Install FTD on 4100 Firepower Appliances

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

Configure

- Network Diagram
- Task 1. FTD Software Download
- Task 2. Verify FXOS-FTD Compatibility
  - Task Requirement
  - Solution
  - Verify the FXOS Image
- Task 3. Upload FTD Image into Firepower Appliance
  - Task Requirement
  - Solution
- Task 4. Configure FTD Management and Data Interfaces
  - Task Requirement
  - Solution
- Task 5. Create and Configure New Logical Device
  - Task Requirement
  - Solution
- Task 6. Register FTD into the Cisco Secure Firewall Management Center (FMC)
  - Task Requirement
  - Solution

Related Information

Introduction

This document demonstrates how to install and register Cisco Secure Firewall Threat Defense (FTD) software on Firepower 4100 security appliances.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Firepower 4125 Security Appliance, which runs FXOS 2.16(0.128) and FTD 7.6.0

- Cisco Secure Firewall Management Center, which runs 7.6.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

FTD is a unified software image that can be installed on these platforms:

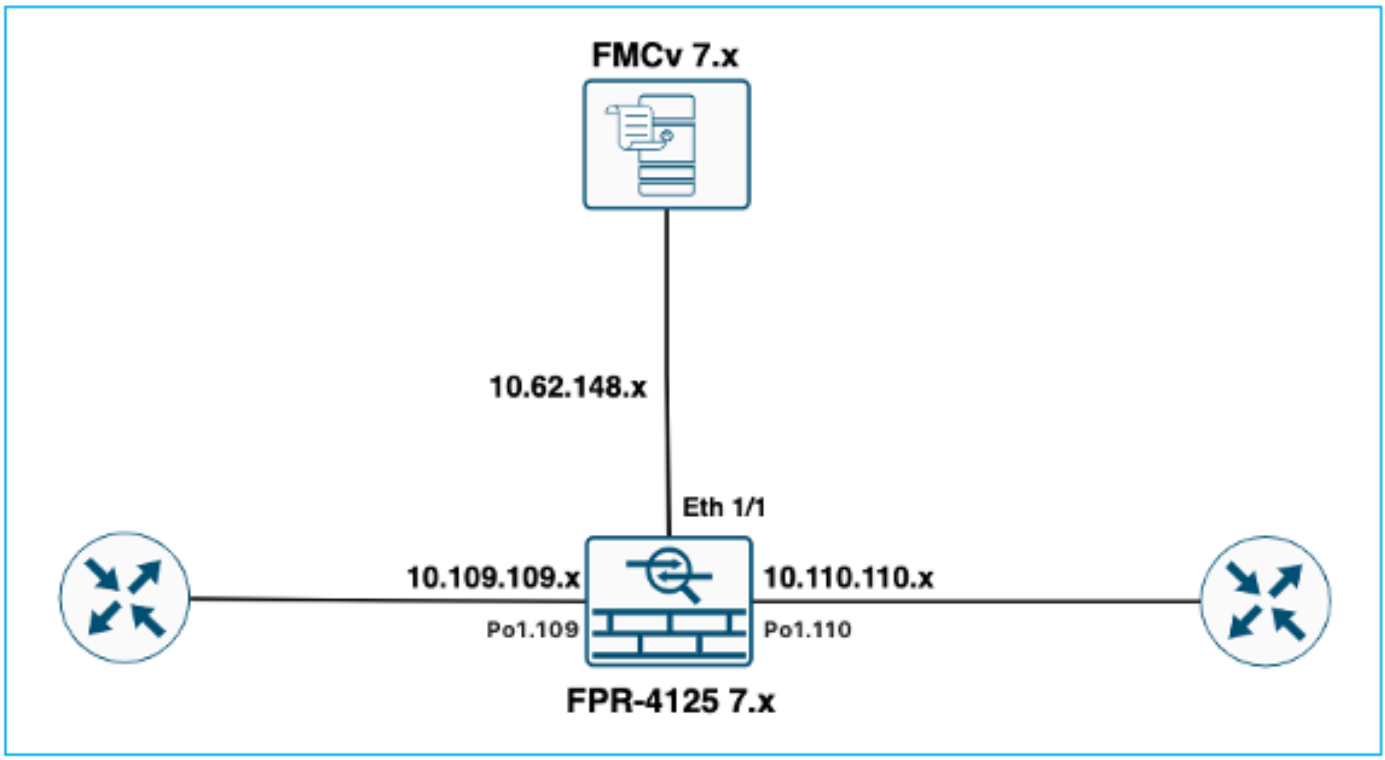
- Cisco Secure Firewall Devices (FPR1xxx, FPR12xx, FPR21xx, FPR31xx, FPR42xx)
- Firepower Security Appliances (FPR41xx and FPR9300)
- 3000 Series Industrial Security Appliances (ISA)
- Integrated Service Router (ISR) module

- Private Cloud:
  - VMware (ESXi)
  - Kernel-based Virtual Machine (KVM)
  - OpenStack
  - Cisco HyperFlex

- Public Cloud:
  - Amazon Web Services (AWS)
  - Microsoft Azure
  - Google Cloud Platform
  - Oracle Cloud Infrastructure
  - Nutanix Cloud
  - Equinix

Configure

Network Diagram



Task 1. FTD Software Download

Navigate to **Security > Firewalls > Next-Generation Firewalls (NGFW) > Firepower 4100 Series > Firepower 4125 Security Appliance** and choose **Firepower Threat Defense Software** as shown in this image:



Task 2. Verify FXOS-FTD Compatibility

Task Requirement

Verify that the FXOS version that runs on the chassis is compatible with the FTD version you want to install in the security module.

Solution

Step 1. Check the FXOS-FTD compatibility.

Before you install an FTD image into the module/blade, ensure the Firepower chassis runs a compatible

FXOS software. In the FXOS Compatibility Guide, check the Logical Device Compatibility table. The minimum required FXOS version to run FTD 7.6.0 is 2.16, as shown in Table 1:

Table 1. Firepower 4100/9300 Compatibility with ASA and Threat Defense

FXOS Version	Model	ASA Version	Threat Defense Version
2.17	Firepower 4112	**9.23 (recommended)** 9.22 9.20 9.19 9.18	**7.7** (recommended) 7.6 7.4 7.3 7.2
	Firepower 4145 Firepower 4125 Firepower 4115	**9.23 (recommended)** 9.22 9.20 9.19 9.18	**7.7** (recommended) 7.6 7.4 7.3 7.2
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
2.16	Firepower 4112	**9.22** (recommended) 9.20 9.19 9.18 9.17	**7.6** (recommended) 7.4 7.3 7.2 7.1
	Firepower 4145 Firepower 4125 Firepower 4115	**9.22** (recommended) 9.20 9.19 9.18 9.17	**7.6** (recommended) 7.4 7.3 7.2 7.1
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		

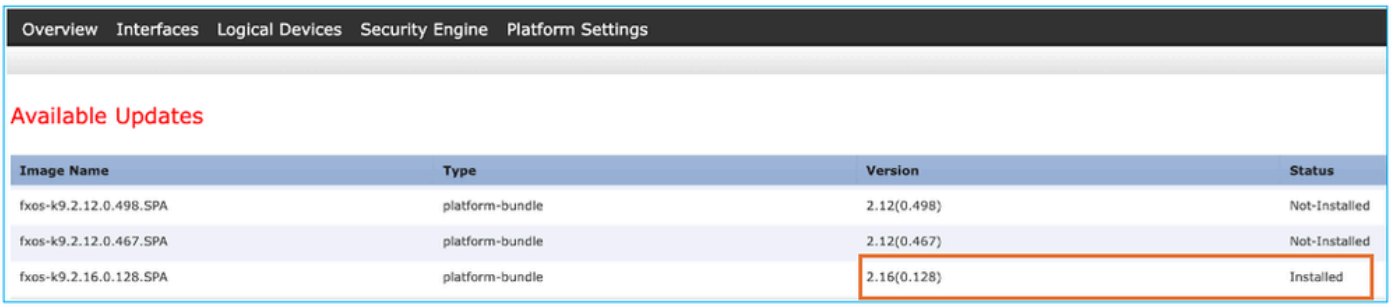
If the FXOS image is not compatible with the target FTD image, upgrade the FXOS software first.

