Cisco Firepower 4100 Getting Started Guide

First Published: 2019-03-05

Last Modified: 2023-01-23

Which Application and Manager is Right for You?

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

Applications

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

- ASA—The ASA is a traditional, advanced stateful firewall and VPN concentrator.

  You may want to use the ASA if you do not need the advanced capabilities of the threat defense, or if you need an ASA-only feature that is not yet available on the threat defense. 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.

- Threat Defense—The threat defense is a next-generation firewall that combines an advanced stateful firewall, VPN concentrator, and next generation IPS. In other words, the threat defense takes the best of ASA functionality and combines it with the best next-generation firewall and IPS functionality.

  We recommend using the threat defense over the ASA because it contains most of the major functionality of the ASA, plus additional next generation firewall and IPS functionality.

Managers

The threat defense and ASA support multiple managers.

Threat Defense Managers

Table 1: Threat Defense Managers

Manager	Description
Secure Firewall Management Center (formerly Firepower Management Center)	The management center is a powerful, web-based, multi-device manager that runs on its own server hardware, or as a virtual device on a hypervisor. You should use the management center if you want a multi-device manager, and you require all features on the threat defense. The management center also provides powerful analysis and monitoring of traffic and events. **Note** The management center is not compatible with other managers because the management center owns the threat defense configuration, and you are not allowed to configure the threat defense directly, bypassing the management center. To get started with the management center, first set up the chassis according to Firepower 4100 Chassis Initial Configuration, on page 5, and then see Threat Defense Deployment with the Management Center, on page 29.
Secure Firewall Device Manager (formerly Firepower Device Manager)	The device manager is a web-based, simplified, on-device manager. Because it is simplified, some threat defense features are not supported using the device manager. You should use the device manager if you are only managing a small number of devices and don't need a multi-device manager. **Note** Both the device manager and CDO in FDM mode can discover the configuration on the firewall, so you can use the device manager and CDO to manage the same firewall. The management center is not compatible with other managers. To get started with the device manager, first set up the chassis according to Firepower 4100 Chassis Initial Configuration, on page 5, and then see Threat Defense Deployment with the Device Manager, on page 57.
Cisco Defense Orchestrator (CDO)	CDO offers two management modes: • (7.2 and later) Cloud-delivered management center mode with all of the configuration functionality of an on-premises management center. For the analytics functionality, you can use either Secure Cloud Analytics in the cloud or an on-prem management center. • (Existing CDO users only) Device manager mode with a simplified user experience. This mode is only available to users who are already using CDO to manage threat defenses in device manager mode. This mode is not covered in this guide. Because CDO is cloud-based, there is no overhead of running CDO on your own servers. CDO also manages other security devices, such as ASAs, so you can use a single manager for all of your security devices. To get started with CDO provisioning, see Threat Defense Deployment with CDO, on page 85.

Manager	Description
Secure Firewall Threat Defense REST API	The threat defense REST API lets you automate direct configuration of the threat defense. This API is compatible with the device manager and CDO use because they can both discover the configuration on the firewall. You cannot use this API if you are managing the threat defense using the management center.
	The threat defense REST API is not covered in this guide. For more information, see the Cisco Secure Firewall Threat Defense REST API Guide.
Secure Firewall Management Center REST API	The management center REST API lets you automate configuration of management center policies that can then be applied to managed threat defenses. This API does not manage the threat defense directly.
	The management center REST API is not covered in this guide. For more information, see the Secure Firewall Management Center REST API Quick Start Guide.

ASA Managers

Table 2: ASA Managers

Manager	Description
Adaptive Security Device Manager (ASDM)	ASDM is a Java-based, on-device manager that provides full ASA functionality. You should use ASDM if you prefer using a GUI over the CLI, and you only need to manage a small number of ASAs. ASDM can discover the configuration on the firewall, so you can also use the CLI, CDO, or CSM with ASDM.
	To get started with ASDM, first set up the chassis according to Firepower 4100 Chassis Initial Configuration, on page 5, and then see ASA Deployment with ASDM, on page 113.
CLI	You should use the ASA CLI if you prefer CLIs over GUIs.
	The CLI is not covered in this guide. For more information, see the ASA configuration guides.
CDO	CDO is a simplified, cloud-based multi-device manager. Because it is simplified, some ASA features are not supported using CDO. You should use CDO if you want a multi-device manager that offers a simplified management experience. And because CDO is cloud-based, there is no overhead of running CDO on your own servers. CDO also manages other security devices, such as threat defenses, so you can use a single manager for all of your security devices. CDO can discover the configuration on the firewall, so you can also use the CLI or ASDM.
	CDO is not covered in this guide. To get started with CDO, see the CDO home page.
Cisco Security Manager (CSM)	CSM is a powerful, multi-device manager that runs on its own server hardware. You should use CSM if you need to manage large numbers of ASAs. CSM can discover the configuration on the firewall, so you can also use the CLI or ASDM. CSM does not support managing the threat defenses.
	CSM is not covered in this guide. For more information, see the CSM user guide.

Manager	Description
ASA REST API	The ASA REST API lets you automate ASA configuration. However, the API does not include all ASA features, and is no longer being enhanced.
	The ASA REST API is not covered in this guide. For more information, see the Cisco ASA REST API Quick Start Guide.

C H A P T E R **2**

Firepower 4100 Chassis Initial Configuration

Is This Chapter for You?

This chapter describes how to perform the initial setup for the Cisco Firepower 4100 chassis, including configuring interfaces for use with the ASA and the threat defense logical devices.

Is This Guide for You?

This guide describes how to set up the Firepower 4100 chassis for use with the ASA and/or threat defense application. This guide describes the following deployments:

- Standalone threat defense as either a native or container instance (multi-instance capability) using the management center

- Standalone threat defense using the device manager

Note   The device manager does not support multi-instance.

- Standalone threat defense using CDO

Note   CDO does not support multi-instance.

• Standalone ASA using ASDM

This guide does not cover the following deployments, for which you should refer to the FXOS, ASA, FDM, CDO, and FMC configuration guides:

• High Availability/Failover

• Clustering (ASA, or threat defense using the management center only)

• Multi-instance (threat defense using the management center only)

• Radware DefensePro decorator application

• CLI configuration (ASA or FXOS only)

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

About the Firepower 4100 Chassis

The Firepower 4100 chassis is a next-generation platform for network and content security solutions. The Firepower 4100 includes a supervisor and a single security engine, on which you can install logical devices. It also accepts multiple high performance network modules.

How the Logical Device Works with the Firepower 4100/9300

The Firepower 4100/9300 runs its own operating system on the supervisor called the Firepower eXtensible Operating System (FXOS). The on-the-box chassis manager provides simple, GUI-based management capabilities. You configure hardware interface settings, smart licensing (for the ASA), and other basic operating parameters on the supervisor using the chassis manager. To use the FXOS CLI, see the FXOS CLI configuration guide.

A logical device lets you run one application instance and also one optional decorator application to form a service chain. When you deploy the logical device, the supervisor downloads an application image of your choice and establishes a default configuration. You can then configure the security policy within the application operating system.

Logical devices cannot form a service chain with each other, and they cannot communicate over the backplane with each other. All traffic must exit the chassis on one interface and return on another interface to reach another logical device. For container instances, you can share data interfaces; only in this case can multiple logical devices communicate over the backplane.

Supported Applications

You can deploy logical devices on your chassis using the following application types.

Threat Defense

The threat defense provides next-generation firewall services, including stateful firewalling, routing, VPN, Next-Generation Intrusion Prevention System (NGIPS), Application Visibility and Control (AVC), URL filtering, and malware defense.

You can manage the threat defense using one of the following managers:

- Management Center—A full-featured, multidevice manager on a separate server.

- Device Manager—A simplified, single device manager included on the device.

- CDO—A cloud-based, multidevice manager.

ASA

The ASA provides advanced stateful firewall and VPN concentrator functionality in one device. You can manage the ASA using one of the following managers:

- ASDM—A single device manager included on the device. *This guide describes how to manage the ASA using ASDM.*

- CLI

- CDO—A cloud-based, multidevice manager.

- CSM—A multidevice manager on a separate server.

Radware DefensePro (Decorator)

You can install Radware DefensePro (vDP) to run in front of the ASA or the threat defense as a decorator application. vDP is a KVM-based virtual platform that provides distributed denial-of-service (DDoS) detection and mitigation capabilities on the Firepower 4100/9300. Traffic from the network must first pass through the vDP before reaching the ASA or the threat defense.

To deploy vDP, see the FXOS configuration guide.

Logical Device Application Instances: Container or Native

Logical device application instances run in the following deployment types:

- Native instance—A native instance uses all of the resources (CPU, RAM, and disk space) of the security engine, so you can only install one native instance.

- Container instance—A container instance uses a subset of resources of the security engine, so you can install multiple container instances. **Note:** Multi-instance capability is only supported for the threat defense; it is not supported for the ASA or in conjunction with vDP.

Maximum Container Instances per Model

- Firepower 4110—3

- Firepower 4112—3

- Firepower 4115—7

- Firepower 4120—3

- Firepower 4125—10

- Firepower 4140—7

- Firepower 4145—14

• Firepower 4150—7

End-to-End Procedure

See the following tasks to set up the Firepower 4100 chassis, and to deploy logical devices on your chassis.

Pre-Configuration	① Set up hardware	② Cable the chassis		
FXOS CLI or Web	③ Perform initial setup			
Chassis Manager	④ Log into the chassis manager	⑤ Configure NTP	⑥ Add FXOS Users	⑦ Configure Interfaces	⑧ Create a logical device (see application chapters)
Application	⑨ Complete application configuration			
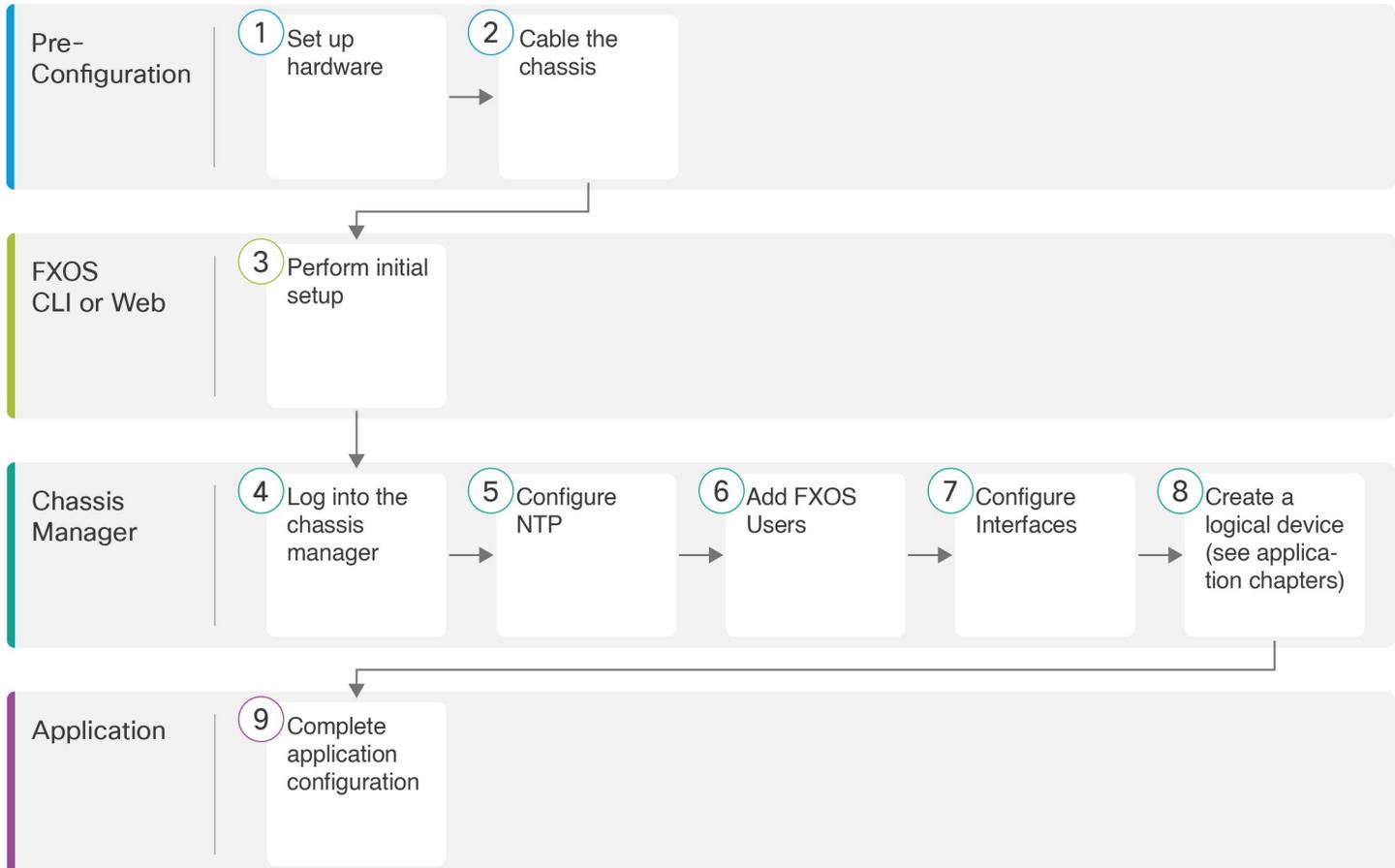
①	Pre-Configuration	Set up the Firepower 4100 hardware. See the Firepower 4100 hardware guide.
②	Pre-Configuration	Cable the Chassis, on page 9.
③	FXOS CLI or Web	Perform Initial Chassis Setup, on page 13.
④	Chassis Manager	Log Into the Chassis Manager, on page 17.
⑤	Chassis Manager	Configure NTP, on page 17.

⑥	Chassis Manager	Add FXOS Users, on page 19.
⑦	Chassis Manager	Configure Interfaces, on page 21.
⑧	Chassis Manager	Create logical devices: • Threat Defense with the management center—See Threat Defense Deployment with the Management Center, on page 29. • Threat Defense with the device manager—See Threat Defense Deployment with the Device Manager, on page 57. • Threat Defense with the CDO—See Threat Defense Deployment with CDO, on page 85. • ASA—See ASA Deployment with ASDM, on page 113. **Note** Support for threat defense with the device manager was added in FXOS 2.7.1/threat defense 6.5
⑨	Application	Complete application configuration: • Threat Defense with the management center—See Threat Defense Deployment with the Management Center, on page 29. • Threat Defense with the device manager—See Threat Defense Deployment with the Device Manager, on page 57. • Threat Defense with the CDO—See Threat Defense Deployment with CDO, on page 85. • ASA—See ASA Deployment with ASDM, on page 113.

Cable the Chassis

Cable the following interfaces for initial chassis setup, continued monitoring, and logical device use.

- Console port—(Optional) If you do not perform initial setup on the chassis Management port, connect your management computer to the console port to perform initial setup of the chassis. The Firepower 4100 includes an RS-232–to–RJ-45 serial console cable. You might need to use a third party serial-to-USB cable to make the connection.

- Chassis Management port—Connect the chassis Management port to your management network for configuration and ongoing chassis management. You can perform initial setup on this port if it receives an IP address from a DHCP server.

- Logical device Management interface—Use one or more interfaces to manage the logical devices. This guide assumes that you have a separate management network with its own internet access. You can choose any interfaces on the chassis for this purpose other than the chassis Management port, which is reserved for FXOS management. For multi-instance support, Management interfaces can be shared among logical devices, or you can use a separate interface per logical device. Typically, you share a Management

interface with all logical devices, or if you use separate interfaces, put them on a single management network. But your exact network requirements may vary. For the threat defense, the Management interface is a separate interface from data interfaces, with its own network settings. In 6.7 and later, you can optionally configure a data interface for manager access instead of using the Management interface. In this case, you must still assign a Management interface to the logical device for internal architectural reasons, but you do not need to cable it. Note that for the management center, manager access from a data interface is not supported in High Availability or Clustering deployments. For more information, see the **configure network management-data-interface** command in the FTD command reference.

- Data interfaces—Connect the data interfaces to your logical device data networks. You can configure physical interfaces, EtherChannels, VLAN subinterfaces (for container instances only), and breakout ports to divide up high-capacity interfaces. For multi-instance support, you can cable multiple logical devices to the same networks or to different networks, as your network needs dictate. For container instances, you can share data interfaces; only in this case can multiple logical devices communicate over the backplane. Otherwise, all traffic must exit the chassis on one interface and return on another interface to reach another logical device. For details about shared interface limitations and guidelines, see the FXOS configuration guide.

Note All interfaces other than the console port require SFP/SFP+/QSFP transceivers. See the hardware installation guide for supported transceivers.

Note Although not covered in this guide, for High Availability, use a Data interface for the failover/state link. For inter-chassis clustering, use an EtherChannel that is defined on the chassis as a Cluster type interface.

**Threat Defense with the Management Center Cabling**
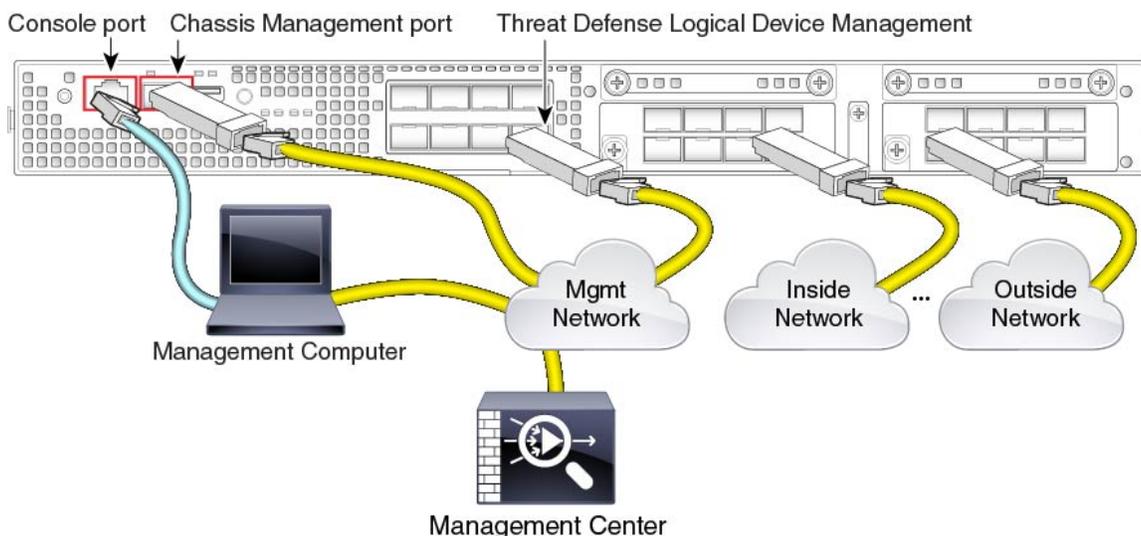
This guide assumes that you have a separate management network with its own internet access. By default, the Management interface is preconfigured when you deploy, but you have to configure data interfaces later.

