

Create and Manage Logical Devices in FXOS Chassis Manager

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Additional Information](#)

[Choose the FTD Product Version](#)

[Configure](#)

[Access Cisco FCM GUI](#)

[Upload Package](#)

[Creating a Logical Device](#)

[Verify](#)

[Manage Logical Instance](#)

[Troubleshoot](#)

Introduction

This document describes how to create and manage Logical Devices in Cisco Firepower 4100/9300 FXOS using Firepower Chassis Manager.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Firepower 4100/9300 Initial Chassis configuration.
- Firepower 4100/9300 FXOS CLI configuration.

Components Used

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

- Cisco Firepower 4125 Security Appliance.
- Cisco Firepower Extensible Operating System (FXOS) - 2.12(1.29)
- Cisco Secure Firepower Threat Defense (FTD) - 7.2.5-208

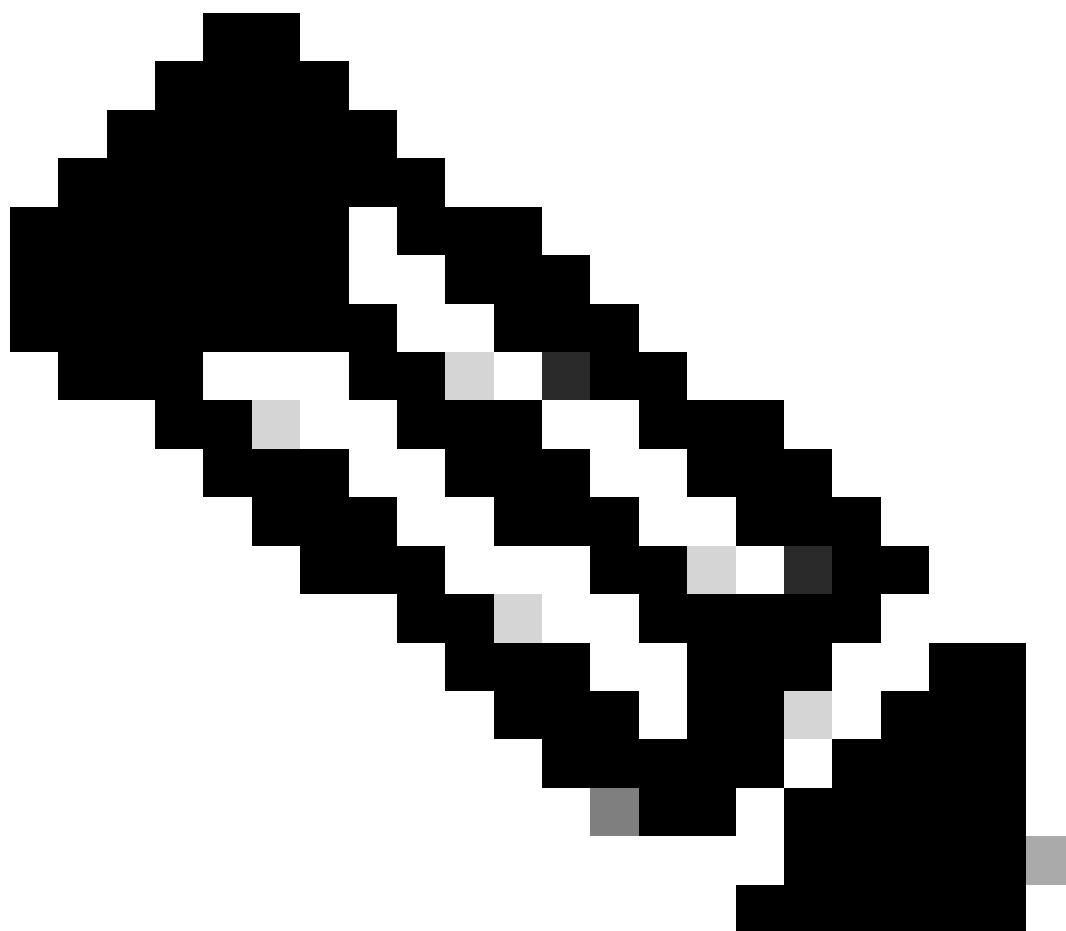
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Additional Information

Choose the FTD Product Version

Before starting, consider upgrading to the latest FPR4145 FXOS version or a compatible version with your target FTD logical instance version.

The target FTD version for this document is 7.2.5-208. Hence, the recommended FXOS version for the FPR4145 chassis is 2.12.0-519.



Note: Refer to this document in order to review FXOS and FTD compatibility: Section Table 14 - https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/compatibility/threat-defense-compatibility.html#id_67425.