Verify the FXOS Image

Method 1. From Firepower Chassis Manager (FCM) UI **Overview page**, as shown in this image:



Method 2. Navigate to FCM **System > Update** page, as shown in this image:



Method 3. From FXOS CLI:

```
<#root>
FPR4125#
```

```
show fabric-interconnect firmware

Fabric Interconnect A:
    Running-Kern-Vers: 5.0(3)N2(4.160.555)
    Running-Sys-Vers: 5.0(3)N2(4.160.555)

Package-Vers: 2.16(0.128)

    Startup-Kern-Vers: 5.0(3)N2(4.160.555)
    Startup-Sys-Vers: 5.0(3)N2(4.160.555)
    Act-Kern-Status: Ready
    Act-Sys-Status: Ready
    Bootloader-Vers:
```

Task 3. Upload FTD Image into Firepower Appliance

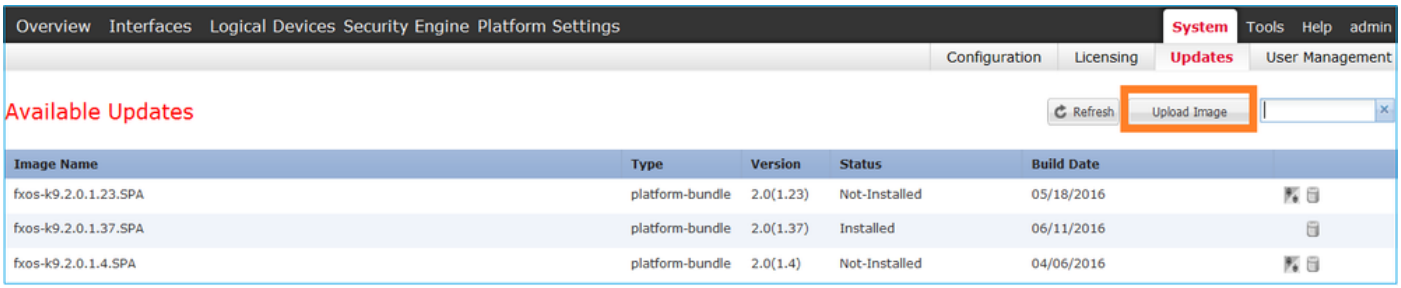
Task Requirement

Upload the FTD image into FPR4100 chassis.

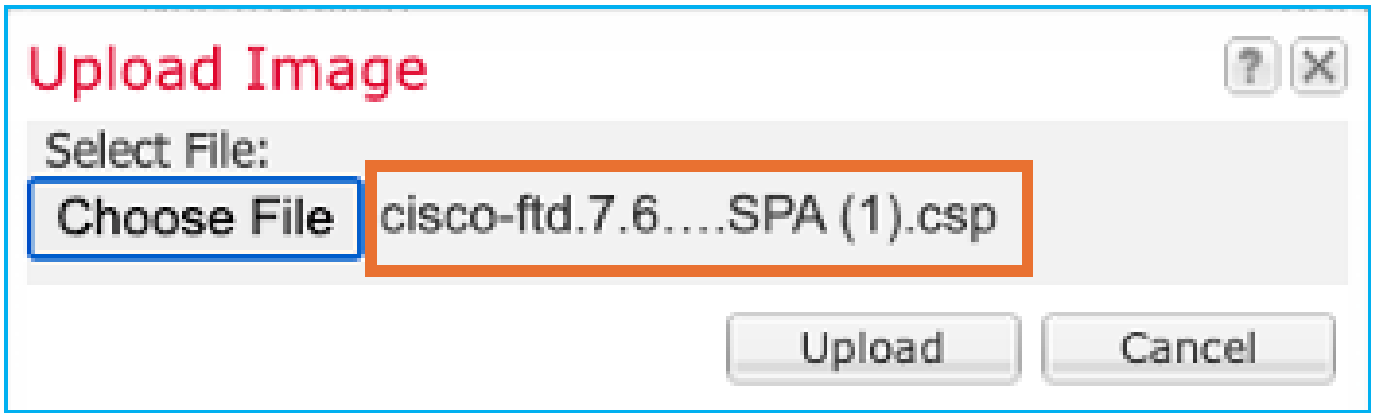
Solution

Method 1. Upload the FTD image from the FCM UI.

Log into the FPR4100 Chassis Manager and navigate to **System > Updates** tab. Choose **Upload Image** to upload the file, as shown in this image:

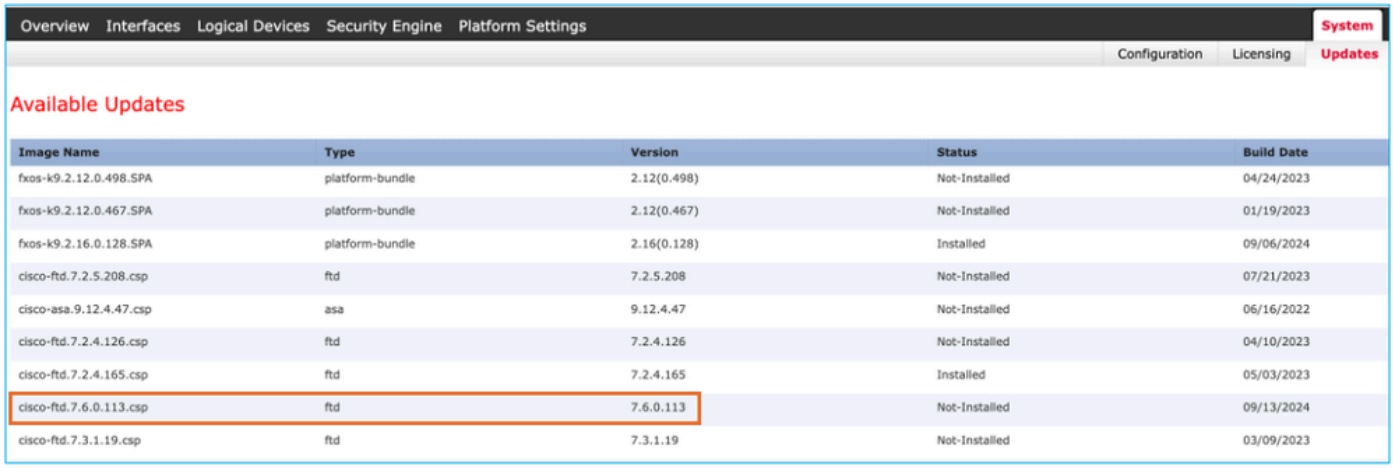


Browse to choose the FTD image file and click **Upload**, as shown in ths image:



Accept the End User License Agreement (EULA).

