



## **Cisco Secure Firewall 4200 Getting Started Guide**

**First Published:** 2023-09-07

**Last Modified:** 2024-01-26

### **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: Secure Firewall Threat Defense or ASA. For each application, you have a choice of managers. This chapter explains the application and manager choices.

- [Applications, on page 1](#)
- [Managers, on page 1](#)

## Applications

You can use either of the following applications on your hardware platform:

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

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



---

**Note** Secure Firewall Device Manager (formerly Firepower Device Manager) is not supported on the Secure Firewall 4200.

---

Table 1: Threat Defense Managers

Manager	Description
Secure Firewall Management Center (formerly Firepower Management Center)	<p>The management center is a multi-device manager that runs on its own server hardware, or as a virtual device on a hypervisor.</p> <p>For a local management center, see <a href="#">Threat Defense Deployment with the Management Center, on page 5</a>.</p> <p>For a remote management center, see <a href="#">Threat Defense Deployment with a Remote Management Center, on page 41</a>.</p>
Cisco Defense Orchestrator (CDO) Cloud-delivered Firewall Management Center	<p>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.</p> <p>See <a href="#">Threat Defense Deployment with CDO, on page 83</a>.</p>
Secure Firewall Threat Defense REST API	<p>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 or CDO.</p> <p>The threat defense REST API is not covered in this guide. For more information, see the <a href="#">Cisco Secure Firewall Threat Defense REST API Guide</a>.</p>
Secure Firewall Management Center REST API	<p>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.</p> <p>The management center REST API is not covered in this guide. For more information, see the <a href="#">Secure Firewall Management Center REST API Quick Start Guide</a>.</p>

## ASA Managers

Table 2: ASA Managers

Manager	Description
CLI	<p>You can use the CLI to configure all ASA functionality.</p> <p>The CLI is not covered in this guide. For more information, see the <a href="#">ASA configuration guides</a>.</p>
Adaptive Security Device Manager (ASDM)	<p>ASDM is a Java-based, on-device manager that provides full ASA functionality.</p> <p>See <a href="#">ASA Deployment with ASDM, on page 125</a>.</p>
CDO	<p>CDO is a cloud-based, multi-device manager. CDO also manages other security devices, such as threat defenses.</p> <p>CDO for ASA is not covered in this guide. To get started with CDO, see the <a href="#">CDO home page</a>.</p>

Manager	Description
Cisco Security Manager (CSM)	<p>CSM is a multi-device manager that runs on its own server hardware. CSM does not support managing the threat defenses.</p> <p>CSM is not covered in this guide. For more information, see the <a href="#">CSM user guide</a>.</p>
ASA HTTP Interface	<p>Using HTTP, an automation tool can execute commands on the ASAs by accessing specifically formatted URLs.</p> <p>The ASA HTTP interface is not covered in this guide. For more information, see the <a href="#">Cisco Secure Firewall ASA HTTP Interface for Automation</a>.</p>





## 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 manage the threat defense with a management center located on your management network. For remote branch deployment, where the management center resides at a central headquarters, see [Threat Defense Deployment with a Remote Management Center](#), on page 41.

### 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](#), on page 6
- [End-to-End Tasks](#), on page 6
- [Review the Network Deployment](#), on page 8
- [Cable the Firewall](#), on page 10
- [Power on the Firewall](#), on page 12
- [\(Optional\) Check the Software and Install a New Version](#), on page 13
- [Complete the Threat Defense Initial Configuration Using the CLI](#), on page 15
- [Log Into the Management Center](#), on page 18
- [Obtain Licenses for the Management Center](#), on page 18
- [Register the Threat Defense with the Management Center](#), on page 20
- [Configure a Basic Security Policy](#), on page 23

- [Access the Threat Defense and FXOS CLI, on page 38](#)
- [Power Off the Firewall, on page 39](#)
- [What's Next?, on page 40](#)

## Before You Start

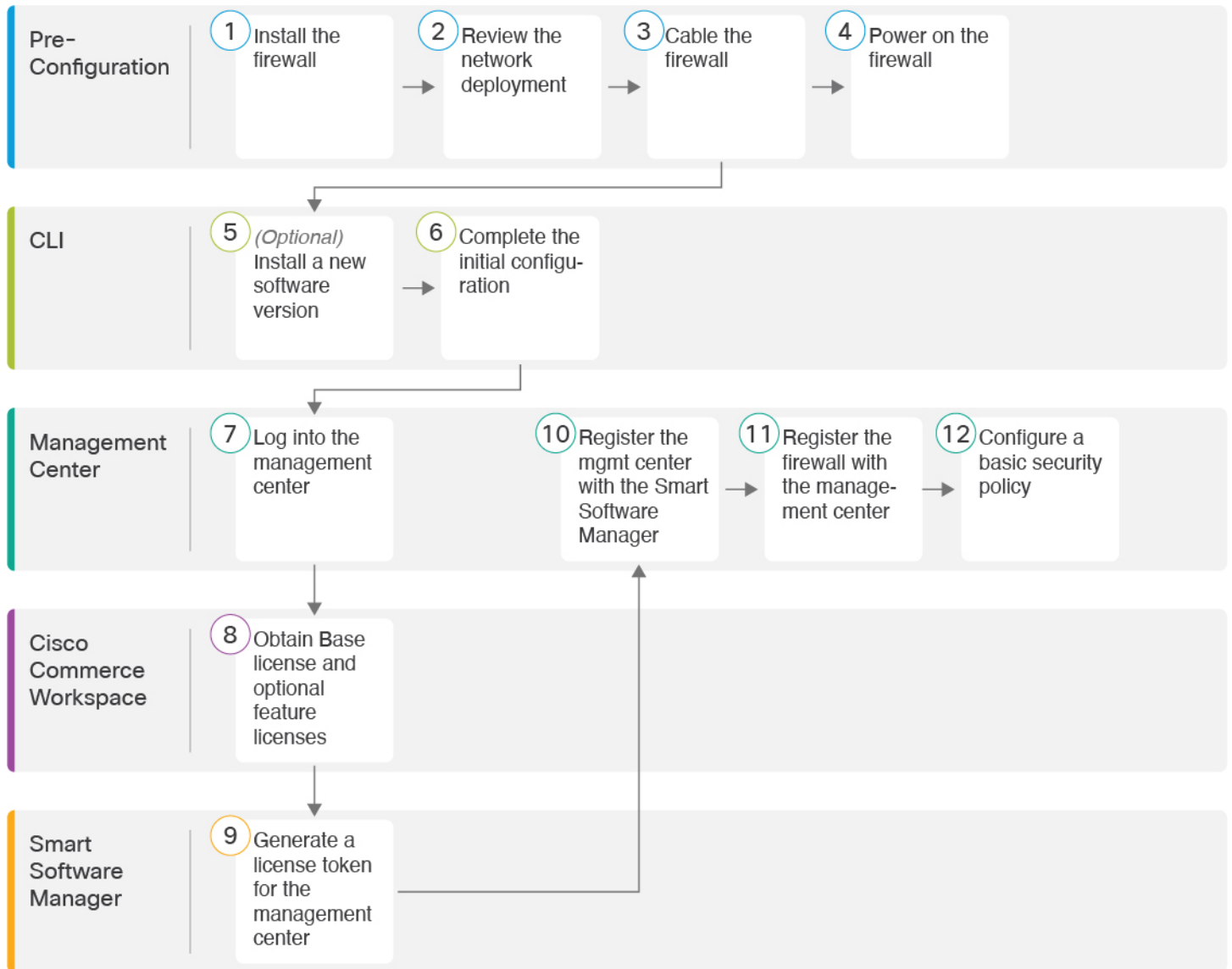
Deploy and perform initial configuration of the management center. See the getting started guide for your model.

## End-to-End Tasks

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



Figure 1: End-to-End Tasks



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

6	CLI	<a href="#">Complete the Threat Defense Initial Configuration Using the CLI, on page 15.</a>
7	Management Center	<a href="#">Log Into the Management Center, on page 18.</a>
8	Cisco Commerce Workspace	Buy Base license and optional feature licenses ( <a href="#">Obtain Licenses for the Management Center, on page 18.</a> ).
9	Smart Software Manager	Generate a license token for the management center ( <a href="#">Obtain Licenses for the Management Center, on page 18.</a> ).
10	Management Center	Register the management center with the Smart Licensing server ( <a href="#">Obtain Licenses for the Management Center, on page 18.</a> ).
11	Management Center	<a href="#">Register the Threat Defense with the Management Center, on page 20.</a>
12	Management Center	<a href="#">Configure a Basic Security Policy, on page 23.</a>

## 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 defense and 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.

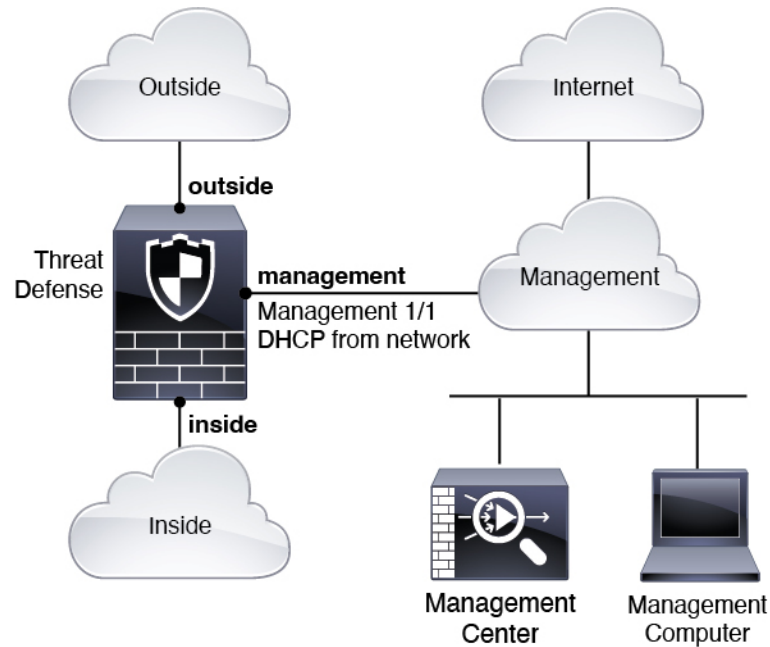
### Typical Separate Management Network Deployment

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 2: Separate Management Network**



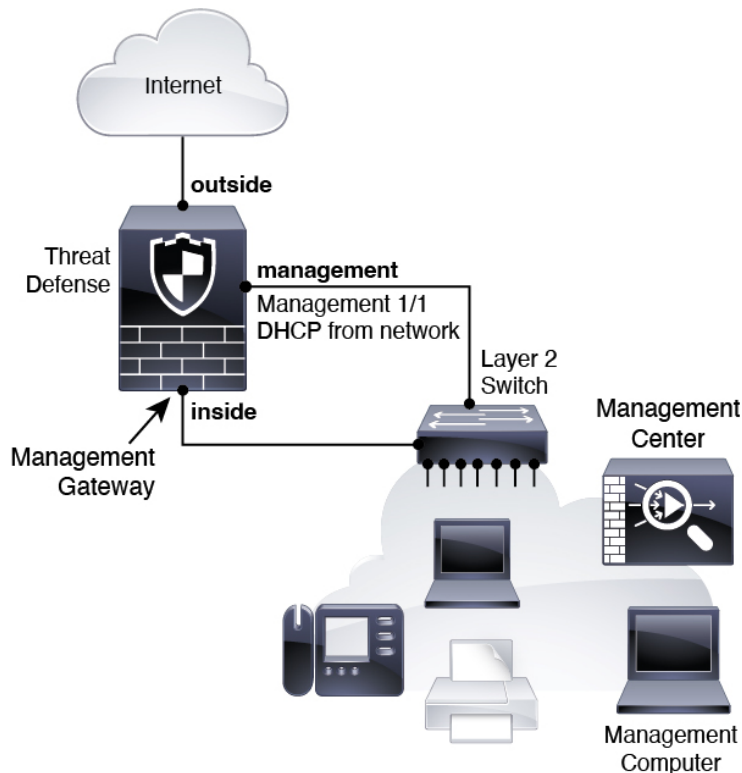
### Typical Edge Network Deployment

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 3: Edge Network Deployment



## Cable the Firewall

To cable one of the recommended scenarios on the Secure Firewall 4200, see the following steps.



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

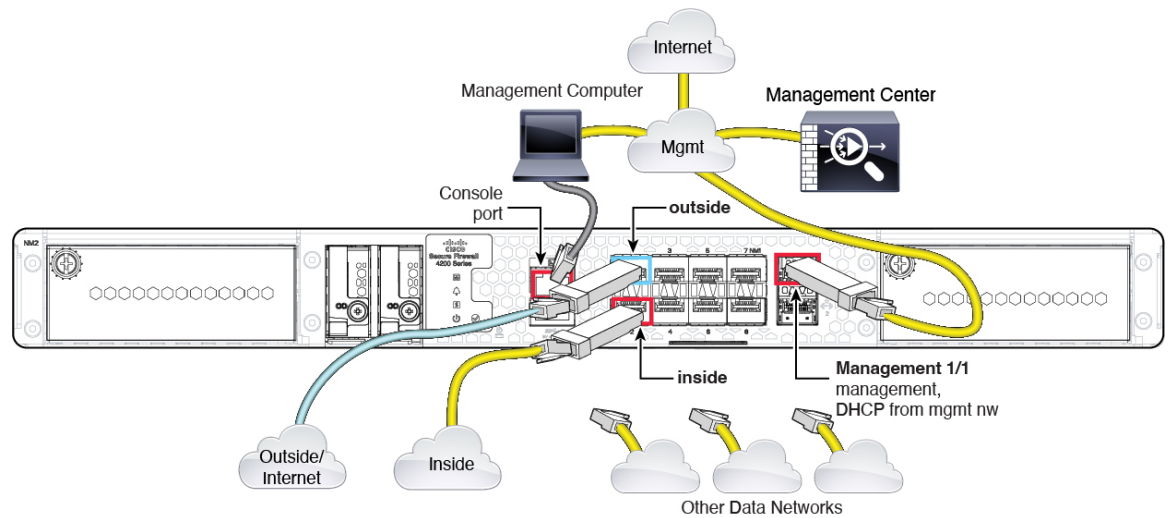
### Before you begin

- Install SFPs into the Management and data interface ports—The built-in ports are 1/10/25-Gb SFP ports that require SFP modules.
- Obtain a console cable—The firewall does not ship with a console cable by default, so you will need to buy a third-party USB-to-RJ-45 serial cable, for example.

