

Install and Upgrade FTD on 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 3. Upload FTD Image into Firepower Appliance](#)

[Task 4. Configure FTD Management and Data Interfaces](#)

[Task 5. Create and Configure New Logical Device](#)

[Task 6. Register FTD into the Firepower Management Center \(FMC\)](#)

[Task 7. Upgrade FTD](#)

[Solution](#)

[Verification](#)

[Firepower 2100](#)

[FTD Installation on FP2100](#)

[FTD Upgrade on FP2100](#)

[Verify](#)

[Troubleshoot](#)

[Related Information](#)

Introduction

This document describes the installation, upgrade, and registration of Firepower Threat Defense (FTD) software on Firepower 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 4140 Security Appliance, which runs FXOS 2.0(1.37)
- Firepower Management Center, which runs 6.1.0.330

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.

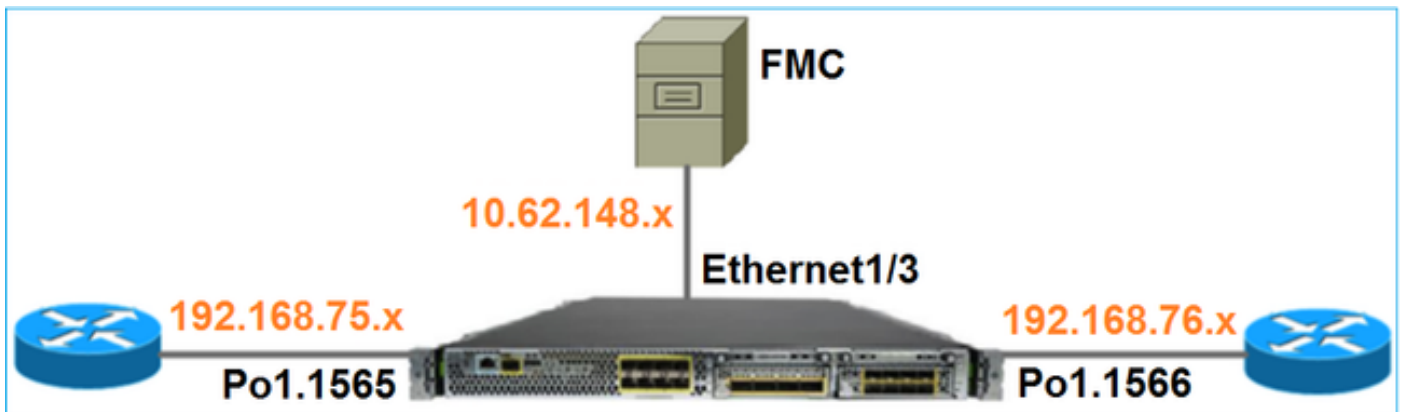
Background Information

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

- ASA5506-X, ASA5506W-X, ASA5506H-X, ASA5508-X, ASA5516-X
- ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X
- Firepower devices (FPR2100, FPR4100, FPR9300)
- VMware (ESXi)
- Amazon Web Services (AWS)
- Kernel-based Virtual Machine (KVM)
- Integrated Service Router (ISR) module

Configure

Network Diagram



Task 1. FTD Software Download

Navigate to **Next-Generation Firewalls (NGFW) > FirePOWER 4100 Series > FirePOWER 4140 Security Appliance** and select **Firepower Threat Defense Software** as shown in the image.

Download Software

 Download Cart (0 items)

[Downloads Home](#) > [Products](#) > [Security](#) > [Firewalls](#) > [Next-Generation Firewalls \(NGFW\)](#) > [Firepower 4100 Series](#) > [Firepower 4140 Security Appliance](#)

Select a Software Type:

[Adaptive Security Appliance \(ASA\) Device Manager](#)
[Adaptive Security Appliance \(ASA\) Software](#)
[Adaptive Security Appliance REST API Plugin](#)
[Firepower Extensible Operating System](#)
[Firepower Threat Defense Software](#)

Task 2. Verify FXOS-FTD Compatibility

Task requirement

Verify 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 6.1.x is 1.1(4.95), as shown in Table 2:

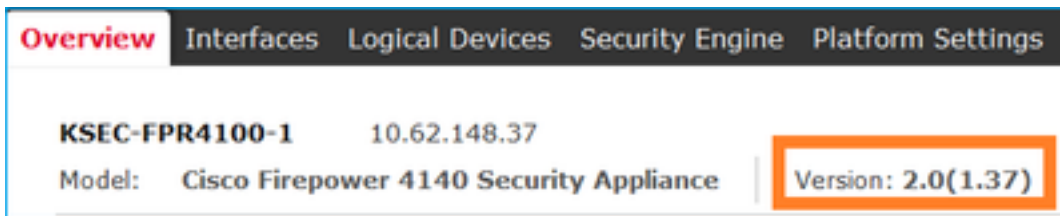
Table 2 Logical Device Compatibility

FXOS	ASA OS	Firepower Threat Defense
1.1(1.147)	9.4(1)	not supported
1.1(1.160)	9.4(1)	
...	...	
1.1(4.95)	9.6(1)	6.0.1.x
	9.6(2)	6.1

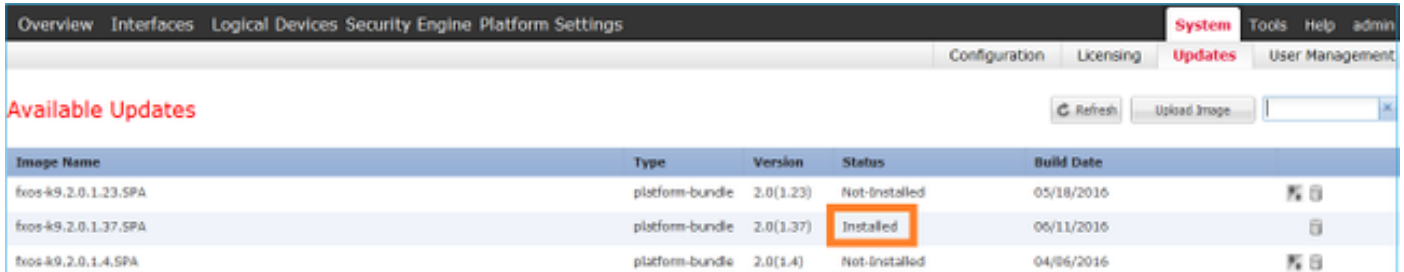
If the FXOS image is not compatible with the target FTD image, upgrade the FXOS software first.

