table to determine the correct egress interface. When you access the ASA data IP address for the management application, you must log in using an FXOS username; ASA usernames only apply for ASA management access.

You can also enable FXOS management traffic *initiation* on ASA data interfaces, which is required for SNMP traps, or NTP and DNS server access, for example. By default, FXOS management traffic initiation is enabled for the ASA outside interface for DNS and NTP server communication (required for Smart Software Licensing communication).

Before you begin

- Single context mode only.
- Excludes ASA management-only interfaces.
- You cannot use a VPN tunnel to an ASA data interface and access FXOS directly. As a workaround for SSH, you can VPN to the ASA, access the *ASA* CLI, and then use the **connect fxos** command to access the FXOS CLI. Note that SSH, HTTPS, and SNMPv3 are/can be encrypted, so direct connection to the data interface is safe.
- Ensure that the FXOS gateway is set to forward traffic to the ASA data interfaces (the default). If you changed the gateway, then see (Optional) Change the FXOS and ASA Management IP Addresses or Gateway, on page 220.

Procedure

Step 1 In ASDM, choose **Configuration** > **Device Management** > **Management Access** > **FXOS Remote Management**.

Step 2 Enable FXOS remote management.

a) Choose **HTTPS**, **SNMP**, or **SSH** from the navigation pane.

b) Click **Add**, and set the **Interface** where you want to allow management, set the **IP Address** allowed to connect, and then click **OK**.

You can create multiple entries for each protocol type. Set the **Port** if you do not want to use the following defaults:

- HTTPS default port—3443
- SNMP default port—3061
- SSH default port—3022

Step 3 Allow FXOS to initiate management connections from an ASA interface.

a) Choose **FXOS Traffic Initiation** from the navigation pane.

b) Click **Add**, and enable the ASA interfaces where you need to send FXOS management traffic. By default, the outside interface is enabled.

Step 4 Click **Apply**.

Step 5 Connect to the chassis manager (by default https://192.168.45.45, with the username: **admin** and the password you set at initial login).

Step 6 Click the **Platform Settings** tab, and enable **SSH**, **HTTPS**, or **SNMP**.

SSH and HTTPS are enabled by default.

Step 7 Configure an **Access List** on the **Platform Settings** tab to allow your management addresses. SSH and HTTPS only allow the Management 1/1 192.168.45.0 network by default. You need to allow any addresses that you specified in the **FXOS Remote Management** configuration on the ASA.

Access the ASA and FXOS CLI

This section describes how to connect to the FXOS and ASA console and how to connect to FXOS using SSH.

Connect to the Console Port to Access FXOS and ASA CLI

The Firepower 2100 console port connects you to the FXOS CLI. From the FXOS CLI, you can then connect to the ASA console, and back again.

You can only have one console connection at a time. When you connect to the ASA console from the FXOS console, this connection is a persistent console connection, not like a Telnet or SSH connection.

Procedure

Step 1 Connect your management computer to the console port. The Firepower 2100 ships with a DB-9 to RJ-45 serial cable, so you will need a third party serial-to-USB cable to make the connection. Be sure to install any necessary USB serial drivers for your operating system. Use the following serial settings:

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

You connect to the FXOS CLI. Enter the user credentials; by default, you can log in with the **admin** user and the default password, **Admin123**. You are prompted to change the **admin** password when you first log in.

Step 2 Connect to the ASA:

connect asa

Example:

```
firepower-2110# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
ciscoasa>
```

Step 3 To return to the FXOS console, enter **Ctrl+a**, **d**.

Connect to FXOS with SSH

You can connect to FXOS on Management 1/1 with the default IP address, 192.168.45.45. If you configure remote management ((Optional) Configure Management Access for FXOS on Data Interfaces, on page 236), you can also connect to the data interface IP address on the non-standard port, by default, 3022.

To connect using SSH to the ASA, you must first configure SSH access according to the ASA general operations configuration guide.

You can connect to the ASA CLI from FXOS, and vice versa.

FXOS allows up to 8 SSH connections.

Before you begin

To change the management IP address, see (Optional) Change the FXOS and ASA Management IP Addresses or Gateway, on page 220.

Procedure

Step 1 On the management computer connected to Management 1/1, SSH to the management IP address (by default https://192.168.45.45, with the username: **admin** and password: **Admin123**).

You can log in with any username if you added users in FXOS. If you configure remote management, SSH to the ASA data interface IP address on port 3022 (the default port).

Step 2 Connect to the ASA CLI.

connect asa

To return to the FXOS CLI, enter **Ctrl+a**, **d**.

Example:

```
firepower-2110# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
ciscoasa>
```

Step 3 If you SSH to the ASA (after you configure SSH access in the ASA), connect to the FXOS CLI.

connect fxos

You are prompted to authenticate for FXOS; use the default username: **admin** and password: **Admin123**. To return to the ASA CLI, enter **exit** or type **Ctrl-Shift-6**, **x**.

Example:

```
ciscoasa# connect fxos
Connecting to fxos.
Connected to fxos. Escape character sequence is 'CTRL-^X'.

FXOS 2.2(2.32) kp2110

firepower-2110 login: admin
Password: Admin123
Last login: Sat Jan 23 16:20:16 UTC 2017 on pts/1
Successful login attempts for user 'admin' : 4
Cisco Firepower Extensible Operating System (FX-OS) Software

[…]

firepower-2110#
firepower-2110# exit
Remote card closed command session. Press any key to continue.
Connection with fxos terminated.
Type help or '?' for a list of available commands.
ciscoasa#
```

What's Next

- To continue configuring your ASA, see the documents available for your software version at Navigating the Cisco ASA Series Documentation.
- To configure FXOS chassis settings, see the FXOS configuration guide.
- For troubleshooting, see the FXOS troubleshooting guide.

History for the Firepower 2100 in Platform Mode

Feature Name	Version	Feature Information
The default mode changed to Appliance mode	9.13(1)	With the introduction of Appliance mode, the default mode was changed to Appliance mode. In earlier releases, the only mode available was Platform mode. If you are upgrading to 9.13(1), the mode will remain in Platform mode. New/Modified commands: **fxos mode appliance**, **show fxos mode**
Prompt to set admin password	9.13(1)	You are not prompted to set the admin password when you first log into the chassis manager. Formerly, the default password was **Admin123**.