Configure

Access Cisco FCM GUI

Log into the Firepower Chassis Manager, and enter the URL in the address bar (from a supported browser):

<#root>

https://<chassis_mgmt_ip_address>

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

FPR4125
Model: Cisco Firepower 4125 Security Appliance | Version: 2.12(1.29) | Operational State: Power-problem | Chassis Uptime 00:00:18:01

CONSOLE MGMT USB
Power 1 - Running Power 2 - Running

Network Module 1 Network Module 2 Network Module 3 : Empty

FAULTS 0(0) CRITICAL 0(2) MAJOR
INTERFACES 16 DOWN 0 UP
INSTANCES 0 DOWN 0 UP
LICENSE Smart Agent UNREGISTERED
INVENTORY 1(1) Security Engine 6(6) Fans 1(2) Power Supplies

Severity	Description	Cause	Occurrence	Time	Acknowledged
INFO	[FSM:STAGE:RETRY:]: Check for the image tftp status on blade 1/1(FSM-STAG...	host-check-upgrade-imag...	1	2023-09-27T17:44:21.401	no
CLEARED	[FSM:STAGE:RETRY:]: rescanning image files(FSM-STAGE:sam:dme:Capability...	rescan-images-failed	1	2023-09-27T17:21:36.338	no
CLEARED	[FSM:STAGE:RETRY:]: Waiting for Activation to complete on Local Fabric Inter...	poll-activate-of-localfi-failed	1	2023-09-27T17:30:11.237	no
CLEARED	[FSM:STAGE:REMOTE-ERROR]: Result: timeout Code: unspecified Message: So...	execute-failed	1	2023-09-27T17:23:08.895	no
CLEARED	Security module 1 - network adapter 1 is not responding	slot-not-responding	1	2023-09-27T17:23:08.896	no
CLEARED	[FSM:STAGE:RETRY:]: Soft shutdown of server sys/chassis-1/blade-1(FSM-STA...	execute-failed	1	2023-09-27T17:23:26.838	no
CLEARED	[FSM:STAGE:RETRY:]: Waiting for blade shutdown(FSM-STAGE:sam:dme:Equi...	wait-for-blade-shutdown-f...	1	2023-09-27T17:30:11.236	no

Access FMC GUI

Download the corresponding Secure FTD install package for the Firepower 4100/9300 series from <https://software.cisco.com/>.

The image name is cisco-ftd.7.2.5.208.SPA.csp.

Upload Package

Upload the FTD install package to the FXOS chassis. Navigate to System > Updates.

Choose Upload image, then browse and upload:

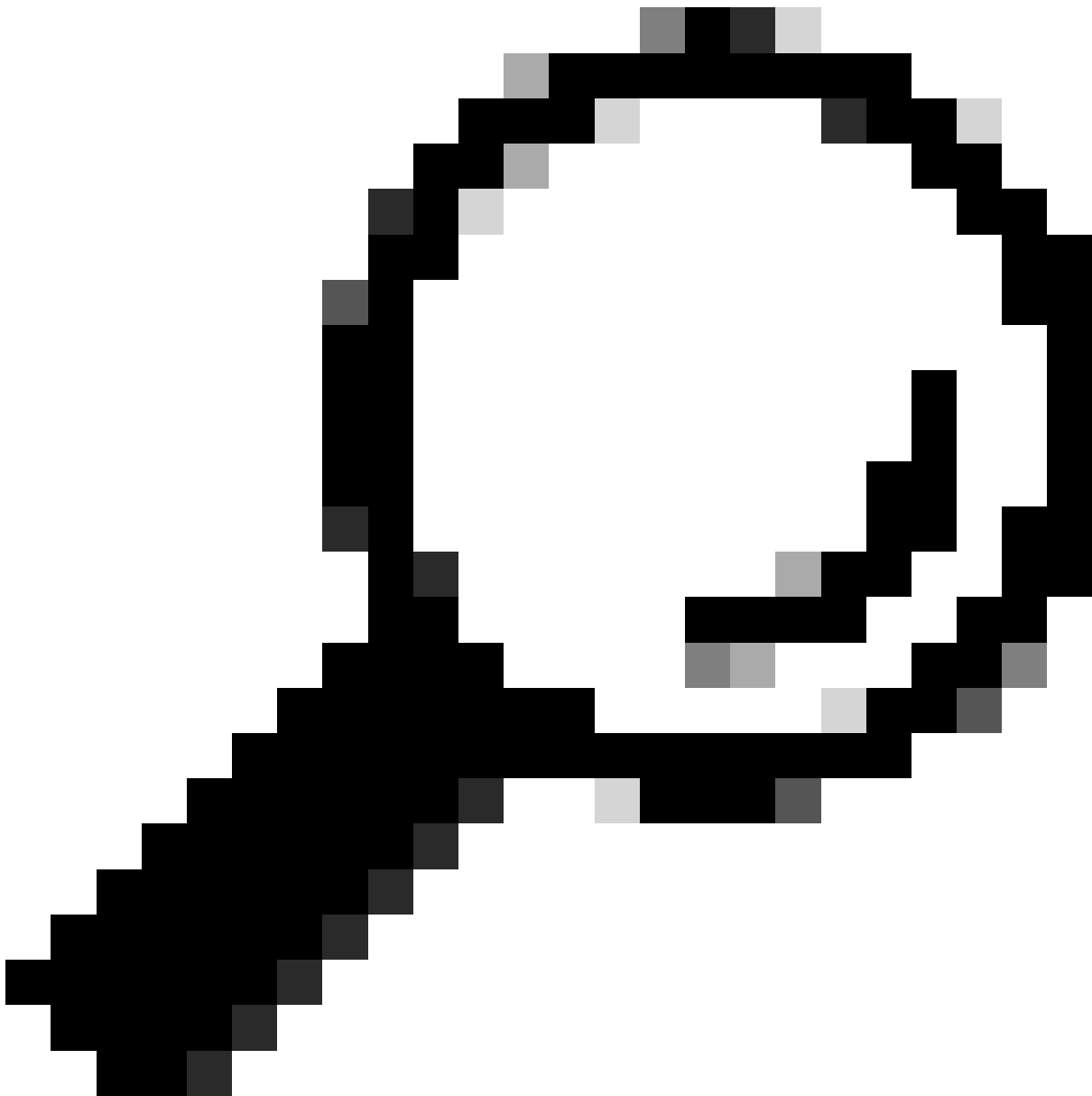
Overview Interfaces Logical Devices Security Engine Platform Settings **System** Tools Help admin

Configuration Licensing **Updates** User Management

Available Updates Filter..