Verify the FXOS image

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



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



Method 3. From FXOS CLI:

```
FPR4100# show fabric-interconnect firmware
Fabric Interconnect A:
  Running-Kern-Vers: 5.0(3)N2(4.01.35)
  Running-Sys-Vers: 5.0(3)N2(4.01.35)
  Package-Vers: 2.0(1.37)
  Startup-Kern-Vers: 5.0(3)N2(4.01.35)
  Startup-Sys-Vers: 5.0(3)N2(4.01.35)
  Act-Kern-Status: Ready
  Act-Sys-Status: Ready
  Bootloader-Vers:
```

Task 3. Upload FTD Image into Firepower Appliance

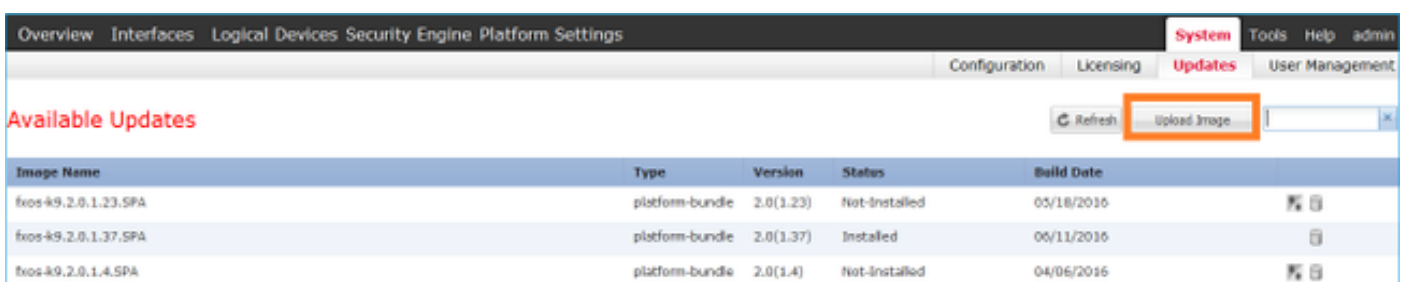
Task requirement

Upload the FTD image into FPR4100 chassis.

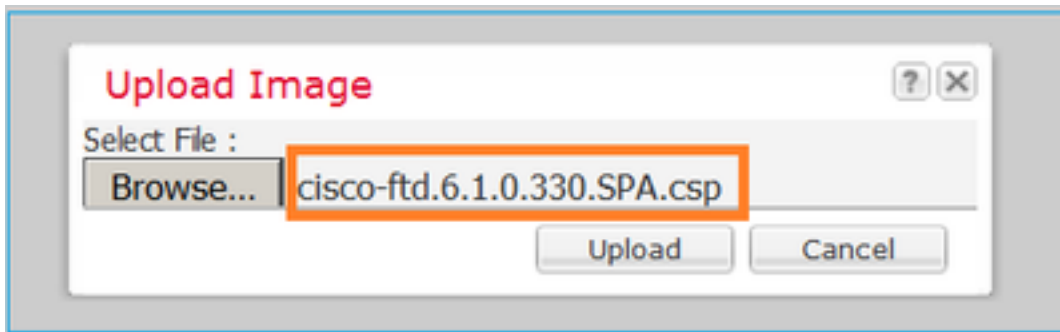
Solution

Method 1 - Upload the FTD image from the FCM UI

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



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



Accept the **End User License Agreement (EULA)**.

Verification is as shown in the image.

Overview Interfaces Logical Devices Security Engine Platform Settings					System	Tools	Help	admin
					Configuration	Licensing	Updates	User Management
Available Updates					Refresh	Upload Image	Filter...	
Image Name	Type	Version	Status	Build Date				
fxos-k9.2.0.1.86.SPA	platform-bundle	2.0(1.86)	Installed	10/15/2016				
fxos-k9.2.0.1.4.SPA	platform-bundle	2.0(1.4)	Not-Installed	04/06/2016				
cisco-ftd.6.1.0.330.csp	ftd	6.1.0.330	Not-Installed	08/26/2016				

Method 2 - Upload the FTD image from the FXOS CLI

You can upload the FTD image from an FTP, Secure Copy (SCP), Secure FTP (SFTP), or a TFTP server.

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

```
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:

```
FPR4100# scope ssa
FPR4100 /ssa # scope app-software
FPR4100 /ssa/app-software # download image ftp://ftp_username@10.229.24.22/cisco-
ftd.6.1.0.330.SPA.csp
Password:
```

To monitor the image upload progress:

```
FPR4100 /ssa/app-software # show download-task detail
```

Downloads for Application Software:

```
File Name: cisco-ftd.6.1.0.330.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.6.1.0.330.SPA.csp from 10.229.24.22(FSM-STAGE:sam:dme:ApplicationDownloaderDownload:Local)

Use this command to verify the successful download:

```
FPR4100 /ssa/app-software # show download-task
```

Downloads for Application Software:

File Name	Protocol	Server	Port	Userid	State
cisco-ftd.6.1.0.330.SPA.csp	Ftp	10.229.24.22		0 ftp	Downloaded

For additional details:

```
KSEC-FPR4100 /ssa/app-software # show download-task fsm status expand
```

File Name: cisco-ftd.6.1.0.330.SPA.csp

FSM Status:

Affected Object: sys/app-catalogue/dnld-cisco-ftd.6.1.0.330.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-6.1.0-330.sh