Verification is as shown in this image:



Method 2. Upload the FTD image from the FXOS CLI.

You can upload the FTD image from an FTP, HTTP, HTTPS, Secure Copy (SCP), Secure FTP (SFTP), TFTP or via USB. (In this example, FTP is utilized):

<#root>

FPR4100#

scope ssa

FPR4100 /ssa #

scope app-software

FPR4100 /ssa/app-software #

download image ?

```
  ftp: Location of the image file
  http: Location of the image file
  https: Location of the image file
  scp: Location of the image file
  sftp: Location of the image file
  tftp: Location of the image file
  usbA: Location of the image file
```

Before the image transfer starts, verify connectivity between the chassis management interface and the remote server:

<#root>

FPR4100#

connect local-mgmt

FPR4100(local-mgmt)#

ping 10.229.24.22

```
PING 10.229.24.22 (10.229.24.22) from 10.62.148.88 eth0: 56(84) bytes of data.
64 bytes from 10.229.24.22: icmp_seq=1 ttl=124 time=0.385 ms
64 bytes from 10.229.24.22: icmp_seq=2 ttl=124 time=0.577 ms
64 bytes from 10.229.24.22: icmp_seq=3 ttl=124 time=0.347 ms
```

To download the FTD image, navigate to this scope and use the **download image** command:

```
<#root>

FPR4100#

scope ssa

FPR4100 /ssa #

scope app-software

FPR4100 /ssa/app-software #

download image ftp://ftp_username@10.229.24.22/cisco-ftd.7.6.0.113.SPA.csp

Password:
```

To monitor the image upload progress:

```
<#root>

FPR4100 /ssa/app-software #

show download-task detail

Downloads for Application Software:

 File Name: cisco-ftd.7.6.0.113.SPA.csp

    Protocol: Ftp
    Server: 10.229.24.22
    Port: 0
    Userid: ftp
    Path:
    Downloaded Image Size (KB): 95040
    Time stamp: 2016-12-11T20:27:47.856

State: Downloading

Transfer Rate (KB/s): 47520.000000

    Current Task: downloading image cisco-ftd.7.6.0.113.SPA.csp from 10.229.24.22(FSM-STAGE:sam:dme:App
```

Use this command to verify the successful download:

<#root>

FPR4100 /ssa/app-software #

show download-task

Downloads for Application Software:

File Name	Protocol	Server	Port	Userid	State
cisco-ftd.7.6.0.113.SPA.csp	Ftp	10.229.24.22	0	ftp	

Downloaded

For additional details:

<#root>

KSEC-FPR4100 /ssa/app-software #

show download-task fsm status expand

File Name: cisco-ftd.7.6.0.113.SPA.csp

FSM Status:

Affected Object: sys/app-catalogue/dnld-cisco-ftd.7.6.0.113.SPA.csp/fsm

Current FSM: Download

Status: Success

Completion Time: 2016-12-11T20:28:12.889
Progress (%): 100

FSM Stage:

Order	Stage Name	Status	Try
1	DownloadLocal		

Success

1

2	DownloadUnpackLocal		

Success

1

File Name: Cisco_FTD_SSP_Upgrade-7.6.0-113.sh

The image is shown in the chassis repository:

<#root>

```
KSEC-FPR4100 /ssa/app-software # exit
KSEC-FPR4100 /ssa #
```

show app

```
Application:
    Name       Version    Description Author     Deploy Type CSP Type    Is Default App
    ---------- ---------- ----------- ---------- ----------- ----------- --------------
    asa        9.6.2.3    N/A         cisco      Native      Application No

ftd        7.6.0.113

  N/A          cisco      Native      Application No
```

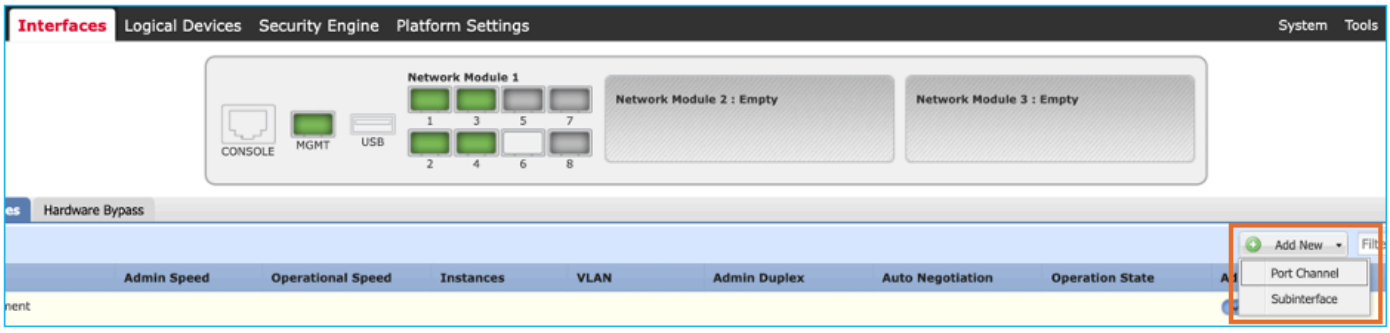
Task 4. Configure FTD Management and Data Interfaces

Task Requirement

Configure and enable Management and Data interfaces for FTD on the Firepower appliance.

Solution

To create a new interface, log in to the FCM and navigate to the **Interfaces** tab. The current interfaces are visible. To create a new Port Channel interface, choose the **Add New > Port Channel** button, as shown in the image:



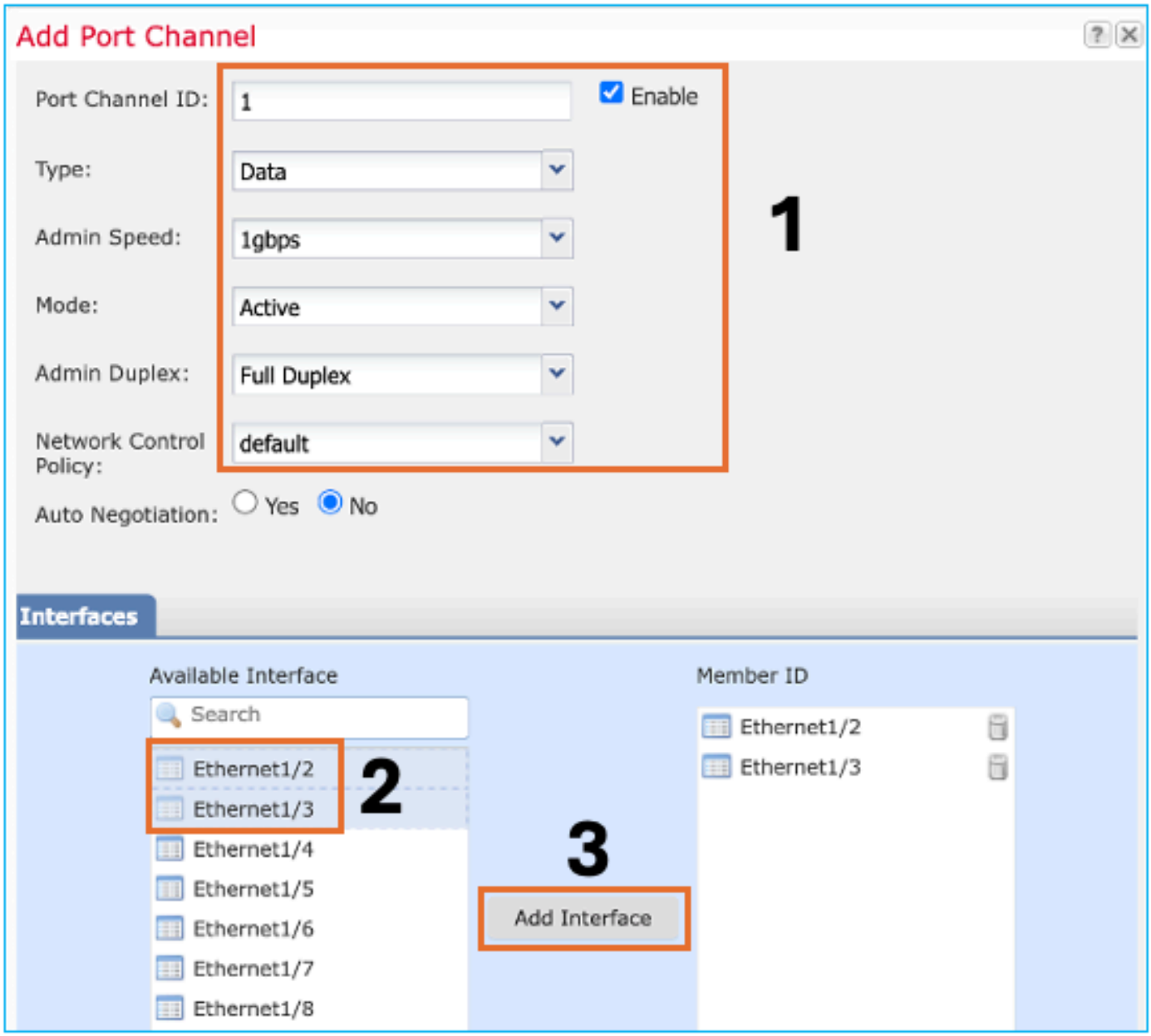
Step 1. Create a Port Channel Data Interface.