Place the management center on (or accessible from) the logical device management network. The threat defense and the management center need access to the internet via the Management network for updates and licensing. In 6.7 and later, you can optionally configure a data interface for the management center management instead of the Management interface. Note that the management center access from a data interface is not supported in High Availability or Clustering deployments. For more information about configuring a data interface for the management center access, see the **configure network management-data-interface** command in the FTD command reference.

Note
The management connection is a secure, SSL-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.

Threat Defense with the Device Manager Cabling
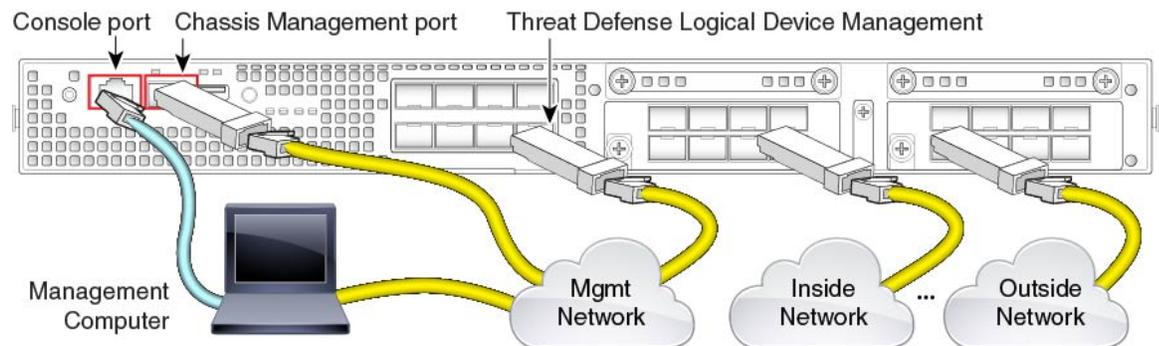
This guide assumes that you have a separate management network with its own internet access. By default, the Management interface is preconfigured when you deploy, but you have to configure data interfaces later.

Perform initial the threat defense configuration on the logical device Management interface. The threat defense requires internet access for licensing, updates, and CDO management, and the default behavior is to route management traffic to the gateway IP address you specified when you deployed the threat defense. You can later enable the device manager management from any data interface.

Threat Defense with CDO Cabling
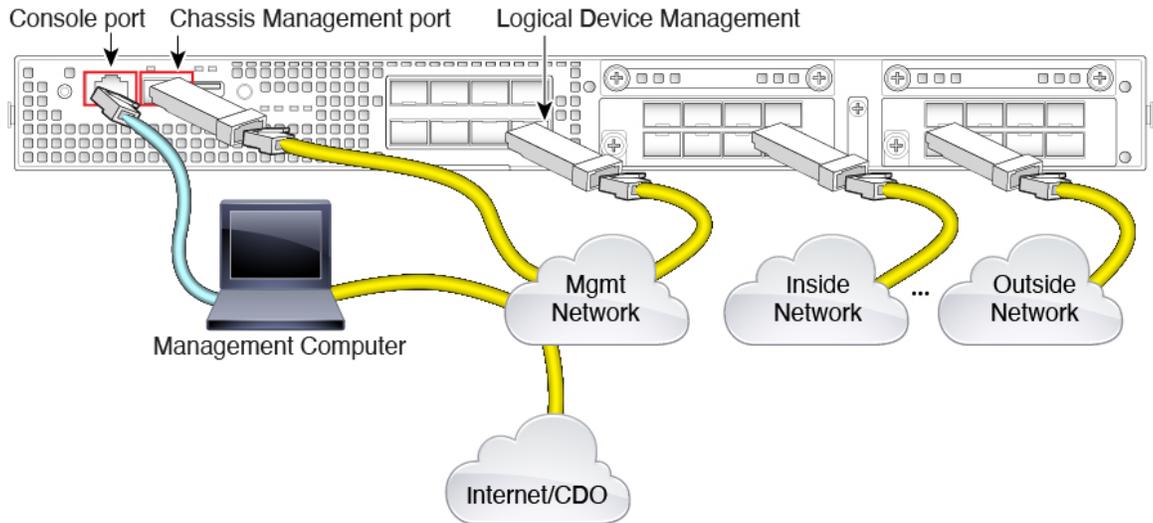
This guide assumes that you have a separate management network with its own internet access. By default, the Management interface is preconfigured when you deploy, but you have to configure data interfaces later.

Make sure the internet is accessible from the logical device management network. The threat defense needs access to the internet via the Management network for CDO management, updates, and licensing. You can optionally configure a data interface for CDO management instead of the Management interface. For more information about configuring a data interface for manager access, see the **configure network management-data-interface** command in the FTD command reference.

> **Note** The management connection is a secure, SSL-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.

ASA Cabling
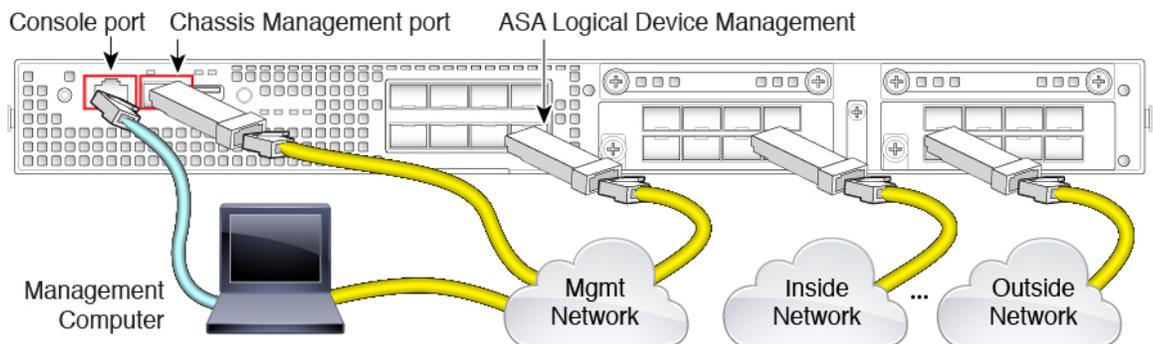
This guide assumes that you have a separate management network with its own internet access. By default, the Management interface is preconfigured when you deploy, but you have to configure data interfaces later.

Perform initial ASA configuration on the logical device Management interface. You can later enable management from any data interface.

Perform Initial Chassis Setup

Before you can use the chassis manager to configure and manage your system, you must perform some initial configuration tasks. You can perform the initial configuration using the FXOS CLI on the console port or an SSH session to the chassis Management port, or by using HTTPS on the chassis Management port.

Perform Initial Chassis Setup Using a Browser

The chassis Management port obtains an IP address using DHCP. For initial configuration, you can use a web browser to configure basic settings for the chassis. If you do not have a DHCP server, you need to use the console port for initial setup.

Note   To repeat the initial setup, you need to erase any existing configuration using the following commands from the CLI:

```
Firepower-chassis# connect local-mgmt
firepower-chassis(local-mgmt)# erase configuration
```

Before you begin

Gather the following information for use with the setup script:

- New admin password

- Management IP address and subnet mask

- Gateway IP address

- Subnets from which you want to allow HTTPS and SSH access

- Hostname and domain name

- DNS server IP address

Procedure

Step 1   Configure your DHCP server to assign an IP address to the chassis Management port.

The DHCP client request from the chassis contains the following information:

- The management interface's MAC address.

- DHCP option 60 (vendor-class-identifier)—Set to "FPR4100".

- DHCP option 61 (dhcp-client-identifier)—Set to the chassis serial number. This serial number can be found on a pull-out tab on the chassis.

Step 2   Power on the chassis.

Step 3   Enter the following URL in your browser:

https://*ip_address***/api**

Specify the IP address assigned by the DHCP server to the chassis Management port.

Step 4   When prompted, log in with the username **install** and the password *chassis_serial_number*.

The *chassis_serial_number* can be found on a pull-out tab on the chassis.

Step 5   Complete the system configuration as prompted.

- Strong password enforcement policy.

- Password for the admin account.

- System name

- Supervisor Management IPv4 address and subnet mask, or IPv6 address and prefix.

- Default gateway IPv4 or IPv6 address.

- Host/network address and netmask/prefix from which SSH access is allowed.

- Host/network address and netmask/prefix from which HTTPS access is allowed.

- DNS Server IPv4 or IPv6 address.

- Default domain name.

Step 6   Click **Submit**.

Perform Initial Chassis Setup at the CLI

The first time you access the FXOS CLI at the console or using an SSH session to the chassis Management port, a setup wizard prompts you for the basic network configuration so you can access the chassis manager (using HTTPS) or the FXOS CLI (using SSH) from the chassis Management port.

The chassis Management port obtains an IP address using DHCP. If you do not have a DHCP server, you need to use the console port for initial setup.

Note   To repeat the initial setup, you need to erase any existing configuration using the following commands:

```
Firepower-chassis# connect local-mgmt
firepower-chassis(local-mgmt)# erase configuration
```

Before you begin

Gather the following information for use with the setup script:

- New admin password

- Management IP address and subnet mask

- Gateway IP address

- Subnets from which you want to allow HTTPS and SSH access

- Hostname and domain name

- DNS server IP address

Procedure

Step 1   Power on the chassis.

Step 2   Connect to the serial console port using a terminal emulator or use SSH to the chassis Management port.

The Firepower 4100 includes an RS-232–to–RJ-45 serial console cable. You might need to use a third party serial-to-USB cable to make the connection. Use the following serial parameters:

- 9600 baud

- 8 data bits

- No parity

- 1 stop bit

Step 3   When prompted, log in with the username **admin** and the password **cisco123**.

Step 4   Complete the system configuration as prompted.

Example:

```
            ---- Basic System Configuration Dialog ----

 This setup utility will guide you through the basic configuration of
 the system. Only minimal configuration including IP connectivity to
 the FXOS Supervisor is performed through these steps.

 Type Ctrl-C at any time for more options or to abort configuration
 and reboot system.
 To back track or make modifications to already entered values,
 complete input till end of section and answer no when prompted
 to apply configuration.


 You have chosen to setup a new Security Appliance.
       Continue? (yes/no): y

 Enforce strong password? (yes/no) [y]: n

 Enter the password for "admin": Farscape&32
 Confirm the password for "admin": Farscape&32
 Enter the system name:   firepower-4125

 Supervisor Mgmt IP address : 10.80.6.12

 Supervisor Mgmt IPv4 netmask : 255.255.255.0

 IPv4 address of the default gateway : 10.80.6.1
```

```
        The system cannot be accessed via SSH if SSH Mgmt Access is not configured.

        Do you want to configure SSH Mgmt Access? (yes/no) [y]: y

        SSH Mgmt Access host/network address (IPv4/IPv6): 10.0.0.0

        SSH Mgmt Access IPv4 netmask: 255.0.0.0

        Firepower Chassis Manager cannot be accessed if HTTPS Mgmt Access is not configured.

        Do you want to configure HTTPS Mgmt Access? (yes/no) [y]: y

        HTTPS Mgmt Access host/network address (IPv4/IPv6): 10.0.0.0

        HTTPS Mgmt Access IPv4 netmask: 255.0.0.0

        Configure the DNS Server IP address? (yes/no) [n]: y

          DNS IP address : 10.164.47.13

        Configure the default domain name? (yes/no) [n]: y

          Default domain name : cisco.com

        Following configurations will be applied:

          Switch Fabric=A
          System Name=firepower-4125
          Enforced Strong Password=no
          Supervisor Mgmt IP Address=10.89.5.14
          Supervisor Mgmt IP Netmask=255.255.255.192
          Default Gateway=10.89.5.1
          SSH Access Configured=yes
              SSH IP Address=10.0.0.0
              SSH IP Netmask=255.0.0.0
          HTTPS Access Configured=yes
              HTTPS IP Address=10.0.0.0
              HTTPS IP Netmask=255.0.0.0
          DNS Server=72.163.47.11
          Domain Name=cisco.com

         Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): y
         Applying configuration. Please wait...  Configuration file – Ok
.....

Cisco FPR Series Security Appliance
firepower-9300 login:  admin
Password: Farscape&32
Successful login attempts for user 'admin' : 1
Cisco Firepower Extensible Operating System (FX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009-2019, Cisco Systems, Inc. All rights reserved.

[...]

firepower-chassis#
```

Step 5   You can disconnect from the console port, if used, or end your SSH session.

Log Into the Chassis Manager

Use the chassis manager to configure chassis settings, including enabling interfaces and deploying logical devices.

Before you begin

- For information on supported browsers, refer to the release notes for the version you are using (see http://www.cisco.com/c/en/us/support/security/firepower-9000-series/products-release-notes-list.html).

- You can only access the chassis manager from a management computer with an IP address in the range you specified during the initial chassis setup.

Procedure

Step 1   Using a supported browser, enter the following URL.

https://*chassis_mgmt_ip_address*

- *chassis_mgmt_ip_address*—Identifies the IP address or hostname of the chassis management port that you entered during initial configuration.

Step 2   Enter the username **admin** and new password.

You can add more users later according to .

Step 3   Click **Login**.
You are logged in, and the chassis manager opens to show the **Overview** page.

Configure NTP

Although you can set the time manually, we recommend that you use an NTP server. The correct time is required for Smart Software Licensing for the ASA and for the threat defense with the device manager. For the threat defense with the management center, the time must match between the chassis and the management center. In this case, we recommend that you use the same NTP server on the chassis as on the management center. Do not use the management center itself as the NTP server; this method is not supported.

Before you begin

If you use a hostname for the NTP server, you must configure a DNS server if you did not already do so in the initial setup. See **Platform Settings** > **DNS**.

Procedure

Step 1   Choose **Platform Settings** > **NTP**.

The **Time Synchronization** page is selected by default.

Step 2   Click the **Use NTP Server** radio button.
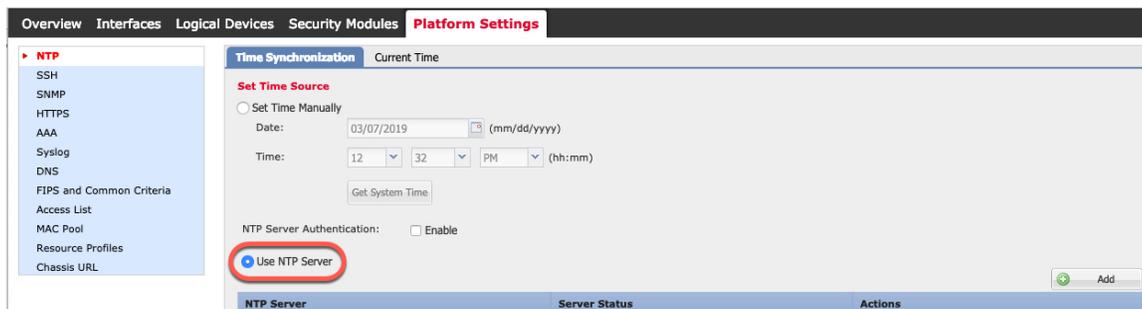
Step 3   (Optional) Check the **NTP Server Authentication: Enable** check box if you need to authenticate the NTP server.

You are prompted to enable NTP authentication. Click **Yes** to require an authentication key ID and value for all NTP server entries.

Only SHA1 is supported for NTP server authentication.

Step 4   Click **Add**, and set the following parameters:

- • **NTP Server**—The IP address or hostname of the NTP server.

- • **Authentication Key** and **Authentication Value**—Obtain the key ID and value from the NTP server. For example, to generate the SHA1 key on NTP server Version 4.2.8p8 or later with OpenSSL installed, enter the **ntp-keygen -M** command, and then view the key ID and value in the ntp.keys file. The key is used to tell both the client and server which value to use when computing the message digest.

Step 5   Click **Add** to add the server.

You can add up to 4 NTP servers.

Step 6   Click **Save** to save the servers.

Step 7   Click **Current Time**, and from the **Time Zone** drop-down list, choose the appropriate time zone for the chassis.

Step 8 Click **Save**.

> **Note** If you modify the system time by more than 10 minutes, the system will log you out and you will need to log in to the chassis manager again.

Add FXOS Users

Add local users for the chassis manager and FXOS CLI logins.

Procedure

Step 1 Choose **System** > **User Management**.

Step 2 Click **Local Users**.

Step 3 Click **Add User** to open the **Add User** dialog box.
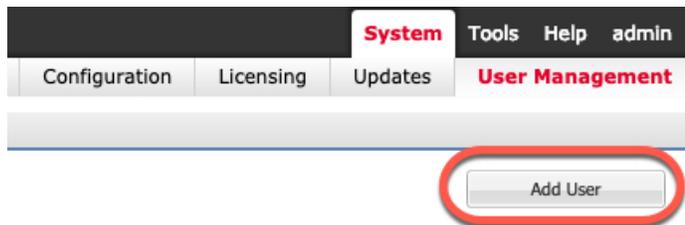
Step 4 Complete the following fields with the required information about the user:

- **User Name**—Sets the username, up to 32 characters. After you save the user, the login ID cannot be changed. You must delete the user account and create a new one.

- (Optional) **First Name**—Sets the first name of the user, up to 32 characters.

- (Optional) **Last Name**—Sets the last name of the user, up to 32 characters.

- (Optional) **Email**—Sets the email address for the user.

- (Optional) **Phone Number**—Sets the telephone number for the user.

- **Password** and **Confirm Password**—Sets the password associated with this account. If you enable the password strength check, then the password must be strong, and FXOS rejects any password that does not meet the strength check requirements. See the FXOS configuration guide for strong password guidelines.

- **Account Status**—Sets the status to **Active** or **Inactive**.

- **User Role**—Sets the role that represents the privileges you want to assign to the user account. All users are assigned the **Read-Only** role by default, and this role cannot be deselected. To assign a different role, click the role name in the window so that it is highlighted. You can use one of the following user roles:

- **Admin**—Complete read-and-write access to the entire system.

- **Read-Only**—Read-only access to system configuration with no privileges to modify the system state.

- **Operations**—Read-and-write access to NTP configuration, Smart Call Home configuration for Smart Licensing, and system logs, including syslog servers and faults. Read access to the rest of the system.

- **AAA Administrator**—Read-and-write access to users, roles, and AAA configuration. Read access to the rest of the system.

- (Optional) **Account Expires**—Sets that this account expires. The account cannot be used after the date specified in the **Expiry Date** field. After you configure a user account with an expiration date, you cannot reconfigure the account to not expire. You can, however, configure the account with the latest expiration date available. By default, user accounts do not expire.

- (Optional) **Expiry Date**—The date on which the account expires. The date should be in the format *yyyy-mm-dd*. Click the calendar icon at the end of this field to view a calendar that you can use to select the expiration date.

Step 5 Click **Add**.

Configure Interfaces

By default, physical interfaces are disabled. In FXOS, you can enable interfaces, add EtherChannels, add VLAN subinterfaces, and edit interface properties. To use an interface, you must physically enable it in FXOS, and then logically enable it in the application.

To configure breakout ports, see the FXOS configuration guide.