The image is shown in the chassis repository:

```
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	6.1.0.330	N/A	cisco	Native	Application	No

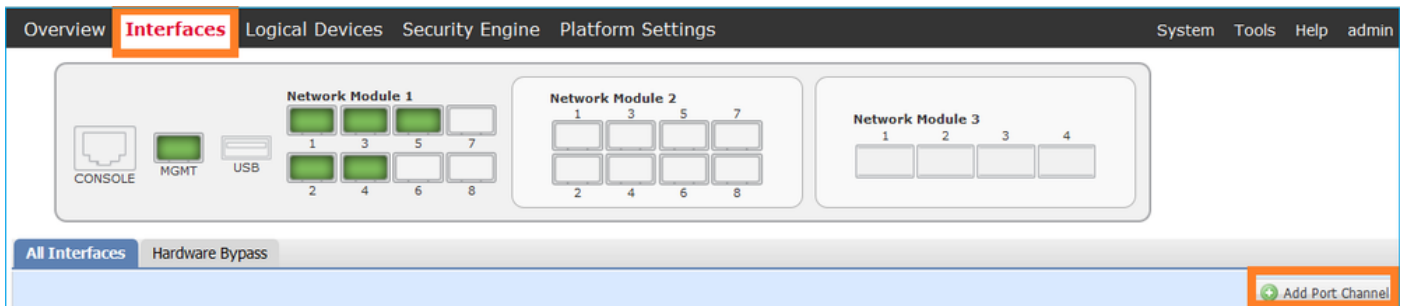
Task 4. Configure FTD Management and Data Interfaces

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 seen. To create a new Port Channel interface, select the **Add Port Channel** button, as shown in the image:



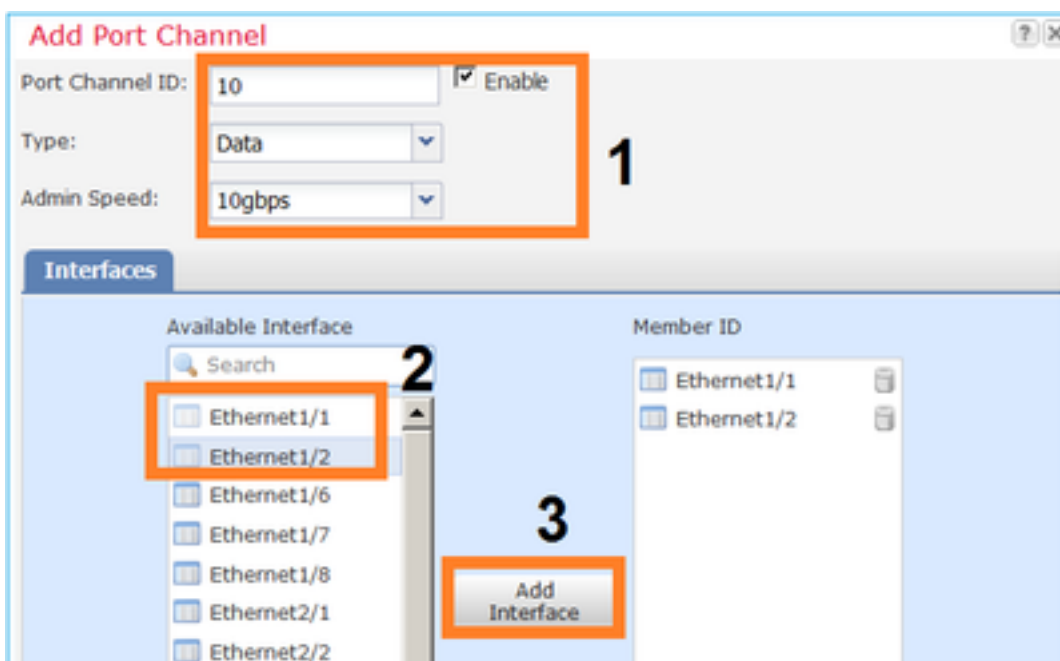
Step 1. Create a Port Channel Data Interface

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

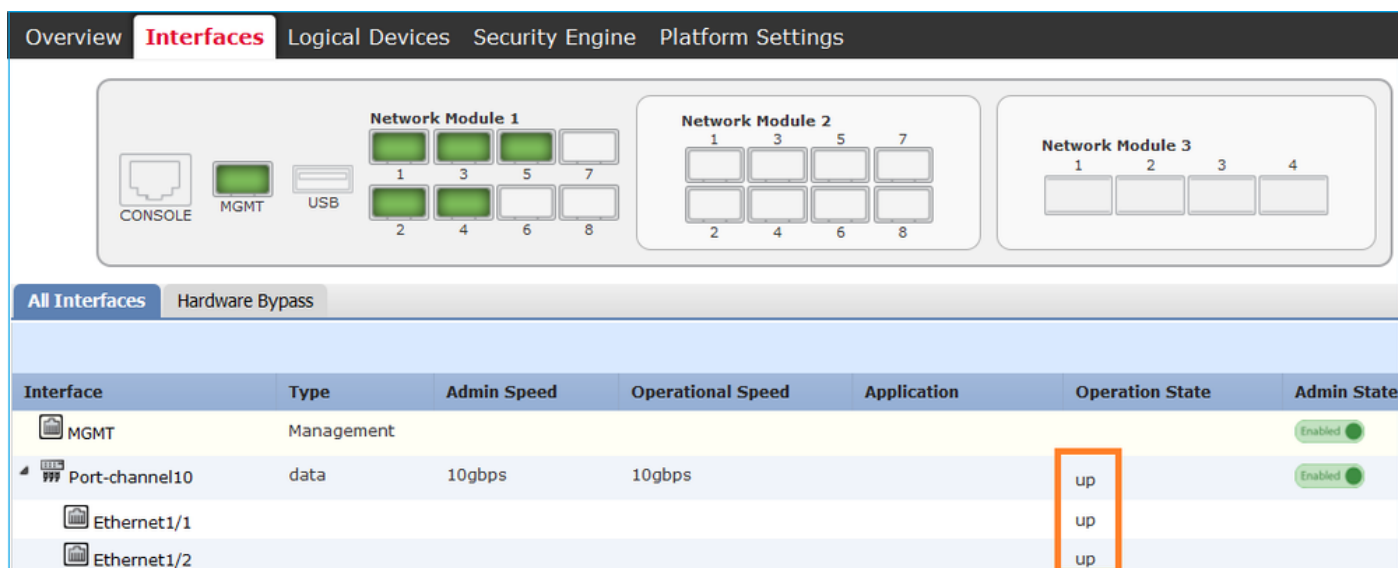
Port Channel ID	10
Type	Data
Enable	Yes
Member ID	Ethernet1/1, Ethernet 1/2

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

Note: PortChannel 48 is used for clusters.

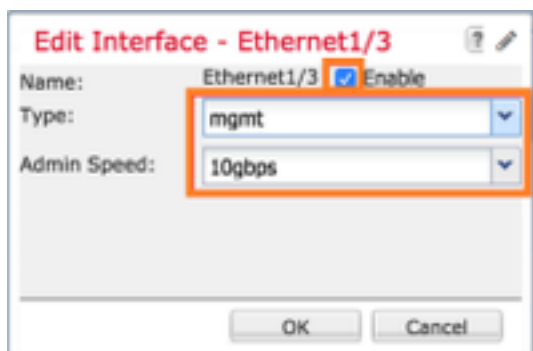


Verification is as shown in the image.



Step 2. Create a Management Interface.

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



Task 5. Create and Configure New Logical Device

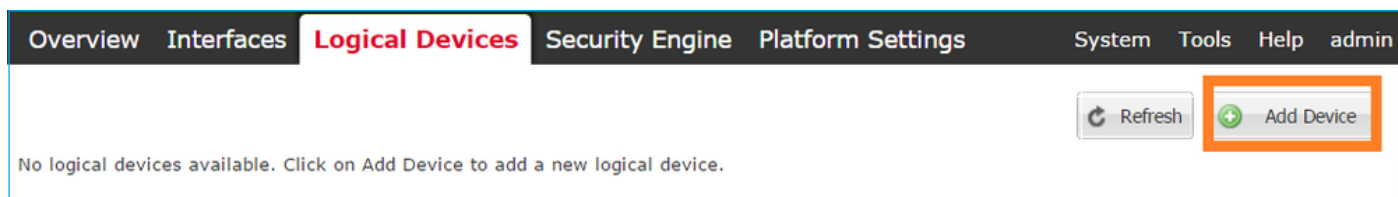
Task requirement

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

Solution

Step 1. Add a Logical Device.

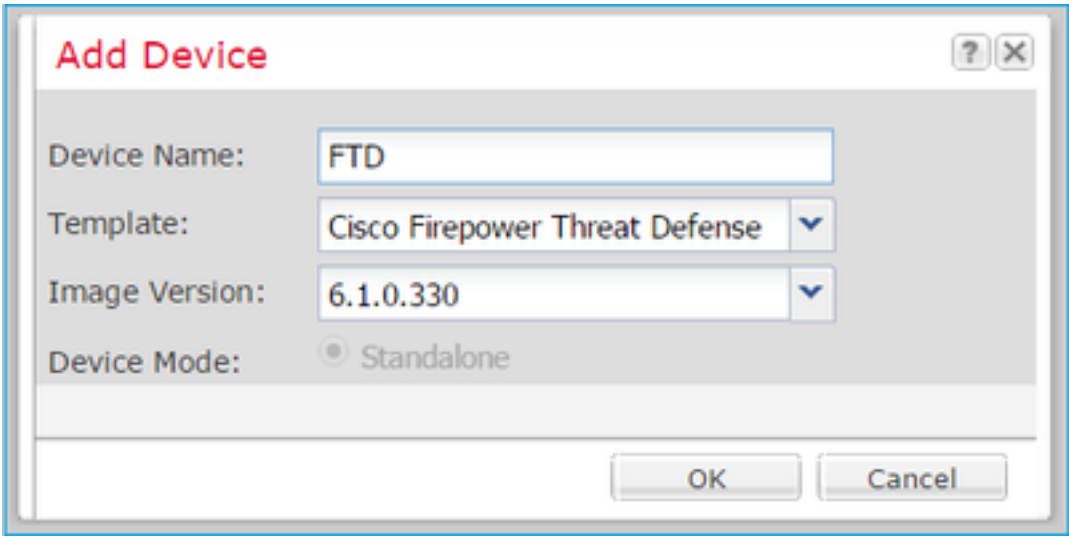
Navigate to the **Logical Devices** tab and select the **Add Device** button to create a new Logical Device, as shown in the image:



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

Device Name FTD

Template Cisco Firepower Threat Defense
Image Version 6.1.0.330



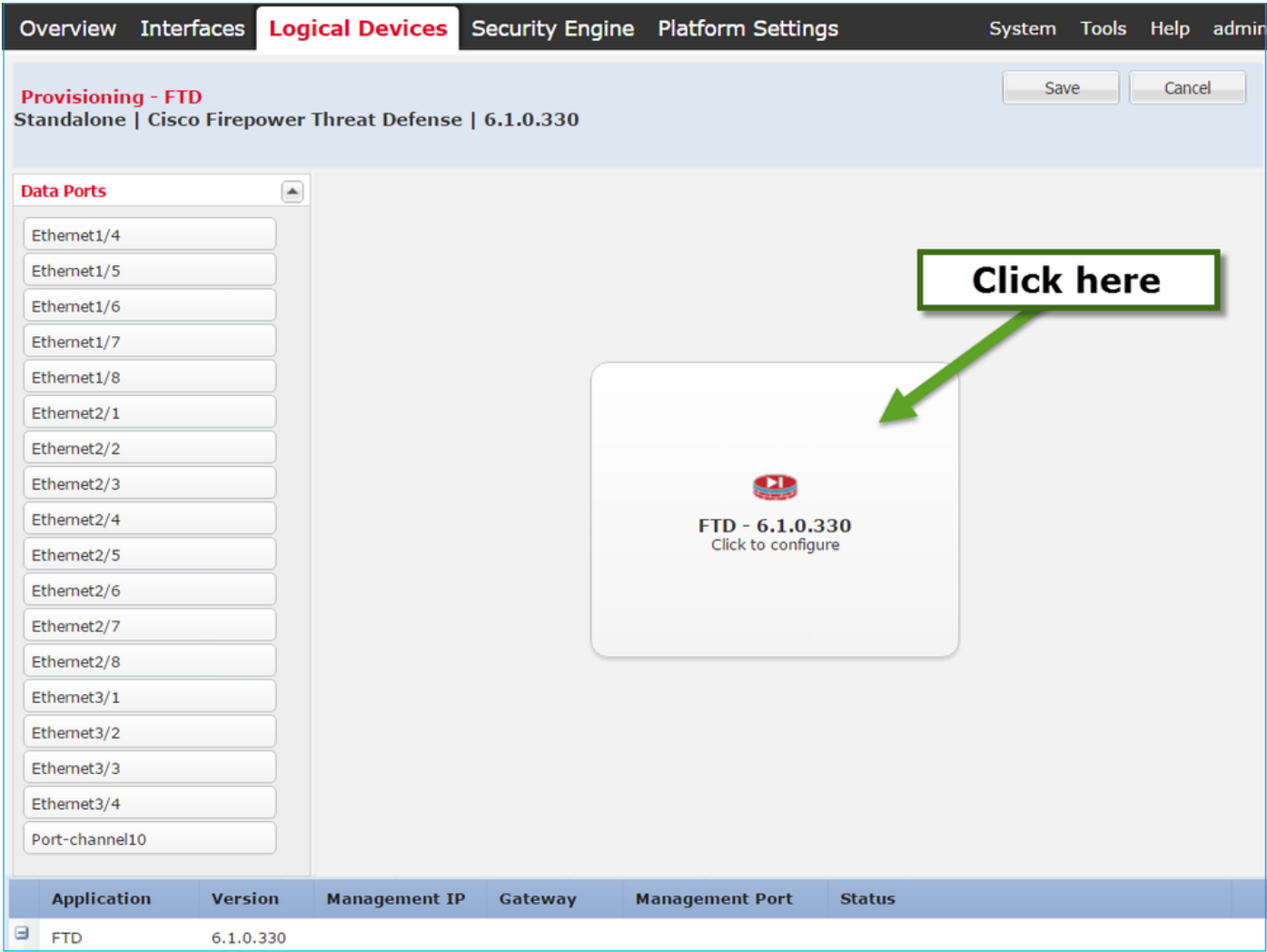
The 'Add Device' dialog box contains the following fields and options:

- Device Name: FTD
- Template: Cisco Firepower Threat Defense
- Image Version: 6.1.0.330
- Device Mode: Standalone (selected)

Buttons: OK, Cancel

Step 2. Bootstrap the Logical Device.

After creation of the logical device, the Provisioning – **device_name** window displays. Select the device icon to start the configuration, as shown in the image.



The 'Provisioning - FTD' window shows the configuration for the logical device. It includes a 'Data Ports' list on the left and a central area with a device icon and the text 'FTD - 6.1.0.330 Click to configure'. A green arrow points to the device icon with the label 'Click here'.

Data Ports

- Ethernet1/4
- Ethernet1/5
- Ethernet1/6
- Ethernet1/7
- Ethernet1/8
- Ethernet2/1
- Ethernet2/2
- Ethernet2/3
- Ethernet2/4
- Ethernet2/5
- Ethernet2/6
- Ethernet2/7
- Ethernet2/8
- Ethernet3/1
- Ethernet3/2
- Ethernet3/3
- Ethernet3/4
- Port-channel10

Click here

FTD - 6.1.0.330
Click to configure

Application	Version	Management IP	Gateway	Management Port	Status
FTD	6.1.0.330				

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

Management Interface	Ethernet1/3
Address Type	IPv4 only
Management IP	10.62.148.84
Network Mask	255.255.255.128
Network Gateway	10.62.148.1

The screenshot shows the 'Cisco Firepower Threat Defense - Configuration' window with the 'General Information' tab selected. The 'Interface Information' section is visible, showing the following configuration:

Management Interface:	Ethernet1/3