Create a new Port Channel Interface, as shown in this image:

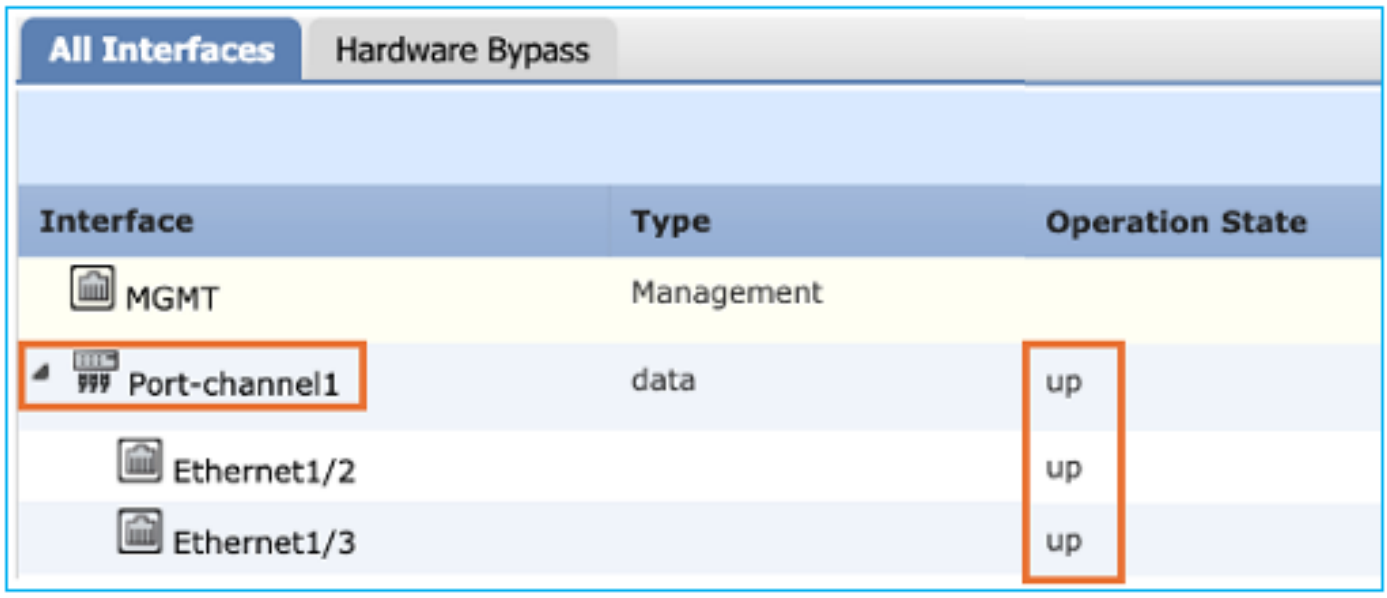
Port Channel ID	1
Type	Data
Enable	Yes
Member ID	Ethernet1/2, Ethernet 1/3

For the Port Channel ID, a value from 1 to 47.

Note: PortChannel 48 is used for clusters.