### Procedure

- Step 1** Install the chassis. See the [hardware installation guide](#).
- Step 2** Cable for a separate management network:

Figure 4: Cabling a Separate Management Network



a) Cable the following to your management network:

- Management 1/1 interface

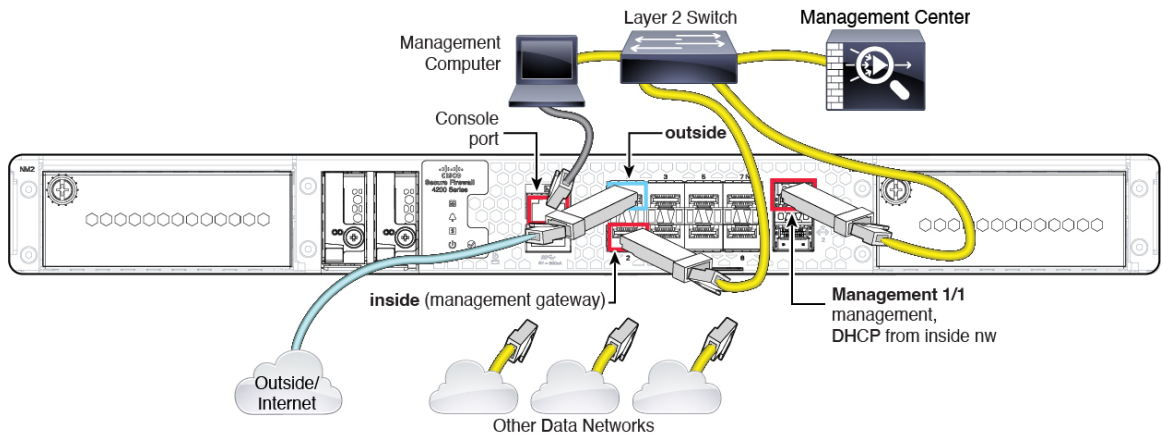
The Management 1/2 interface can be used as a separate eventing interface if the management center has a dedicated eventing interface. See the management center admin and device configuration guides for more information.

- Secure Firewall Management Center
- Management computer

- b) Connect the management computer to the console port. You need to use the console port to access the CLI for initial setup if you do not use SSH to the Management interface.
- c) Connect the inside interface (for example, Ethernet 1/2) to your inside router.
- d) Connect the outside interface (for example, Ethernet 1/1) to your outside router.
- e) Connect other networks to the remaining interfaces.

**Step 3** Cable for an edge deployment:

Figure 5: Cabling an Edge Deployment



a) Cable the following to a Layer 2 Ethernet switch:

- Inside interface (for example, Ethernet 1/2)
- Management 1/1 interface

The Management 1/2 interface can be used as a separate eventing interface if the management center has a dedicated eventing interface. See the management center admin and device configuration guides for more information.

- Secure Firewall Management Center
  - Management computer
- b) Connect the management computer to the console port. You need to use the console port to access the CLI for initial setup if you do not use SSH to the Management interface.
- c) Connect the outside interface (for example, Ethernet 1/1) to your outside router.
- d) Connect other networks to the remaining interfaces.

## Power on the Firewall

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



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

### Before you begin

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

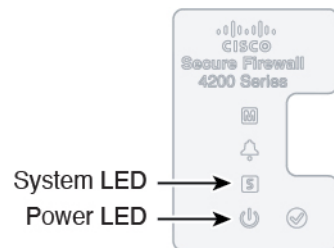
many processes running in the background all the time, and losing power does not allow the graceful shutdown of your system.

### Procedure

---

- Step 1** Attach the power cord to the firewall, and connect it to an electrical outlet.
- Step 2** Turn the power on using the standard rocker-type power on/off switch located on the rear of the chassis, adjacent to the power cord.
- Step 3** Check the Power LED on the back of the firewall; if it is solid green, the firewall is powered on.

**Figure 6: System and Power LEDs**



- Step 4** Check the System LED on the back of the firewall; after it is solid green, the system has passed power-on diagnostics.

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

## (Optional) Check the Software and Install a New Version

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

### What Version Should I Run?

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

### Procedure

---

- Step 1** Connect to the console port. See [Access the Threat Defense and FXOS CLI, on page 38](#) 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 [Complete the Threat Defense Initial Configuration Using the CLI, on page 15](#). 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.



# 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. 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.

## 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 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.
- **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'
```

```
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 alphanumeric 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 alphanumeric 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
- **Carrier**—Diameter, GTP/GPRS, M3UA, SCTP

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

### Before you begin

- Have a master account on the [Smart Software Manager](#).

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

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

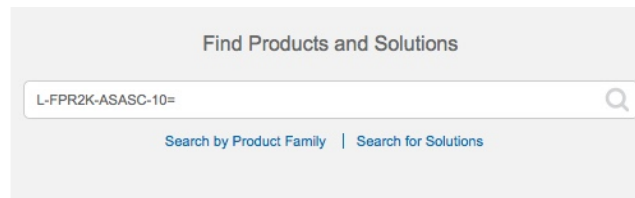
### Procedure

#### Step 1

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

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

**Figure 7: License Search**



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

- Essentials license:
  - L-FPR4215-BSE=
  - L-FPR4225-BSE=
  - L-FPR4245-BSE=
- IPS, Malware Defense, and URL license combination:
  - L-FPR4215T-TMC=
  - L-FPR4225T-TMC=
  - L-FPR4245T-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-FPR4215T-TMC-1Y
  - L-FPR4215T-TMC-3Y
  - L-FPR4215T-TMC-5Y
  - L-FPR4225T-TMC-1Y
  - L-FPR4225T-TMC-3Y
  - L-FPR4225T-TMC-5Y
  - L-FPR4245T-TMC-1Y
  - L-FPR4245T-TMC-3Y
  - L-FPR4245T-TMC-5Y
- Carrier license:
    - L-FPR4200-FTD-CAR=
  - Cisco Secure Client—See the [Cisco Secure Client Ordering Guide](#).

- Step 2** If you have not already done so, register the management center with the Smart Licensing server. Registering requires you to generate a registration token in the Smart Software Manager. See the [Cisco Secure Firewall Management Center Administration Guide](#) for detailed instructions.
- 

## Register the Threat Defense with the Management Center

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

### Before you begin

- 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

### Add Device ?

Select the Provisioning Method:

Registration Key    Serial Number

CDO Managed Device

Host:†

Display Name:

Registration Key:\*

Group:

Access Control Policy:\*

**Smart Licensing**

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

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

Carrier

Malware Defense

IPS

URL

**Advanced**

Unique NAT ID:†

Transfer Packets

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 35.

**Figure 9: New Policy**

The screenshot shows the 'New Policy' configuration page. It has a title bar with a question mark icon. Below the title bar are several form elements:
 

- Name:** A text input field containing 'ftd-ac-policy'.
- Description:** An empty text input field.
- Select Base Policy:** A dropdown menu with 'None' selected.
- Default Action:** Three radio button options: 'Block all traffic' (which is selected and highlighted with a red box), 'Intrusion Prevention', and 'Network Discovery'.

 At the bottom right of the form are two buttons: 'Cancel' and 'Save'.

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

**Step 3** Click **Register**, and confirm a successful registration.



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

- Ping—Access the threat defense CLI, and ping the management center IP address using the following command:

```
ping system ip_address
```

If the ping is not successful, check your network settings using the **show network** command. If you need to change the threat defense Management IP address, use the **configure network {ipv4 | ipv6} manual** command.

- Registration key, NAT ID, and the management center IP address—Make sure you are using the same registration key, and if used, NAT ID, on both devices. You can set the registration key and NAT ID on the 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 24.
2	Configure the DHCP Server, on page 28.
3	Add the Default Route, on page 30.
4	Configure NAT, on page 32.
5	Allow Traffic from Inside to Outside, on page 35.
6	Deploy the Configuration, on page 36.

## Configure Interfaces

Enable the threat defense interfaces, assign them to security zones, and set the IP addresses. Also configure breakout ports. 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**

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router	
Management0/0	management	Physical				Disabled	Global	🔍 ↶
<input checked="" type="checkbox"/> GigabitEthernet0/0		Physical				Disabled		✎
<input checked="" type="checkbox"/> GigabitEthernet0/1		Physical				Disabled		✎
<input checked="" type="checkbox"/> GigabitEthernet0/2		Physical				Disabled		✎
<input checked="" type="checkbox"/> GigabitEthernet0/3		Physical				Disabled		✎
<input checked="" type="checkbox"/> GigabitEthernet0/4		Physical				Disabled		✎
<input checked="" type="checkbox"/> GigabitEthernet0/5		Physical				Disabled		✎
<input checked="" type="checkbox"/> GigabitEthernet0/6		Physical				Disabled		✎
<input checked="" type="checkbox"/> GigabitEthernet0/7		Physical				Disabled		✎

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

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

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

The **General** tab appears.

Figure 11: General Tab

Edit Physical Interface

General IPv4 IPv6 Path Monitoring

Name:

Enabled  
 Management Only

Description:

Mode:

Security Zone:

Interface ID:

MTU:  
  
(64 - 9000)

Priority:  
 (0 - 65535)

Propagate Security Group Tag:

NVE Only:

- 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

The screenshot shows the 'Edit Physical Interface' window with the 'IPv4' tab selected. The 'IP Type' dropdown is set to 'Use Static IP'. The 'IP Address' field contains '192.168.1.1/24'. Below the field, there is a small text example: 'eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25'.

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

Figure 13: IPv6 Tab

The screenshot shows the 'Edit Physical Interface' window with the 'IPv6' tab selected. The 'Basic' sub-tab is active. The 'Enable IPV6' checkbox is unchecked. The 'Enforce EUI 64' checkbox is unchecked. The 'Link-Local address' field is empty. The 'Autoconfiguration' checkbox is checked. The 'Obtain Default Route' checkbox is unchecked.

f) Click **OK**.

- Step 5** Click the **Edit** (✎) for the interface that you want to use for *outside*. The **General** tab appears.

Figure 14: General Tab

Edit Physical Interface

General IPv4 IPv6 Path Monitoring Hardware

Name:

Enabled  
 Management Only

Description:

Mode:

Security Zone:

Interface ID:

MTU:  
  
(64 - 9000)

Priority:  
 (0 - 65535)

Propagate Security Group Tag:

NVE Only:

- 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

Edit Physical Interface

General IPv4 IPv6 Path Monitoring

IP Type:  
Use DHCP

Obtain default route using DHCP:

DHCP route metric:  
1  
(1 - 255)

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

Figure 16: IPv6 Tab

Edit Physical Interface

General IPv4 IPv6 Path Monitoring Hardware Configuration

Basic Address Prefixes Settings DHCP

Enable IPv6:

Enforce EUI 64:

Link-Local address:

Autoconfiguration:

Obtain Default Route:

f) Click **OK**.

**Step 6** Click **Save**.

## Configure the DHCP Server

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

### Procedure

- Step 1** Choose **Devices > Device Management**, and click the **Edit** (✎) for the device.
- Step 2** Choose **DHCP > DHCP Server**.

Figure 17: DHCP Server

The screenshot shows the DHCP Server configuration page. The left sidebar contains a navigation menu with 'DHCP Server' selected. The main content area has tabs for 'Device', 'Routing', 'Interfaces', 'Inline Sets', 'DHCP', and 'VTEP'. The 'DHCP' tab is active, showing configuration fields for Ping Timeout (50), Lease Length (3600), and an unchecked 'Auto-Configuration' checkbox. Below these are fields for Domain Name, Primary and Secondary DNS Servers, and Primary and Secondary WINS Servers. At the bottom, there are tabs for 'Server' and 'Advanced'. A table at the bottom right shows a table with columns 'Interface', 'Address Pool', and 'Enable DHCP Server', and a red box highlights the '+ Add' button in the top right corner of the table area.

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

Figure 18: Add Server

The screenshot shows the 'Add Server' dialog box. It has a title bar with a question mark icon. The main content area contains the following fields: 'Interface\*' with a dropdown menu showing 'inside'; 'Address Pool\*' with a text input field containing '10.9.7.9-10.9.7.25' and a smaller text '(2.2.2.10-2.2.2.20)' below it; and a checked checkbox labeled 'Enable DHCP Server'. At the bottom, there are two buttons: 'Cancel' and 'OK'.

- **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**.

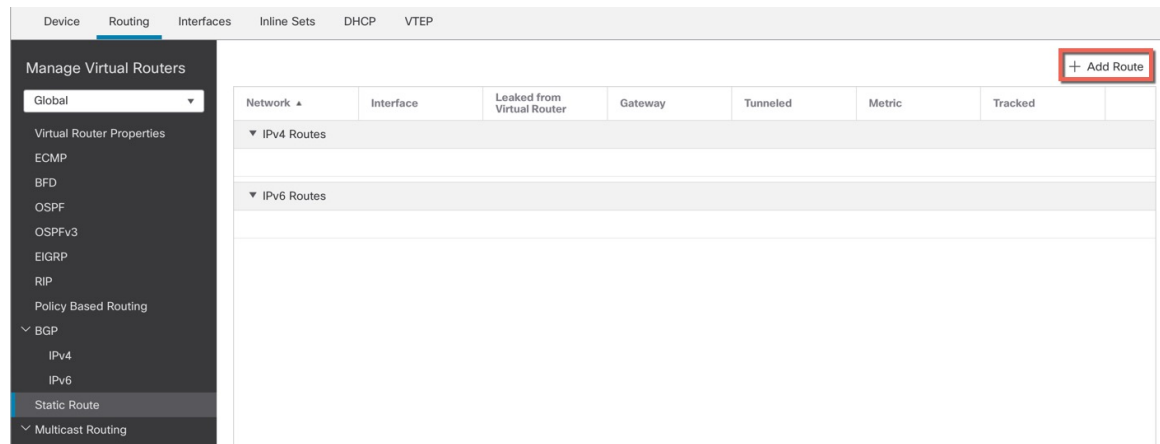
## Add the Default Route

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 screenshot shows a 'New Policy' configuration window. It has a title bar with a question mark icon. Below the title bar, there are two input fields: 'Name:' with the value 'interface\_PAT' and 'Description:' which is empty. Under the heading 'Targeted Devices', there is a sub-heading 'Select devices to which you want to apply this policy.' and a checkbox labeled 'Available Devices' which is currently unchecked. Below this is a search box with the placeholder text 'Search by name or value'. Underneath the search box is a list of available devices: '10.10.0.6' and '10.10.0.7'. The '10.10.0.6' entry is highlighted in blue. To the right of this list is a button labeled 'Add to Policy'. To the right of the 'Add to Policy' button is a list of 'Selected Devices' containing '10.10.0.6' and '10.10.0.7'. Each entry in the 'Selected Devices' list has a trash icon to its right. At the bottom right of the window are two buttons: 'Cancel' and 'Save'.