Image Name	Type	Version	Status	Build Date	Image Integrity
fxos-k9.2.12.1.29.SPA	platform-bundle	2.12(1.29)	Installed	07/24/2023	Verified - Wed 27 Sep 2023, 05:08...

Upload FTD image



Tip: Once the image is uploaded, the End User License Agreement is displayed, and you can accept by selecting 'I understand and accept the agreement'.

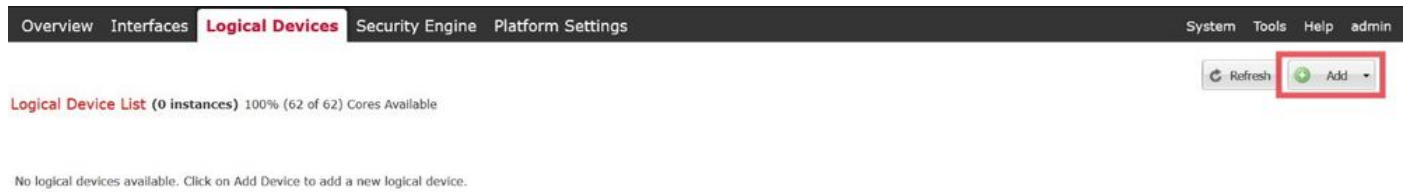
The FTD install package is successfully uploaded to the chassis:

Available Updates						Refresh	Upload Image	Filter..
Image Name	Type	Version	Status	Build Date	Image Integrity			
fxos-k9.2.12.1.29.SPA	platform-bundle	2.12(1.29)	Installed	07/24/2023	Verified - Wed 27 Sep 2023, 05:08...	✓	🗑️	
cisco-ftd.7.2.5.208.csp	ftd	7.2.5.208	Not-Installed	07/21/2023	Verified - Wed 27 Sep 2023, 07:54 PM	✓	🗑️	

FTD image uploaded successfully to Chassis

Creating a Logical Device

Now you can create a Logical Device by navigating to the Logical Devices tab and clicking Add:



Select Add Logical Instance

Next, choose Standalone.



Add Standalone Instance



Warning: Choose **Standalone** for Logical Devices in HA or standalone. For multiple containers in cluster mode, choose **Cluster**. Note that if choosing Cluster, all modules created within the cluster must have the same Type.

Specify the Device Name and Instance Type (Native or Container):

Add Standalone

Device Name:

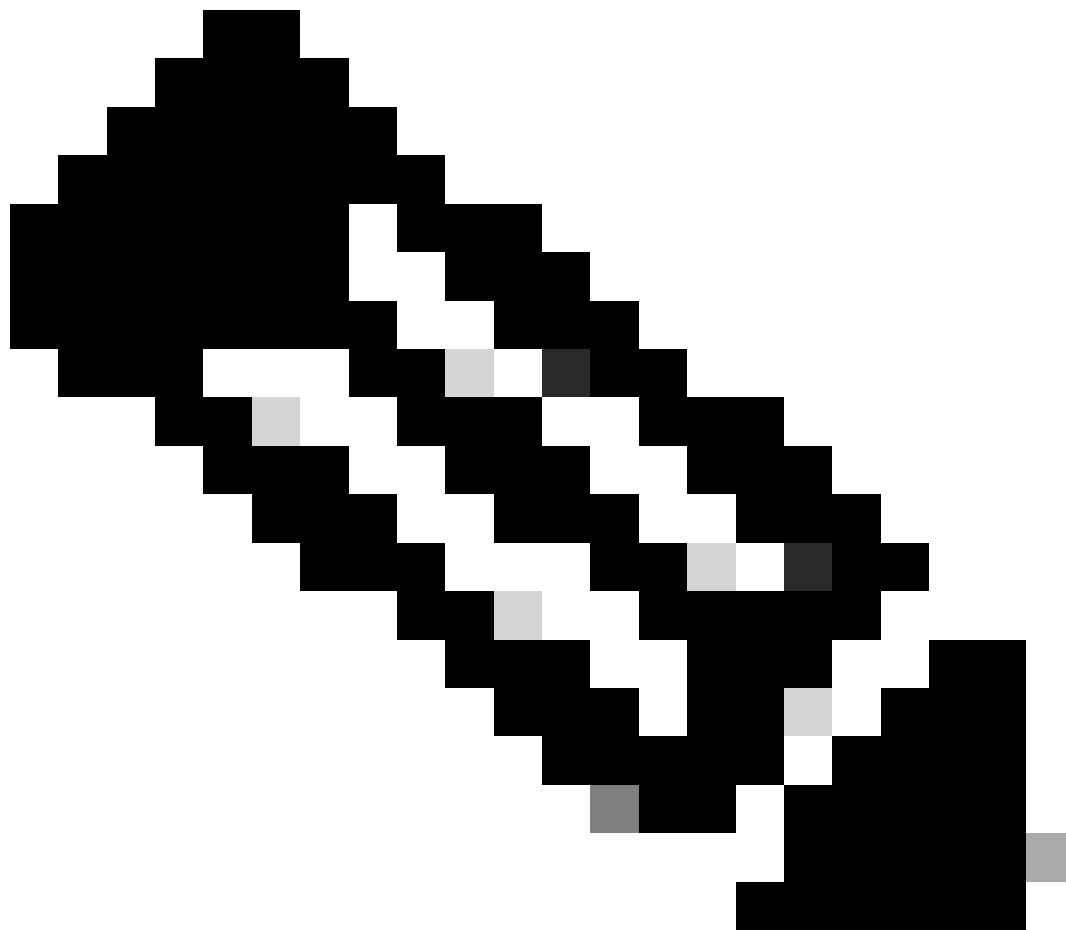
Template: Cisco Secure Firewall Threat Defense