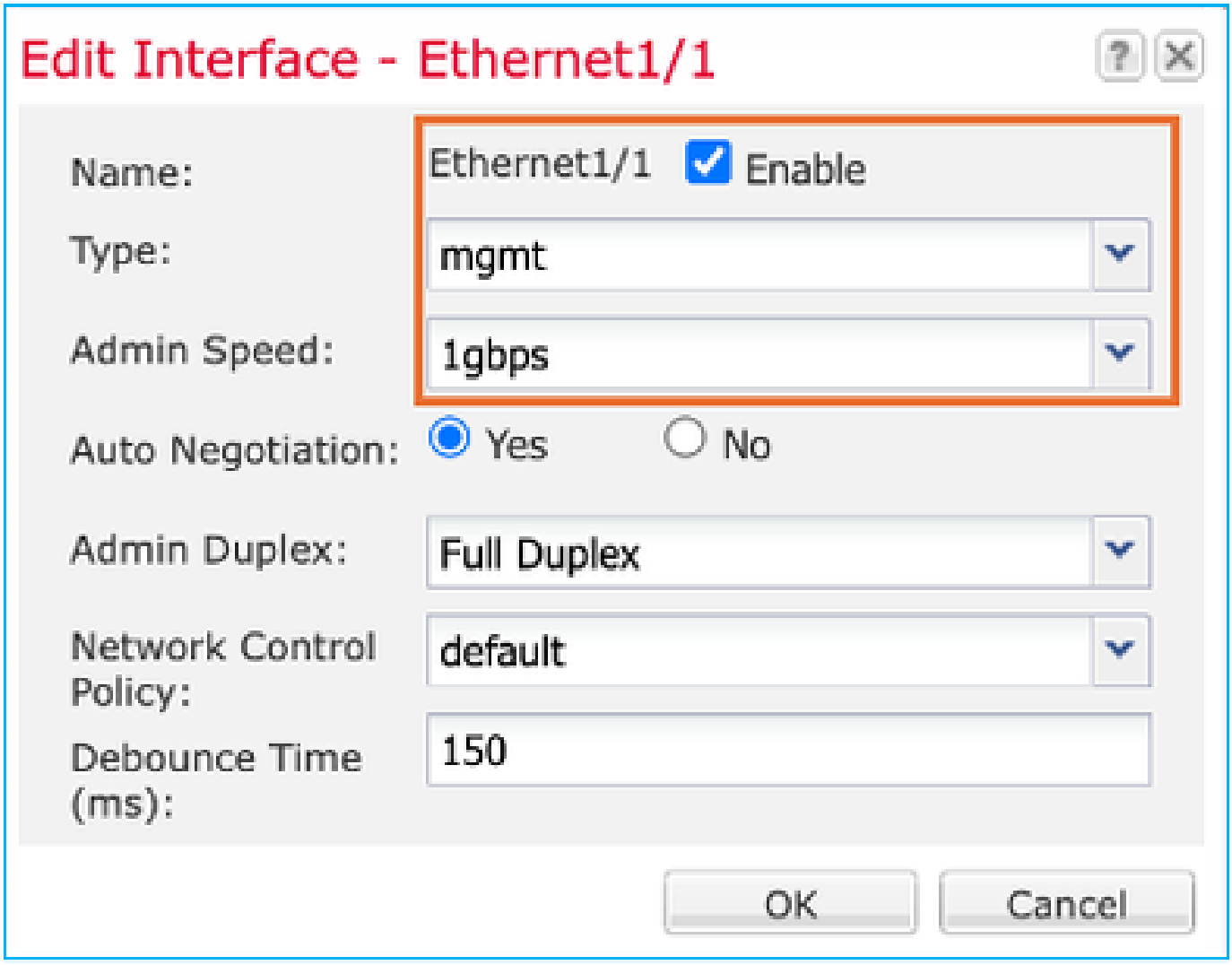


Verification is as shown in this image:



Step 2. Create a Management Interface.

On the **Interfaces** tab, choose the interface, select **Edit**, and configure the Management interface, as shown in this image:



Task 5. Create and Configure New Logical Device

Task Requirement

Create an FTD as a Standalone Logical Device and deploy it.

Solution

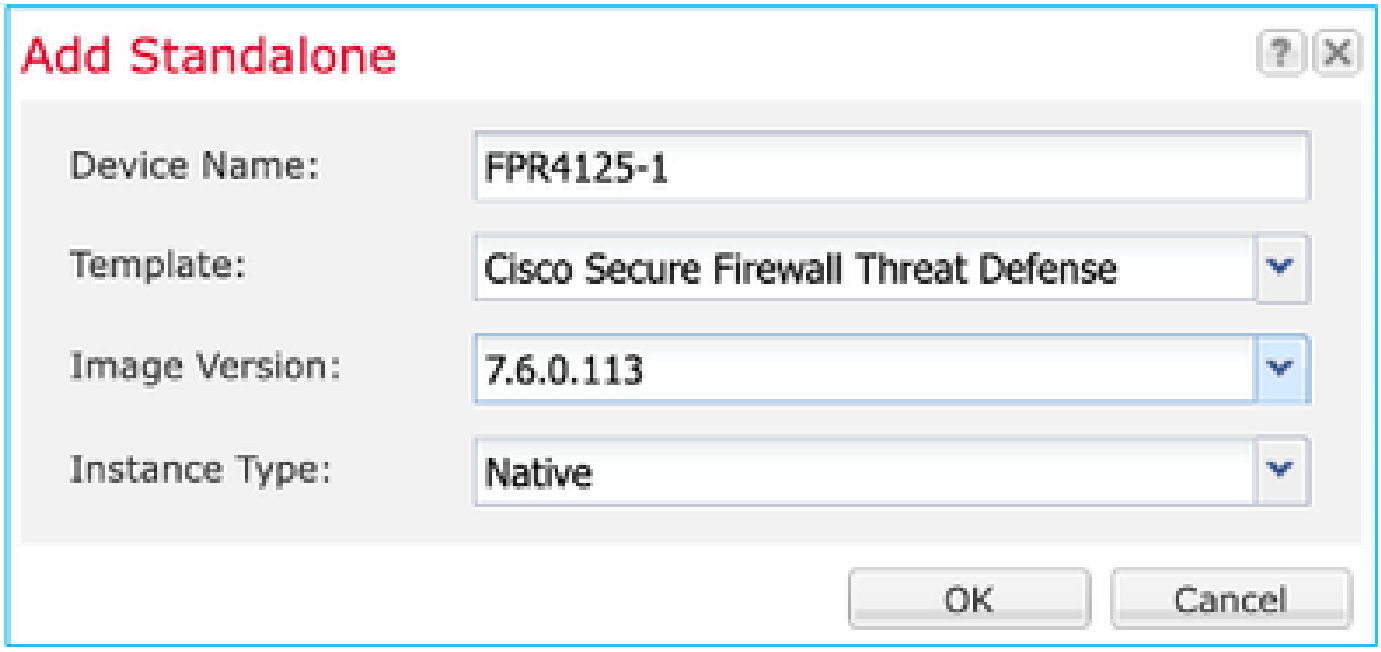
Step 1. Add a Logical Device.

Navigate to the **Logical Devices** tab and choose the **Add Device** button to create a new Logical Device, as shown in this image:



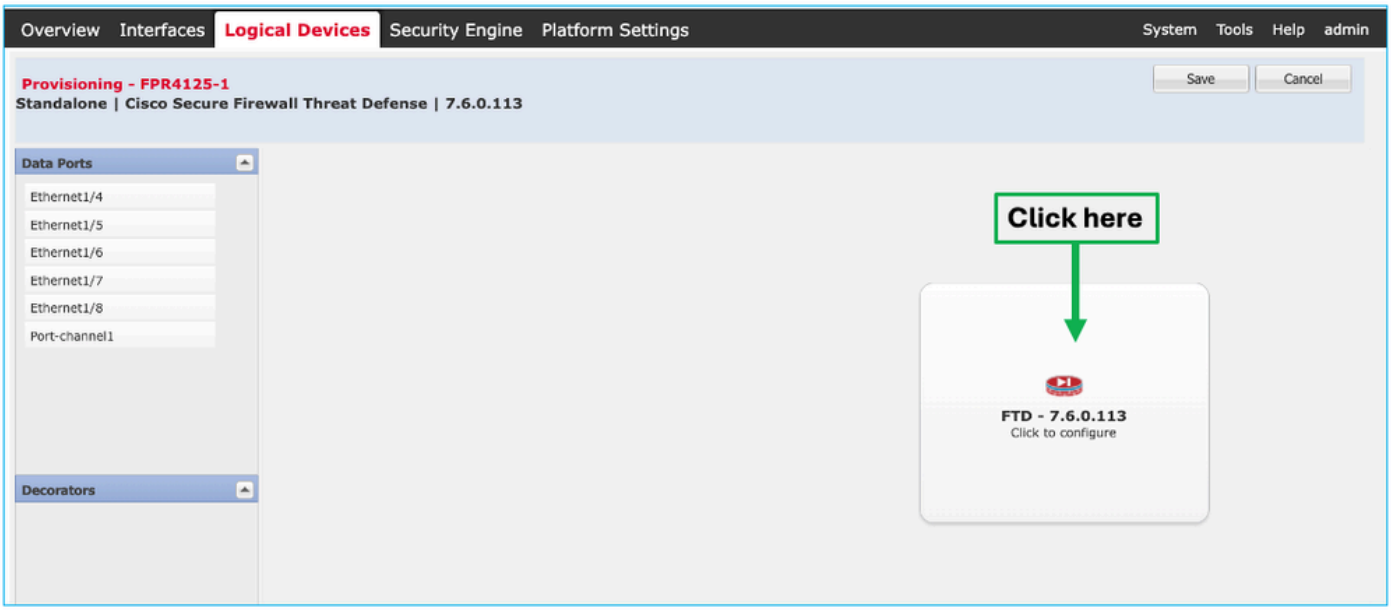
Configure an FTD device with the settings shown in this image:

Device Name	FPR4125-1
Template	Cisco Secure Firewall Threat Defense
Image Version	7.6.0.113



Step 2. Bootstrap the Logical Device.