Interface Types

Each interface is one of the following types:

- Data—Use for regular data. Data interfaces cannot be shared between logical devices, and logical devices cannot communicate over the backplane to other logical devices. For traffic on Data interfaces, all traffic must exit the chassis on one interface and return on another interface to reach another logical device.

- Data-sharing—Use for regular data. Only supported with container instances, these data interfaces can be shared by one or more logical devices/container instances (threat defense-using-management center only). Each container instance can communicate over the backplane with all other instances that share this interface. Shared interfaces can affect the number of container instances you can deploy. Shared interfaces are not supported for bridge group member interfaces (in transparent mode or routed mode), inline sets, passive interfaces, clusters, or failover links.

- Mgmt—Use to manage application instances. These interfaces can be shared by one or more logical devices to access external hosts; logical devices cannot communicate over this interface with other logical devices that share the interface. You can only assign one management interface per logical device. Depending on your application and manager, you can later enable management from a data interface;

but you must assign a Management interface to the logical device even if you don't intend to use it after you enable data management.

✎

Note Mgmt interface change will cause reboot of the logical device, for example one change mgmt from e1/1 to e1/2 will cause the logical device to reboot to apply the new management.

- Eventing—Use as a secondary management interface for threat defense-using-management center devices. To use this interface, you must configure its IP address and other parameters at the threat defense CLI. For example, you can separate management traffic from events (such as web events). See the management center configuration guide for more information. Eventing interfaces can be shared by one or more logical devices to access external hosts; logical devices cannot communicate over this interface with other logical devices that share the interface. If you later configure a data interface for management, you cannot use a separate eventing interface.

✎

Note A virtual Ethernet interface is allocated when each application instance is installed. If the application does not use an eventing interface, then the virtual interface will be in an admin down state.

```
Firepower # show interface Vethernet775
Firepower # Vethernet775 is down (Administratively down)
Bound Interface is Ethernet1/10
Port description is server 1/1, VNIC ext-mgmt-nic5
```

- Cluster—Use as the cluster control link for a clustered logical device. By default, the cluster control link is automatically created on Port-channel 48. The Cluster type is only supported on EtherChannel interfaces. For multi-instance clustering, you cannot share a Cluster-type interface across devices. You can add VLAN subinterfaces to the Cluster EtherChannel to provide separate cluster control links per cluster. If you add subinterfaces to a Cluster interface, you cannot use that interface for a native cluster. The device manager and CDO does not support clustering.

You must configure a Management interface and at least one Data (or Data-sharing) interface before you deploy a logical device.

Configure a Physical Interface

You can physically enable and disable interfaces, as well as set the interface speed and duplex. To use an interface, you must physically enable it in FXOS, and then logically enable it in the application.

Before you begin

Interfaces that are already a member of an EtherChannel cannot be modified individually. Be sure to configure settings before you add an interface to the EtherChannel.

Procedure

Step 1 Click **Interfaces**.

The **All Interfaces** page shows a visual representation of the currently-installed interfaces at the top of the page and provides a listing of the installed interfaces in the table below.

Step 2 Click the **Edit** ( ) for the interface you want to edit to open the **Edit Interface** dialog box.

Step 3 Check the **Enable** check box.

Step 4 Choose the interface **Type**: **Data**, **Data-sharing**, **Mgmt**, or **Firepower-eventing**

Note There are limitations when using Data-sharing type interfaces; see the FXOS configuration guide for more information.

For Firepower-eventing, see the Firepower Management Center Configuration Guide.

Step 5 (Optional) Choose the **Speed** of the interface.

Step 6 (Optional) If your interface supports **Auto Negotiation**, click the **Yes** or **No** radio button.

Step 7 (Optional) Choose the **Duplex** of the interface.

Step 8 Click **OK**.

Add an EtherChannel (Port Channel)

An EtherChannel (also known as a port channel) can include up to 16 member interfaces of the same media type and capacity, and must be set to the same speed and duplex. The media type can be either RJ-45 or SFP; SFPs of different types (copper and fiber) can be mixed. You cannot mix interface capacities (for example 1GB and 10GB interfaces) by setting the speed to be lower on the larger-capacity interface.

Note When the chassis creates an EtherChannel, the EtherChannel stays in a **Suspended** state for Active LACP mode or a **Down** state for On LACP mode until you assign it to a logical device, even if the physical link is up.

Procedure

Step 1 Click **Interfaces**.

The **All Interfaces** page shows a visual representation of the currently-installed interfaces at the top of the page and provides a listing of the installed interfaces in the table below.

Step 2 Click **Add New** > **Port Channel**.

Step 3 Enter a **Port Channel ID**, between 1 and 47.

Step 4 Check the **Enable** check box.

Step 5 Choose the interface **Type**:

- **Data**

- **Data-sharing**—For container instances only.

- **Mgmt**

- **Firepower-eventing**—For threat defense only.

- **Cluster**—For clustering only.

Note There are limitations when using Data-sharing type interfaces; see the FXOS configuration guide for more information.

For Firepower-eventing, see the Firepower Management Center Configuration Guide.

Step 6 Set the **Admin Speed** of the member interfaces from the drop-down list.

Step 7 For Data or Data-sharing interfaces, choose the LACP port-channel **Mode**: **Active** or **On**.

For non-Data or non-Data-sharing interfaces, the mode is always active. You should use the active mode unless you need to minimize the amount of LACP traffic.

Step 8 Set the **Admin Duplex** from the drop-down list.

Step 9 To add an interface to the port channel, select the interface in the **Available Interface** list and click **Add Interface** to move it to the **Member ID** list.

You can add up to 16 interfaces.

Tip	You can add multiple interfaces at a time. Click on the desired interfaces while holding down the **Ctrl** key. To select a range of interfaces, select the first interface in the range, and then, while holding down the **Shift** key, click to select the last interface in the range.

Step 10 To remove an interface from the port channel, click the **Delete** (🗑) to the right of the interface in the **Member ID** list.

Step 11 Click **OK**.

Add a VLAN Subinterface for Container Instances

You can add up to 500 subinterfaces to your chassis. Subinterfaces are supported for container instances only; for more information, see Logical Device Application Instances: Container or Native, on page 7.

For multi-instance clustering, you can only add subinterfaces to the Cluster-type interface; subinterfaces on data interfaces are not supported.

VLAN IDs per interface must be unique, and within a container instance, VLAN IDs must be unique across all assigned interfaces. You can reuse VLAN IDs on *separate* interfaces as long as they are assigned to different container instances. However, each subinterface still counts towards the limit even though it uses the same ID.

You can also add subinterfaces within the application. For more information on when to use FXOS subinterfaces vs. application subinterfaces, see the FXOS configuration guide.

Procedure

Step 1 Click **Interfaces**.

The **All Interfaces** page shows a visual representation of the currently installed interfaces at the top of the page and provides a listing of the installed interfaces in the table below.

Step 2 Click **Add New** > **Subinterface** to open the **Add Subinterface** dialog box.

Step 3 Choose the interface **Type**:
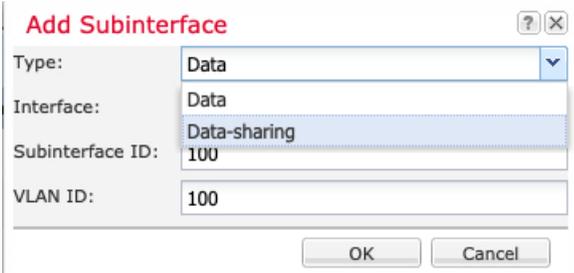
- **Data**

- **Data-sharing**

- **Cluster**—If you add subinterfaces to a Cluster interface, you cannot use that interface for a native cluster.

For Data and Data-sharing interfaces: The type is independent of the parent interface type; you can have a Data-sharing parent and a Data subinterface, for example.

There are limitations when using Data-sharing type interfaces; see the FXOS configuration guide for more information.

Step 4 Choose the parent **Interface** from the drop-down list.

You cannot add a subinterface to a physical interface that is currently allocated to a logical device. If other subinterfaces of the parent are allocated, you can add a new subinterface as long as the parent interface itself is not allocated.

Step 5 Enter a **Subinterface ID**, between 1 and 4294967295.

This ID will be appended to the parent interface ID as *interface_id*.*subinterface_id*. For example, if you add a subinterface to Ethernet1/1 with the ID of 100, then the subinterface ID will be: Ethernet1/1.100. This ID is not the same as the VLAN ID, although you can set them to match for convenience.

Step 6 Set the **VLAN ID** between 1 and 4095.

Step 7 Click **OK**.

Expand the parent interface to view all subinterfaces under it.

Upload Software Images to the Chassis

This procedure describes how to upload new FXOS and application images, as well as how to upgrade the FXOS image. You might need to upload new images if the pre-installed images are not the versions you require.

Before you begin

- Check compatibility between FXOS, ASA, and the threat defense versions in the FXOS compatibility guide.

- Make sure the image you want to upload is available on your local computer. To obtain FXOS and application software for the Firepower 4100, see:

  http://www.cisco.com/go/firepower4100-software

- To make sure your upload succeeds during your HTTPS session, you might need to change the absolute timeout at the FXOS CLI. The absolute timeout is 60 minutes (the maximum), and large uploads might take longer than 60 minutes. To disable the absolute timeout, enter:

```
Firepower-chassis# scope security
Firepower-chassis /security # scope default-auth
Firepower-chassis /security/default-auth # set absolute-session-timeout 0
Firepower-chassis /security/default-auth* # commit-buffer
```

Procedure

Step 1 Check your current FXOS version by looking at the **Overview** page.

| Overview | Interfaces | Logical Devices | Security Modules | Platform Settings |

firepower-9300   10.89.5.14

Model: **Cisco Firepower 9300 Security Appliance AC** | Version: **2.6(1.131)** |

You can view application images currently available on the chassis in the next step.

Step 2 Choose **System** > **Updates**.

The **Available Updates** page shows a list of the FXOS platform bundle images and application images.

Step 3 Click **Upload Image** to open the **Upload Image** dialog box.

Step 4 Click **Browse** to navigate to and select the image that you want to upload.

Step 5 Click **Upload**. The selected image is uploaded to the chassis.

The **Upload Image** dialog box shows a progress bar, and then a **Success** dialog box when the image finishes uploading.

Step 6 To upgrade the FXOS image:

a) Click the Upgrade icon (⚙) for the FXOS platform bundle to which you want to upgrade.
b) Click **Yes** to confirm that you want to proceed with installation.

The chassis reloads. The upgrade process typically takes between 20 and 30 minutes.

History for FXOS

Feature Name	Version	Feature Information
VLAN subinterfaces for use with container instances	2.4.1	To provide flexible physical interface use, you can create VLAN subinterfaces in FXOS and also share interfaces between multiple instances. **Note** Requires the threat defense Version 6.3 or later. New/Modified screens: **Interfaces** > **All Interfaces** > **Add New** drop-down menu **> Subinterface** New/Modified management center screens: **Devices** > **Device Management** > **Edit** icon **> Interfaces**

Feature Name	Version	Feature Information
Data-sharing interfaces for container instances	2.4.1	To provide flexible physical interface use, you can share interfaces between multiple instances. **Note** Requires the threat defense Version 6.3 or later. New/Modified screens: **Interfaces** > **All Interfaces** > **Type**
Support for data EtherChannels in On mode	2.4.1	You can now set data and data-sharing EtherChannels to either Active LACP mode or to On mode. Other types of EtherChannels only support Active mode. New/Modified screens: **Interfaces** > **All Interfaces** > **Edit Port Channel** > **Mode**
Support for EtherChannels in the threat defense inline sets	2.1.1	You can now use EtherChannels in the threat defense inline set.
Inline set link state propagation support for the threat defense	2.0.1	When you configure an inline set in the threat defense application and enable link state propagation, the threat defense sends inline set membership to the FXOS chassis. Link state propagation means that the chassis automatically brings down the second interface in the inline interface pair when one of the interfaces in an inline set goes down. New/Modified commands: **show fault |grep link-down**, **show interface detail**
Support for Hardware bypass network modules for the threat defense	2.0.1	Hardware Bypass ensures that traffic continues to flow between an inline interface pair during a power outage. This feature can be used to maintain network connectivity in the case of software or hardware failures. New/Modified management center screens: **Devices** > **Device Management** > **Interfaces** > **Edit Physical Interface**
Firepower-eventing type interface for the threat defense	1.1.4	You can specify an interface as firepower-eventing for use with the threat defense. This interface is a secondary management interface for the threat defense devices. To use this interface, you must configure its IP address and other parameters at the threat defense CLI. For example, you can separate management traffic from events (such as web events). See the "Management Interfaces" section in the management center configuration guide *System Configuration* chapter. New/Modified chassis manager screens: **Interfaces** > **All Interfaces** > **Type**

C H A P T E R **3**

Threat Defense Deployment with the Management Center

Is This Chapter for You?

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

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

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

Privacy Collection Statement—The Firepower 4100 does not require or actively collect personally-identifiable information. However, you can use personally-identifiable information in the configuration, for example for usernames. In this case, an administrator might be able to see this information when working with the configuration or when using SNMP.

Before You Start

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

End-to-End Procedure

See the following tasks to deploy and configure the threat defense on your chassis.
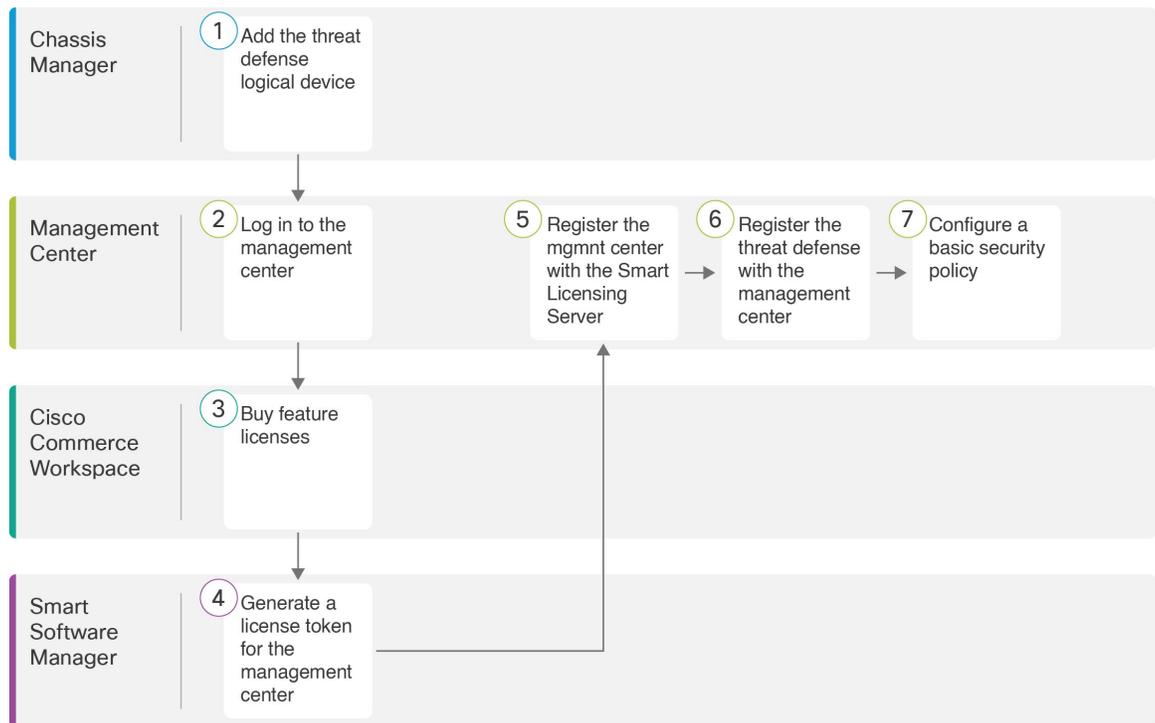
	Workspace	Steps
1	Chassis Manager	Chassis Manager: Add the Threat Defense Logical Device, on page 31.
2	Management Center	Log Into the Management Center, on page 36.
3	Cisco Commerce Workspace	Obtain Licenses for the Management Center, on page 37: Buy feature licenses.
4	Smart Software Manager	Obtain Licenses for the Management Center, on page 37: Generate a license token for the management center.
5	Management Center	Obtain Licenses for the Management Center, on page 37: Register the management center with the Smart Licensing server.

	Workspace	Steps
6	Management Center	Register the Threat Defense with the Management Center, on page 39.
7	Management Center	Configure a Basic Security Policy, on page 42.

Chassis Manager: Add the Threat Defense Logical Device

You can deploy the threat defense from the Firepower 4100 as either a native or container instance. You can deploy multiple container instances per security engine, but only one native instance. See Logical Device Application Instances: Container or Native, on page 7 for the maximum container instances per model.

To add a High Availability pair or a cluster, see the Firepower Management Center Configuration Guide.

This procedure lets you configure the logical device characteristics, including the bootstrap configuration used by the application.

Before you begin

- Configure a Management interface to use with the threat defense; see Configure Interfaces, on page 21. The Management interface is required. In 6.7 and later, you can later enable management from a data interface; but you must assign a Management interface to the logical device even if you don't intend to use it after you enable data management. Note that this Management interface is not the same as the chassis management port that is used only for chassis management (and that appears at the top of the **Interfaces** tab as **MGMT**).

- You must also configure at least one Data interface.

- For container instances, if you do not want to use the default profile, which uses the minimum resources, add a resource profile on **Platform Settings** > **Resource Profiles**.

- For container instances, before you can install a container instance for the first time, you may need to reinitialize the security engine so that the disk has the correct formatting. If this action is required, you will not be able to save your logical device. Click **Security Engine**, and then click the Reinitialize icon (⟳).

- Gather the following information:
    - Interface IDs for this device
    - Management interface IP address and network mask
    - Gateway IP address
    - Management Center IP address and/or NAT ID of your choosing
    - DNS server IP address

Procedure

Step 1 In the chassis manager, choose **Logical Devices**.

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

Add Standalone	? ✕
Device Name:	FTD_Instance2
Template:	Cisco Firepower Threat Defense ▾
Image Version:	6.5.0.1159 ▾
Instance Type:	Container ▾

ⓘ Before you add the first container instance, you must reinitialize the security module/engine so that the disk has the correct formatting. You only need to perform this action once.

[OK] [Cancel]

a) Provide a **Device Name**.

   This name is used by the chassis supervisor to configure management settings and to assign interfaces; it is not the device name used in the application configuration.

   Note   You cannot change this name after you add the logical device.

b) For the **Template**, choose **Cisco Firepower Threat Defense**.

c) Choose the **Image Version**.

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

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

e) Click **OK**.

   You see the Provisioning - *device name* window.