Management	
Address Type:	IPv4 only
IPv4	
Management IP:	10.62.148.84
Network Mask:	255.255.255.128
Network Gateway:	10.62.148.1

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

Registration Key	cisco
Password	Pa\$\$w0rd
Firepower Management Center IP	10.62.148.50
Search Domains	cisco.com
Firewall Mode	Routed
DNS Servers	192.168.0.1
Fully Qualified Hostname	FTD4100.cisco.com
Eventing Interface	-

Cisco Firepower Threat Defense - Configuration

General Information **Settings** Agreement

Registration Key:
Password:
Firepower Management Center IP:	10.62.148.50
Search domains:	cisco.com
Firewall Mode:	Routed ▼
DNS Servers:	192.168.0.1
Fully Qualified Hostname:	FTD4100.cisco.com
Eventing Interface:	▼

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

Step 3. Assign the Data Interfaces

Expand the Data Ports area and select each interface to assign to FTD. In this scenario, one interface (Port-channel10) was assigned as shown in the image:

Overview Interfaces **Logical Devices** Security Engine Platform Settings System Tools Help admin

Provisioning - FTD Standalone | Cisco Firepower Threat Defense | 6.1.0.330

Save Cancel

Data Ports

- Ethernet1/4
- Ethernet1/5
- Ethernet1/6
- Ethernet1/7
- Ethernet1/8
- Ethernet2/1
- Ethernet2/2
- Ethernet2/3
- Ethernet2/4
- Ethernet2/5
- Ethernet2/6
- Ethernet2/7
- Ethernet2/8
- Ethernet3/1
- Ethernet3/2
- Ethernet3/3
- Ethernet3/4
- Port-channel10**

Port-channel10

FTD - 6.1.0.330
Ethernet1/3
Click to configure

Application	Version	Management IP	Gateway	Management Port	Status
FTD	6.1.0.330	10.62.148.84	10.62.148.1	Ethernet1/3	

Ports:

Data Interfaces: Port-channel10

Select **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 the images:

Overview Interfaces **Logical Devices** Security Engine Platform Settings System Tools Help admin

Refresh Add Device

FTD Standalone Status: ok

Application	Version	Management IP	Gateway	Management Port	Status
FTD	6.1.0.330	10.62.148.84	10.62.148.1	Ethernet1/3	installing

Ports:

Data Interfaces: Port-channel10

Overview Interfaces **Logical Devices** Security Engine Platform Settings System Tools Help admin

Refresh Add Device

FTD Standalone Status: ok

Application	Version	Management IP	Gateway	Management Port	Status
FTD	6.1.0.330	10.62.148.84	10.62.148.1	Ethernet1/3	offline

Ports:

Data Interfaces: Port-channel10

Overview Interfaces **Logical Devices** Security Engine Platform Settings System Tools Help admin

Refresh Add Device

FTD Standalone Status: ok

Application	Version	Management IP	Gateway	Management Port	Status
FTD	6.1.0.330	10.62.148.84	10.62.148.1	Ethernet1/3	starting

Ports:

Data Interfaces: Port-channel10

Overview Interfaces **Logical Devices** Security Engine Platform Settings System Tools Help admin

Refresh Add Device

FTD Standalone Status: ok

Application	Version	Management IP	Gateway	Management Port	Status
FTD	6.1.0.330	10.62.148.84	10.62.148.1	Ethernet1/3	started

Ports:

Data Interfaces: Port-channel10

Monitor the installation process from the Firepower CLI:

```

FPR4100# 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

```

```

Cisco FTD: CMD=-start, CSP-ID=cisco-ftd.6.1.0.330__ftd_001_JAD19500F7YHCNL7715, FLAG=''
Cisco FTD starting ...

```

```

Registering to process manager ...
VNICs requested: 9,22
Cisco FTD started successfully.
Cisco FTD initializing ...
Firepower-module1>Setting up VNICs ...
Found Firepower management vnic 18.
No Firepower eventing vnic configured.
Updating /ngfw/etc/sf/arc.conf ...
Deleting previous CGroup Configuration ...

```

```

Initializing Threat Defense ...

```

```

[ OK ]

```

```

Starting system log daemon...

```

```

[ OK ]

```

```

Stopping mysql...

```

```

Dec 12 17:12:17 Firepower-module1 SF-IMS[14629]: [14629] pmtool:pmtool [ERROR] Unable to connect

```

```

to UNIX socket at /ngfw/var/sf/run/PM_Control.sock: No such file or directory
Starting mysql...
Dec 12 17:12:17 Firepower-module1 SF-IMS[14641]: [14641] pmtool:pmtool [ERROR] Unable to connect
to UNIX socket at /ngfw/var/sf/run/PM_Control.sock: No such file or directory
Flushing all current IPv4 rules and user defined chains: ...success
Clearing all current IPv4 rules and user defined chains: ...success
Applying iptables firewall rules:
Flushing chain `PREROUTING'
Flushing chain `INPUT'
Flushing chain `FORWARD'
Flushing chain `OUTPUT'
Flushing chain `POSTROUTING'
Flushing chain `INPUT'
Flushing chain `FORWARD'
Flushing chain `OUTPUT'
Applying rules succeeded
Flushing all current IPv6 rules and user defined chains: ...success
Clearing all current IPv6 rules and user defined chains: ...success
Applying ip6tables firewall rules:
Flushing chain `PREROUTING'
Flushing chain `INPUT'
Flushing chain `FORWARD'
Flushing chain `OUTPUT'
Flushing chain `POSTROUTING'
Flushing chain `INPUT'
Flushing chain `FORWARD'
Flushing chain `OUTPUT'
Applying rules succeeded
Starting nscd...
mkdir: created directory '/var/run/nscd' [ OK ]
Starting , please wait.....complete.
Firstboot detected, executing scripts
Executing S01virtual-machine-reconfigure [ OK ]
Executing S02aws-pull-cfg [ OK ]
Executing S02configure_onbox [ OK ]
Executing S04fix-httpd.sh [ OK ]
Executing S06addusers [ OK ]
Executing S07uuid-init [ OK ]
Executing S08configure_mysql [ OK ]

***** Attention *****

    Initializing the configuration database. Depending on available
    system resources (CPU, memory, and disk), this may take 30 minutes
    or more to complete.