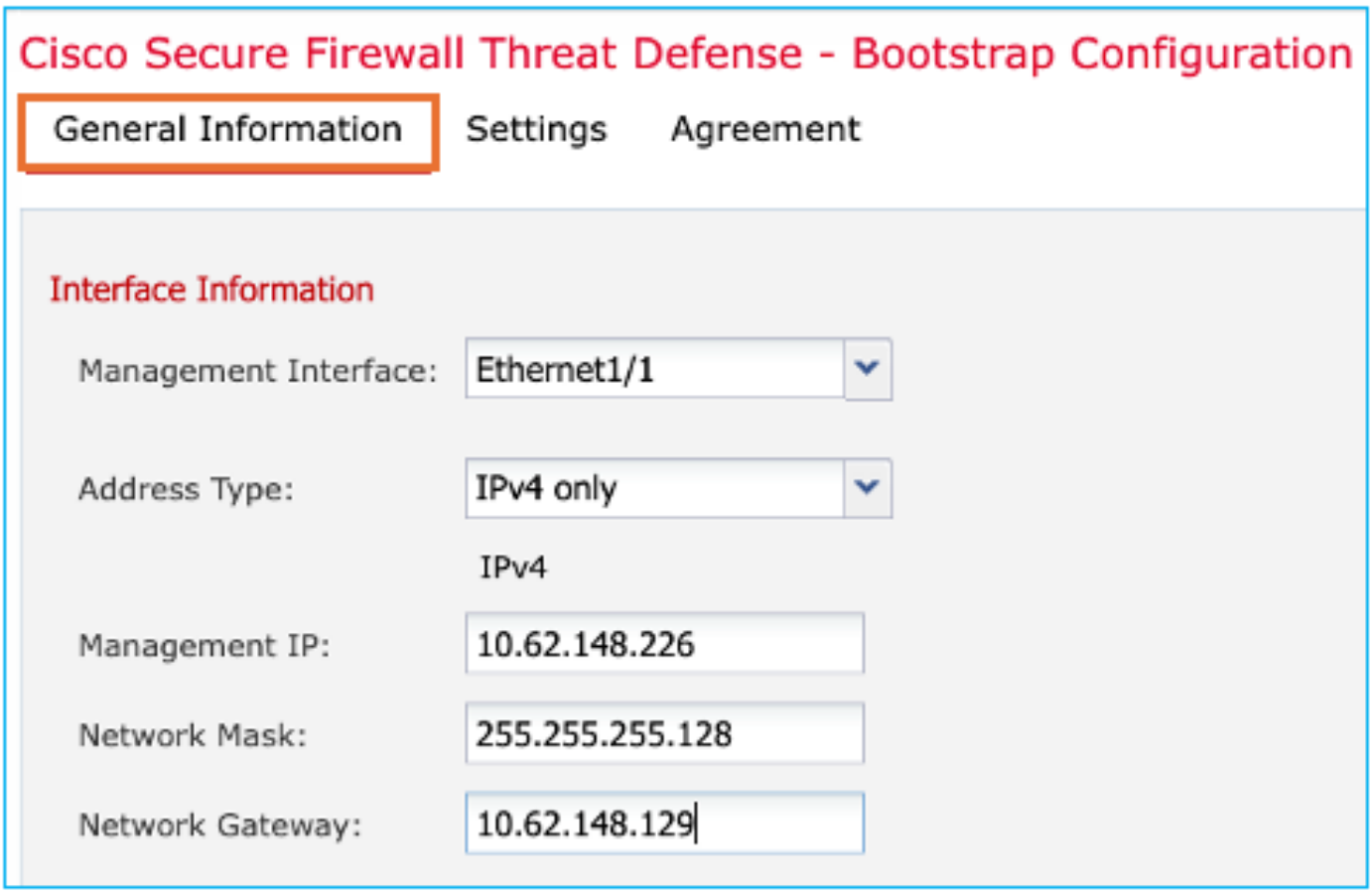
After creating the logical device, the **Provisioning – device_name** window displays. Choose the device icon to start the configuration, as shown in this image:



Configure the FTD **General Information** tab, as shown in this image:

Management Interface	Ethernet1/1
Address Type	IPv4 only
Management IP	10.62.148.226

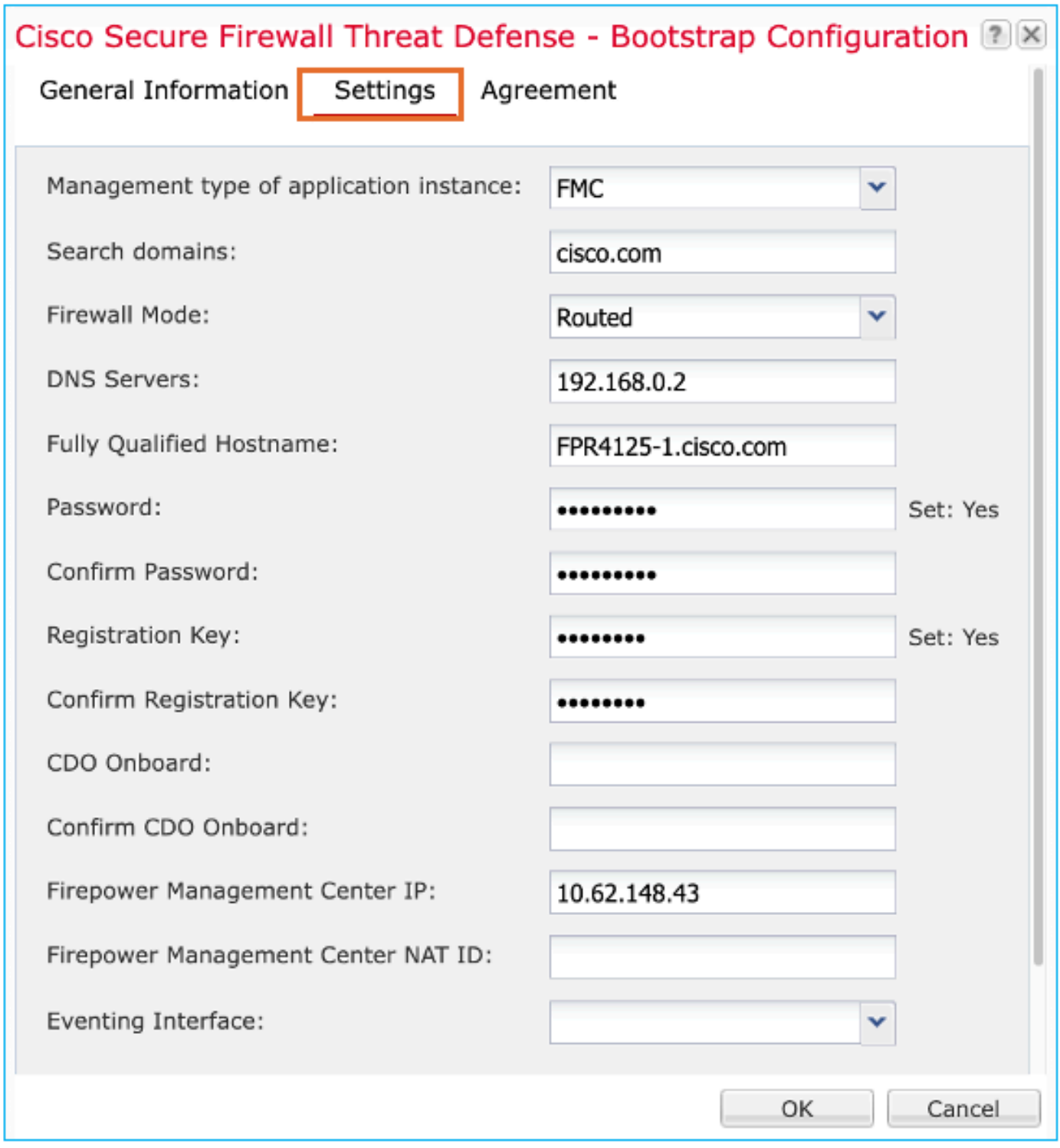
Network Mask	255.255.255.128
Network Gateway	10.62.148.129