Image Version: 7.2.5.208

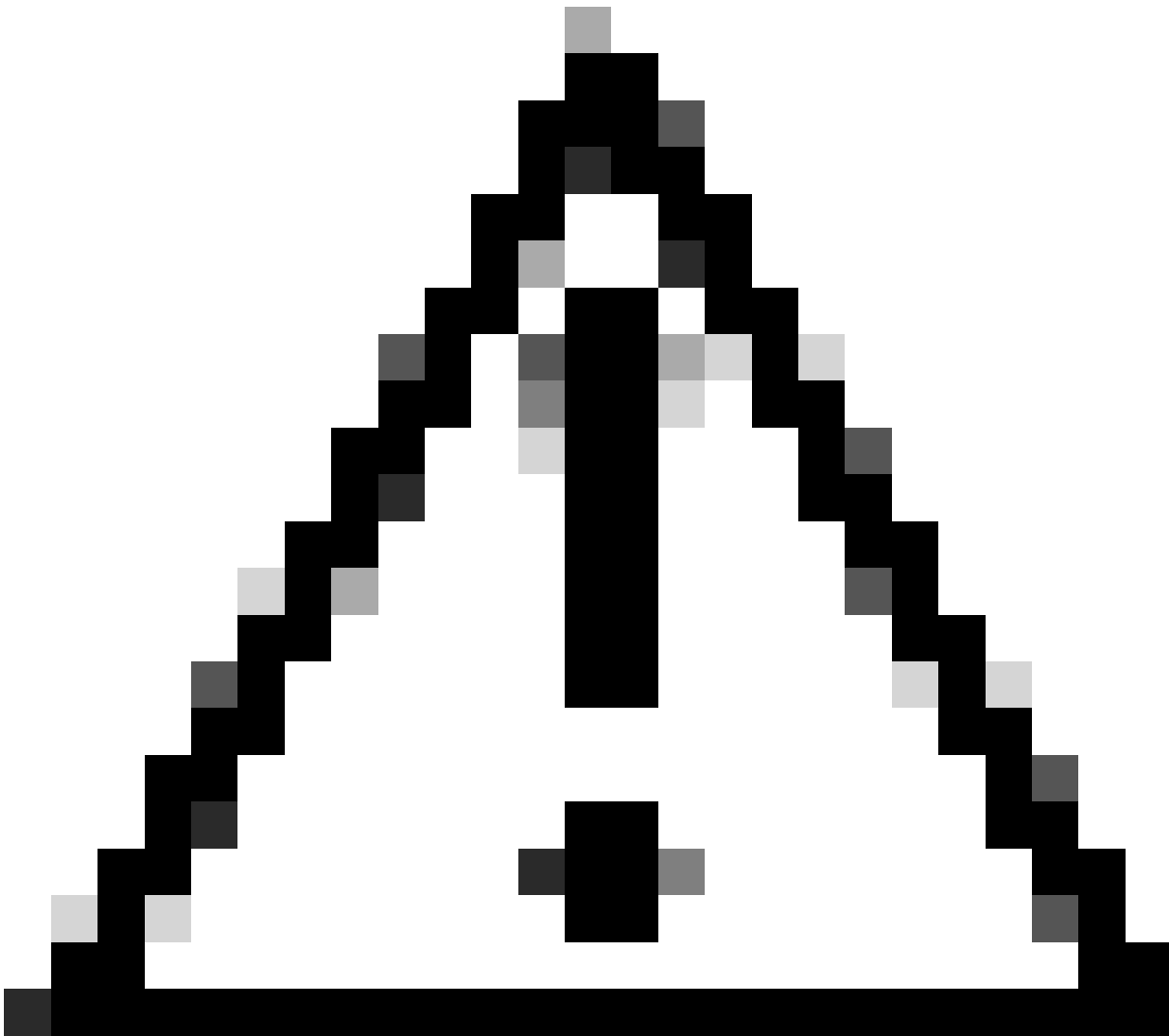
Instance Type: Native

OK Cancel

Specify Device Name and Instance Type



Note: The **Instance Type** can be elected as Native or Container. Creating a **Native Instance** allocates all the available resources in the chassis and Security Modules such as CPU, RAM, and disk space. Container Instance Type uses a fraction of the available resources. This enables the capability of installing multiple container FTD instances in the same chassis.