Step 3 Expand the **Data Ports** area, and click each interface that you want to assign to the device.
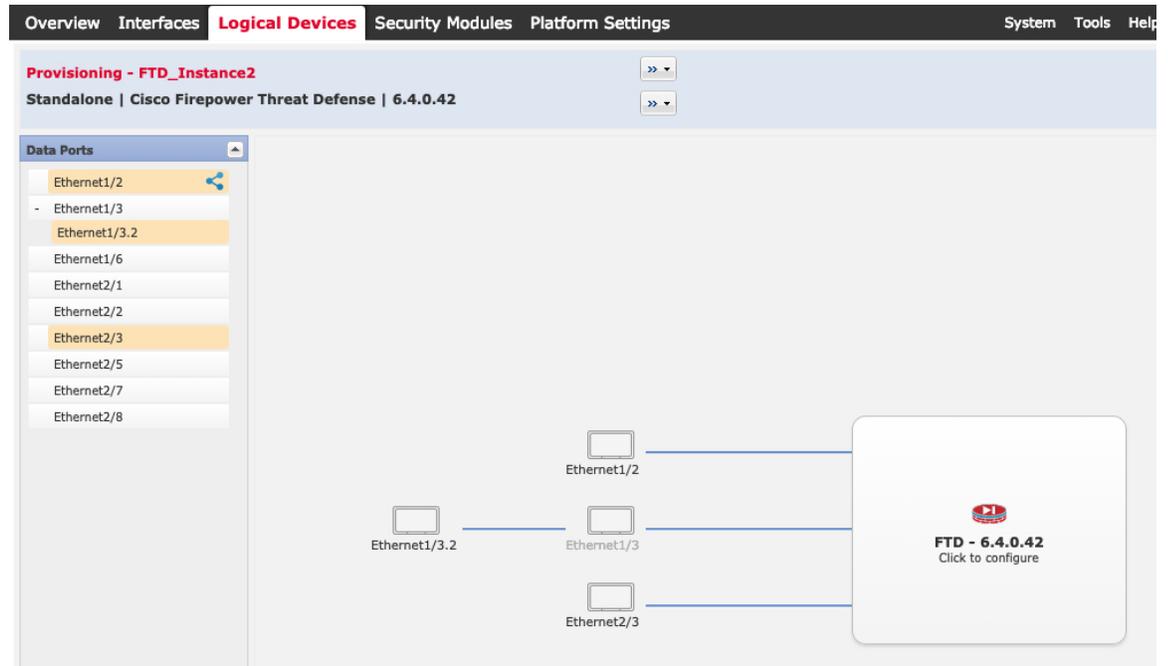
You can only assign Data and Data-sharing interfaces that you previously enabled on the **Interfaces** page. You will later enable and configure these interfaces in the management center, including setting the IP addresses.

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

Hardware Bypass–capable ports are shown with the following icon: . For certain interface modules, you can enable the Hardware Bypass feature for Inline Set interfaces only (see the Firepower Management Center Configuration Guide for information about Inline Sets). Hardware Bypass ensures that traffic continues to flow between an inline interface pair during a power outage. This feature can be used to maintain network connectivity in the case of software or hardware failures. If you do not assign both interfaces in a Hardware Bypass pair, you see a warning message to make sure your assignment is intentional. You do not need to use the Hardware Bypass feature, so you can assign single interfaces if you prefer.

Step 4 Click the device icon in the center of the screen.

A dialog box appears where you can configure initial bootstrap settings. These settings are meant for initial deployment only, or for disaster recovery. For normal operation, you can later change most values in the application CLI configuration.

Step 5 On the **General Information** page, complete the following:

Cisco Firepower Threat Defense - Bootstrap Configuration

General Information Settings Agreement

SM 1 - 22 Cores Available

Resource Profile: Default-Small

Interface Information

Management Interface: Ethernet1/8

Management

Address Type: IPv4 only

IPv4

Management IP: 10.83.58.239

Network Mask: 255.255.252.0

Network Gateway: 10.83.56.1

a) For a container instance, specify the **Resource Profile**.

If you later assign a different resource profile, then the instance will reload, which can take approximately 5 minutes. Note that for established High Availability pairs or clusters, if you assign a different-sized resource profile, be sure to make all members the same size as soon as possible.

b) Choose the **Management Interface**.

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

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

d) Configure the **Management IP** address.

Set a unique IP address for this interface.

e) Enter a **Network Mask** or **Prefix Length**.

f) Enter a **Network Gateway** address.

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

Cisco Firepower Threat Defense - Bootstrap Configuration

General Information **Settings** Agreement

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

a) For a native instance, in the **Management type of application instance** drop-down list, choose **FMC**.

   Native instances also support the device manager as a manager. After you deploy the logical device, you cannot change the manager type.

b) Enter the **Firepower Management Center IP** or hostname of the managing the management center. If you do not know the management center IP address, leave this field blank and enter a passphrase in the **Firepower Management Center NAT ID** field.

c) For a container instance, **Permit Expert mode from FTD SSH sessions**: **Yes** or **No**. Expert Mode provides the threat defense shell access for advanced troubleshooting.

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

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

d) Enter the **Search Domains** as a comma-separated list.

e) Choose the **Firewall Mode**: **Transparent** or **Routed**.

   In routed mode, the threat defense is considered to be a router hop in the network. Each interface that you want to route between is on a different subnet. A transparent firewall, on the other hand, is a Layer 2 firewall that acts like a "bump in the wire," or a "stealth firewall," and is not seen as a router hop to connected devices.

   The firewall mode is only set at initial deployment. If you re-apply the bootstrap settings, this setting is not used.

f) Enter the **DNS Servers** as a comma-separated list.

   The threat defense uses DNS if you specify a hostname for the management center, for example.

g) Enter the **Fully Qualified Hostname** for the threat defense.

h) Enter a **Registration Key** to be shared between the management center and the device during registration.

You can choose any text string for this key between 1 and 37 characters; you will enter the same key on the management center when you add the threat defense.

i) Enter a **Password** for the threat defense admin user for CLI access.

j) Choose the **Eventing Interface** on which events should be sent. If not specified, the management interface will be used.

This interface must be defined as a Firepower-eventing interface.

k) For a container instance, set the **Hardware Crypto** as **Enabled** or **Disabled**.

This setting enables TLS crypto acceleration in hardware, and improves performance for certain types of traffic. For more information, see the Firepower Management Center Configuration Guide. This feature is not supported for native instances. To view the percentage of hardware crypto resources allocated to this instance, enter the **show hw-crypto** command.

Step 7 On the **Agreement** tab, read and accept the end user license agreement (EULA).

Step 8 Click **OK** to close the configuration dialog box.

Step 9 Click **Save**.

The chassis deploys the logical device by downloading the specified software version and pushing the bootstrap configuration and management interface settings to the application instance. Check the **Logical Devices** page for the status of the new logical device. When the logical device shows its **Status** as **online**, you can start configuring the security policy in the application.
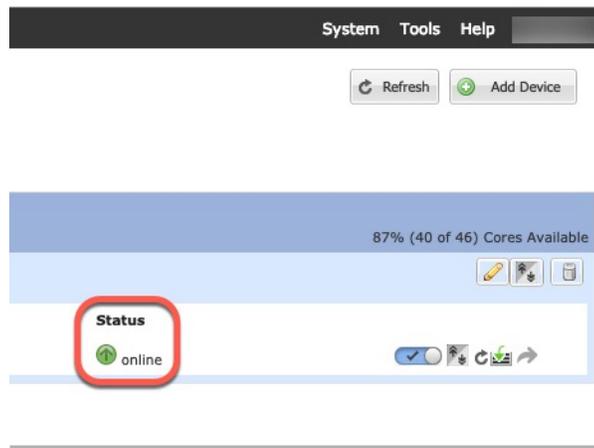
Log Into the Management Center

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

Before you begin

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

Procedure

Step 1 Using a supported browser, enter the following URL.

https://*fmc_ip_address*

Step 2 Enter your username and password.

Step 3 Click **Log In**.

Obtain Licenses for the Management Center

All licenses are supplied to the threat defense by the management center. You can purchase the following licenses:

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

- **Malware Defense**—Malware defense

- **URL**—URL Filtering

- **Cisco Secure Client**—Secure Client Advantage, Secure Client Premier, or Secure Client VPN Only

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

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

Before you begin

- Have a master account on the Smart Software Manager.

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

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

Procedure

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

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

Figure 1: License Search

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

- IPS, Malware Defense, and URL license combination:

  - L-FPR4112T-TMC=

  - L-FPR4115T-TMC=

  - L-FPR4125T-TMC=

  - L-FPR4145T-TMC=

  When you add one of the above PIDs to your order, you can then choose a term-based subscription corresponding with one of the following PIDs:

  - L-FPR4112T-TMC-1Y

  - L-FPR4112T-TMC-3Y

  - L-FPR4112T-TMC-5Y

  - L-FPR4115T-TMC-1Y

  - L-FPR4115T-TMC-3Y

  - L-FPR4115T-TMC-5Y

  - L-FPR4125T-TMC-1Y

  - L-FPR4125T-TMC-3Y

  - L-FPR4125T-TMC-5Y

  - L-FPR4145T-TMC-1Y

  - L-FPR4145T-TMC-3Y

  - L-FPR4145T-TMC-5Y

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

- Carrier license:

  - L-FPR4K-FTD-CAR=

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

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

Register the Threat Defense with the Management Center

Register each logical device individually to the same management center.

Before you begin

- Make sure the threat defense logical device **Status** is **online** on the chassis manager **Logical Devices** page.

- Gather the following information that you set in the threat defense initial bootstrap configuration (see Chassis Manager: Add the Threat Defense Logical Device, on page 31):

    - The threat defense management IP address or hostname, and NAT ID

    - The management center registration key

- In 6.7 and later, if you want to use a data interface for management, use the **configure network management-data-interface** command at the threat defense CLI. See the Cisco Secure Firewall Threat Defense Command Reference for more information.

Procedure

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

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

Set the following parameters:

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

  Note　In an HA environment, when both the management centers are behind a NAT, you can register the threat defense without a host IP or name in the primary management center. However, for registering the threat defense in a secondary management center, you must provide the IP address or hostname for the threat defense.

- **Display Name**—Enter the name for the threat defense as you want it to display in the management center.

- **Registration Key**—Enter the same registration key that you specified in the threat defense initial bootstrap configuration.

- **Domain**—Assign the device to a leaf domain if you have a multidomain environment.

- **Group**—Assign it to a device group if you are using groups.

- **Access Control Policy**—Choose an initial policy. Unless you already have a customized policy you know you need to use, choose **Create new policy**, and choose **Block all traffic**. You can change this later to allow traffic; see Allow Traffic from Inside to Outside, on page 50.

Figure 2: New Policy

- **Smart Licensing**—Assign the Smart Licenses you need for the features you want to deploy: **Malware** (if you intend to use malware inspection), **Threat** (if you intend to use intrusion prevention), and **URL** (if you intend to implement category-based URL filtering). **Note:** You can apply an Secure Client remote access VPN license after you add the device, from the **System** > **Licenses** > **Smart Licenses** page.

- **Unique NAT ID**—Specify the NAT ID that you specified in the threat defense initial bootstrap configuration.

- **Transfer Packets**—Allow the device to transfer packets to the management center. When events like IPS or Snort are triggered with this option enabled, the device sends event metadata information and packet data to the management center for inspection. If you disable it, only event information will be sent to the management center, but packet data is not sent.

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

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

- Ping—Access the threat defense CLI (Access the Threat Defense CLI, on page 53), and ping the management center IP address using the following command:

ping system *ip_address*

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

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

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

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

Configure a Basic Security Policy

This section describes how to configure a basic security policy with the following settings:

• Inside and outside interfaces—Assign a static IP address to the inside interface, and use DHCP for the outside interface.

• DHCP server—Use a DHCP server on the inside interface for clients.

• Default route—Add a default route through the outside interface.

• NAT—Use interface PAT on the outside interface.

• Access control—Allow traffic from inside to outside.

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

1	Configure Interfaces, on page 42.
2	Configure the DHCP Server, on page 46.
3	Add the Default Route, on page 47.
4	Configure NAT, on page 48.
5	Allow Traffic from Inside to Outside, on page 50.
6	Deploy the Configuration, on page 51.

Configure Interfaces

Enable the threat defense interfaces, assign them to security zones, and set the IP addresses. Typically, you must configure at least a minimum of two interfaces to have a system that passes meaningful traffic. Normally, you would have an outside interface that faces the upstream router or internet, and one or more inside interfaces for your organization's networks. Some of these interfaces might be "demilitarized zones" (DMZs), where you place publically-accessible assets such as your web server.

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

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

Procedure

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

Step 2   Click **Interfaces**.

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

The **General** tab appears.

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**

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

f) Click **OK**.

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

The **General** tab appears.

Note	If you pre-configured this interface for manager access, then the interface will already be named, enabled, and addressed. You should not alter any of these basic settings because doing so will disrupt the management center management connection. You can still configure the Security Zone on this screen for through traffic policies.

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

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

b) Check the **Enabled** check box.
c) Leave the **Mode** set to **None**.
d) From the **Security Zone** drop-down list, choose an existing outside security zone or add a new one by clicking **New**.

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

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

- **IPv4**—Choose **Use DHCP**, and configure the following optional parameters:

    - **Obtain default route using DHCP**—Obtains the default route from the DHCP server.

    - **DHCP route metric**—Assigns an administrative distance to the learned route, between 1 and 255. The default administrative distance for the learned routes is 1.

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

 f)   Click **OK**.

Step 5   Click **Save**.

Configure the DHCP Server

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

Procedure

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

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

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

• **Interface**—Choose the interface from the drop-down list.

• **Address Pool**—Set the range of IP addresses from lowest to highest that are used by the DHCP server. The range of IP addresses must be on the same subnet as the selected interface and cannot include the IP address of the interface itself.

• **Enable DHCP Server**—Enable the DHCP server on the selected interface.

Step 4   Click **OK**.

Step 5   Click **Save**.

Add the Default Route

The default route normally points to the upstream router reachable from the outside interface. If you use DHCP for the outside interface, your device might have already received a default route. If you need to manually add the route, complete this procedure. If you received a default route from the DHCP server, it will show in the **IPv4 Routes** or **IPv6 Routes** table on the **Devices** > **Device Management** > **Routing** > **Static Route** page.

Procedure

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

Step 2   Choose **Routing** > **Static Route**, click **Add Route**, and set the following:

- **Type**—Click the **IPv4** or **IPv6** radio button depending on the type of static route that you are adding.

- **Interface**—Choose the egress interface; typically the outside interface.

- **Available Network**—Choose **any-ipv4** for an IPv4 default route, or **any-ipv6** for an IPv6 default route and click **Add** to move it to the **Selected Network** list.

- **Gateway** or **IPv6 Gateway**—Enter or choose the gateway router that is the next hop for this route. You can provide an IP address or a Networks/Hosts object.

- **Metric**—Enter the number of hops to the destination network. Valid values range from 1 to 255; the default value is 1.

Step 3   Click **OK**.

The route is added to the static route table.

Step 4 Click **Save**.

Configure NAT

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

Procedure

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

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

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

Step 3 Click **Add Rule**.

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

Step 4 Configure the basic rule options:

- **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.

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

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

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:

- **Name**—Name this rule, for example, **inside_to_outside**.

- **Source Zones**—Select the inside zone from **Available Zones**, and click **Add to Source**.

- **Destination Zones**—Select the outside zone from **Available Zones**, and click **Add to Destination**.

Leave the other settings as is.

Step 3 Click **Add**.

The rule is added to the **Rules** table.

Step 4 Click **Save**.

Deploy the Configuration

Deploy the configuration changes to the threat defense; none of your changes are active on the device until you deploy them.

Procedure

Step 1 Click **Deploy** in the upper right.

Figure 3: Deploy

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

Figure 4: Deploy All
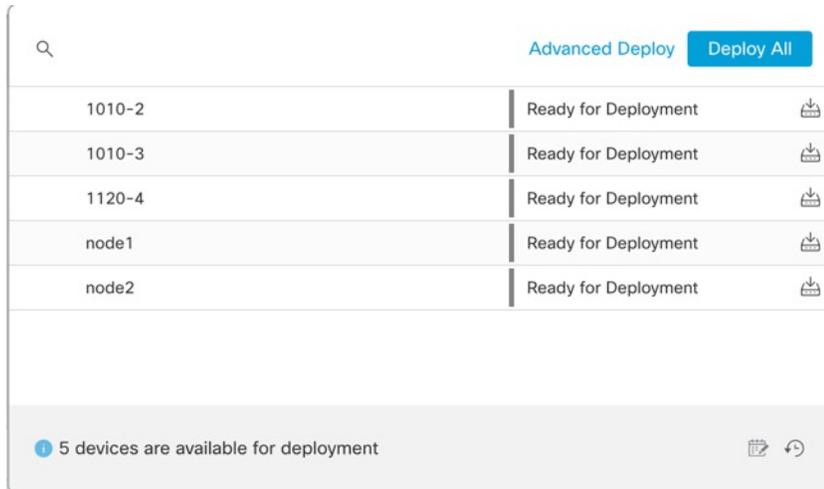
Figure 5: Advanced Deploy
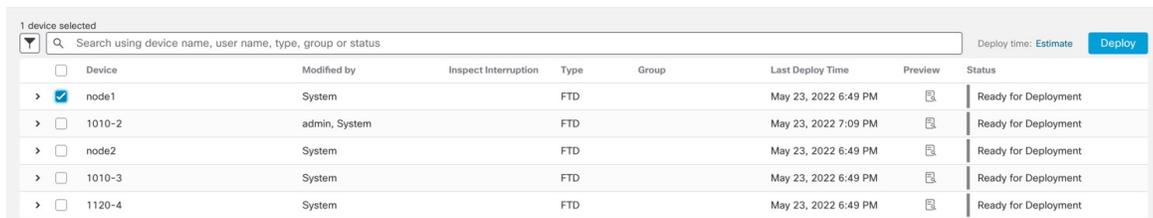
Step 3   Ensure that the deployment succeeds. Click the icon to the right of the **Deploy** button in the menu bar to see status for deployments.

Figure 6: Deployment Status

Access the Threat Defense CLI

You can use the threat defense CLI to change management interface parameters and for troubleshooting purposes. You can access the CLI using SSH to the Management interface, or by connecting from the FXOS CLI.

Procedure

Step 1   (Option 1) SSH directly to the threat defense management interface IP address.

You set the management IP address when you deployed the logical device. Log into the threat defense with the admin account and the password you set during initial deployment.

If you forgot the password, you can change it by editing the logical device in the chassis manager.

Step 2   (Option 2) From the FXOS CLI, connect to the module CLI using a console connection or a Telnet connection.

a)   Connect to the security engine.

connect module 1 {**console** | **telnet**}

The benefits of using a Telnet connection is that you can have multiple sessions to the module at the same time, and the connection speed is faster.

Example:

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

b) Connect to the threat defense console.

connect ftd *name*

If you have multiple application instances, you must specify the name of the instance. To view the instance names, enter the command without a name.

Example:

```
Firepower-module1> connect ftd FTD_Instance1

============================= ATTENTION =============================
You are connecting to ftd from a serial console. Please avoid
executing any commands which may produce large amount of output.
Otherwise, data cached along the pipe may take up to 12 minutes to be
drained by a serial console at 9600 baud rate after pressing Ctrl-C.

To avoid the serial console, please login to FXOS with ssh and use
'connect module <slot> telnet' to connect to the security module.
====================================================================

Connecting to container ftd(FTD_Instance1) console... enter "exit" to return to bootCLI
>
```

c) Exit the application console to the FXOS module CLI by entering **exit**.