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

Figure 22: NAT Policy

interface\_PAT

Enter Description

Rules

Show Warnings Save Cancel

NAT Exemptions Policy Assignments (2)

Filter by Device Filter Rules X Add Rule

	#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Packet			Translated Packet			Options
						Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	
NAT Rules Before												
Auto NAT Rules												
NAT Rules After												

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

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

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

Figure 23: Basic Rule Options

Add NAT Rule

NAT Rule:  
Auto NAT Rule

Type:  
Dynamic

Enable

Interface Objects Translation PAT Pool Advanced

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

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

Figure 24: Interface Objects

**Add NAT Rule**

NAT Rule: Auto NAT Rule

Type: Dynamic

Enable

Interface Objects   Translation   PAT Pool   Advanced

Available Interface Objects

- inside\_zone
- 1 outside\_zone** **2 Add to Destination**
- wfxAutomationZone

Source Interface Objects (0)

Destination Interface Objects (1)

- 3 outside\_zone**

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

Figure 25: Translation

**Add NAT Rule**

NAT Rule: Auto NAT Rule

Type: Dynamic

Enable

Interface Objects   **Translation**   PAT Pool   Advanced

Original Packet

Original Source:\* **all-ipv4** +

Original Port: TCP

Translated Packet

Translated Source: **Destination Interface IP**

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

Translated Port:

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

Figure 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

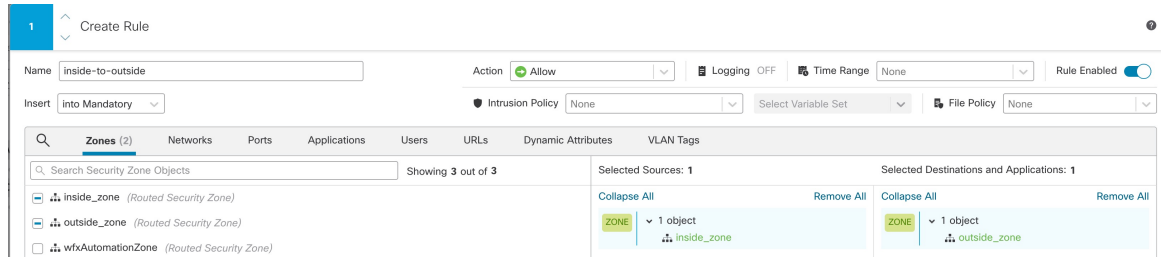
If you created a basic **Block all traffic** access control policy when you registered the threat defense, then you need to add rules to the policy to allow traffic through the device. The following procedure adds a rule to allow traffic from the inside zone to the outside zone. If you have other zones,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

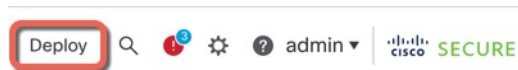
## Deploy the Configuration

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

The screenshot shows a search bar at the top left and a search icon. To the right, there are two buttons: 'Advanced Deploy' and 'Deploy All'. Below these is a table with five rows, each representing a device. Each row has a device ID, a status of 'Ready for Deployment', and a download icon.

Device ID	Status	Action
1010-2	Ready for Deployment	Download
1010-3	Ready for Deployment	Download
1120-4	Ready for Deployment	Download
node1	Ready for Deployment	Download
node2	Ready for Deployment	Download

At the bottom of the interface, there is a summary bar that says '5 devices are available for deployment' with a calendar icon and a refresh icon.

Figure 30: Advanced Deploy

The screenshot shows the 'Advanced Deploy' interface. At the top, it says '1 device selected'. Below this is a search bar and a 'Deploy' button. A table lists the selected devices with columns for Device, Modified by, Inspect Interruption, Type, Group, Last Deploy Time, Preview, and Status.

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

**Step 3**

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

Figure 31: Deployment Status

The screenshot shows the 'Deployment Status' interface. At the top, there are navigation tabs for 'Deployments', 'Upgrades', 'Health', and 'Tasks'. The 'Deployments' tab is active. Below the tabs, there is a summary bar showing '5 total' deployments, with '0 running', '5 success', '0 warnings', and '0 failures'. A search bar is also present. The main content area shows a list of deployment records, each with a green checkmark, the device ID, the deployment message, and the time taken.

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

# Access the Threat Defense and FXOS CLI

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

You can also access the FXOS CLI for troubleshooting purposes.



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

## Procedure

**Step 1** To log into the CLI, connect your management computer to the console port. The Secure Firewall 4200 does not ship with a console cable by default, so you will need to buy a third-party USB-to-RJ-45 serial cable, for example. Be sure to install any necessary USB serial drivers for your operating system. The console port defaults to the FXOS CLI. Use the following serial settings:

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

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

### Example:

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

firepower#
```

**Step 2** Access the threat defense CLI.

**connect ftd**

### Example:

```
firepower# connect ftd
>
```



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

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

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

**Example:**

```
> exit
firepower#
```

---

## Power Off the Firewall

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

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

## Power Off the Firewall Using the Management Center

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

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

**Procedure**

---

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

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

**Step 3** Click the **Device** tab.

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

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

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

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

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

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

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

## Power Off the Firewall at the CLI

You can use the FXOS CLI to safely shut down the system and power off the device. You access the CLI by connecting to the console port; see [Access the Threat Defense and FXOS CLI, on page 38](#).

### 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 with the management center.

This chapter explains how to manage the threat defense with a management center located at a central headquarters. For local deployment, where the management center resides on your local management network, see [Threat Defense Deployment with the Management Center](#), on page 5.

### 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](#), on page 41
- [Before You Start](#), on page 44
- [End-to-End Tasks](#), on page 44
- [Central Administrator Pre-Configuration](#), on page 46
- [Branch Office Installation](#), on page 53
- [Central Administrator Post-Configuration](#), on page 54

## 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.

---

- An administrator at the central headquarters pre-configures the threat defense at the CLI, 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.

- You cannot use separate management and event-only interfaces.
- Clustering is not supported. You must use the Management interface in this case.

### High Availability Requirements

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

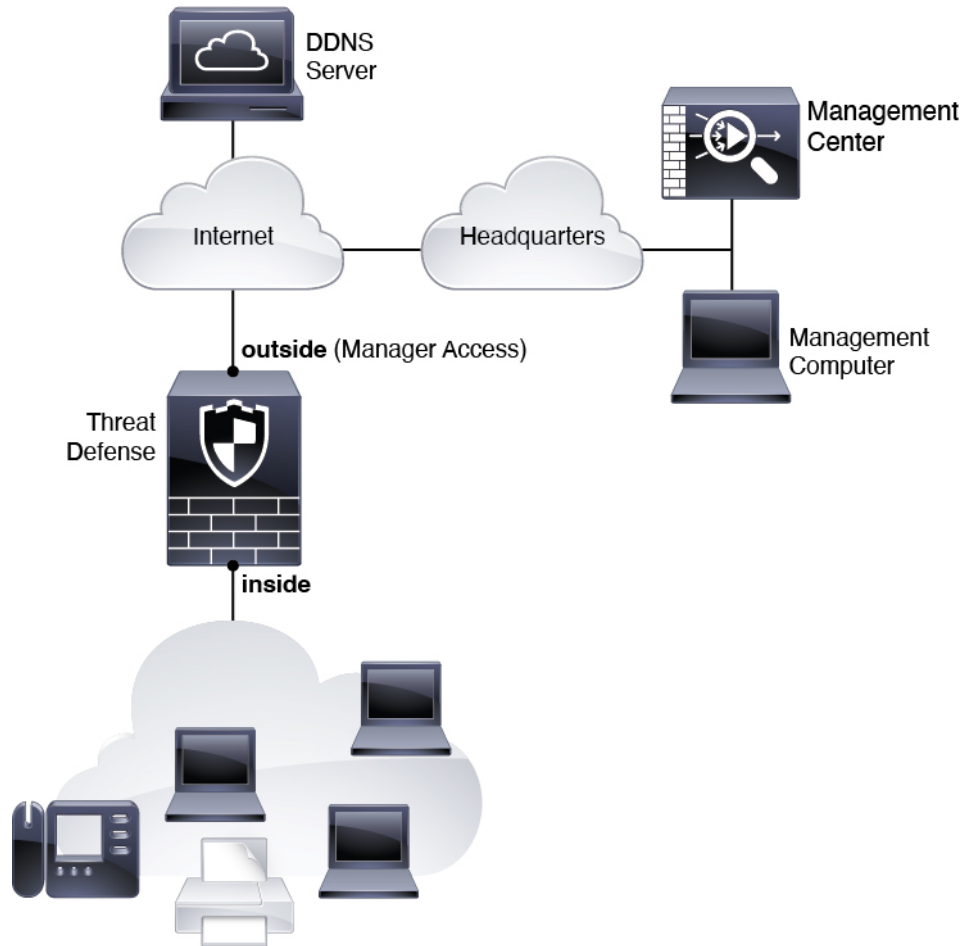
- Use the same data interface on both devices for manager access.
- Redundant manager access data interface is not supported.
- You cannot use DHCP; only a static IP address is supported. Features that rely on DHCP cannot be used, including DDNS and low-touch provisioning.
- Have different static IP 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.

### Remote Branch 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 32:



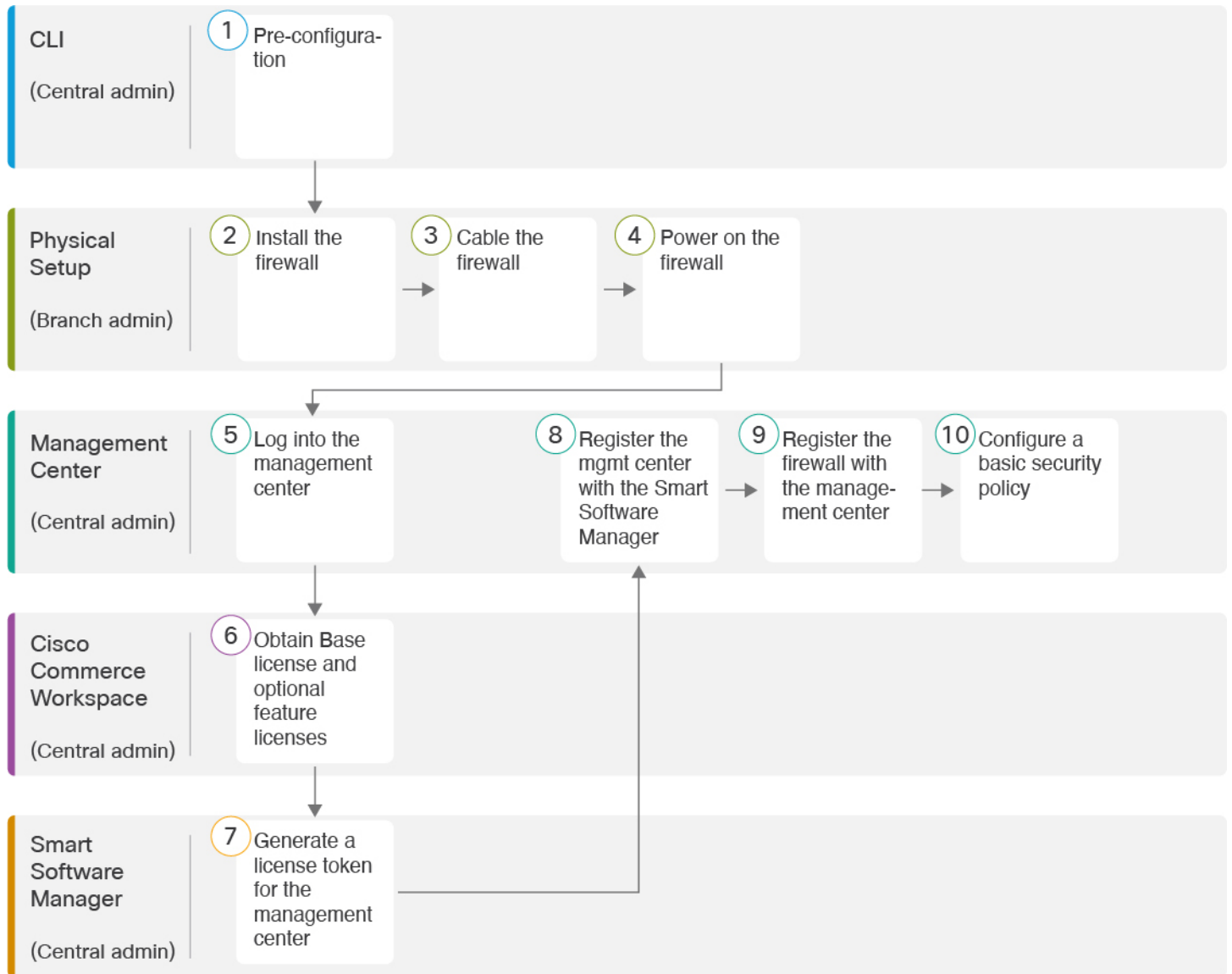
## Before You Start

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.

Figure 33: End-to-End Tasks



1	CLI (Central admin)	<ul style="list-style-type: none"> <li>• (Optional) Check the Software and Install a New Version, on page 46</li> <li>• Pre-Configuration Using the CLI, on page 48.</li> </ul>
2	Physical Setup (Branch admin)	Install the firewall. See the <a href="#">hardware installation guide</a> .
3	Physical Setup (Branch admin)	<a href="#">Cable the Firewall</a> , on page 53.
4	Physical Setup (Branch admin)	<a href="#">Power on the Firewall</a> , on page 54

5	Management Center (Central admin)	<a href="#">Log Into the Management Center, on page 18.</a>
6	Cisco Commerce Workspace (Central admin)	Buy a Base license and optional feature licenses ( <a href="#">Obtain Licenses for the Management Center, on page 55</a> ).
7	Smart Software Manager (Central admin)	Generate a license token for the management center ( <a href="#">Obtain Licenses for the Management Center, on page 55</a> ).
8	Management Center (Central admin)	Register the management center with the Smart Licensing server ( <a href="#">Obtain Licenses for the Management Center, on page 55</a> ).
9	Management Center (Central admin)	<a href="#">Add a Device to the Management Center, on page 57.</a>
10	Management Center (Central admin)	<a href="#">Configure a Basic Security Policy, on page 60.</a>

## 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 console port. See [Access the Threat Defense and FXOS CLI, on page 73](#) 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 [Pre-Configuration Using the CLI, on page 48](#). 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 Firewall at the CLI, on page 81](#).

## Pre-Configuration Using the CLI

Connect to the threat defense CLI to perform initial setup.

### 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.
- **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'

```
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 management, 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.