Caution: Multi-instance capability is only supported for the FTD using FMC; it is not supported for the Adaptive Security Appliance (ASA) or the FTD using Firepower Device Manager.

The provisioning screen is loaded afterwards:

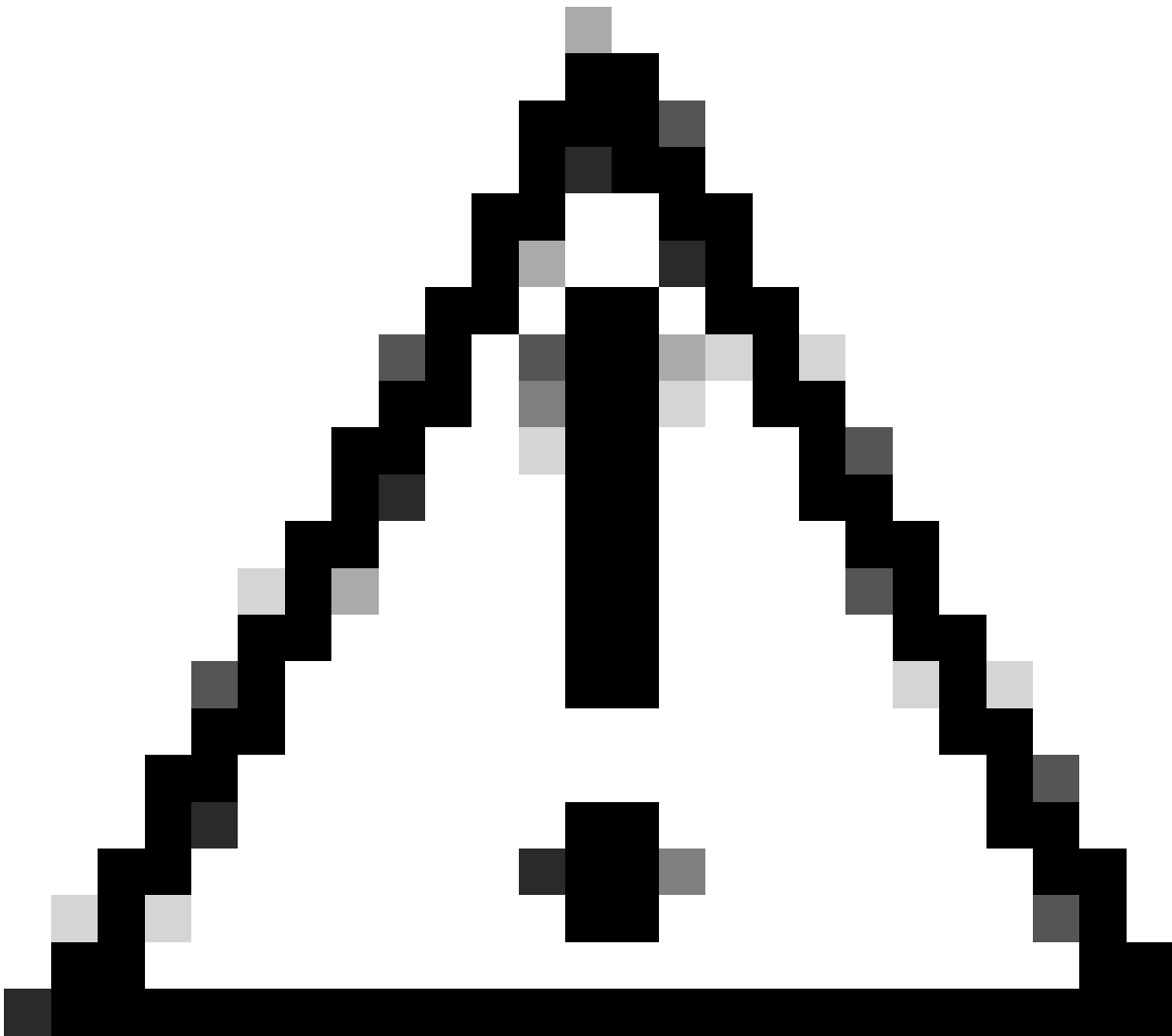
Provisioning - FTD Standalone | Cisco Secure Firewall Threat Defense | 7.2.5.208 Save Cancel

- Data Ports**
- Ethernet1/1
 - Ethernet1/2
 - Ethernet1/3
 - Ethernet1/4
 - Ethernet1/5
 - Ethernet1/6
 - Ethernet1/7
 - Ethernet1/8
- Decorators**