Configure the FTD **Settings** tab, as shown in this image:

Registration Key	cisco
Password	Pa$$w0rd
Cisco Secure Firewall Management Center IP	10.62.148.43
Search Domains	cisco.com
Firewall Mode	Routed
DNS Servers	192.168.0.2
Fully Qualified Hostname	FPR4125-1.cisco.com

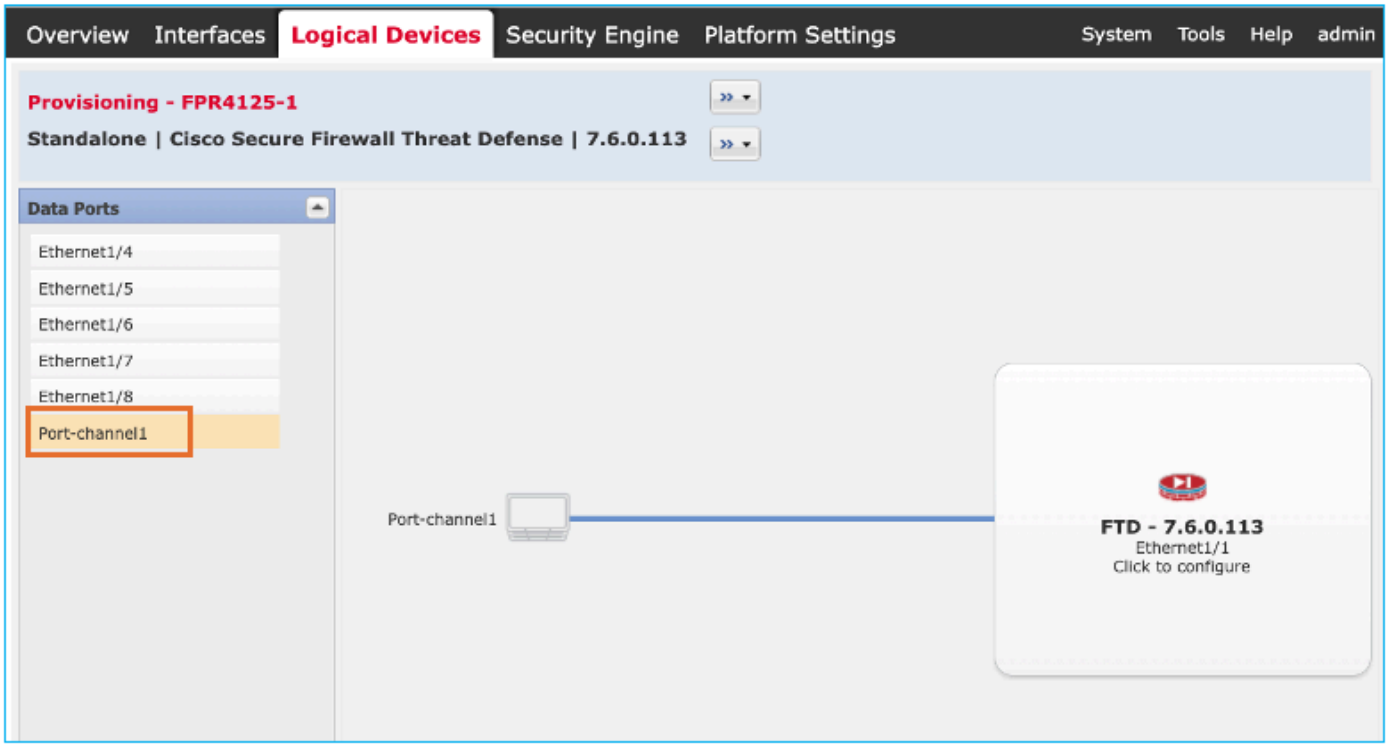
Eventing Interface	-



Ensure the **Agreement** is accepted and select **OK**.

Step 3. Assign the Data Interfaces.

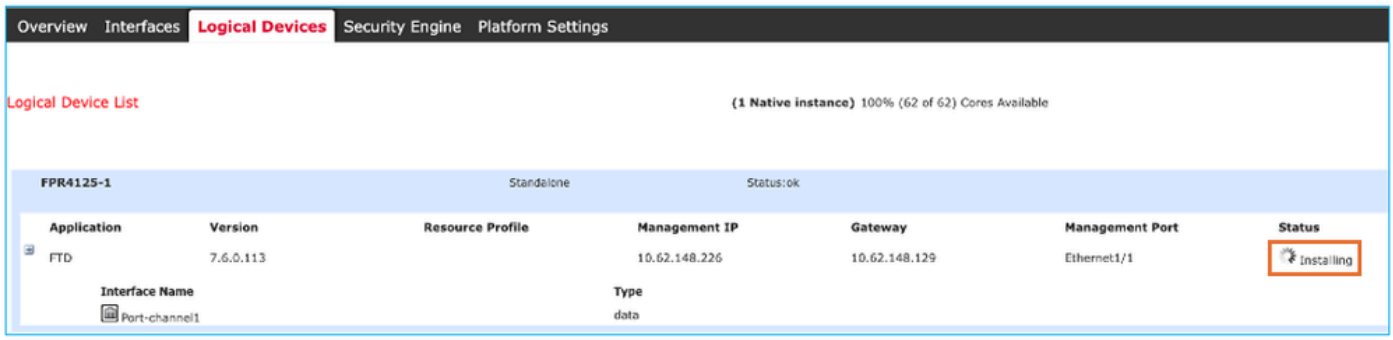
Expand the Data Ports area and choose each interface to assign to FTD. In this scenario, one interface (Port-channel1) was assigned, as shown in this image:

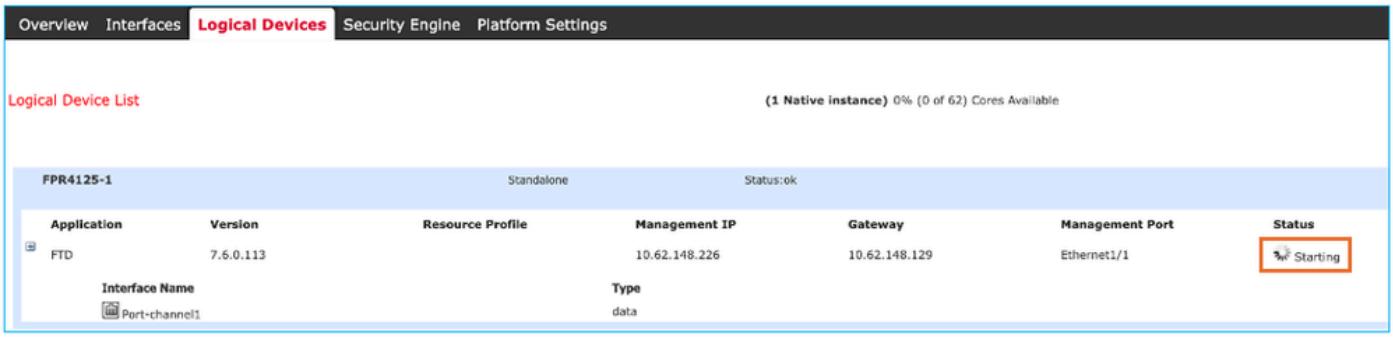


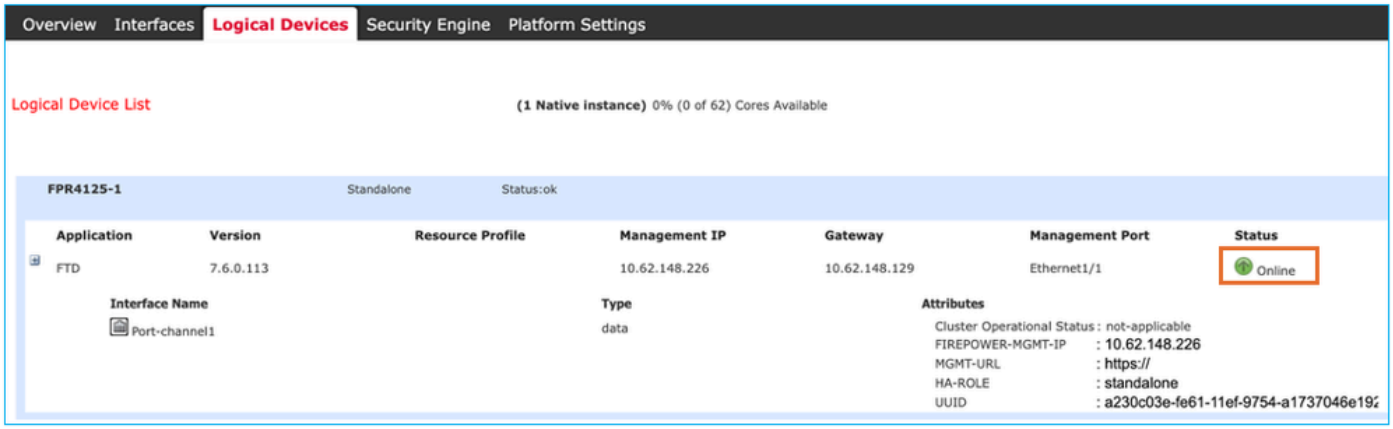
Choose **Save** to finish the configuration.

Step 4. Monitor the Installation Process.

This is how the FTD installation progresses when monitored from the FCM UI, as shown in these images:







Monitor the installation process from the Firepower CLI:

<#root>

FPR4100#

connect module 1 console

```
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

Firepower-module1>
```

show services status all

```
Services currently running:
Application Type | Identifier | Oper State | Up Since | Instance ID
---------------- | ---------- | ---------- | -------- | -----------
ftd (native)     | FPR4125-1  | RUNNING    | 00:01:56 | ftd_001_JAD22360004VWC84030
```

Task 6. Register FTD into the Cisco Secure Firewall Management Center (FMC)

Task Requirement

Register FTD into the FMC.

Solution

Step 1. Verify basic connectivity between the FTD and the FMC.

Before you register the FTD to the FMC, verify basic connectivity between the FTD and the FMC:

<#root>
Firepower-module1>

connect ftd

Connecting to ftd(FPR4125-1) console... enter exit to return to bootCLI

>

ping system 10.62.148.43

PING 10.62.148.43 (10.62.148.43) 56(84) bytes of data.
64 bytes from 10.62.148.43: icmp_seq=1 ttl=63 time=0.254 ms
64 bytes from 10.62.148.43: icmp_seq=2 ttl=63 time=0.283 ms
64 bytes from 10.62.148.43: icmp_seq=3 ttl=63 time=0.217 ms

Due to bootstrap configuration, the FTD has the manager FMC already configured:

<#root>

>

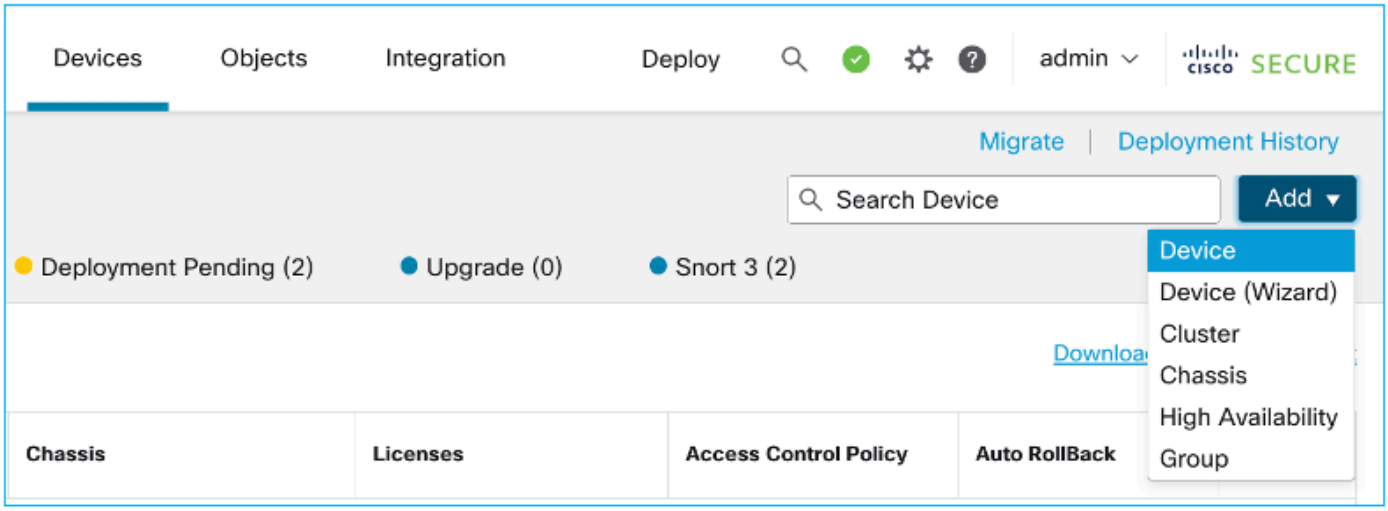
show managers

```
Type                    : Manager
Host                    : 10.62.148.43
Display name            : 10.62.148.43
Identifier              : 10.62.148.43
Registration            :
```

Pending

Step 2. Add the FTD into the FMC.

On the FMC, navigate to the **Devices> Device Management** tab and navigate to **Add... > Add Device**, as shown in this image:



Configure the FTD device settings, as shown in this image:

Add Device

CDO Managed Device

Host:†

10.62.148.226

Display Name:

FPR4125-1

Registration Key:*

••••••••

Group:

None

Access Control Policy:*

ACP_LAB_FTD

Smart Licensing

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

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

Select a recommended Tier

Carrier

Malware Defense

IPS

URL

Advanced

Unique NAT ID:†

Transfer Packets

Cancel

Register