Note   For pre-6.3 versions, enter **Ctrl-a, d**.

d) Return to the supervisor level of the FXOS CLI.

To exit the console:

1. Enter **~**

   You exit to the Telnet application.

2. To exit the Telnet application, enter:

   telnet>**quit**

To exit the Telnet session:

Enter **Ctrl-], .**

Example

The following example connects to the threat defense and then exits back to the supervisor level of the FXOS CLI.

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit
```

```
Firepower-module1>connect ftd FTD_Instance1

============================= ATTENTION =============================
You are connecting to ftd from a serial console. Please avoid
executing any commands which may produce large amount of output.
Otherwise, data cached along the pipe may take up to 12 minutes to be
drained by a serial console at 9600 baud rate after pressing Ctrl-C.

To avoid the serial console, please login to FXOS with ssh and use
'connect module <slot> telnet' to connect to the security module.
====================================================================

Connecting to container ftd(FTD_Instance1) console... enter "exit" to return to bootCLI
> ~
telnet> quit
Connection closed.
Firepower#
```

What's Next?

To continue configuring your threat defense, see the documents available for your software version at Navigating the Cisco Firepower Documentation.

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

History for Threat Defense with the Management Center

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

Feature Name	Version	Feature Information

Multi-instance capability for threat defense on the Firepower 4100/9300	6.3.0	You can now deploy multiple logical devices, each with the threat defense container instance, on a single security engine/module. Formerly, you could only deploy a single native application instance.
		
		To provide flexible physical interface use, you can create VLAN subinterfaces in FXOS and also share interfaces between multiple instances. Resource management lets you customize performance capabilities for each instance.
		
		You can use High Availability using a container instance on 2 separate chassis. Clustering is not supported.
		
		Note Multi-instance capability is similar to ASA multiple context mode, although the implementation is different. Multiple context mode is not available on the threat defense.
		
		New/Modified management center screens:
		
		  • **Devices** > **Device Management** > **Edit** icon **> Interfaces** tab
		
		New/Modified chassis manager screens:
		
		  • **Overview** > **Devices**
		
		  • **Interfaces** > **All Interfaces** > **Add New** drop-down menu **> Subinterface**
		
		  • **Interfaces** > **All Interfaces** > **Type**
		
		  • **Logical Devices** > **Add Device**
		
		  • **Platform Settings** > **Mac Pool**
		
		  • **Platform Settings** > **Resource Profiles**

C H A P T E R 4

Threat Defense Deployment with the Device Manager

Is This Chapter for You?

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

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

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

Privacy Collection Statement—The Firepower 4100 does not require or actively collect personally-identifiable information. However, you can use personally-identifiable information in the configuration, for example for usernames. In this case, an administrator might be able to see this information when working with the configuration or when using SNMP.

End-to-End Procedure

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

	Workspace	Steps
①	Chassis Manager	Chassis Manager: Add the Threat Defense Logical Device, on page 58.
②	Device Manager	Log Into the Device Manager, on page 62.
③	Cisco Commerce Workspace	Configure Licensing, on page 62: Buy feature licenses.
④	Smart Software Manager	Configure Licensing, on page 62: Generate a license token for the device manager.
⑤	Device Manager	Configure Licensing, on page 62: Register the device manager with the Smart Licensing server, and enable feature licenses.
⑥	Device Manager	Configure a Basic Security Policy, on page 68.

Chassis Manager: Add the Threat Defense Logical Device

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

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

Before you begin

- Configure a Management interface to use with the threat defense; see Configure Interfaces, on page 21. The Management interface is required. Note that this Management interface is not the same as the chassis management port that is used only for chassis management (and that appears at the top of the **Interfaces** tab as **MGMT**).

- You must also configure at least one Data interface.

- Gather the following information:
  - Interface IDs for this device
  - Management interface IP address and network mask
  - Gateway IP address
  - DNS server IP address
  - Threat Defense hostname and domain name

Procedure

Step 1   In the Chassis Manager, choose **Logical Devices**.

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

Add Standalone	? ×
Device Name:	FTD_1
Template:	Cisco Firepower Threat Defense ▾
Image Version:	6.5.0.1159 ▾
Instance Type:	Native ▾
	OK Cancel

    a)   Provide a **Device Name**.

      This name is used by the chassis supervisor to configure management settings and to assign interfaces; it is not the device name used in the application configuration.

      Note   You cannot change this name after you add the logical device.

    b)   For the **Template**, choose **Cisco Firepower Threat Defense**.
    c)   Choose the **Image Version**.
    d)   Choose the **Instance Type**: **Native**.

      Container instances are not supported with the device manager.

    e)   Click **OK**.

      You see the Provisioning - *device name* window.

Step 3   Expand the **Data Ports** area, and click each interface that you want to assign to the device.
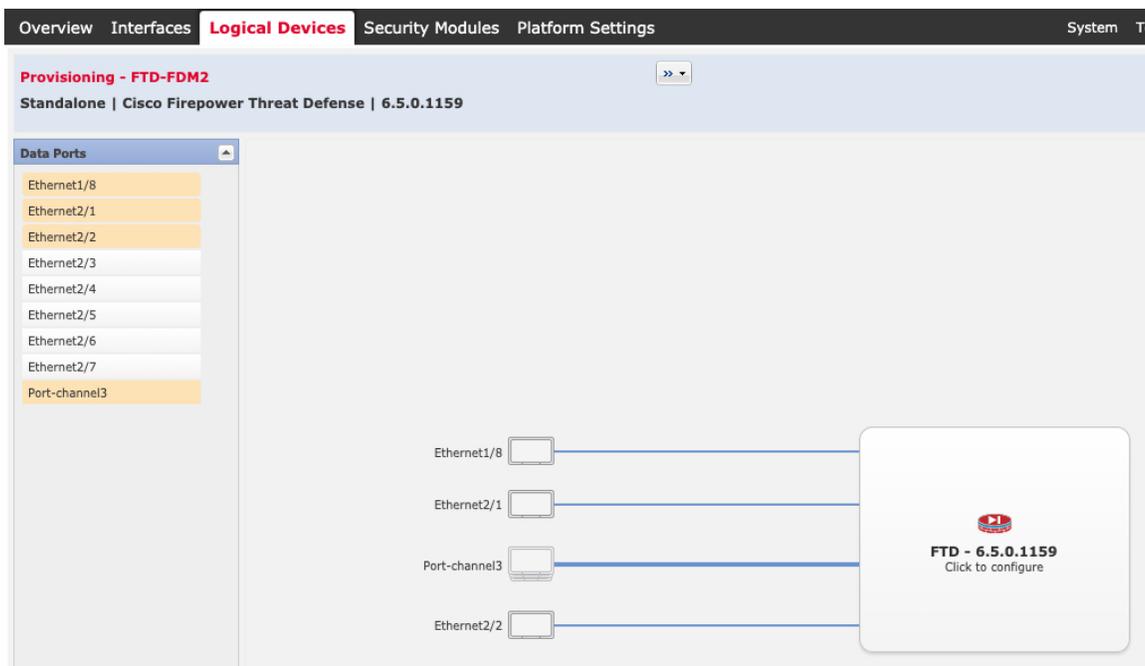
You can only assign data interfaces that you previously enabled on the **Interfaces** page. You will later enable and configure these interfaces in the device manager, including setting the IP addresses.

Step 4   Click the device icon in the center of the screen.

A dialog box appears where you can configure initial bootstrap settings. These settings are meant for initial deployment only, or for disaster recovery. For normal operation, you can later change most values in the application CLI configuration.

Step 5   On the **General Information** page, complete the following:

a) Choose the **Management Interface**.

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

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

c) Configure the **Management IP** address.

Set a unique IP address for this interface.

d) Enter a **Network Mask** or **Prefix Length**.

e) Enter a **Network Gateway** address.

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

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

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

b) Enter the **Search Domains** as a comma-separated list.

c) The **Firewall Mode** only supports **Routed** mode.

d) Enter the **DNS Servers** as a comma-separated list.

e) Enter the **Fully Qualified Hostname** for the threat defense.

f) Enter a **Password** for the threat defense admin user for CLI access.

Step 7 On the **Agreement** tab, read and accept the end user license agreement (EULA).

Step 8 Click **OK** to close the configuration dialog box.

Step 9 Click **Save**.

The chassis deploys the logical device by downloading the specified software version and pushing the bootstrap configuration and management interface settings to the application instance. Check the **Logical Devices** page for the status of the new logical device. When the logical device shows its **Status** as **online**, you can start configuring the security policy in the application.
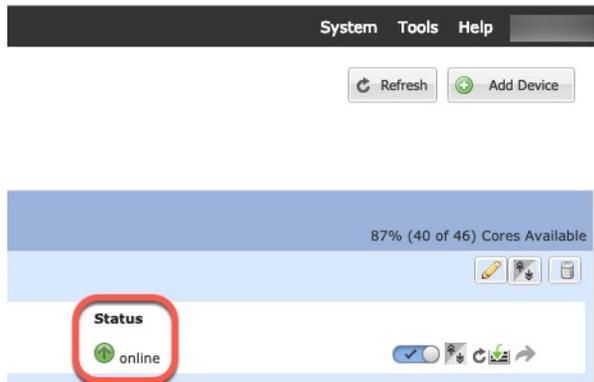
Log Into the Device Manager

Log into the device manager to configure your threat defense.

Before you begin

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

- Make sure the threat defense logical device **Status** is **online** on the chassis manager **Logical Devices** page.

Procedure

Step 1 Enter the following URL in your browser.

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

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

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

Configure Licensing

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

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

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

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

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

- **Malware Defense**—Malware defense

- **URL**—URL Filtering

- **Cisco Secure Client**—Secure Client Advantage, Secure Client Premier, or Secure Client VPN Only

Before you begin

- Have a master account on the Smart Software Manager.

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

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

Procedure

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

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

Figure 7: License Search
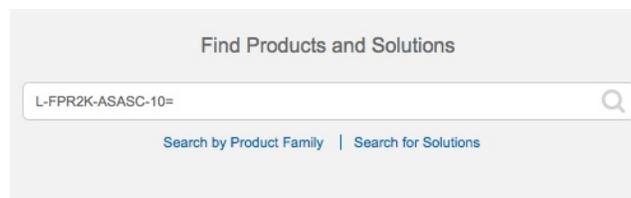
Note   If a PID is not found, you can add the PID manually to your order.

- IPS, Malware Defense, and URL license combination:
  - L-FPR4112T-TMC=
  - L-FPR4115T-TMC=
  - L-FPR4125T-TMC=
  - L-FPR4145T-TMC=

When you add one of the above PIDs to your order, you can then choose a term-based subscription corresponding with one of the following PIDs:

- L-FPR4112T-TMC-1Y

- L-FPR4112T-TMC-3Y

- L-FPR4112T-TMC-5Y

- L-FPR4115T-TMC-1Y

- L-FPR4115T-TMC-3Y

- L-FPR4115T-TMC-5Y

- L-FPR4125T-TMC-1Y

- L-FPR4125T-TMC-3Y

- L-FPR4125T-TMC-5Y

- L-FPR4145T-TMC-1Y

- L-FPR4145T-TMC-3Y

- L-FPR4145T-TMC-5Y

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

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

a) Click **Inventory**.

Cisco Software Central > Smart Software Licensing

Smart Software Licensing

Alerts | **Inventory** | License Conversion | Reports | Email Notification | Satellites | Activity

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

| General | Licenses | Product Instances | Event Log |

Virtual Account

Description:

Default Virtual Account: No

Product Instance Registration Tokens

The registration tokens below can be used to register new product instances to this virtual account.

New Token...

Token	Expiration Date	Description
NWU1MzY1MzEtZjNmOS00MjF..	2018-Jul-06 14:20:13 (in 354 days)	FTD-5506

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

• **Description**

• **Expire After**—Cisco recommends 30 days.

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

The token is added to your inventory.

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

Figure 8: View Token

Figure 9: Copy Token

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

You see the **Smart License** page.

Step 4 Click **Register Device**.
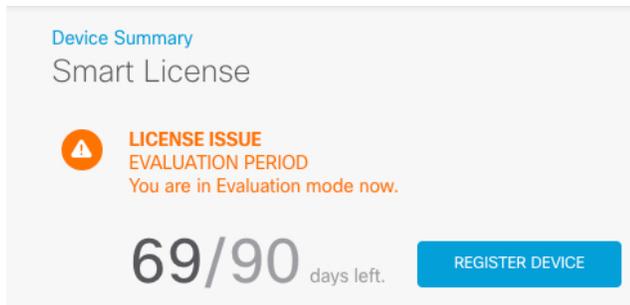
Device Summary
Smart License

⚠ **LICENSE ISSUE**
EVALUATION PERIOD
You are in Evaluation mode now.

69/90 days left.

REGISTER DEVICE

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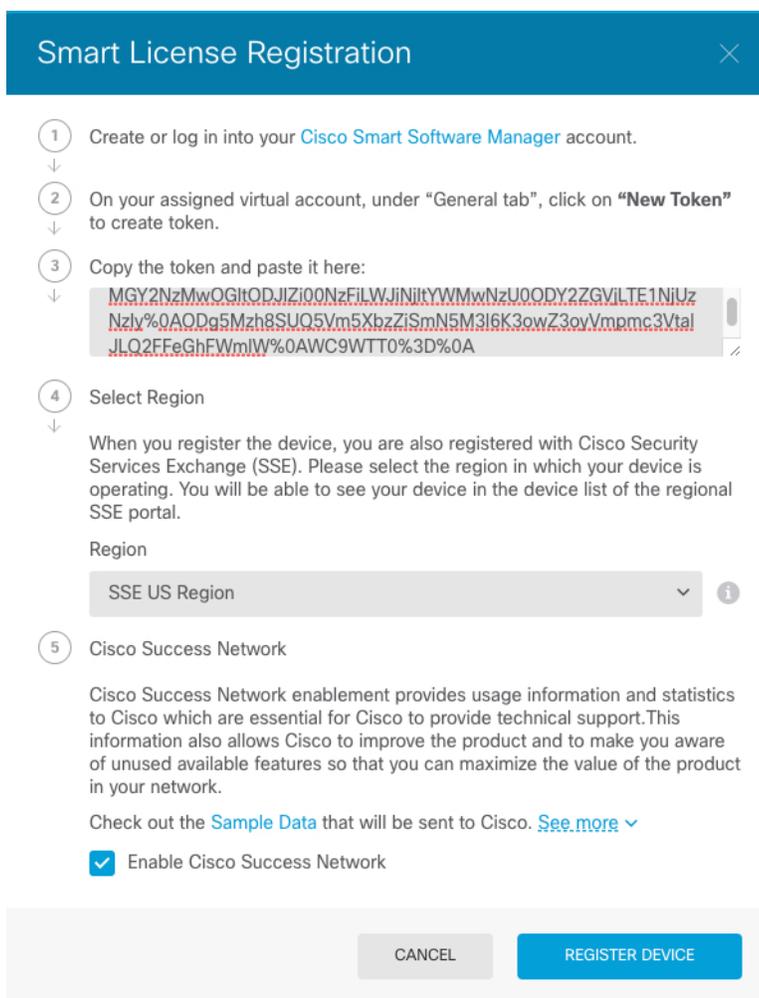
Smart License Registration ✕

① Create or log in into your Cisco Smart Software Manager account.

② On your assigned virtual account, under "General tab", click on **"New Token"** to create token.

③ Copy the token and paste it here:

MGY2NzMwOGltODJlZi00NzFiLWJiNiltYWMwNzU0ODY2ZGViLTE1NjUz
Nzlv%0AODg5Mzh8SUQ5Vm5XbzZiSmN5M3l6K3owZ3oyVmpmc3Vtal
JLQ2FFeGhFWmlW%0AWC9WTT0%3D%0A

④ Select Region

When you register the device, you are also registered with Cisco Security Services Exchange (SSE). Please select the region in which your device is operating. You will be able to see your device in the device list of the regional SSE portal.

Region

SSE US Region ⌄ ⓘ

⑤ Cisco Success Network

Cisco Success Network enablement provides usage information and statistics to Cisco which are essential for Cisco to provide technical support.This information also allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product in your network.

Check out the Sample Data that will be sent to Cisco. See more ⌄

☑ Enable Cisco Success Network

CANCEL   REGISTER DEVICE

Step 5 Click **Register Device**.

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

> Registration request sent on 10 Jul 2019. Please wait. Normally, it takes about one minute to complete the registration. You can check the task status in Task List. Refresh this page to see the updated status.

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

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

- **Enable**—Registers the license with your Cisco Smart Software Manager account and enables the controlled features. You can now configure and deploy policies controlled by the license.

- **Disable**—Unregisters the license with your Cisco Smart Software Manager account and disables the controlled features. You cannot configure the features in new policies, nor can you deploy policies that use the feature.

- If you enabled the **Cisco Secure Client** license, select the type of license you want to use: **Advantage**, **Premier**, **VPN Only**, or **Premier and Advantage**.

After you enable features, if you do not have the licenses in your account, you will see the following non-compliance message after you refresh the page:
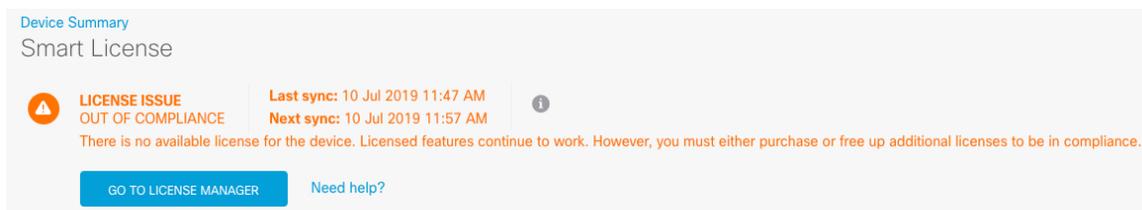
Step 7 Choose **Resync Connection** from the gear drop-down list to synchronize license information with Cisco Smart Software Manager.
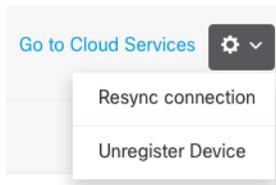
Configure a Basic Security Policy

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

1	Configure Interfaces, on page 69. Assign a static IP address to the inside interface, and use DHCP for the outside interface.
2	Add Interfaces to Security Zones, on page 71. Add the inside and outside interfaces to inside and outside security zones, which are required for access control.
3	Add the Default Route, on page 73. If you do not receive the default route from the outside DHCP server, you need to manually add it.
4	Configure NAT, on page 75. Use interface PAT on the outside interface.
5	Allow Traffic from Inside to Outside, on page 77. Allow traffic from inside to outside.
6	(Optional) Configure the DHCP Server, on page 78. Use a DHCP server on the inside interface for clients.
7	(Optional) Configure the Management Gateway and Allow Management on Data Interfaces, on page 79. Change the management gateway and/or allow management from a data interface.
8	Deploy the Configuration, on page 81.

Configure Interfaces

Enable the threat defense interfaces and set the IP addresses. Typically, you must configure at least a minimum of two interfaces to have a system that passes meaningful traffic. Normally, you would have an outside interface that faces the upstream router or internet, and one or more inside interfaces for your organization's networks. Some of these interfaces might be "demilitarized zones" (DMZs), where you place publically-accessible assets such as your web server.

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

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

Procedure

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

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

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

Step 3   Set the following:

a) Set the **Interface Name**.

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

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

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

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

Important   You must also enable the interface in FXOS.

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

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

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

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

Step 4   Click **OK**.

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

Port-channel1
Edit Physical Interface

Interface Name

outside

Most features work with named interfaces only, although some require unnamed interfaces.

Mode

Routed

Status

Description

IPv4 Address   IPv6 Address   Advanced

⚠ If the DHCP server supplies an address on the same network configured statically for another interface, this interface will be disabled. Ensure that there is no overlap between the network addresses on this interface and the other interfaces on the device.

Type

DHCP

Route Metric

☑ Obtain Default Route using DHCP

1 - 255

CANCEL   OK

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

Add Interfaces to Security Zones

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

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

- **inside_zone**—This zone is intended to represent internal networks.

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

Procedure

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

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

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

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

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

Add the Default Route

The default route normally points to the upstream router reachable from the outside interface. If you use DHCP for the outside interface, your device might have already received a default route. If you need to manually add the route, complete this procedure. If you received a default route from the DHCP server, it will show on the **Device Summary** > **Static Routing** page.

Procedure

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

The **Static Routing** page appears.

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

Step 3   Configure the default route properties.

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

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

c) Click **Gateway**, and then click **Create New Network** to add the gateway IP address as a host object.
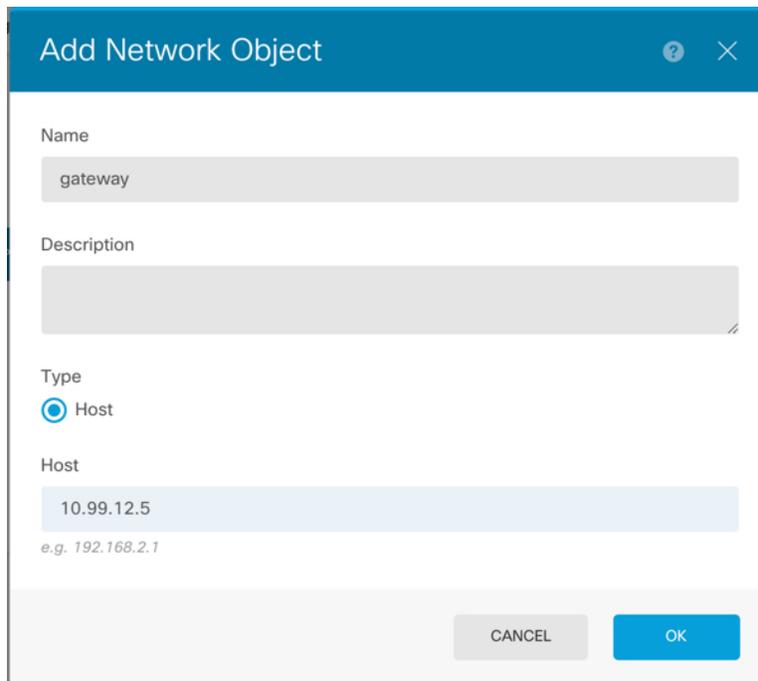
d) Choose the gateway **Interface**, for example **outside**.

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

Step 4 Click **OK**.

Configure NAT

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

Procedure

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

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

Step 3 Configure the basic rule options:
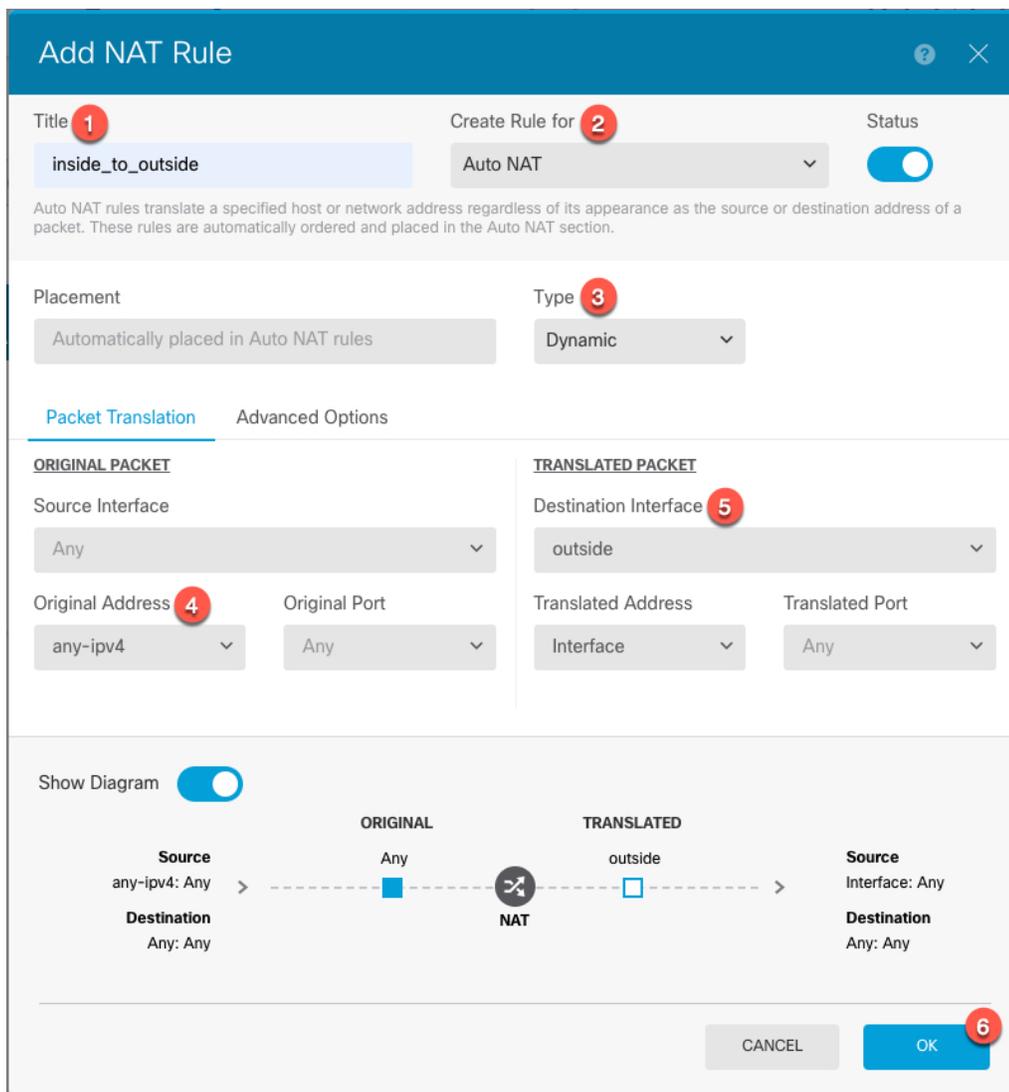
a) Set the **Title**.

b) Choose **Create Rule For** > **Auto NAT**.

c) Choose **Type** > **Dynamic**.

Step 4   Configure the following packet translation options:

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

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

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

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

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

Step 6   Click **OK**.

Allow Traffic from Inside to Outside

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

Procedure

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

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

Step 3   Configure the basic rule options:

a)   Set the **Title**.

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

c) For the **Destination**, click the **Zones** ＋ icon, and choose the outside zone.

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

e) Click **OK**.

(Optional) Configure the DHCP Server

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

Procedure

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

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

Step 3 Configure the server properties.
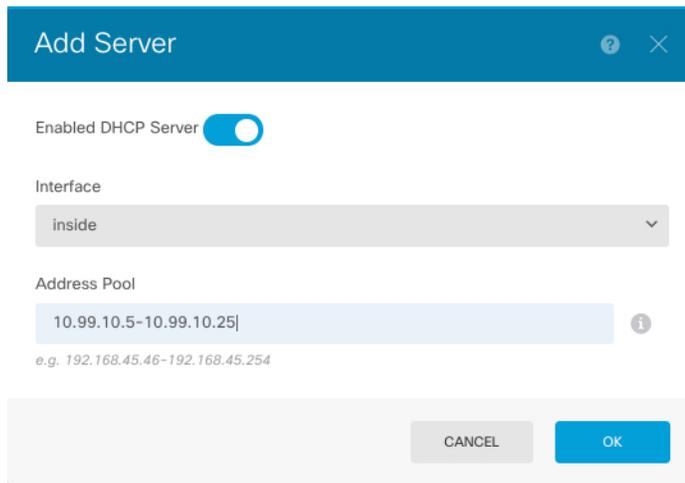
a) Click the **Enable DHCP Server** slider so that it shows enabled (   ).

b) Choose the **Interface** on which you want to enable the DHCP server.

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

c) Enter the **Address Pool**

The range of IP addresses must be on the same subnet as the selected interface and cannot include: the IP address of the interface itself, the broadcast address, or the subnet network address.

d) Click **OK**.

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

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

a) Click the **Enable Auto Configuration** slider so that it shows enabled ( ).

b) Choose the interface in the **From Interface** drop-down menu from which you want clients to inherit server settings.

c) If you do not enable auto-configuration, or if you want to override any of the automatically configured settings, configure one or more global options. These settings will be sent to DHCP clients on all interfaces that run a DHCP server.

d) Click **Save**.

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

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

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

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

Before you begin

Configure data interfaces according to .

Procedure

Step 1 Allow management from a data interface.

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

b) Click **Data Interfaces**.

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

- **Interface**—Choose the interface on which you want to allow management access.

- **Protocols**—Choose whether the rule is for HTTPS (port 443), SSH (port 22), or both.

- **Allowed Networks**—Choose the network objects that define the IPv4 or IPv6 network or host that should be able to access the system. To specify "any" address, select **any-ipv4** (0.0.0.0/0) and **any-ipv6** (::/0).

d) Click **OK**.

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

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

b) Choose **Use the Data Interfaces as the Gateway**.
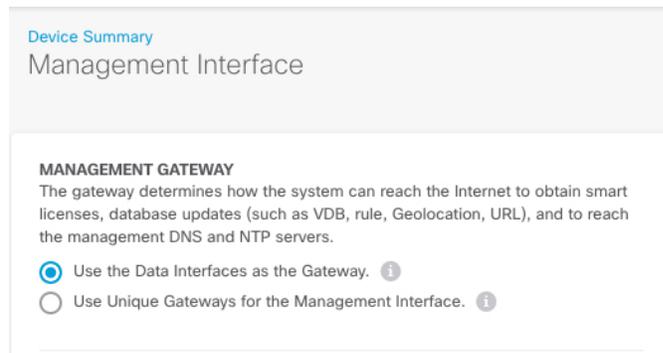
c)   Click **Save**, read the warning, and click **OK**.

Deploy the Configuration

Deploy the configuration changes to the threat defense; none of your changes are active on the device until you deploy them.

Procedure

Step 1   Click the **Deploy Changes** icon in the upper right of the web page.

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

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

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

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

Access the Threat Defense CLI

You can use the threat defense CLI to change management interface parameters and for troubleshooting purposes. You can access the CLI using SSH to the Management interface, or by connecting from the FXOS CLI.

Procedure

Step 1 (Option 1) SSH directly to the threat defense management interface IP address.

You set the management IP address when you deployed the logical device. Log into the threat defense with the admin account and the password you set during initial deployment.

If you forgot the password, you can change it by editing the logical device in the chassis manager.

Step 2 (Option 2) From the FXOS CLI, connect to the module CLI using a console connection or a Telnet connection.

a) Connect to the security engine.

connect module 1 {**console** | **telnet**}

The benefits of using a Telnet connection is that you can have multiple sessions to the module at the same time, and the connection speed is faster.

Example:

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

b) Connect to the threat defense console.

connect ftd *name*

If you have multiple application instances, you must specify the name of the instance. To view the instance names, enter the command without a name.

Example:

```
Firepower-module1> connect ftd FTD_Instance1

============================= ATTENTION =============================
You are connecting to ftd from a serial console. Please avoid
executing any commands which may produce large amount of output.
Otherwise, data cached along the pipe may take up to 12 minutes to be
drained by a serial console at 9600 baud rate after pressing Ctrl-C.

To avoid the serial console, please login to FXOS with ssh and use
'connect module <slot> telnet' to connect to the security module.
====================================================================

Connecting to container ftd(FTD_Instance1) console... enter "exit" to return to bootCLI
>
```

c) Exit the application console to the FXOS module CLI by entering **exit**.

Note For pre-6.3 versions, enter **Ctrl-a, d**.

    d)   Return to the supervisor level of the FXOS CLI.

        To exit the console:

        1. Enter **~**

            You exit to the Telnet application.

        2. To exit the Telnet application, enter:

            telnet>**quit**

        To exit the Telnet session:

        Enter **Ctrl-], .**

Example

The following example connects to the threat defense and then exits back to the supervisor level of the FXOS CLI.

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>connect ftd FTD_Instance1

============================= ATTENTION ==============================
You are connecting to ftd from a serial console. Please avoid
executing any commands which may produce large amount of output.
Otherwise, data cached along the pipe may take up to 12 minutes to be
drained by a serial console at 9600 baud rate after pressing Ctrl-C.

To avoid the serial console, please login to FXOS with ssh and use
'connect module <slot> telnet' to connect to the security module.
=====================================================================

Connecting to container ftd(FTD_Instance1) console... enter "exit" to return to bootCLI
> ~
telnet> quit
Connection closed.
Firepower#
```

What's Next?

To continue configuring your threat defense, see the documents available for your software version at Navigating the Cisco Firepower Documentation.

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

History for Threat Defense with the Device Manager

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

Threat Defense Deployment with CDO

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 the threat defense using Cisco Defense Orchestrator (CDO)'s cloud-delivered Secure Firewall Management Center. To use CDO using device manager functionality, see the CDO documentation.

Note The cloud-delivered management center supports threat defense 7.2 and later. For earlier versions, you can use CDO's device manager functionality. However, device manager mode is only available to existing CDO users who are already managing threat defenses using this mode.

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

About the Firewall

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

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 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

The cloud-delivered management center 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.

✎

Note   CDO does not support container instances or clusters.

End-to-End Procedure

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

Figure 10: End-to-End Procedure
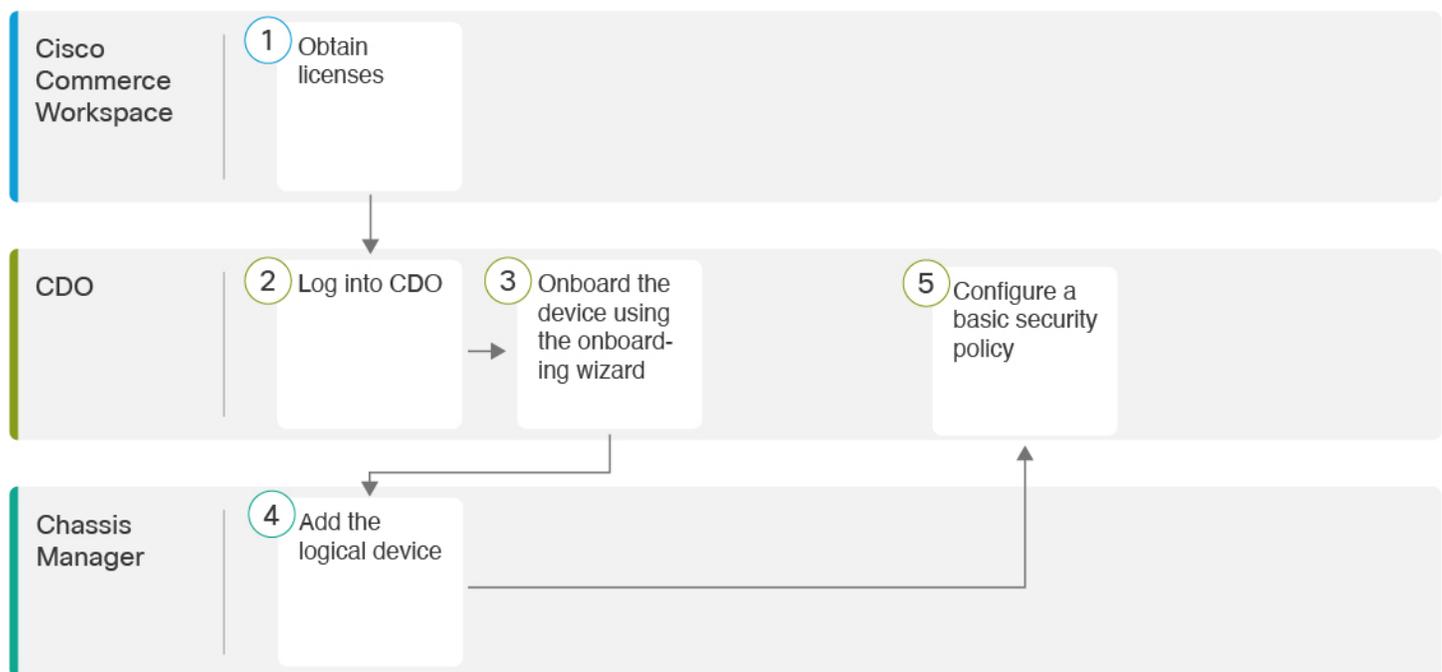
1	Cisco Commerce Workspace	Obtain Licenses, on page 87.
2	CDO	Log Into CDO, on page 89.

3	CDO	Onboard a Device with the Onboarding Wizard, on page 93.
4	Chassis Manager	Chassis Manager: Add the Threat Defense Logical Device, on page 94.
5	CDO	Configure a Basic Security Policy, on page 42.

Obtain Licenses

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

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

- **Malware Defense**—Malware defense

- **URL**—URL Filtering

- **Cisco Secure Client**—Secure Client Advantage, Secure Client Premier, or Secure Client VPN Only

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

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

Before you begin

- Have a master account on the Smart Software Manager.

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

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

Procedure

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

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

Figure 11: License Search

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

- IPS, Malware Defense, and URL license combination:
  - L-FPR4112T-TMC=
  - L-FPR4115T-TMC=
  - L-FPR4125T-TMC=
  - L-FPR4145T-TMC=

  When you add one of the above PIDs to your order, you can then choose a term-based subscription corresponding with one of the following PIDs:
  - L-FPR4112T-TMC-1Y
  - L-FPR4112T-TMC-3Y
  - L-FPR4112T-TMC-5Y
  - L-FPR4115T-TMC-1Y
  - L-FPR4115T-TMC-3Y
  - L-FPR4115T-TMC-5Y
  - L-FPR4125T-TMC-1Y
  - L-FPR4125T-TMC-3Y
  - L-FPR4125T-TMC-5Y
  - L-FPR4145T-TMC-1Y
  - L-FPR4145T-TMC-3Y
  - L-FPR4145T-TMC-5Y

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

- Carrier license:
  - L-FPR4K-FTD-CAR=

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.