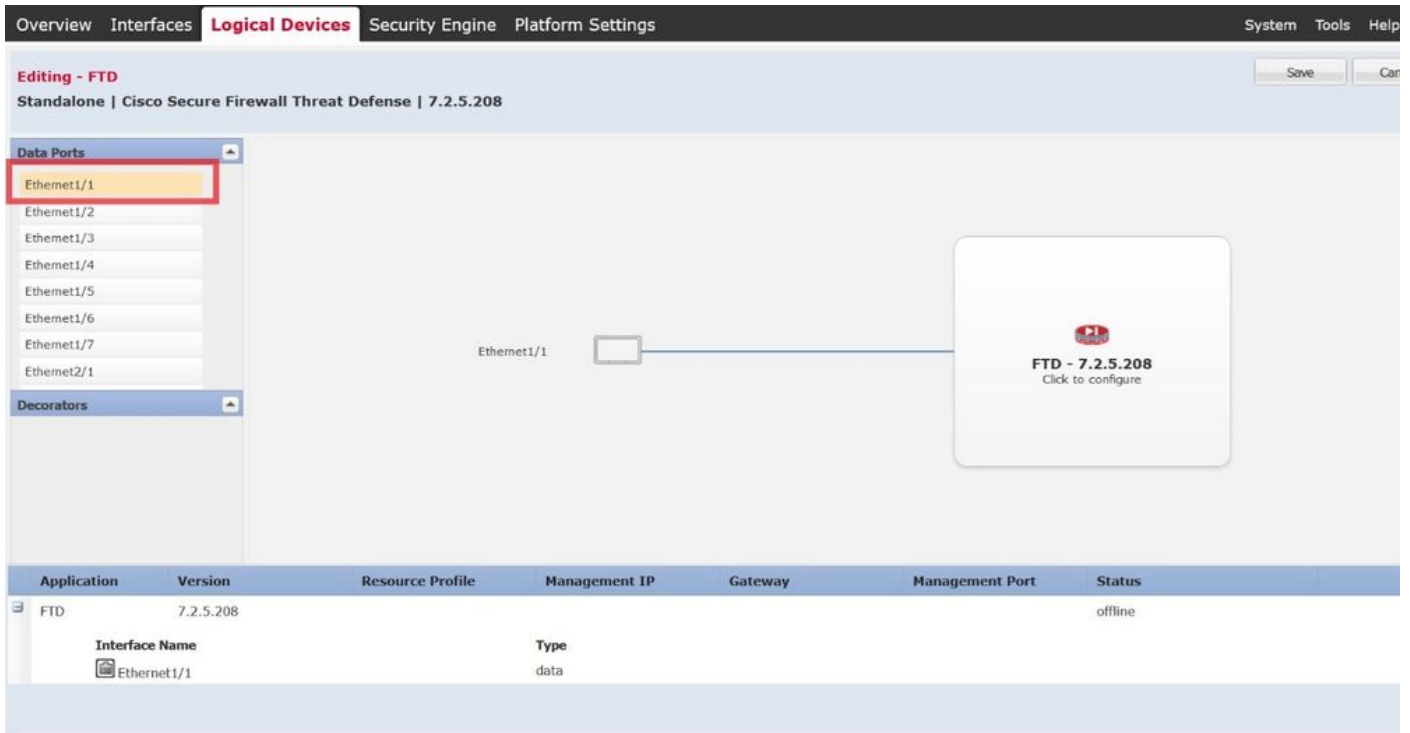
Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status
FTD	7.2.5.208					

Logical Device Provisioning

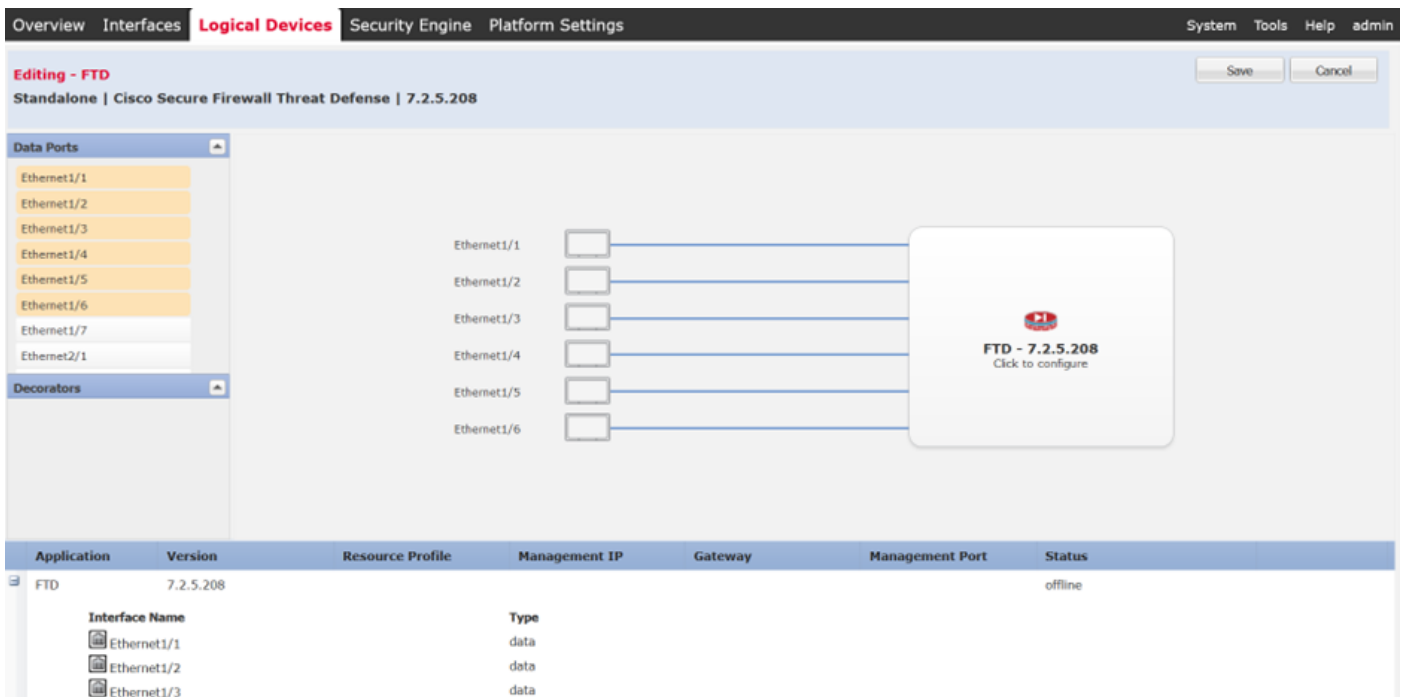


Caution: Ensure there is at least one Management Interface for the FTD Logical instance you are creating. You can validate this by navigating to the *Interfaces Tab > Edit Interface > Type* . Change the type to **management**.