***** Attention *****

Executing S09database-init [ OK ]
Executing S11database-populate [ OK ]
Executing S12install_infodb [ OK ]
Executing S15set-locale.sh [ OK ]
Executing S16update-sensor.pl [ OK ]
Executing S19cert-tun-init [ OK ]
Executing S20cert-init [ OK ]
Executing S21disable_estreamer [ OK ]
Executing S25create_default_des.pl [ OK ]
Executing S30init_lights_out_mgmt.pl [ OK ]
Executing S40install_default_filters.pl [ OK ]
Executing S42install_default_dashboards.pl [ OK ]
Executing S43install_default_report_templates.pl [ OK ]
Executing S44install_default_app_filters.pl [ OK ]
Executing S45install_default_realms.pl [ OK ]
Executing S47install_default_sandbox_EO.pl [ OK ]

```

```

Executing S50install-remediation-modules [ OK ]
Executing S51install_health_policy.pl [ OK ]
Executing S52install_system_policy.pl [ OK ]
Executing S53change_reconciliation_baseline.pl [ OK ]
Executing S70remove_casuser.pl [ OK ]
Executing S70update_sensor_objects.sh [ OK ]
Executing S85patch_history-init [ OK ]
Executing S90banner-init [ OK ]
Executing S96grow_var.sh [ OK ]
Executing S96install_vmware_tools.pl [ OK ]

```

***** Attention *****

Initializing the system's localization settings. Depending on available system resources (CPU, memory, and disk), this may take 10 minutes or more to complete.

***** Attention *****

```

Executing S96localize-templates [ OK ]
Executing S96ovf-data.pl [ OK ]
Executing S97compress-client-resources [ OK ]
Executing S97create_platinum_forms.pl [ OK ]
Executing S97install_cas [ OK ]
Executing S97install_cloud_support.pl [ OK ]
Executing S97install_geolocation.pl [ OK ]
Executing S97install_ssl_inspection.pl [ OK ]
Executing S97update_modprobe.pl [ OK ]
Executing S98check-db-integrity.sh [ OK ]
Executing S98htaccess-init [ OK ]
Executing S98is-sru-finished.sh [ OK ]
Executing S99correct_ipmi.pl [ OK ]
Executing S99start-system [ OK ]
Executing S99z_db_restore [ OK ]
Executing S99_z_cc-integrity.sh [ OK ]
Firstboot scripts finished.
Configuring NTP... [ OK ]

```

```

insmod: ERROR: could not insert module /lib/modules/kernel/drivers/uio/igb_uio.ko: File exists
rw console=ttyS0,38400 loglevel=2 auto kstack=128 reboot=force panic=1
ide_generic.probe_mask=0x1 ide1=noprobe pci=nocrs processor.max_cstate=1 iommu=pt
platform=sspxru boot_img=disk0:/fxos-lfbff-k8.9.6.1.150.SPA ciscodmasz=786432
cisconrsvsz=2359296 hugepagesz=1g hugepages=24 ssp_mode=0
Fru Size : 512 bytes
Done

```

```

VNIC command successful
VNIC command successful
fatattr: FAT_IOCTL_GET_ATTRIBUTES: Inappropriate ioctl for device
fatattr: can't open '/mnt/disk0/.private2': No such file or directory
fatattr: can't open '/mnt/disk0/.ngfw': No such file or directory
Model reconfigure detected, executing scripts

```

```

Pinging mysql
Found mysql is running
Executing 45update-sensor.pl [ OK ]
Executing 55recalculate_arc.pl [ OK ]
Mon Dec 12 17:16:15 UTC 2016
Starting MySQL...
Pinging mysql
Pinging mysql, try 1
Found mysql is running
Detecting expanded storage...
Running initializeObjects...
Stopping MySQL...
Killing mysqld with pid 32651
Wait for mysqld to exit\c
done

```

```
Mon Dec 12 17:16:21 UTC 2016
Starting sfid... [ OK ]
Starting Cisco Firepower 4140 Threat Defense, please wait...No PM running!
...started.
```

```
Cisco FTD initialization finished successfully.
... output omitted ...
```

```
Reading from flash...
```

```
!
```

```
Cryptochecksum (changed): blabfa7e 63faee14 affdddb0 9bc9d8cd
```

```
INFO: Power-On Self-Test in process.
```

```
.....
INFO: Power-On Self-Test complete.
```

```
INFO: Starting HW-DRBG health test (DRBG 0)...
```

```
INFO: HW-DRBG health test (DRBG 0) passed.
```

```
INFO: Starting HW-DRBG health test (DRBG 1)...
```

```
INFO: HW-DRBG health test (DRBG 1) passed.
```

```
INFO: Starting SW-DRBG health test...
```

```
INFO: SW-DRBG health test passed.
```

```
Firepower-module1>
```

```
Firepower-module1>show services status
```

```
Services currently running:
```

```
Feature | Instance ID | State | Up Since
```

```
-----
ftd | 001_JAD19500F7YHCNL7715 | RUNNING | :00:08:07
```

Task 6. Register FTD into the Firepower Management Center (FMC)

Task requirement

Register FTD to 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:

```
Firepower-module1>connect ftd
```

```
Connecting to ftd console... enter exit to return to bootCLI
```

```
>ping system 10.62.148.50
```

```
PING 10.62.148.50 (10.62.148.50) 56(84) bytes of data.
```

```
64 bytes from 10.62.148.50: icmp_seq=1 ttl=64 time=0.133 ms
```

```
64 bytes from 10.62.148.50: icmp_seq=2 ttl=64 time=0.132 ms
```

```
64 bytes from 10.62.148.50: icmp_seq=3 ttl=64 time=0.123 ms
```

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

```
> show managers
```

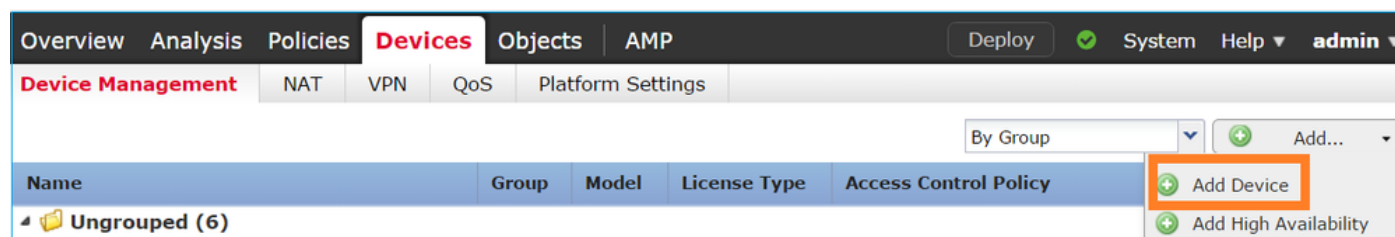
```
Host : 10.62.148.50
```

```
Registration Key : ****
```

```
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 the image.