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.

Create a New Cisco Secure Sign-On Account

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

Before you begin

• **Install DUO Security**—We recommend that you install the Duo Security app on a mobile phone. Review Duo Guide to Two Factor Authentication: Enrollment Guide if you have questions about installing Duo.

• **Time Synchronization**—You are going to use your mobile device to generate a one-time password. It is important that your device clock is synchronized with real time as the OTP is time-based. Make sure your device clock is set to the correct time.

• Use a current version of Firefox or Chrome.

Procedure

Step 1 **Sign Up for a New Cisco Secure Sign-On Account.**
a) Browse to https://sign-on.security.cisco.com.
b) At the bottom of the Sign In screen, click **Sign up**.

Figure 12: Cisco SSO Sign Up

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

Figure 13: Create Account

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

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

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

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

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

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

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

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

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

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

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

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

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

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

    c) Choose a security image.

    d) Click **Create My Account**.

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

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

Figure 14: Cisco SSO Dashboard
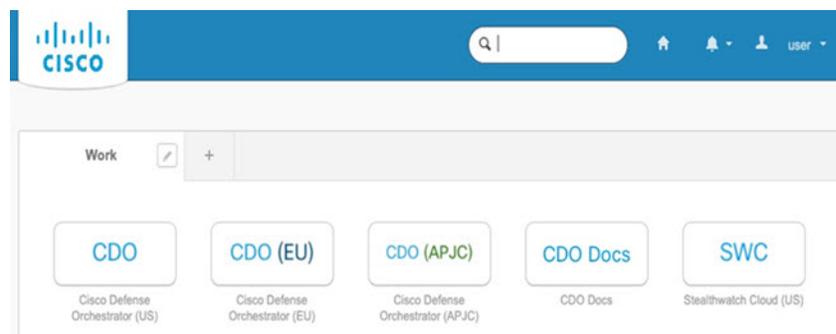
Log Into CDO with Cisco Secure Sign-On

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 89.

- Use a current version of Firefox or Chrome.

Procedure

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

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

Step 3 Click **Log in**.

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

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

Figure 15: Cisco SSO Dashboard
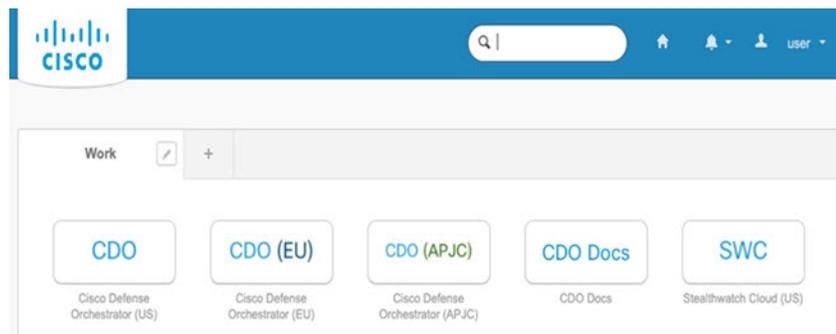
Step 6 Click the authenticator logo to choose **Duo Security** or **Google Authenticator**, if you have set up both authenticators.

- 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.

Onboard a Device with the Onboarding Wizard

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

Procedure

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

Step 2 Select the **FTD** tile.

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

At any point after selecting **FTD** as the management mode, you can click **Manage Smart License** to enroll in or modify the existing smart licenses available for your device. See Obtain Licenses, on page 87 to see which licenses are available.

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

Figure 16: Use CLI Registration Key
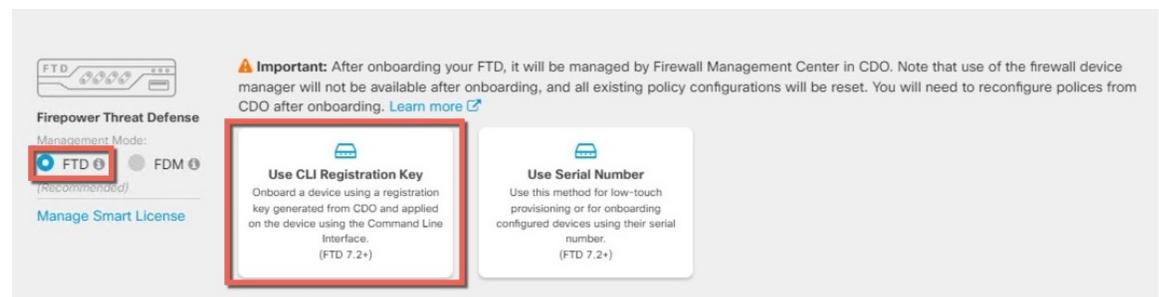
Step 5 Enter the **Device Name** and click **Next**.

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**.

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**.

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

configure manager add *cdo_hostname registration_key nat_id display_name*

In the chassis manager when you deploy the logical device (see Chassis Manager: Add the Threat Defense Logical Device, on page 94), copy this command into the **CDO Onboard** and **Confirm CDO Onboard** fields.

Example:

Sample command:

```
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.

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.

Chassis Manager: Add the Threat Defense Logical Device

You can deploy the threat defense from the Firepower 4100 as a standalone, native instance. CDO does not support container instances or clusters.

This procedure lets you configure the logical device characteristics, including the bootstrap configuration used by the application.

Before you begin

- Configure a Management interface to use with the threat defense; see Configure Interfaces, on page 21. The Management interface is required. You can later enable management from a data interface; but you must assign a Management interface to the logical device even if you don't intend to use it after you enable data management. Note that this Management interface is not the same as the chassis management port that is used only for chassis management (and that appears at the top of the **Interfaces** tab as **MGMT**).

- You must also configure at least one Data interface.

- Gather the following information:

  - Interface IDs for this device

  - Management interface IP address and network mask

  - Gateway IP address

  - CDO hostname, registration key, and NAT ID generated by CDO. See Onboard a Device with the Onboarding Wizard, on page 93.

  - DNS server IP address

Procedure

Step 1 In the chassis manager, choose **Logical Devices**.

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

Figure 17: Add a Standalone Device

a) Provide a **Device Name**.

This name is used by the chassis supervisor to configure management settings and to assign interfaces; it is not the device name used in the application configuration.

Note You cannot change this name after you add the logical device.

b) For the **Template**, choose **Cisco Firepower Threat Defense**.

c) Choose the **Image Version**.

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

e) Click **OK**.

You see the Provisioning - *device name* window.

Step 3 Expand the **Data Ports** area, and click each interface that you want to assign to the device.

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

Hardware Bypass–capable ports are shown with the following icon: ⚙. For certain interface modules, you can enable the Hardware Bypass feature for Inline Set interfaces only. Hardware Bypass ensures that traffic

continues to flow between an inline interface pair during a power outage. This feature can be used to maintain network connectivity in the case of software or hardware failures. If you do not assign both interfaces in a Hardware Bypass pair, you see a warning message to make sure your assignment is intentional. You do not need to use the Hardware Bypass feature, so you can assign single interfaces if you prefer.

Step 4 Click the device icon in the center of the screen.

A dialog box appears where you can configure initial bootstrap settings. These settings are meant for initial deployment only, or for disaster recovery. For normal operation, you can later change most values in the application CLI configuration.

Step 5 On the **General Information** page, complete the following:

Figure 18: General Information

a) Choose the **Management Interface**.

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

b) Choose the management interface **Address Type**: **IPv4 only**, **IPv6 only**, or **IPv4 and IPv6**.
c) Configure the **Management IP** address.

Set a unique IP address for this interface.

d) Enter a **Network Mask** or **Prefix Length**.
e) Enter a **Network Gateway** address.

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

Figure 19: Settings

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

b) Enter the **Search Domains** as a comma-separated list.

c) Choose the **Firewall Mode**: **Transparent** or **Routed**.

In routed mode, the threat defense is considered to be a router hop in the network. Each interface that you want to route between is on a different subnet. A transparent firewall, on the other hand, is a Layer 2 firewall that acts like a "bump in the wire," or a "stealth firewall," and is not seen as a router hop to connected devices.

The firewall mode is only set at initial deployment. If you re-apply the bootstrap settings, this setting is not used.

d) Enter the **DNS Servers** as a comma-separated list.

The threat defense uses DNS if you specify a hostname for the management center, for example.

e) Enter the **Fully Qualified Hostname** for the threat defense.

f) Enter a **Password** for the threat defense admin user for CLI access.

g) Copy the command generated by CDO into the **CDO Onboard** and **Confirm CDO Onboard** fields.

h) A separate **Eventing Interface** is not supported for CDO, so this setting will be ignored.

Step 7   On the **Agreement** tab, read and accept the end user license agreement (EULA).

Step 8   Click **OK** to close the configuration dialog box.

Step 9   Click **Save**.

The chassis deploys the logical device by downloading the specified software version and pushing the bootstrap configuration and management interface settings to the application instance. Check the **Logical Devices** page

for the status of the new logical device. When the logical device shows its **Status** as **online**, you can start configuring the security policy in the application.

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.

Configure Interfaces

Enable the threat defense interfaces, assign them to security zones, and set the IP addresses. Typically, you must configure at least a minimum of two interfaces to have a system that passes meaningful traffic. Normally, you would have an outside interface that faces the upstream router or internet, and one or more inside interfaces for your organization's networks. Some of these interfaces might be "demilitarized zones" (DMZs), where you place publically-accessible assets such as your web server.

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

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

Procedure

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

Step 2   Click **Interfaces**.

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

The **General** tab appears.

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**

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

    f) Click **OK**.

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

The **General** tab appears.

> **Note** If you pre-configured this interface for manager access, then the interface will already be named, enabled, and addressed. You should not alter any of these basic settings because doing so will disrupt the management center management connection. You can still configure the Security Zone on this screen for through traffic policies.

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

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

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

    c) Leave the **Mode** set to **None**.

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

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

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

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

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

f) Click **OK**.

Step 5 Click **Save**.

Configure the DHCP Server

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

Procedure

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

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

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

• **Interface**—Choose the interface from the drop-down list.

• **Address Pool**—Set the range of IP addresses from lowest to highest that are used by the DHCP server. The range of IP addresses must be on the same subnet as the selected interface and cannot include the IP address of the interface itself.

• **Enable DHCP Server**—Enable the DHCP server on the selected interface.

Step 4 Click **OK**.

Step 5 Click **Save**.

Add the Default Route

The default route normally points to the upstream router reachable from the outside interface. If you use DHCP for the outside interface, your device might have already received a default route. If you need to manually add the route, complete this procedure. If you received a default route from the DHCP server, it will show in the **IPv4 Routes** or **IPv6 Routes** table on the **Devices** > **Device Management** > **Routing** > **Static Route** page.

Procedure

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

Step 2   Choose **Routing** > **Static Route**, click **Add Route**, and set the following:

- **Type**—Click the **IPv4** or **IPv6** radio button depending on the type of static route that you are adding.

- **Interface**—Choose the egress interface; typically the outside interface.

- **Available Network**—Choose **any-ipv4** for an IPv4 default route, or **any-ipv6** for an IPv6 default route and click **Add** to move it to the **Selected Network** list.

- **Gateway** or **IPv6 Gateway**—Enter or choose the gateway router that is the next hop for this route. You can provide an IP address or a Networks/Hosts object.

- **Metric**—Enter the number of hops to the destination network. Valid values range from 1 to 255; the default value is 1.

Step 3   Click **OK**.

The route is added to the static route table.

Step 4 Click **Save**.

Configure NAT

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

Procedure

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

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

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

Step 3   Click **Add Rule**.

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

Step 4   Configure the basic rule options:

- **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.

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

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

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:

- **Name**—Name this rule, for example, **inside_to_outside**.

- **Source Zones**—Select the inside zone from **Available Zones**, and click **Add to Source**.

- **Destination Zones**—Select the outside zone from **Available Zones**, and click **Add to Destination**.

Leave the other settings as is.

Step 3   Click **Add**.

The rule is added to the **Rules** table.


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 20: Deploy

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

Figure 21: Deploy All
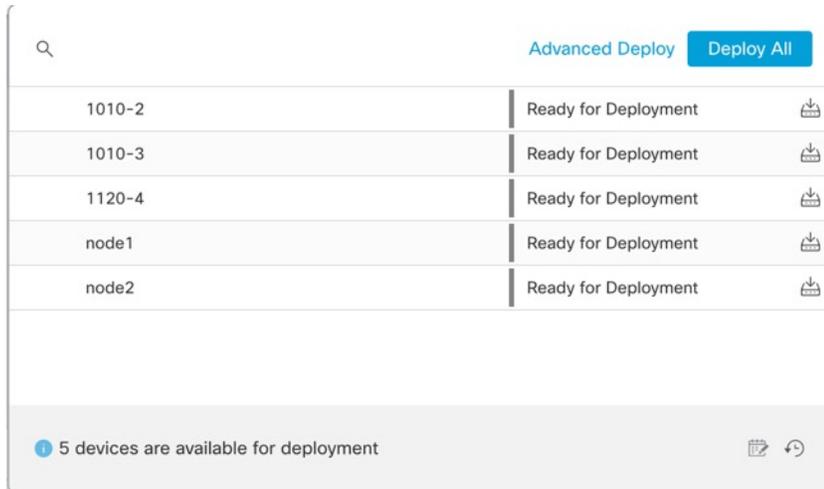
Figure 22: Advanced Deploy
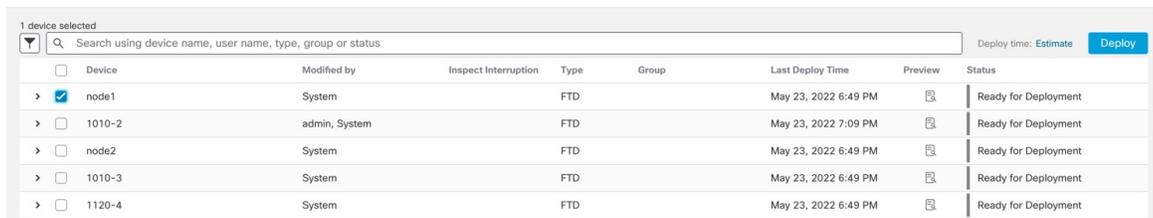
Step 3 Ensure that the deployment succeeds. Click the icon to the right of the **Deploy** button in the menu bar to see status for deployments.

Figure 23: Deployment Status
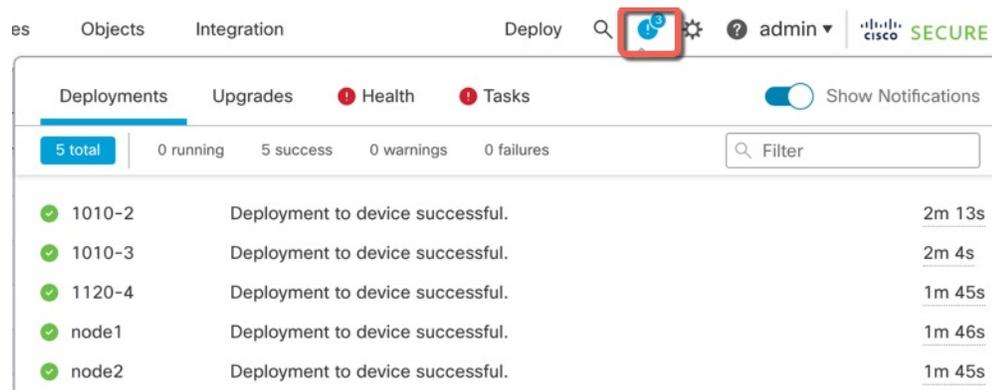
Access the Threat Defense and FXOS CLI

You can use the threat defense CLI to change management interface parameters and for troubleshooting purposes. You can access the CLI using SSH to the Management interface, or by connecting from the FXOS CLI.

Procedure

Step 1 (Option 1) SSH directly to the threat defense management interface IP address.

You set the management IP address when you deployed the logical device. Log into the threat defense with the admin account and the password you set during initial deployment.

If you forgot the password, you can change it by editing the logical device in the chassis manager.

Step 2 (Option 2) From the FXOS CLI, connect to the module CLI using a console connection or a Telnet connection.

a) Connect to the security engine.

connect module 1 {**console** | **telnet**}

The benefits of using a Telnet connection is that you can have multiple sessions to the module at the same time, and the connection speed is faster.

Example:

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

b) Connect to the threat defense console.

connect ftd *name*

If you have multiple application instances, you must specify the name of the instance. To view the instance names, enter the command without a name.

Example:

```
Firepower-module1> connect ftd FTD_Instance1

============================= ATTENTION =============================
You are connecting to ftd from a serial console. Please avoid
executing any commands which may produce large amount of output.
Otherwise, data cached along the pipe may take up to 12 minutes to be
drained by a serial console at 9600 baud rate after pressing Ctrl-C.

To avoid the serial console, please login to FXOS with ssh and use
'connect module <slot> telnet' to connect to the security module.
====================================================================

Connecting to container ftd(FTD_Instance1) console... enter "exit" to return to bootCLI
>
```

c) Exit the application console to the FXOS module CLI by entering **exit**.

Note　　　For pre-6.3 versions, enter **Ctrl-a, d**.

d) Return to the supervisor level of the FXOS CLI.

To exit the console:

1. Enter **~**

   You exit to the Telnet application.

2. To exit the Telnet application, enter:

   telnet>**quit**

To exit the Telnet session:

Enter **Ctrl-], .**

Example

The following example connects to the threat defense and then exits back to the supervisor level of the FXOS CLI.

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit
```

```
Firepower-module1>connect ftd FTD_Instance1

============================== ATTENTION ==============================
You are connecting to ftd from a serial console. Please avoid
executing any commands which may produce large amount of output.
Otherwise, data cached along the pipe may take up to 12 minutes to be
drained by a serial console at 9600 baud rate after pressing Ctrl-C.

To avoid the serial console, please login to FXOS with ssh and use
'connect module <slot> telnet' to connect to the security module.
======================================================================

Connecting to container ftd(FTD_Instance1) console... enter "exit" to return to bootCLI
> ~
telnet> quit
Connection closed.
Firepower#
```

What's Next

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

ASA Deployment with ASDM

Is This Chapter for You?

This chapter describes how to deploy a standalone ASA logical device, including how to configure smart licensing. This chapter does not cover the following deployments, for which you should refer to the ASA configuration guide:

- Clustering
- Failover
- CLI configuration

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

Privacy Collection Statement—The Firepower 4100 does not require or actively collect personally-identifiable information. However, you can use personally-identifiable information in the configuration, for example for usernames. In this case, an administrator might be able to see this information when working with the configuration or when using SNMP.