From the **Data Ports** panel, you can choose all the management and data interfaces in order to allocate for this instance by clicking on **Ethernet 1/1**. Such interface is allocated to the FTD instance:



You can choose as many interfaces as required. In this example, you can see Interfaces Ethernet 1/1 to Ethernet 1/6 are allocated to this FTD instance:



Interfaces Eth1/1 to Eth1/6 allocated to FTD instance

Moving forward, choose Click to configure. Bootstrap configuration is shown next with the General Information.

Specify the Management Interface, Address Type, Management IP, Network Mask and Gateway:

Cisco Secure Firewall Threat Defense - Bootstrap Configuration

General Information Settings Agreement

Interface Information

Management Interface:

Address Type:

IPv4

Management IP:

Network Mask:

Network Gateway:

OK

Cancel

Bootstrap General Information

Choose OK and you can configure the Bootstrap settings using these:

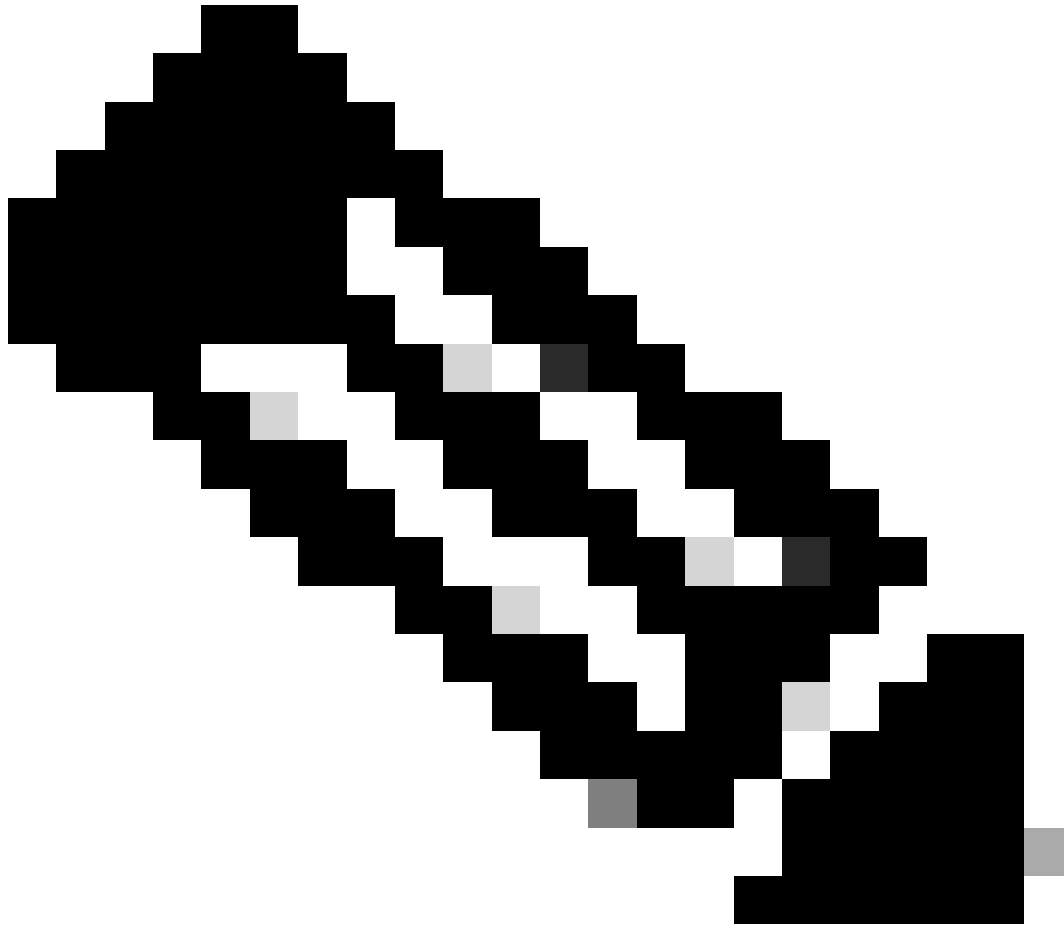
- Management type of application instance
- Search domains
- Firewall Mode
- DNS Servers
- Password
- Confirm Password