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

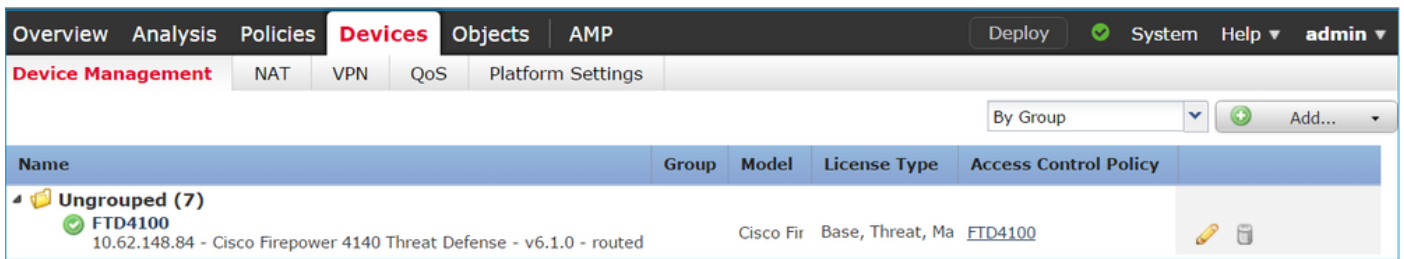
A screenshot of the 'Add Device' dialog box in the FMC. The dialog has a title bar with 'Add Device' and a close button. It contains several input fields: 'Host' (10.62.148.84), 'Display Name' (FTD4100), 'Registration Key' (cisco), 'Group' (None), and 'Access Control Policy' (FTD4100). Below these fields is a section titled 'Smart Licensing' with three checkboxes: 'Malware' (checked), 'Threat' (checked), and 'URL Filtering' (checked). At the bottom, there is an 'Advanced' section with a note: 'On version 5.4 devices or earlier, the licensing options will need to be specified from [licensing page](#).' At the very bottom of the dialog are two buttons: 'Register' and 'Cancel'.

Select the **Register** button.

On the FMC, check the **Tasks** to see how the registration progresses. In addition to the registration, the FMC also:

- Discovers the FTD device (retrieve present interface configuration).
- Deploys the initial policy.

Successful registration is as shown in the image:



Note: In version 6.1, the Firepower Device Manager (FDM) was introduced to provide on-box management. An FTD installed on a Firepower appliance **cannot** be managed by the FDM.

Task 7. Upgrade FTD

Task requirement

Upgrade the FTD from 6.1.0.330 to 6.1.0.1.

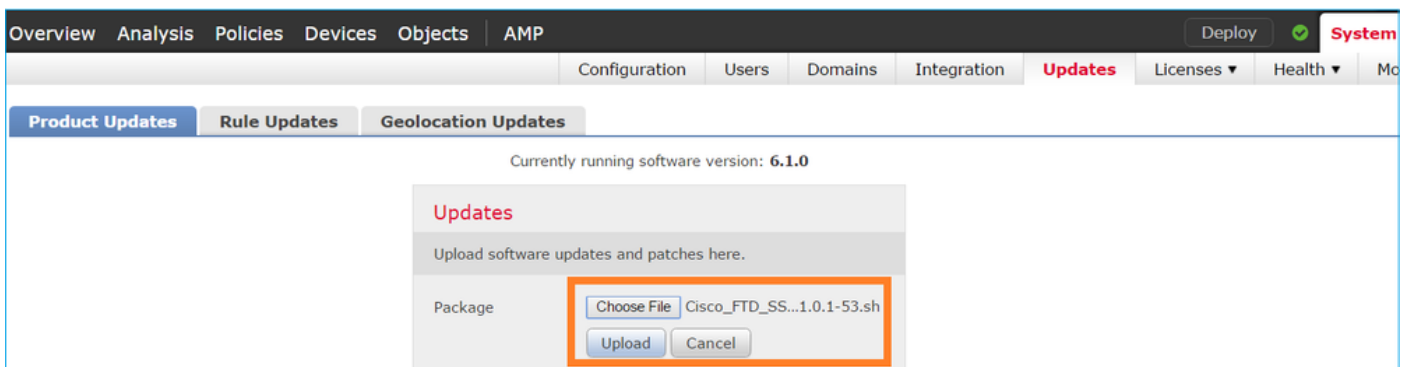
Solution

Step 1. Verify the compatibility

Check the FXOS Release Notes to ensure the target FTD version is compatible with the FXOS software. If needed, first upgrade the FXOS software.

Step 2. Upgrade the FTD

The FTD software is managed by the FMC, not the FCM. To upgrade the FTD module, connect to the FMC, navigate to the **System > Updates** page, and select **Upload Update**, as shown in the image.



Install the update on the FTD module, as shown in the images:

Overview Analysis Policies Devices Objects AMP Deploy System

Configuration Users Domains Integration **Updates** Licenses Health

Product Updates Rule Updates Geolocation Updates Upload Update

Currently running software version: **6.1.0**

Updates

Type	Version	Date	Release Notes	Reboot
Sourcefire Vulnerability And Fingerprint Database Updates	275	Wed Nov 16 16:50:43 UTC 2016		No
Cisco FTD SSP Patch	6.1.0.1-53	Fri Dec 2 17:37:52 UTC 2016		Yes

Optionally, you can launch a Readiness Check:

Product Updates Rule Updates Geolocation Updates Currently running software version: **6.1.0**

Selected Update

Type Cisco FTD SSP Patch
Version 6.1.0.1-53
Date Fri Dec 2 17:37:52 UTC 2016
Release Notes
Reboot Yes

By Group ▼

☒ ▼ Ungrouped (1 total)

☒ FTD4100
10.62.148.84 - Cisco Firepower 4140 Threat Defense v6.1.0

Health Policy
[Initial Health Policy 2016-11-21 12:21:09](#) ✓ ✓

Launch Readiness Check Install Cancel

A successful Readiness Check is shown in the image:

Readiness Check Status

Current Version: 6.1
Update Version: 6.1.0.1-53

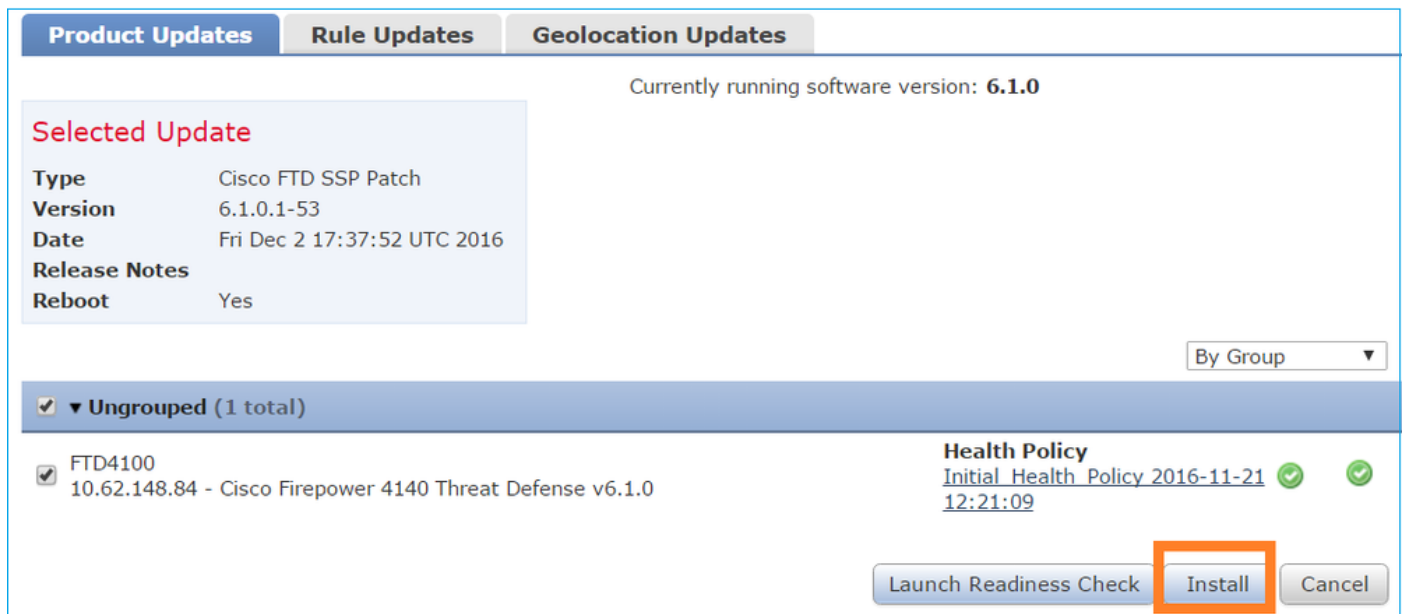
Readiness Check Complete

Total 1 devices Selected

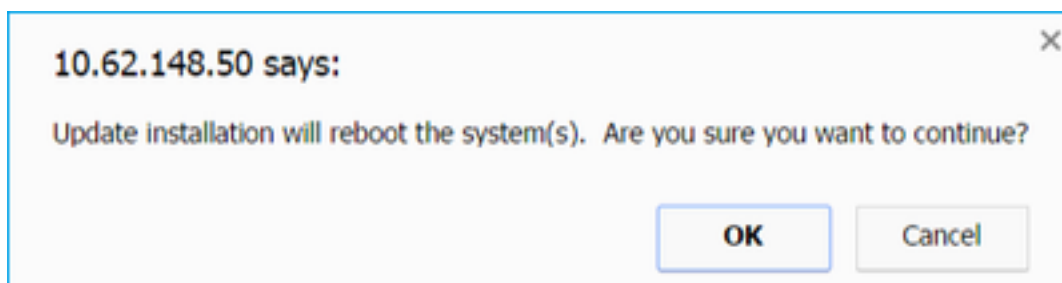
FTD4100
10.62.148.84 - Cisco Firepower 4140 Threat Defense v6.1.0 Success

Status Log: Readiness Check To 10.62.148.84 Success

To start the upgrade process, click **Install**, as shown in the image:

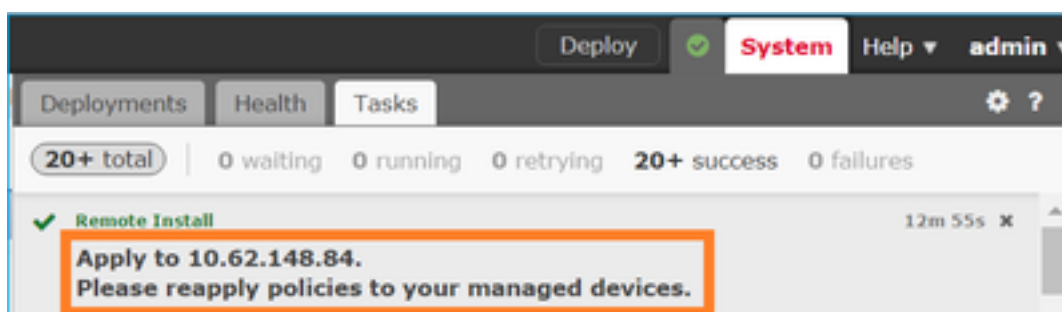


The upgrade requires an FTD reboot, as shown in the image:



Similarly to the FTD installation, the FTD upgrade process can be monitored from the FMC UI (**Tasks**). Upgrade progress can be tracked from the FTD CLI (CLISH mode).

After upgrade completion, deploy a policy to the FTD, as shown in the image:



Verification

From the FMC UI, as shown in the image:



From the FCM UI, as shown in the image:



From the chassis CLI:

```
FPR4100# scope ssa
FPR4100 /ssa # show app-instance
Application Name      Slot ID   Admin State   Operational State   Running Version   Startup
Version Cluster Oper State
-----
ftd                   1         Enabled       Online               6.1.0.1.53        6.1.0.330
Not Applicable
```

From the FTD CLI:

```
FPR4100# 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

> show version
-----[ FTD4100.cisco.com ]-----
Model                  : Cisco Firepower 4140 Threat Defense (76) Version 6.1.0.1 (Build 53)
UUID                   : 22c66994-c08e-11e6-a210-931f3c6bbbea
Rules update version   : 2016-03-28-001-vrt
VDB version            : 275
>
```

Firepower 2100

The FTD on Firepower 2100 uses a single bundle that contains both FXOS and FTD images. Therefore, the installation and upgrade procedures are different than on FP4100/FP9300.

FTD Installation on FP2100

There are 4 different procedures, which are case dependent:

Case 1: Erase configuration and restart the system with the same FTD image

Case 2: Re-image the system with a new application software version

Case 3: Reimage the system to its factory default settings

Case 4: Reimage the system to its factory default settings (admin password recovery)

For details relevant to each case and its procedure, check:

https://www.cisco.com/c/en/us/td/docs/security/firepower/2100/troubleshoot_fxos/b_2100_CLI_Troubleshoot/b_2100_CLI_Troubleshoot_chapter_011.pdf

Case 2 serves the majority of FTD installation cases, while Case 3 (format and boot from ROMMON) can be used in specific cases (for example, system is unstable or in a boot loop, and so on)

FTD Upgrade on FP2100

Because there is no separate FXOS bundle, to upgrade an FTD on FP2100, do the steps listed:

Step 1. Verify the compatibility

If the FTD is managed by FMC (off-box management) check the Compatibility section in the software target FTD Release Notes.

Step 2. If there is a need, first upgrade the FMC. Always run the FMC software version equal to or higher than the FTD target software version.

Step 3. Upgrade the FTD

Follow the same procedure as the one documented for FP4100/9300. Important documents to read before an upgrade of the FTD:

- FTD Release Notes (for example, if you want to upgrade to version 6.3.0.2, check the 6.3.0.2 Release Notes to verify the upgrade paths and all relevant details)

<https://www.cisco.com/c/en/us/support/security/defense-center/products-release-notes-list.html>

- FMC Upgrade Guide (Chapter: Upgrade Firepower Threat Defense: Other Devices)

https://www.cisco.com/c/en/us/td/docs/security/firepower/upgrade/fpmc-upgrade-guide/upgrade_firepower_threat_defense.html

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific information available to troubleshoot this configuration.

Related Information

- [FXOS Compatibility Guide](#)
- [Cisco Firepower NGFW documentation](#)
- [Technical Support & Documentation - Cisco Systems](#)