- Enter the **shutdown** command.
- Observe the Power LED and Status LED to verify that the chassis is powered off (appear unlit).
- After the chassis has successfully powered off, you can then unplug the power to physically remove power from the chassis if necessary.

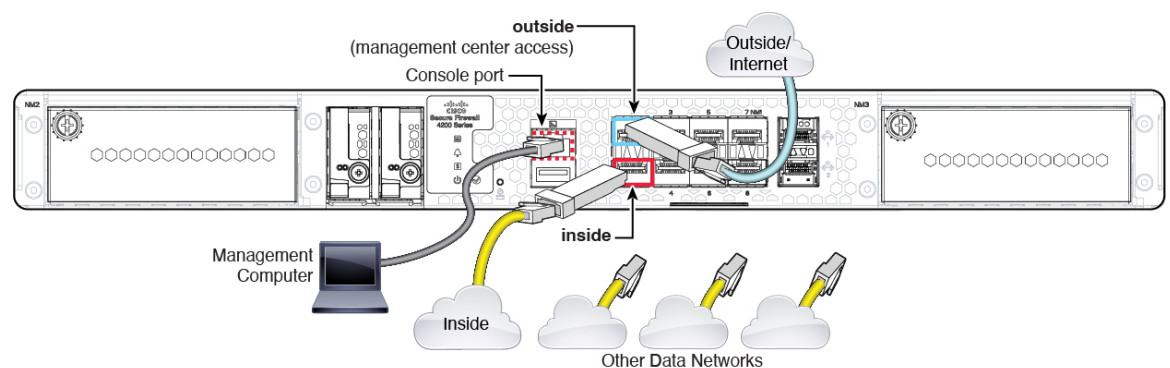
# Branch Office Installation

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 Secure Firewall 4200, see the following steps.

**Figure 34: Cabling a Remote Management Deployment**



### Before you begin

- Install SFPs into the data interface ports—The built-in ports are 1/10/25-Gb SFP ports that require SFP modules.
- (Optional) Obtain a console cable—The firewall does not ship with a console cable by default, so you will need to buy a third-party USB-to-RJ-45 serial cable, for example.

### 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** (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

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



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

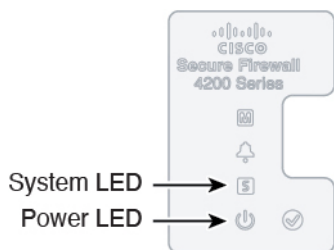
### Before you begin

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

### Procedure

- Step 1** Attach the power cord to the firewall, and connect it to an electrical outlet.
- Step 2** Turn the power on using the standard rocker-type power on/off switch located on the rear of the chassis, adjacent to the power cord.
- Step 3** Check the Power LED on the back of the firewall; if it is solid green, the firewall is powered on.

*Figure 35: System and Power LEDs*



- Step 4** Check the System LED on the back of the firewall; after it is solid green, the system has passed power-on diagnostics.

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

## 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
- **Carrier**—Diameter, GTP/GPRS, M3UA, SCTP

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

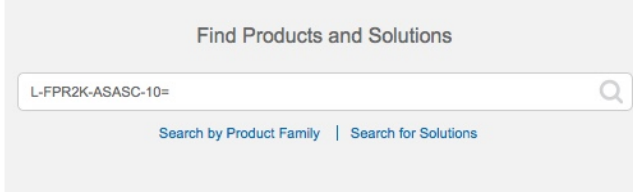
### Procedure

---

- 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 36: License Search**



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

- Essentials license:
  - L-FPR4215-BSE=
  - L-FPR4225-BSE=
  - L-FPR4245-BSE=
- IPS, Malware Defense, and URL license combination:
  - L-FPR4215T-TMC=
  - L-FPR4225T-TMC=
  - L-FPR4245T-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-FPR4215T-TMC-1Y
- L-FPR4215T-TMC-3Y
- L-FPR4215T-TMC-5Y
- L-FPR4225T-TMC-1Y
- L-FPR4225T-TMC-3Y
- L-FPR4225T-TMC-5Y
- L-FPR4245T-TMC-1Y
- L-FPR4245T-TMC-3Y
- L-FPR4245T-TMC-5Y
- Carrier license:
  - L-FPR4200-FTD-CAR=
- Cisco Secure Client—See the [Cisco Secure Client Ordering Guide](#).

- Step 2** If you have not already done so, register the management center with the Smart 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.
- 

## Add a Device to the Management Center

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 37: Add Device Using a Registration Key

### Add Device ?

Select the Provisioning Method:

Registration Key     Serial Number

CDO Managed Device

Host:†

Display Name:

Registration Key:\*

Group:

Access Control Policy:\*

**Smart Licensing**

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

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

- Carrier
- Malware Defense
- IPS
- URL

**Advanced**

Unique NAT ID:†

Transfer Packets

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 35.

**Figure 38: New Policy**

New Policy ?

Name:

Description:

Select Base Policy:

Default Action:  
 Block all traffic  
 Intrusion Prevention  
 Network Discovery

- **Smart Licensing**—Assign the Smart Licenses you need for the features you want to deploy. **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. Also configure breakout interfaces. 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 39: Interfaces**

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router	
Management0/0	management	Physical				Disabled	Global	🔍 ↶
GigabitEthernet0/0		Physical				Disabled		✎
GigabitEthernet0/1		Physical				Disabled		✎
GigabitEthernet0/2		Physical				Disabled		✎
GigabitEthernet0/3		Physical				Disabled		✎
GigabitEthernet0/4		Physical				Disabled		✎
GigabitEthernet0/5		Physical				Disabled		✎
GigabitEthernet0/6		Physical				Disabled		✎
GigabitEthernet0/7		Physical				Disabled		✎

**Step 3** To create 4 x 10-Gb breakout interfaces from a 40-Gb interface (available on some models), click the breakout icon for the interface.

If you already used the 40-Gb interface in your configuration, you will have to remove the configuration before you can proceed with the breakout.

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

The **General** tab appears.

Figure 40: General Tab

Edit Physical Interface

General IPv4 IPv6 Path Monitoring

Name:

Enabled  
 Management Only

Description:

Mode:

Security Zone:

Interface ID:

MTU:  
  
(64 - 9000)

Priority:  
 (0 - 65535)

Propagate Security Group Tag:

NVE Only:

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

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

- Click the **IPv4** and/or **IPv6** tab.
  - IPv4**—Choose **Use Static IP** from the drop-down list, and enter an IP address and subnet mask in slash notation.  
For example, enter **192.168.1.1/24**



Figure 41: IPv4 Tab

Edit Physical Interface

General IPv4 IPv6 Path Monitoring

IP Type:  
Use Static IP

IP Address:  
192.168.1.1/24  
eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25

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

Figure 42: IPv6 Tab

Edit Physical Interface

General IPv4 IPv6 Path Monitoring Hardware Configu

Basic Address Prefixes Settings DHCP

Enable IPv6:

Enforce EUI 64:

Link-Local address:

Autoconfiguration:

Obtain Default Route:

f) Click **OK**.

- Step 5** Click the **Edit** (✎) for the interface that you want to use for *outside*. The **General** tab appears.

Figure 43: General Tab

Edit Physical Interface

General IPv4 IPv6 Path Monitoring Hardware

Name:

Enabled  
 Management Only

Description:

Mode:

Security Zone:

Interface ID:

MTU:  
  
(64 - 9000)

Priority:  
 (0 - 65535)

Propagate Security Group Tag:

NVE Only:

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 6** Click **Save**.

## Configure the DHCP Server

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

## Procedure

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

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

**Figure 44: DHCP Server**

The screenshot shows the DHCP Server configuration page. The left sidebar has 'DHCP Server' selected. The main area has the following fields:

- Ping Timeout: 50 (10 - 10000 ms)
- Lease Length: 3600 (300 - 10,48,575 sec)
- Auto-Configuration:
- Interface:
- Override Auto Configured Settings:
  - Domain Name:
  - Primary DNS Server:  +
  - Secondary DNS Server:  +
  - Primary WINS Server:  +
  - Secondary WINS Server:  +

At the bottom right, there is a red-bordered '+ Add' button.

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

**Figure 45: Add Server**

The 'Add Server' dialog box has the following fields:

- Interface\*:
- Address Pool\*:   
(2.2.2.10-2.2.2.20)
- Enable DHCP Server

At the bottom, there are 'Cancel' and 'OK' buttons.

- **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

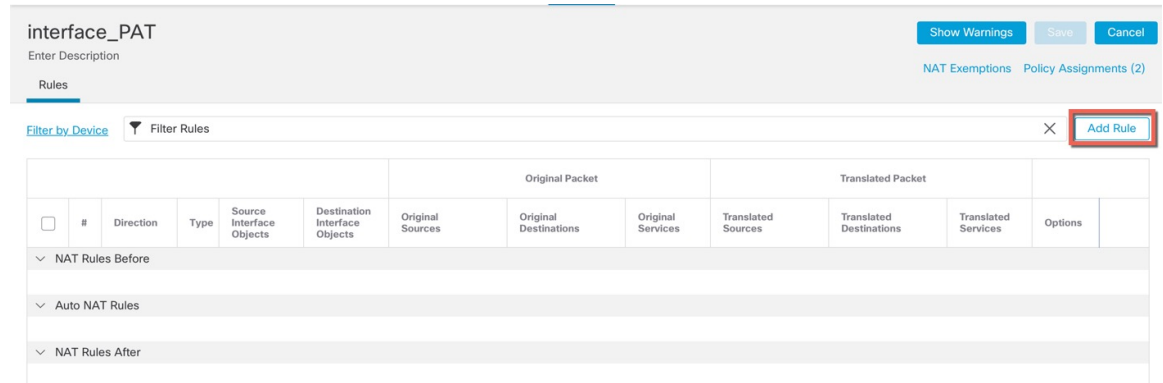
**Step 1** Choose **Devices > NAT**, and click **New Policy > Threat Defense NAT**.

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

**Figure 46: New Policy**

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

Figure 47: NAT Policy

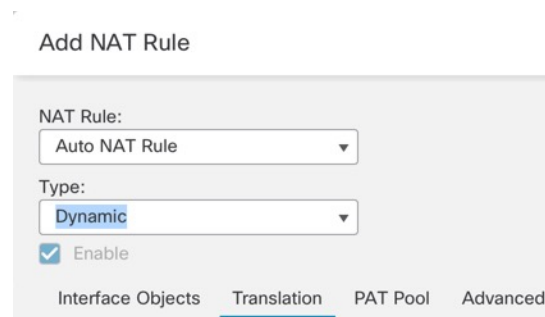


**Step 3** Click **Add Rule**.

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

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

Figure 48: 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 49: Interface Objects

**Add NAT Rule**

NAT Rule: Auto NAT Rule

Type: Dynamic

Enable

Interface Objects   Translation   PAT Pool   Advanced

Available Interface Objects

- inside\_zone
- 1 outside\_zone** **2 Add to Destination**
- wfxAutomationZone

Source Interface Objects (0)

Destination Interface Objects (1)

- 3 outside\_zone**

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

Figure 50: Translation

**Add NAT Rule**

NAT Rule: Auto NAT Rule

Type: Dynamic

Enable

Interface Objects   **Translation**   PAT Pool   Advanced

Original Packet

Original Source:\* **all-ipv4** +

Original Port: TCP

Translated Packet

Translated Source: **Destination Interface IP**

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

Translated Port:

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

Figure 51: 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 52: Add Rule

The screenshot shows the 'Create Rule' configuration page. The rule name is 'inside-to-outside'. The action is set to 'Allow'. The rule is enabled. The 'Selected Sources' section shows 'inside\_zone' selected from a list of zones. The 'Selected Destinations and Applications' section shows 'outside\_zone' selected. Other settings like 'Intrusion Policy', 'Logging', and 'Time Range' are also visible.

- **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 SSH only 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.



SSH supports the following ciphers and key exchange:

- Encryption—aes128-cbc, aes192-cbc, aes256-cbc, aes128-ctr, aes192-ctr, aes256-ctr
- Integrity—hmac-sha2-256
- Key exchange—dh-group14-sha256




---

**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.

- Click **Add** to add a new rule, or click **Edit** to edit an existing rule.
- 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.

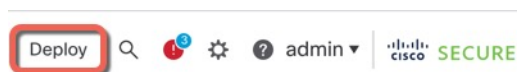
## Deploy the Configuration

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 53: Deploy*



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

*Figure 54: Deploy All*

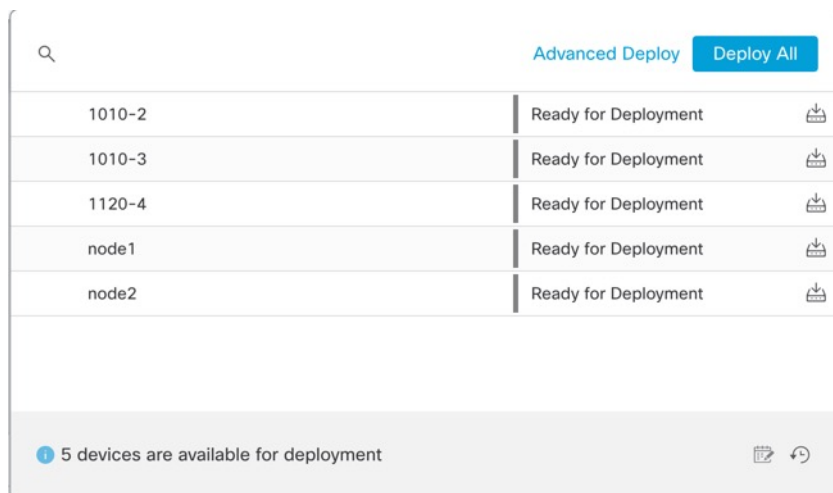


Figure 55: Advanced Deploy

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

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

Figure 56: Deployment Status

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

## Access the Threat Defense and FXOS CLI

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

You can also access the FXOS CLI for troubleshooting purposes.