End-to-End Procedure

See the following tasks to deploy and configure the ASA on your chassis.
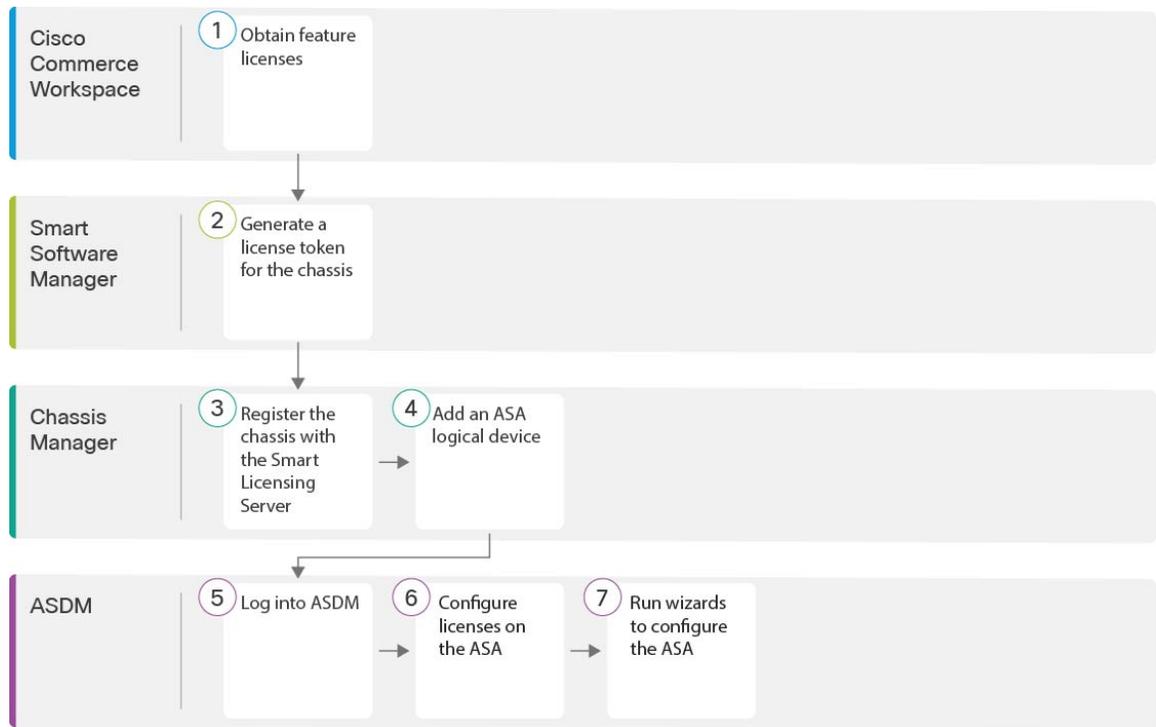
1	Cisco Commerce Workspace	Chassis Manager: Register the Chassis with the Licensing Server, on page 114: Obtain feature licenses.
2	Smart Software Manager	Chassis Manager: Register the Chassis with the Licensing Server, on page 114: Generate a license token for the chassis.
3	Chassis Manager	Chassis Manager: Register the Chassis with the Licensing Server, on page 114: Register the chassis with the Smart Licensing server.
4	Chassis Manager	Chassis Manager: Add an ASA Logical Device, on page 119.
5	ASDM	Log Into the ASDM, on page 122.
6	ASDM	Configure License Entitlements on the ASA, on page 123.
7	ASDM	Configure the ASA, on page 124.

Chassis Manager: Register the Chassis with the Licensing Server

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

For the ASA on the Firepower 4100, Smart Software Licensing configuration is split between FXOS on the chassis and the ASA.

- Firepower 4100—Configure all Smart Software Licensing infrastructure in FXOS, including parameters for communicating with the License Authority. The Firepower 4100 itself does not require any licenses to operate.

- ASA—Configure all license entitlements in the ASA.

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

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

- Strong Encryption (3DES/AES)—If your Smart Account is not authorized for strong encryption, but Cisco has determined that you are allowed to use strong encryption, you can manually add a stong encryption license to your account.

- Cisco Secure Client—Secure Client Advantage, Secure Client Premier, or Secure Client VPN Only.

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.

Strong encryption is required for ASDM access.

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).

- If you have not already done so, Configure NTP, on page 17.

- If you did not configure DNS during the initial setup, add a DNS server on the **Platform Settings** > **DNS** page.

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 24: License Search

Find Products and Solutions

L-FPR2K-ASASC-10=

Search by Product Family | Search for Solutions
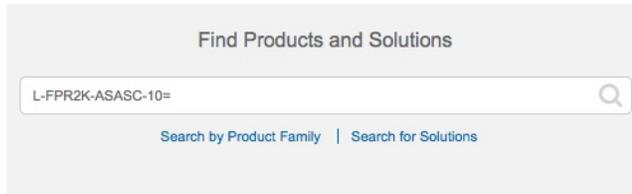
- Essentials license—L-FPR4100-ASA=. The Essentials license is free, but you still need to add it to your Smart Software Licensing account.

- 10 context license—L-FPR4K-ASASC-10=. Context licenses are additive; buy multiple licenses to meet your needs.

- 230 context license—L-FPR4K-ASASC-230=. Context licenses are additive; buy multiple licenses to meet your needs.

- 250 context license—L-FPR4K-ASASC-250=. Context licenses are additive; buy multiple licenses to meet your needs.

- Carrier (Diameter, GTP/GPRS, M3UA, SCTP)—L-FPR4K-ASA-CAR=

- Strong Encryption (3DES/AES) license—L-FPR4K-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**.

Cisco Software Central > Smart Software Licensing

Smart Software Licensing

Alerts | **Inventory** | License Conversion | Reports | Email Notification | Satellites | Activity

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

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

- **Description**

- **Expire After**—Cisco recommends 30 days.

- **Allow export-controlled functionaility on the products registered with this token**—Enables the export-compliance flag.

The token is added to your inventory.

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

Figure 25: View Token

Figure 26: Copy Token

Step 3 In the chassis manager, choose **System** > **Licensing** > **Smart License**.

Step 4 Enter the registration token in the **Enter Product Instance Registration Token** field.

Step 5 Click **Register**.

The Firepower 4100 registers with the License Authority. Successful registration can take several minutes. Refresh this page to see the status.

Figure 27: Registration in Progress

Figure 28: Registration Successful
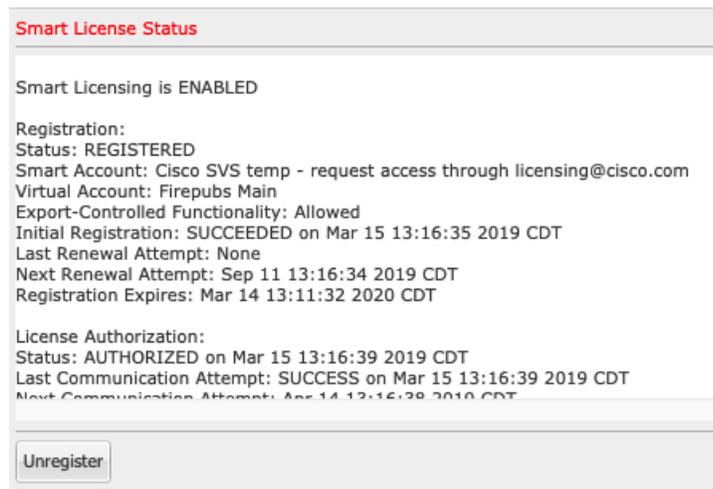
Chassis Manager: Add an ASA Logical Device

You can deploy an ASA from the Firepower 4100 as a native instance.

To add a failover pair or cluster, see the ASA general operations configuration guide.

This procedure lets you configure the logical device characteristics, including the bootstrap configuration used by the application.

Before you begin

- Configure a Management interface to use with the ASA; see Configure Interfaces, on page 21. The Management interface is required. Note that this Management interface is not the same as the chassis management port that is used only for chassis management (and that appears at the top of the **Interfaces** tab as **MGMT**).

- Gather the following information:

    - Interface IDs for this device

    - Management interface IP address and network mask

    - Gateway IP address

    - New admin password/enable password

Procedure

Step 1   In the chassis manager, choose **Logical Devices**.

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

a) Provide a **Device Name**.

This name is used by the chassis supervisor to configure management settings and to assign interfaces; it is not the device name used in the application configuration.

Note   You cannot change this name after you add the logical device.

b) For the **Template**, choose **Cisco: Adaptive Security Appliance**.

c) Choose the **Image Version**.

d) Click **OK**.

You see the Provisioning - *device name* window.

Step 3   Expand the **Data Ports** area, and click each interface that you want to assign to the device.

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

Step 4   Click the device icon in the center of the screen.

A dialog box appears where you can configure initial bootstrap settings. These settings are meant for initial deployment only, or for disaster recovery. For normal operation, you can later change most values in the application CLI configuration.

Step 5 On the **General Information** page, complete the following:

Cisco: Adaptive Security Appliance - Bootstrap Configuration

General Information Settings

Interface Information

Management Interface:	Ethernet1/8

DEFAULT

Address Type:	IPv4 only

IPv4

Management IP:	10.83.58.239
Network Mask:	255.255.252.0
Network Gateway:	10.83.56.1

a) Choose the **Management Interface**.

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

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

c) Configure the **Management IP** address.

Set a unique IP address for this interface.

d) Enter a **Network Mask** or **Prefix Length**.

e) Enter a **Network Gateway** address.

Step 6 Click **Settings**.

Cisco: Adaptive Security Appliance - Bootstrap Configuration

General Information **Settings**

Firewall Mode:	Transparent
Password:	••••••••
Confirm Password:	••••••••

a) Choose the **Firewall Mode**: **Routed** or **Transparent**.

In routed mode, the ASA is considered to be a router hop in the network. Each interface that you want to route between is on a different subnet. A transparent firewall, on the other hand, is a Layer 2 firewall that acts like a "bump in the wire," or a "stealth firewall," and is not seen as a router hop to connected devices.

The firewall mode is only set at initial deployment. If you re-apply the bootstrap settings, this setting is not used.

b) Enter and confirm a **Password** for the admin user and for the enable password.

The preconfigured ASA admin user/password and enable password are useful for password recovery; if you have FXOS access, then you can reset the admin user password/enable password if you forget it.

Step 7 Click **OK** to close the configuration dialog box.

Step 8 Click **Save**.

The chassis deploys the logical device by downloading the specified software version and pushing the bootstrap configuration and management interface settings to the application instance. Check the **Logical Devices** page for the status of the new logical device. When the logical device shows its **Status** as **online**, you can start configuring the security policy in the application.
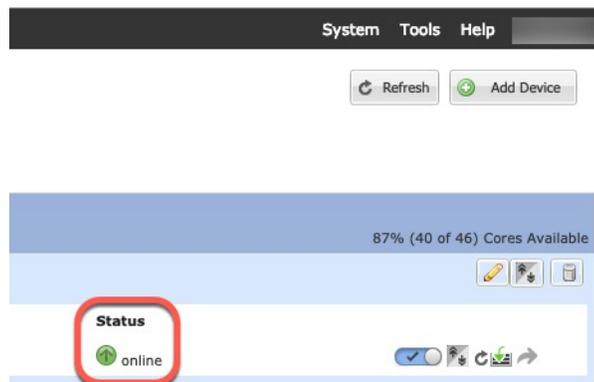
Log Into the ASDM

Launch the ASDM so you can configure the ASA.

Before you begin

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

- Make sure the ASA logical device **Status** is **online** on the chassis manager **Logical Devices** page.

Procedure

Step 1 Enter the following URL in your browser.

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

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 one of these available options: **Install ASDM Launcher** or **Run ASDM**.

Step 3   Follow the onscreen instructions to launch ASDM according to the option you chose.

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

Step 4   Leave the username empty, enter the enable password that you set when you deployed the ASA, and click **OK**.

The main ASDM window appears.

Configure License Entitlements on the ASA

Assign licenses to the ASA. You must at a minimum assign the Standard license.

Before you begin

- Chassis Manager: Register the Chassis with the Licensing Server, on page 114.

Procedure

Step 1   In ASDM, choose **Configuration** > **Device Management** > **Licensing** > **Smart Licensing**.

Step 2   Set the following parameters:

a) Check **Enable Smart license configuration**.

b) From the **Feature Tier** drop-down list, choose **Essentials**.

Only the Essentials tier is available.

c) (Optional) For the **Context** license, enter the number of contexts.

You can use 10 contexts without a license. The maximum number of contexts is 250. For example, to use the maximum, enter 240 for the number of contexts; this value is added to the default of 10.

d) (Optional) Check **Carrier**.

Step 3   Click **Apply**.

If you do not have the appropriate licenses in your account, you cannot apply your license changes.

Step 4   Click the **Save** icon in the toolbar.

Step 5   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.
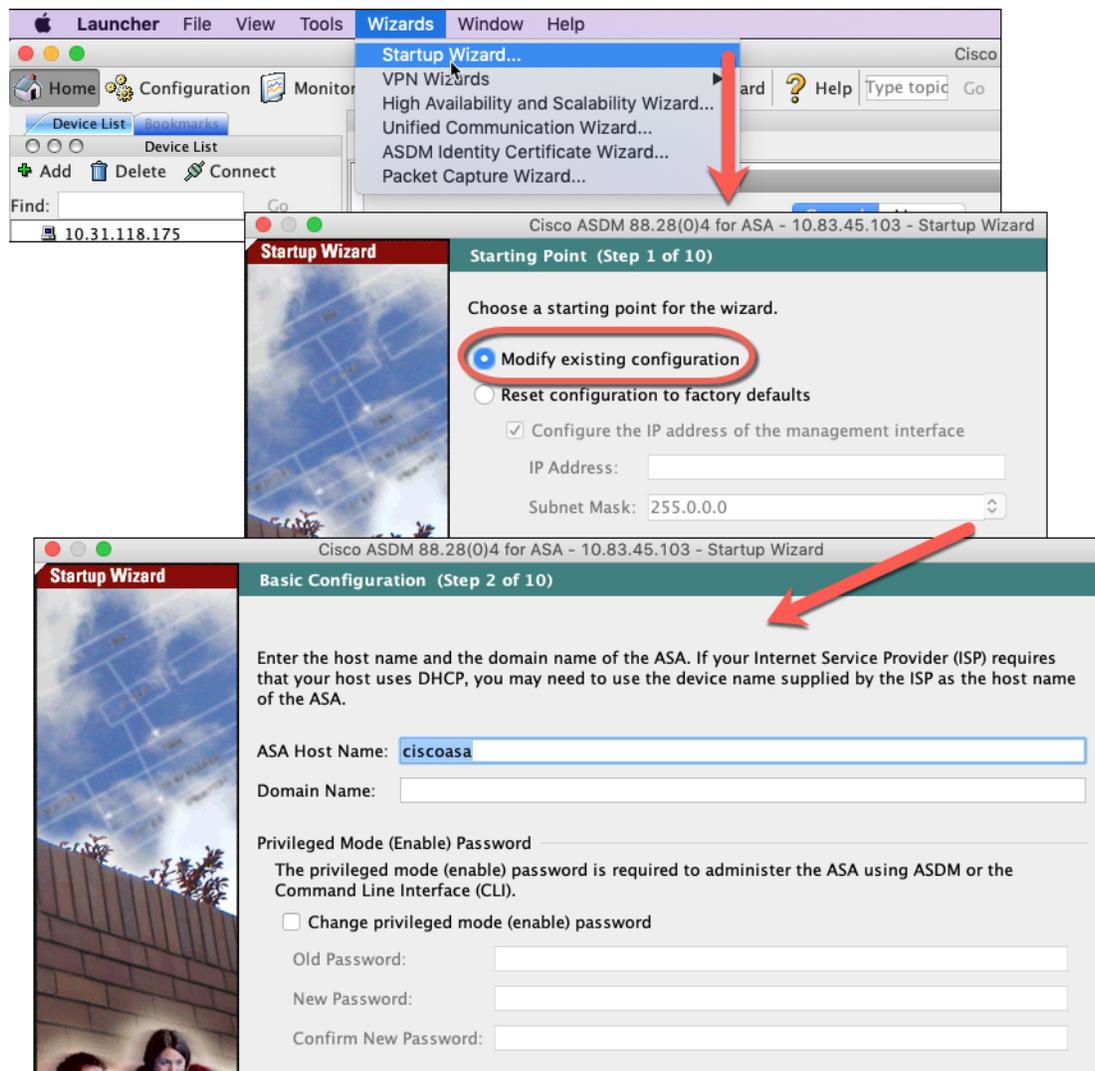
Step 2 The **Startup Wizard** walks you through configuring:

- 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 CLI

You can use the ASA CLI to troubleshoot or configure the ASA instead of using ASDM. You can access the CLI by connecting from the FXOS CLI. You can later configure SSH access to the ASA on any interface. See the ASA general operations configuration guide for more information.

Procedure

Step 1   From the FXOS CLI, connect to the module CLI using a console connection or a Telnet connection.

connect module 1 {**console** | **telnet**}

The benefits of using a Telnet connection is that you can have multiple sessions to the module at the same time, and the connection speed is faster.

Example:

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

Step 2   Connect to the ASA console.

connect asa

Example:

```
Firepower-module1> connect asa
Connecting to asa(asa1) console... hit Ctrl + A + D  to return to bootCLI
[...]
asa>
```

Step 3   Exit the application console to the FXOS module CLI by entering **Ctrl-a, d**.

Step 4   Return to the supervisor level of the FXOS CLI.

Exit the console:

a)   Enter **~**

You exit to the Telnet application.

b)   To exit the Telnet application, enter:

telnet>**quit**

Exit the Telnet session:

a) Enter **Ctrl-], .**

Example

The following example shows how to connect to an ASA and then exit back to the supervisor level of the FXOS CLI.

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>connect asa
asa> ~
telnet> quit
Connection closed.
Firepower#
```

What's Next?

• To continue configuring your ASA, see the documents available for your software version at Navigating the Cisco ASA Series Documentation.

History for the ASA

Feature	Version	Details
ASA for the Firepower 4115, 4125, and 4145	9.12(1)	We introduced the Firepower 4115, 4125, and 4145. **Note** Requires FXOS 2.6.1.
Support for ASA and threat defense on separate modules of the same Firepower 9300	9.12(1)	You can now deploy the ASA and the threat defense logical devices on the same Firepower 9300. **Note** Requires FXOS 2.6.1.
Support for transparent mode deployment for an ASA logical device	9.10(1)	You can now specify transparent or routed mode when you deploy the ASA. **Note** Requires FXOS 2.4.1. New/modified chassis manager screens: **Logical Devices** > **Add Device** > **Settings > Firewall Mode** drop-down list

Feature	Version	Details
Smart Agent Upgrade to v1.6	9.6(2)	The smart agent was upgraded from Version 1.1 to Version 1.6. This upgrade supports permanent license reservation and also supports setting the Strong Encryption (3DES/AES) license entitlement according to the permission set in your license account.
New Carrier license	9.5(2)	The new Carrier license replaces the existing GTP/GPRS license, and also includes support for SCTP and Diameter inspection. For the ASA on the Firepower 9300, the **feature mobile-sp** command will automatically migrate to the **feature carrier** command. We modified the following screen: **Configuration** > **Device Management** > **Licensing** > **Smart License**