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

### Procedure

**Step 1** To log into the CLI, connect your management computer to the console port. The Secure Firewall 4200 does not ship with a console cable by default, so you will need to buy a third-party USB-to-RJ-45 serial cable, for

example. 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 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 > 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                : 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              : 10.10.1.4
Display name      : 10.10.1.4
Identifier        : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration      : Completed
Management type   : Configuration

```

### 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 interface 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 > 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
Successfully 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 manager access, 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 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 supported for high availability but not supported for 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.

## 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.

**Note** If the rollback failed and the management center 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 the management center management access is restored; in this case, you can resolve the management center configuration issues, and redeploy from the management center.

### **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, 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 management center, 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 74](#).

---

## Power Off the Firewall

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

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

### Power Off the Firewall Using the Management Center

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

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

#### Procedure

---

- Step 1** Choose **Devices > Device Management**.
  - Step 2** Next to the device that you want to restart, click **Edit** (✎).
  - Step 3** Click the **Device** tab.
  - Step 4** Click **Shut Down Device** (✕) in the **System** section.
  - Step 5** When prompted, confirm that you want to shut down the device.
  - Step 6** If you have a console connection to the firewall, monitor the system prompts as the firewall shuts down. You will see the following prompt:  
  

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

If you do not have a console connection, wait approximately 3 minutes to ensure the system has shut down.
  - Step 7** You can now turn off the power switch and unplug the power to physically remove power from the chassis if necessary.
- 

### Power Off the Firewall at the CLI

You can use the FXOS CLI to safely shut down the system and power off the device. You access the CLI by connecting to the console port; see [Access the Threat Defense and FXOS CLI, on page 73](#).

## 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 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.

### 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.

- [About Threat Defense Management by CDO](#), on [page 83](#)
- [End-to-End Tasks](#), on [page 85](#)
- [Central Administrator Pre-Configuration](#), on [page 86](#)
- [Deploy the Firewall With the Onboarding Wizard](#), on [page 93](#)
- [Configure a Basic Security Policy](#), on [page 102](#)
- [Troubleshooting and Maintenance](#), on [page 115](#)
- [What's Next](#), on [page 123](#)

## 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.

You can onboard a device using the onboarding wizard and CLI registration.

### 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.
- You cannot use separate management and event-only interfaces.
- Clustering is not supported. You must use the Management interface in this case.

### High Availability Requirements

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

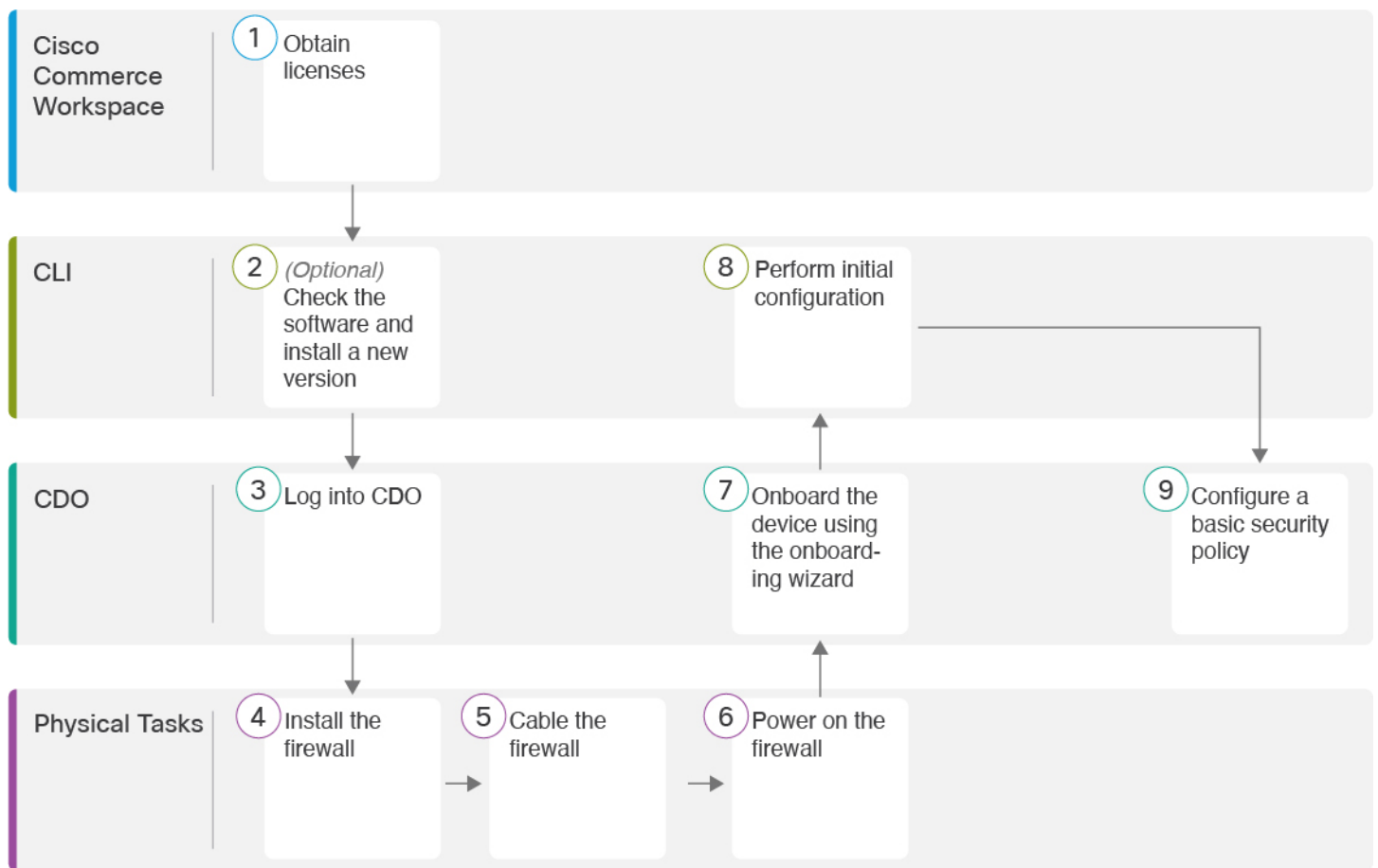
- Use the same data interface on both devices for manager access.
- Redundant manager access data interface is not supported.
- You cannot use DHCP; only a static IP address is supported. Features that rely on DHCP cannot be used, including DDNS and low-touch provisioning.

- 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

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

Figure 57: End-to-End Tasks



1	Cisco Commerce Workspace	<a href="#">Obtain Licenses, on page 86.</a>
2	CLI	<a href="#">(Optional) Check the Software and Install a New Version, on page 88.</a>

3	CDO	<a href="#">Log Into CDO, on page 89.</a>
4	Physical Tasks	Install the firewall. See the <a href="#">hardware installation guide</a> .
5	Physical Tasks	<a href="#">Cable the Firewall, on page 93.</a>
6	Physical Tasks	<a href="#">Power on the Firewall, on page 94.</a>
7	CDO	<a href="#">Onboard a Device with the Onboarding Wizard, on page 95.</a>
8	CLI	<a href="#">Perform Initial Configuration Using the CLI, on page 97.</a>
9	CDO	<a href="#">Configure a Basic Security Policy, on page 102.</a>

## 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
- **Carrier**—Diameter, GTP/GPRS, M3UA, SCTP

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

#### Before you begin

- Have a master account on the [Smart Software Manager](#).

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



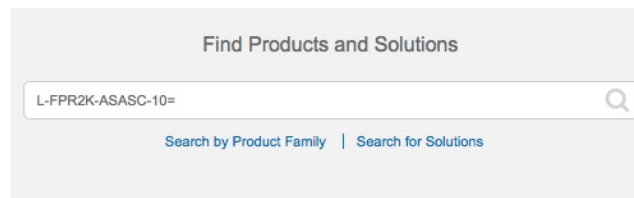
- Your Smart Software Licensing account must qualify for the Strong Encryption (3DES/AES) license to use some features (enabled using the export-compliance flag).

## Procedure

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

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

**Figure 58: License Search**



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

- Essentials license:
  - L-FPR4215-BSE=
  - L-FPR4225-BSE=
  - L-FPR4245-BSE=
- IPS, Malware Defense, and URL license combination:
  - L-FPR4215T-TMC=
  - L-FPR4225T-TMC=
  - L-FPR4245T-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-FPR4215T-TMC-1Y
- L-FPR4215T-TMC-3Y
- L-FPR4215T-TMC-5Y
- L-FPR4225T-TMC-1Y
- L-FPR4225T-TMC-3Y
- L-FPR4225T-TMC-5Y
- L-FPR4245T-TMC-1Y
- L-FPR4245T-TMC-3Y

- L-FPR4245T-TMC-5Y
- Carrier license:
  - L-FPR4200-FTD-CAR=
- 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 94](#) and [Access the Threat Defense and FXOS CLI, on page 115](#) 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
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.

- If you need to set a static IP address for the Management interface, see [Perform Initial Configuration Using the CLI, on page 97](#). By default, the Management interface uses DHCP.  
You will need to download the new image from a server accessible from the Management interface.
- Perform the [reimage procedure](#) in the [FXOS troubleshooting guide](#).  
After the firewall reboots, you connect to the FXOS CLI again.

## 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 92](#).
- If you don't have a Cisco Secure Sign-On account, continue to [Create a New Cisco Secure Sign-On Account, on page 90](#).

## 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

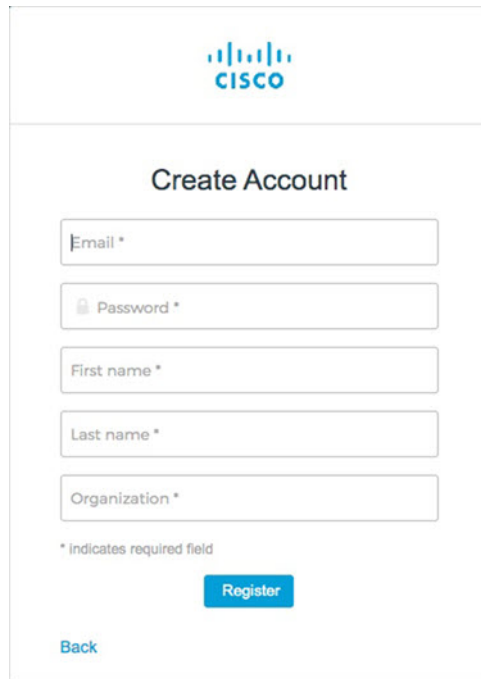
#### Step 1 Sign Up for a New Cisco Secure Sign-On Account.

- Browse to <https://sign-on.security.cisco.com>.
- At the bottom of the Sign In screen, click **Sign up**.

*Figure 59: Cisco SSO Sign Up*

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

Figure 60: Create Account



The screenshot shows the Cisco 'Create Account' form. At the top is the Cisco logo. Below it, the title 'Create Account' is centered. The form contains five input fields: 'Email \*', 'Password \*', 'First name \*', 'Last name \*', and 'Organization \*'. Each field has a small icon to its left (a key for password, a person for first name, and a person for last name). Below the fields is a note: '\* Indicates required field'. At the bottom of the form is a blue 'Register' button and a blue 'Back' link.

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

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

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

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

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

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

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

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

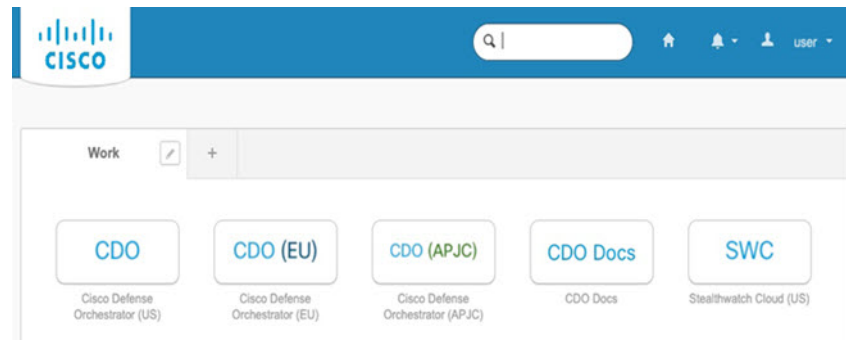
**Step 4 Configure Account Recovery Options for your Cisco Secure Sign-On Account.**

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

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

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

**Figure 61: Cisco SSO Dashboard**



## Log Into CDO with Cisco Secure Sign-On

Log into CDO to onboard and manage your device.

### Before you begin

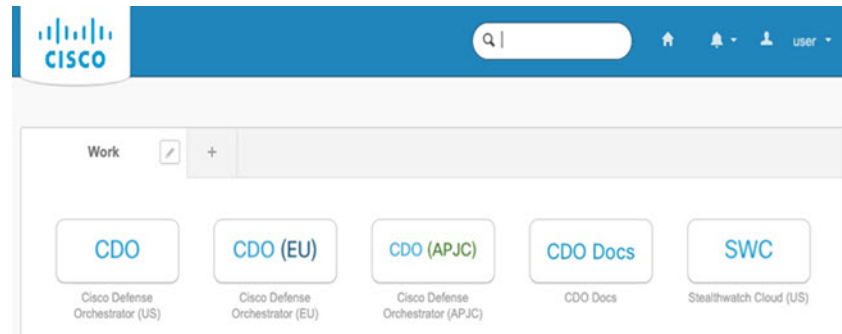
Cisco Defense Orchestrator (CDO) uses Cisco Secure Sign-On as its identity provider and Duo Security for multi-factor authentication (MFA).

- 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 90](#).
- Use a current version of Firefox or Chrome.

### Procedure

- Step 1** In a web browser, navigate to <https://sign-on.security.cisco.com/>.
- Step 2** Enter your **Username** and **Password**.
- Step 3** Click **Log in**.
- Step 4** Receive another authentication factor using Duo Security, and confirm your login. The system confirms your login and displays the Cisco Secure Sign-On dashboard.
- Step 5** Click the appropriate CDO tile on the Cisco Secure Sign-on dashboard. The **CDO** tile directs you to <https://defenseorchestrator.com>, the **CDO (EU)** tile directs you to <https://defenseorchestrator.eu>, and the **CDO (APJC)** tile directs you to <https://www.apj.cdo.cisco.com>.

Figure 62: 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.

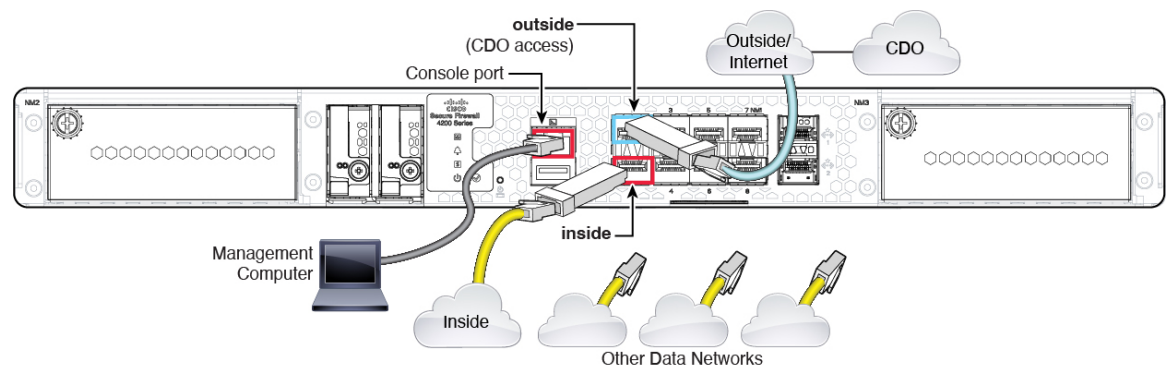
## Deploy the Firewall With the Onboarding Wizard

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 Secure Firewall 4200 to your network so that it can be managed by CDO.

Figure 63: Cabling the Secure Firewall 4200



**Before you begin**

- Install SFPs into the data interface ports—The built-in ports are 1/10/25-Gb SFP ports that require SFP modules.
- Obtain a console cable—The firewall does not ship with a console cable by default, so you will need to buy a third-party USB-to-RJ-45 serial cable, for example.

**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.

You need to perform initial setup using the CLI. The console port may also be required for troubleshooting purposes.

---

## Power on the Firewall

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




---

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

---

**Before you begin**

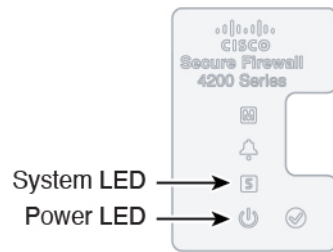
It's important that you provide reliable power for your firewall (for example, using an uninterruptible power supply (UPS)). Loss of power without first shutting down can cause serious file system damage. There are many processes running in the background all the time, and losing power does not allow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

**Procedure**

- 
- Step 1** Attach the power cord to the firewall, and connect it to an electrical outlet.
  - Step 2** Turn the power on using the standard rocker-type power on/off switch located on the rear of the chassis, adjacent to the power cord.
  - Step 3** Check the Power LED on the back of the firewall; if it is solid green, the firewall is powered on.



Figure 64: System and Power LEDs



- Step 4** Check the System LED on the back of the firewall; after it is solid green, the system has passed power-on diagnostics.

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

## Onboard a Device with the Onboarding Wizard

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

### Procedure


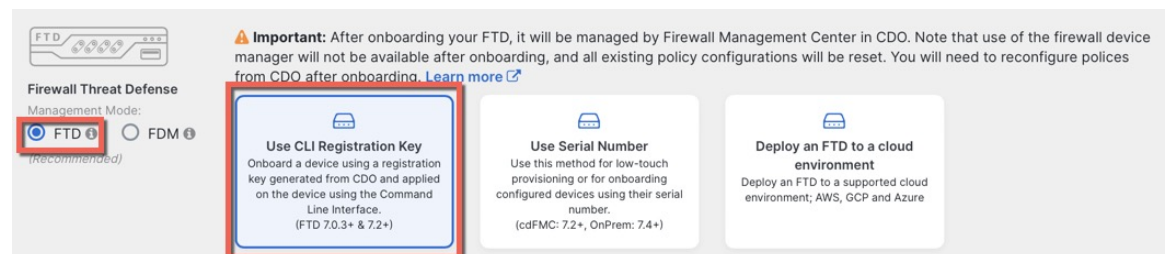
- Step 1** In the CDO navigation pane, click **Inventory**, then click the blue plus button (  ) to **Onboard** a device.
- Step 2** Select the **FTD** tile.
- Step 3** Under **Management Mode**, be sure **FTD** is selected.
- At any point after selecting **FTD** as the management mode, you can click **Manage Smart License** to enroll in or modify the existing smart licenses available for your device. See [Obtain Licenses, on page 86](#) to see which licenses are available.
- Step 4** Select **Use CLI Registration Key** as the onboarding method.

Figure 65: Use CLI Registration Key



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

Figure 66: Device Name

1 Device Name

Device Name

ftd1

Next

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

Figure 67: Access Control Policy

2 Policy Assignment

Access Control Policy

Default Access Control Policy ▾

Next

**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 68: Subscription License

3 Subscription License

Please indicate if this FTD is physical or virtual:

Physical FTD Device

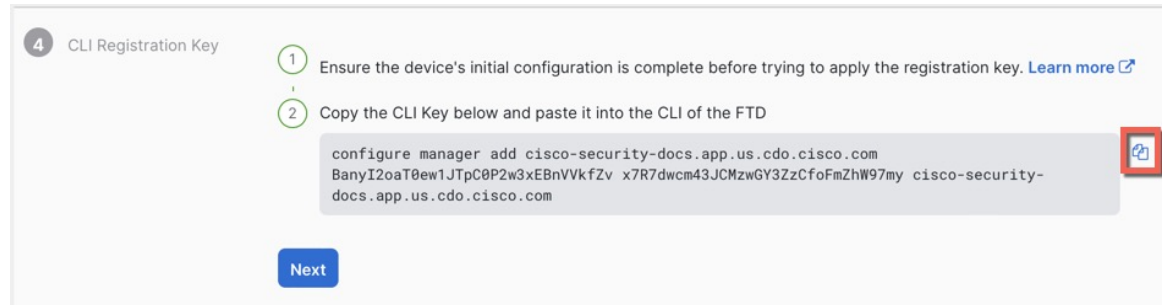
Virtual FTD Device

License Type	Includes
<input checked="" type="checkbox"/> Essentials	Base Firewall Capabilities
<input checked="" type="checkbox"/> Carrier (7.3+ FTDs only)	GTP/GPRS, Diameter, SCTP, M3UA
<input checked="" type="checkbox"/> IPS	Intrusion Policy
<input checked="" type="checkbox"/> Malware Defense	File Policy
<input checked="" type="checkbox"/> URL	URL Reputation
<input checked="" type="checkbox"/> RA VPN <span>Premier ▾</span>	RA VPN

Next

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

Figure 69: CLI Registration Key



**configure manager add** *cdo\_hostname registration\_key nat\_id display\_name*

Copy this command at the threat defense CLI after you complete the startup script. See [Perform Initial Configuration Using the CLI, on page 97](#).

#### Example:

Sample command for CLI setup:

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

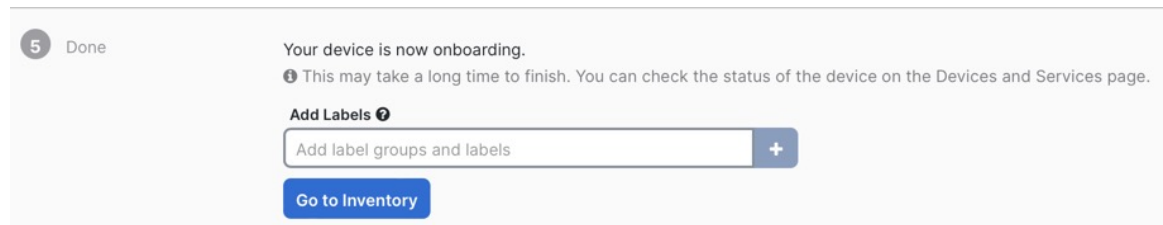
#### Step 9

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

#### Step 10

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

Figure 70: 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 Using the CLI

Connect to the threat defense CLI to perform initial setup.

## 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.
- **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'

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 management, 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 95](#) 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.

---

## 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. Also configure breakout interfaces. 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 71: Interfaces

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router	
Management0/0	management	Physical				Disabled	Global	🔍 ↶
 GigabitEthernet0/0		Physical				Disabled		✎
 GigabitEthernet0/1		Physical				Disabled		✎
 GigabitEthernet0/2		Physical				Disabled		✎
 GigabitEthernet0/3		Physical				Disabled		✎
 GigabitEthernet0/4		Physical				Disabled		✎
 GigabitEthernet0/5		Physical				Disabled		✎
 GigabitEthernet0/6		Physical				Disabled		✎
 GigabitEthernet0/7		Physical				Disabled		✎

**Step 3** To create 4 x 10-Gb breakout interfaces from a 40-Gb interface (available on some models), click the breakout icon for the interface.

If you already used the 40-Gb interface in your configuration, you will have to remove the configuration before you can proceed with the breakout.


**Step 4** Click **Edit** () for the interface that you want to use for *inside*.  
The **General** tab appears.

Figure 72: General Tab

Edit Physical Interface

General IPv4 IPv6 Path Monitoring

Name:

Enabled  
 Management Only

Description:

Mode:

Security Zone:

Interface ID:

MTU:  
  
(64 - 9000)

Priority:  
 (0 - 65535)

Propagate Security Group Tag:

NVE Only:

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

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

- Click the **IPv4** and/or **IPv6** tab.
  - IPv4**—Choose **Use Static IP** from the drop-down list, and enter an IP address and subnet mask in slash notation.  
For example, enter **192.168.1.1/24**

Figure 73: IPv4 Tab

The screenshot shows the 'Edit Physical Interface' window with the 'IPv4' tab selected. The 'IP Type' dropdown is set to 'Use Static IP'. The 'IP Address' field contains '192.168.1.1/24'. Below the field, there is a small text example: 'eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25'.

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

Figure 74: IPv6 Tab

The screenshot shows the 'Edit Physical Interface' window with the 'IPv6' tab selected. The 'Basic' sub-tab is active. The 'Enable IPv6' checkbox is unchecked. The 'Enforce EUI 64' checkbox is unchecked. The 'Link-Local address' field is empty. The 'Autoconfiguration' checkbox is checked. The 'Obtain Default Route' checkbox is unchecked.

f) Click **OK**.

- Step 5** Click the **Edit** (✎) for the interface that you want to use for *outside*. The **General** tab appears.

Figure 75: General Tab

Edit Physical Interface

General IPv4 IPv6 Path Monitoring Hardware

Name:

Enabled  
 Management Only

Description:

Mode:

Security Zone:

Interface ID:

MTU:  
  
(64 - 9000)

Priority:  
 (0 - 65535)

Propagate Security Group Tag:

NVE Only:

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 6** Click **Save**.

## Configure the DHCP Server

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

## Procedure

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

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

**Figure 76: DHCP Server**

The screenshot shows the DHCP Server configuration page. The left sidebar has a menu with 'DHCP Server' selected. The main area has tabs for 'Device', 'Routing', 'Interfaces', 'Inline Sets', 'DHCP', and 'VTEP'. The 'DHCP' tab is active. The configuration fields include: Ping Timeout (50, range 10-10000 ms), Lease Length (3600, range 300-10,48,575 sec), Auto-Configuration (checkbox), Interface (dropdown), and Override Auto Configured Settings (Domain Name, Primary/Secondary DNS and WINS Servers). At the bottom, there is a table with columns 'Interface', 'Address Pool', and 'Enable DHCP Server'. A '+ Add' button is highlighted with a red box.

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

**Figure 77: Add Server**

The screenshot shows the 'Add Server' dialog box. It has a title bar 'Add Server' with a help icon. The fields are: Interface\* (dropdown menu with 'inside' selected), Address Pool\* (text input with '10.9.7.9-10.9.7.25' and '(2.2.2.10-2.2.2.20)' below it), and a checked checkbox for 'Enable DHCP Server'. At the bottom are 'Cancel' and 'OK' buttons.

- **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 78: New Policy**

New Policy

Name:

Description:

Targeted Devices

Select devices to which you want to apply this policy.

Available Devices

Search by name or value

10.10.0.6  
 10.10.0.7

Add to Policy

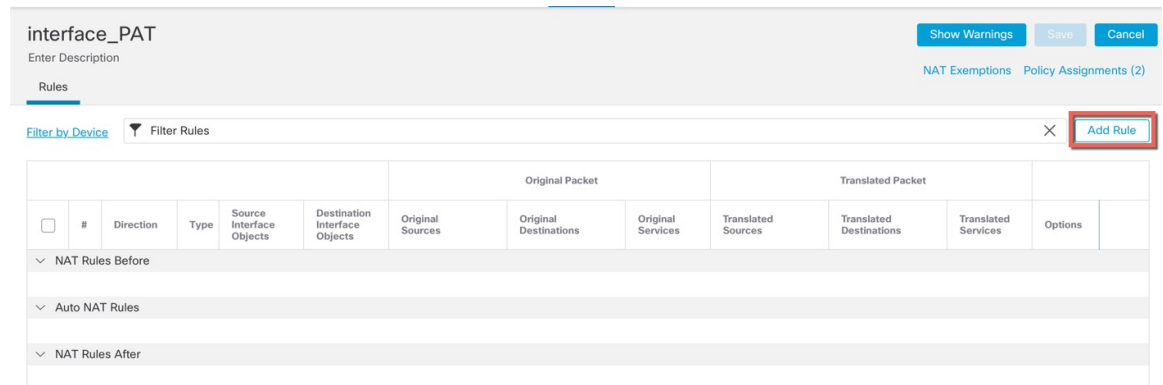
Selected Devices

10.10.0.6  
 10.10.0.7

Cancel Save

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

Figure 79: NAT Policy

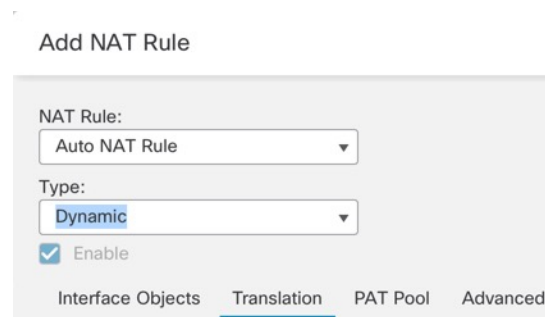


**Step 3** Click **Add Rule**.

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

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

Figure 80: 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 81: Interface Objects

**Add NAT Rule**

NAT Rule: Auto NAT Rule

Type: Dynamic

Enable

Interface Objects   Translation   PAT Pool   Advanced

Available Interface Objects

- inside\_zone
- 1** outside\_zone **2** Add to Destination
- wfxAutomationZone

Source Interface Objects (0)

Destination Interface Objects (1)

- 3** outside\_zone

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

Figure 82: Translation

**Add NAT Rule**

NAT Rule: Auto NAT Rule

Type: Dynamic

Enable

Interface Objects   **Translation**   PAT Pool   Advanced

Original Packet

Original Source:\* all-ipv4 +

Original Port: TCP

Translated Packet

Translated Source: Destination Interface IP

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

Translated Port:

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



Figure 83: 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 84: Add Rule

The screenshot shows the 'Create Rule' configuration page. The rule name is 'inside-to-outside'. The action is set to 'Allow'. The rule is enabled. The rule is applied to the 'inside\_zone' source and 'outside\_zone' destination. The interface shows various configuration options like Logging, Time Range, and File Policy.

- **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 SSH only 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.

SSH supports the following ciphers and key exchange:

- Encryption—aes128-cbc, aes192-cbc, aes256-cbc, aes128-ctr, aes192-ctr, aes256-ctr
- Integrity—hmac-sha2-256
- Key exchange—dh-group14-sha256




---

**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.

- Click **Add** to add a new rule, or click **Edit** to edit an existing rule.
- 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 85: Deploy*



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

*Figure 86: Deploy All*

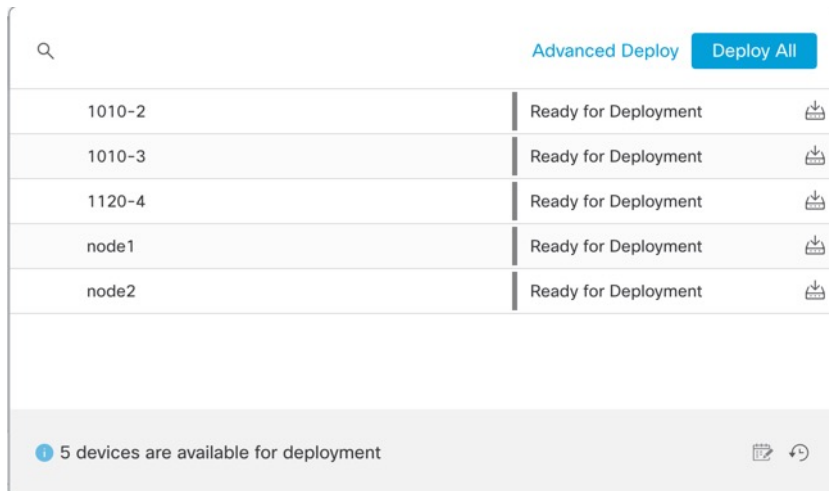


Figure 87: Advanced Deploy

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

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

Figure 88: Deployment Status

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

## 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 Secure Firewall 4200 does not ship with a console cable by default, so you will need to buy a third-party USB-to-RJ-45 serial cable, for example. 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-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 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
Successfully 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 117](#).

---

## 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.
- 

## What's Next

To continue configuring your threat defense using CDO, see the [Cisco Defense Orchestrator](#) home page.





## CHAPTER 5

# ASA Deployment with ASDM

### Is This Chapter for You?

To see all available operating systems and managers, see [Which Application and Manager is Right for You?](#), on [page 1](#). This chapter applies to ASA using ASDM.

### 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.

- [About the ASA, on page 125](#)
- [End-to-End Tasks, on page 127](#)
- [Review the Network Deployment and Default Configuration, on page 129](#)
- [Cable the Firewall, on page 131](#)
- [Power on the Firewall, on page 132](#)
- [\(Optional\) Change the IP Address, on page 133](#)
- [Log Into ASDM, on page 134](#)
- [Configure Licensing, on page 135](#)
- [Configure the ASA, on page 140](#)
- [Access the ASA and FXOS CLI, on page 142](#)
- [What's Next?, on page 143](#)

## About the ASA

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

## Migrating an ASA 5500-X Configuration

You can copy and paste an ASA 5500-X configuration into the Secure Firewall 4200. 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 , 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	Secure Firewall 4200 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.

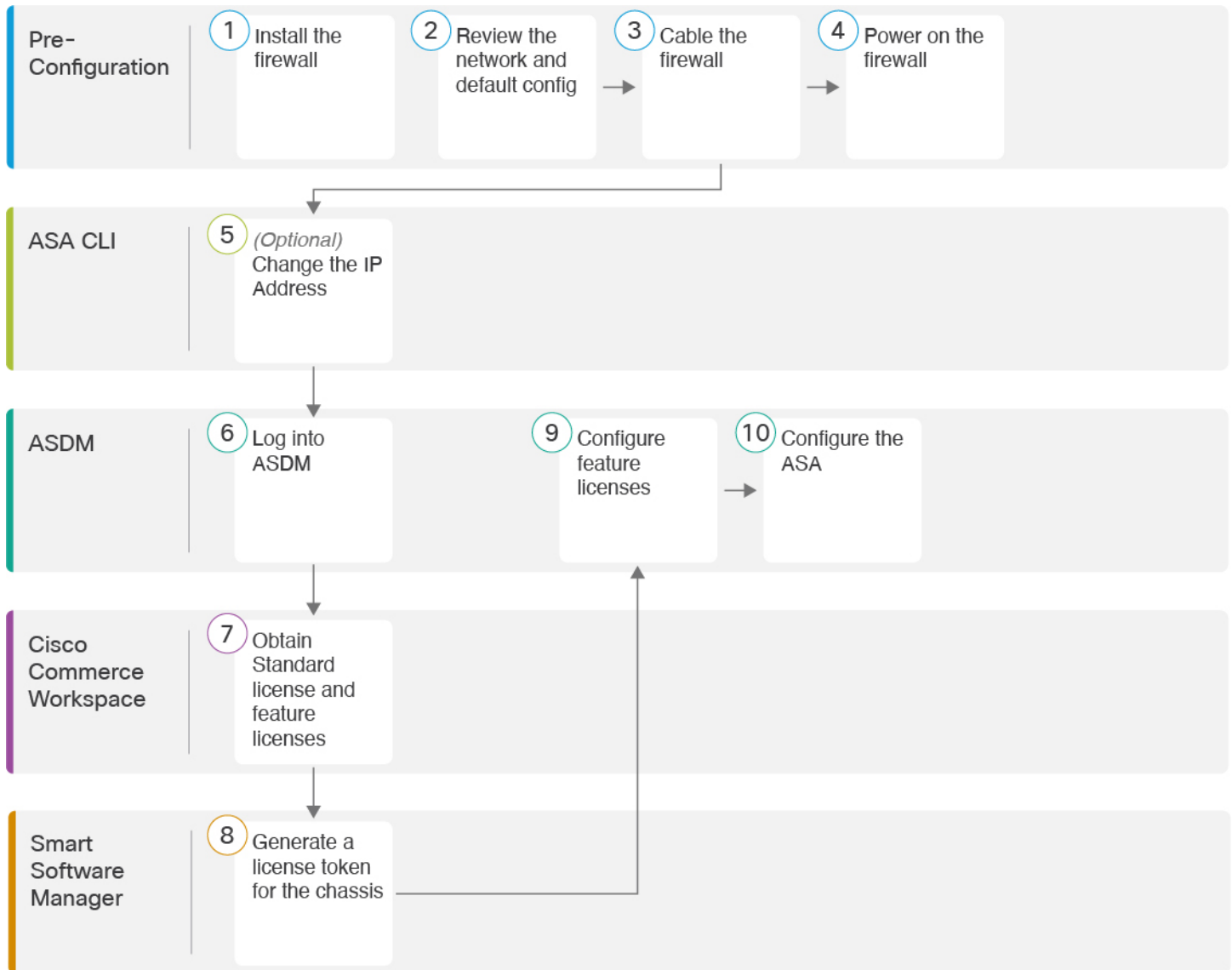


ASA 5500-X Configuration	Secure Firewall 4200 Configuration
<p><b>boot system</b> commands</p> <p>The ASA 5500-X allows up to four <b>boot system</b> commands to specify the booting image to use.</p>	<p>The Secure Firewall 4200 only allows a single <b>boot system</b> command, so you should remove all but one command before you paste. You actually do not need to have <i>any</i> <b>boot system</b> 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.</p> <p>The <b>boot system</b> 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.</p>

## End-to-End Tasks

See the following tasks to deploy and configure the ASA on your chassis.

Figure 89: End-to-End Tasks



1	Pre-Configuration	Install the firewall. See the <a href="#">hardware installation guide</a> .
2	Pre-Configuration	<a href="#">Review the Network Deployment and Default Configuration</a> , on page 129.
3	Pre-Configuration	<a href="#">Cable the Firewall</a> , on page 131.
4	Pre-Configuration	<a href="#">Power on the Firewall</a> , on page 132.
5	ASA CLI	(Optional) <a href="#">Change the IP Address</a> , on page 133.

6	ASDM	<a href="#">Log Into ASDM, on page 134.</a>
7	Cisco Commerce Workspace	Obtain Standard license and optional feature licenses ( <a href="#">Configure Licensing, on page 135</a> ).
8	Smart Software Manager	Generate a license token for the chassis ( <a href="#">Configure Licensing, on page 135</a> ).
9	ASDM	Configure feature licenses ( <a href="#">Configure Licensing, on page 135</a> ).
10	ASDM	<a href="#">Configure the ASA, on page 140.</a>

## Review the Network Deployment and Default Configuration

The following figure shows the default network deployment for the ASA using the default configuration.

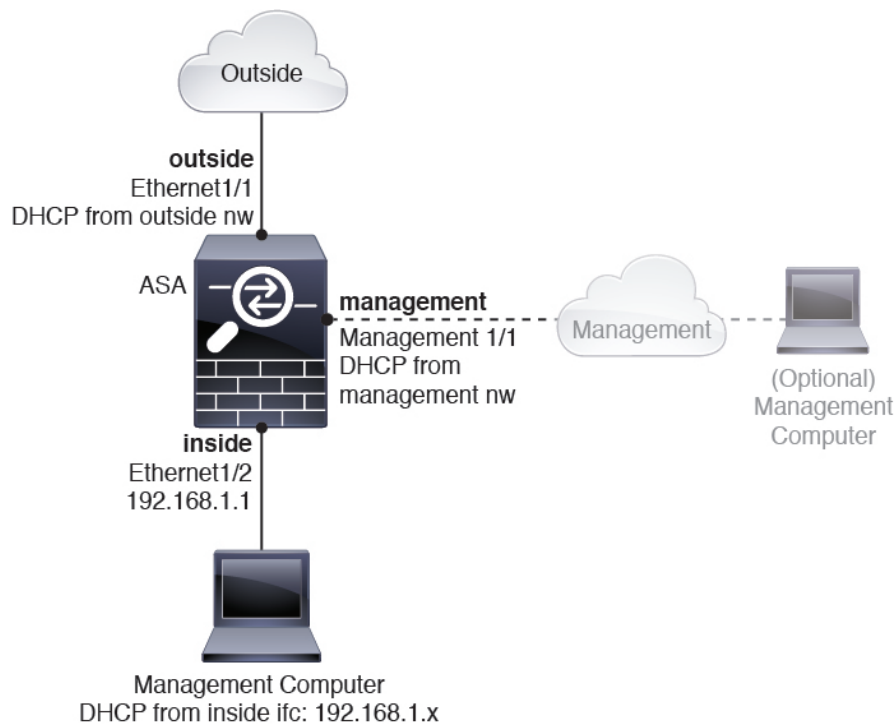
If you connect the outside interface directly to a cable modem or DSL modem, we recommend that you put the modem into bridge mode so the ASA performs all routing and NAT for your inside networks. If you need to configure PPPoE for the outside interface to connect to your ISP, you can do so as part of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



**Note** If you cannot use the default Management IP address for ASDM access, you can set the Management IP address at the ASA CLI. See [\(Optional\) Change the IP Address, on page 133](#).

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.



## Secure Firewall 4200 Default Configuration

The default factory configuration for the Secure Firewall 4200 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**—Management 1/1 (management), IP address from DHCP
- **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
```

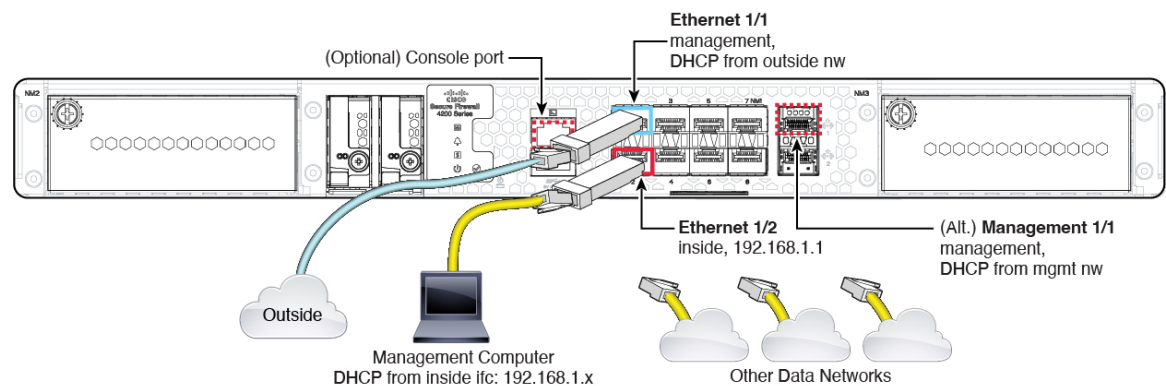
```

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 inside
!
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 Firewall

**Figure 90: Cabling the Secure Firewall 4200**



Manage the Secure Firewall 4200 on either Management 1/1 or Ethernet 1/2. The default configuration also configures Ethernet1/1 as outside.

### Before you begin

- Install SFPs into the data interface and optional Management ports—The built-in ports are 1/10/25-Gb SFP ports that require SFP modules.
- (Optional) Obtain a console cable—The firewall does not ship with a console cable by default, so you will need to buy a third-party USB-to-RJ-45 serial cable, for example.

## 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**—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 [Secure Firewall 4200 Default Configuration, on page 130](#)). Only clients on 192.168.1.0/24 can access the ASA.  
  
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 133](#).
  - **Management 1/1**—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.  
  
You can later set up Management 1/2 if you need another management interface.
- 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.  
  
For Smart Software Licensing, the ASA needs internet access.
- Step 4** Connect other networks to the remaining interfaces.
- 

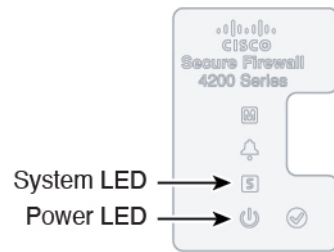
# Power on the Firewall

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

## Procedure

---

- Step 1** Attach the power cord to the firewall, and connect it to an electrical outlet.
- Step 2** Turn the power on using the standard rocker-type power on/off switch located on the rear of the chassis, adjacent to the power cord.
- Step 3** Check the Power LED on the back of the firewall; if it is solid green, the firewall is powered on.

**Figure 91: System and Power LEDs**

- Step 4** Check the System LED on the back of the firewall; after it is solid green, the system has passed power-on diagnostics.

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

## (Optional) 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 142](#) for more information.
- Step 2** Restore the default configuration with your chosen IP address.

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

#### 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](https://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 strong 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).

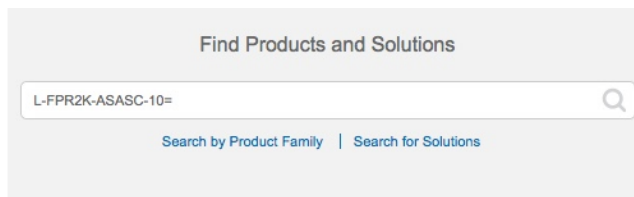
### Procedure

#### 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 92: License Search*



- Essentials license—L-FPR4215-BSE=. The Essentials license is a required license.
- Essentials license—L-FPR4225-BSE=. The Essentials license is a required license.
- Essentials license—L-FPR4245-BSE=. The Essentials license is a required license.
- 5 context license—L-FPR4200-ASASC-5=. Context licenses are additive; buy multiple licenses to meet your needs.
- 10 context license—L-FPR4200-ASASC-10=. Context licenses are additive; buy multiple licenses to meet your needs.
- Carrier (Diameter, GTP/GPRS, M3UA, SCTP)—L-FPR4200-ASA-CAR=
- Strong Encryption (3DES/AES) license—L-FPR4200-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.

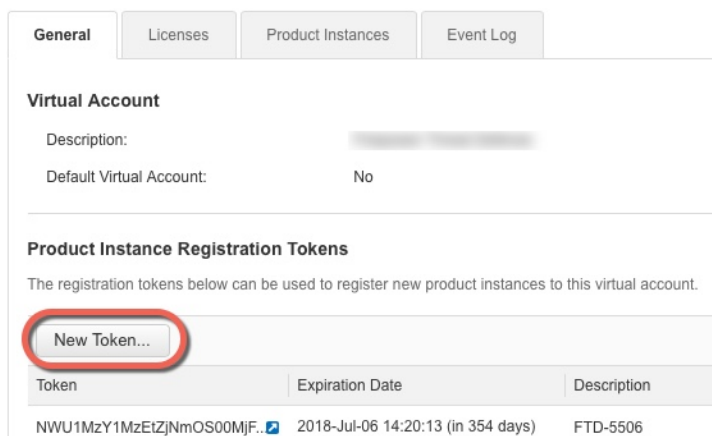
**Step 2**

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**:

**Create Registration Token**

This dialog will generate the token required to register your product instances with your Smart Account.

Virtual Account: [Redacted]

Description: [Empty text box]

\* Expire After: 30 Days

*Enter the value between 1 and 365, but Cisco recommends a maximum of 30 days.*

Allow export-controlled functionality on the products registered with this token

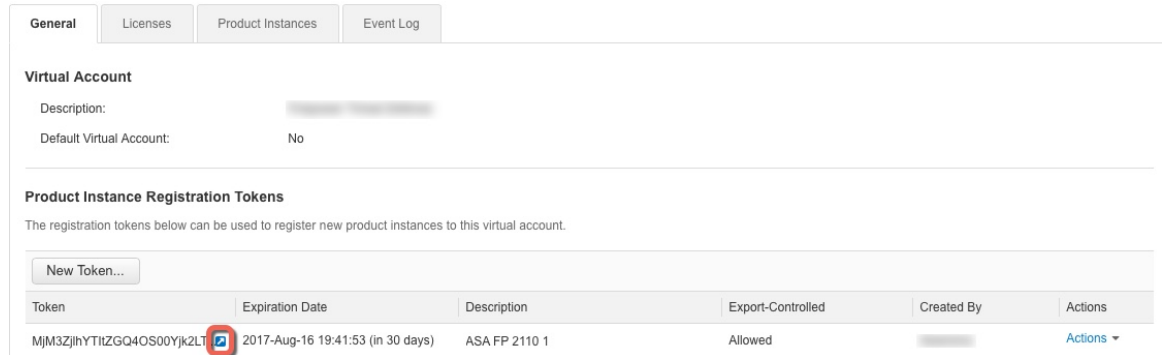
Create Token Cancel

- **Description**
- **Expire After**—Cisco recommends 30 days.
- **Allow export-controlled functionality 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.

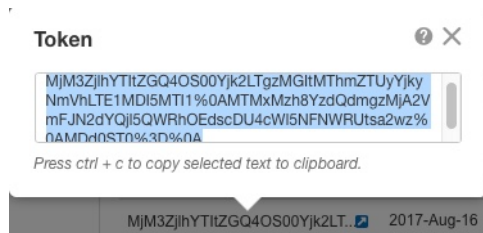
**Figure 93: View Token**



The screenshot shows the ASDM interface with the 'General' tab selected. Under 'Virtual Account', the 'Default Virtual Account' is set to 'No'. The 'Product Instance Registration Tokens' section contains a table with the following data:

Token	Expiration Date	Description	Export-Controlled	Created By	Actions
MjM3ZjhhYTItZGQ4OS00Yjk2LT...	2017-Aug-16 19:41:53 (in 30 days)	ASA FP 2110 1	Allowed		Actions

**Figure 94: Copy Token**



The 'Token' dialog box displays the token ID: `MjM3ZjhhYTItZGQ4OS00Yjk2LTg2MGltMThmZTUyYjkyNmVhLTE1MDI5MTI1%0AMTMxMzh8YzdQdmgzMjA2VmFjN2dYQjI5QWRhOEpscDU4cWl5NFNWRUtsa2wz%0AMdndST0%3D%0A`. Below the text, it says 'Press ctrl + c to copy selected text to clipboard.' The token ID is also visible in the table below the dialog box.

**Step 3** In ASDM, choose **Configuration** > **Device Management** > **Licensing** > **Smart Licensing**.

**Step 4** Click **Register**.

Configuration > Device Management > Licensing > Smart Licensing

To configure an HTTP proxy for smart licensing, see the [Smart Call-Home](#) page. Note that Smart Call Home is automatically enabled and is required for smart licensing.

Enable Smart license configuration

Feature Tier:

Throughput Level:

Privacy  Host Name  Version

Transport  Call Home  Smart Transport

Configure Transport URL

Default  URL

Registration

Utility

Proxy URL

Proxy Port

Configure Utility Mode

Enable Standard Utility Mode

Custom ID

Customer Company Identifier

Customer Company Name

Customer Street

Customer City

Customer State

Customer Country

Customer Postal Code

Registration Status: UNREGISTERED

Effective Running Licenses

License Feature	License Value
Maximum VLANs	200
Inside Hosts	Unlimited
Failover	Active/Active
Encryption-DES	Enabled
Encryption-3DES-AES	Enabled
Security Contexts	2
Carrier	Disabled

**Step 5** Enter the registration token in the **ID Token** field.

Smart License Registration

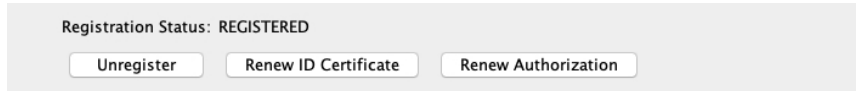
ID Token:

Force registration

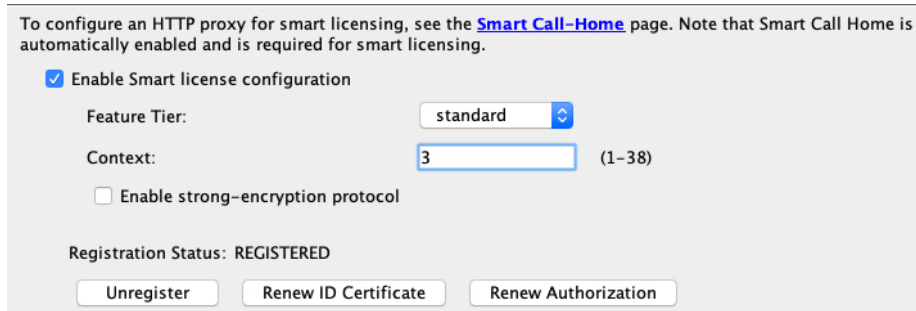
You can optionally check the **Force registration** check box to register the ASA that is already registered, but that might be out of sync with the Smart Software Manager. For example, use **Force registration** if the ASA was accidentally removed from the Smart Software Manager.

**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.
  - Secure Firewall 4200—100 contexts

For example, to use the maximum of 100 contexts on the Secure Firewall 4215, enter 98 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.

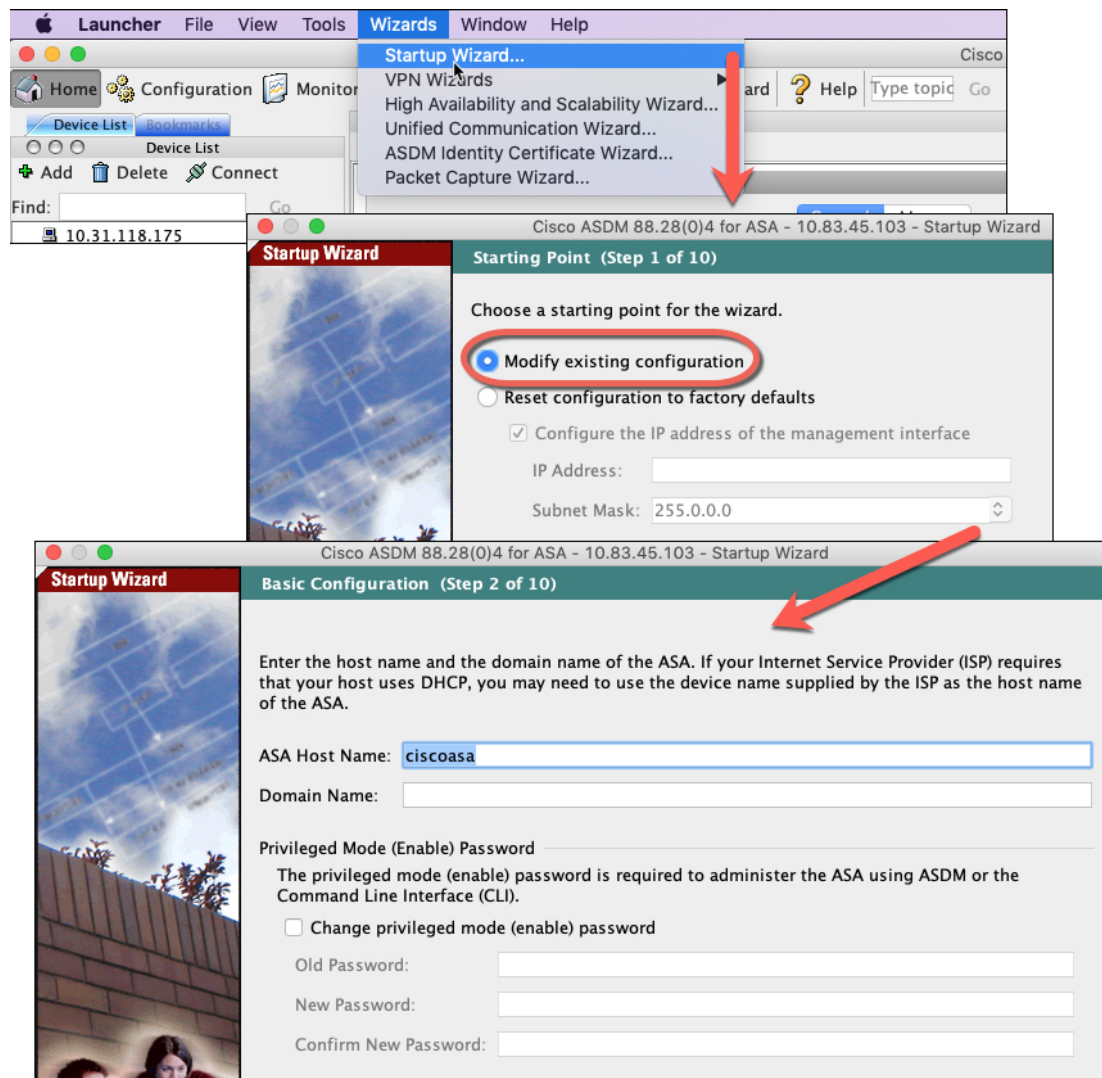
When you change licenses, you need to relaunch ASDM to show updated screens.

## 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](#).