Cisco Secure Firewall Threat Defense - Bootstrap Configuration ? X

General Information Settings Agreement

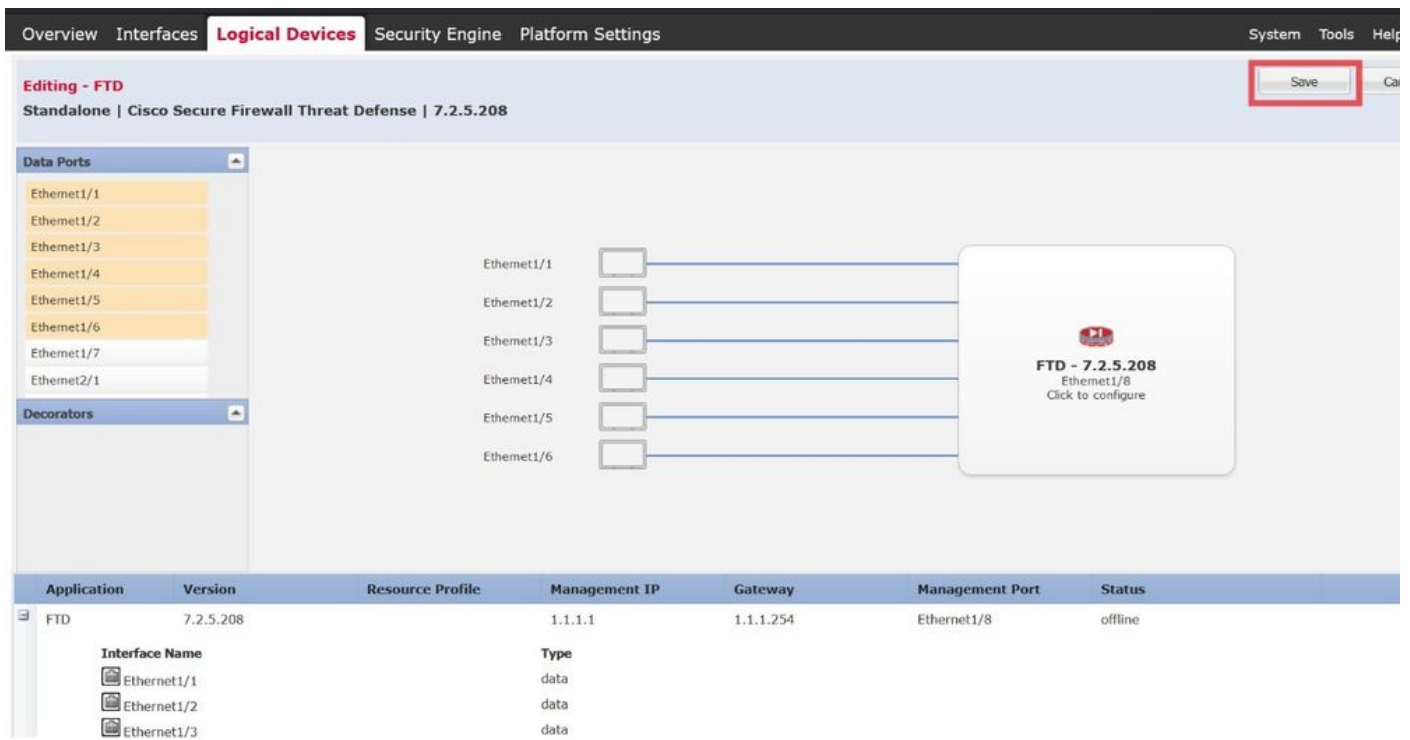
Management type of application instance:	<input type="text" value="FMC"/>
Search domains:	<input type="text" value="cisco.com"/>
Firewall Mode:	<input type="text" value="Routed"/>
DNS Servers:	<input type="text" value="1.1.1.5"/>
Fully Qualified Hostname:	<input type="text"/>
Password:	<input type="password" value="....."/>
Confirm Password:	<input type="password" value="....."/>
Registration Key:	<input type="text"/>
Confirm Registration Key:	<input type="text"/>
Firepower Management Center IP:	<input type="text"/>
Firepower Management Center NAT ID:	<input type="text"/>
Eventing Interface:	<input type="text"/>

Bootstrap Configuration Settings.



Note: You can configure FMC settings and register the FTD at this stage or later using the FTD CLI initial configuration.

Choose **Ok**, and **Save**:



The Logical Device List page is displayed automatically, and your Application Status is shown as Starting:



Logical Device List with Application Status as Starting.

You can also confirm and track the Logical instance status using the CLI. Connect via SSH or console to FPR4125 Chassis:

```
<#root>
```

```
FPR4125# scope ssa
```

```
FPR4125 /ssa # show app-instance
```

Admin State is **Enabled** and Operational State shows **Starting**:

```

FPR4125#
FPR4125#
FPR4125# scope ssa
FPR4125 /ssa # show app-instance
App Name Identifier Slot ID Admin State Oper State Running Version Startup Version Deploy Type Turbo Mode Profile Name Cluster State Cluster Role
-----
ftd FTD 1 Enabled Starting 7.2.5.208 7.2.5.208 Native No Not Applicable None
FPR4125 /ssa #
FPR4125 /ssa #
FPR4125 /ssa #
FPR4125 /ssa #

```

Operational State is Starting.

After a few minutes, the Operational State displays **Started**:

```

FPR4125 /ssa # show app-instance
App Name Identifier Slot ID Admin State Oper State Running Version Startup Version Deploy Type Turbo Mode Profile Name Cluster State Cluster Role
-----
ftd FTD 1 Enabled Started 7.2.5.208 7.2.5.208 Native No Not Applicable None
FPR4125 /ssa #
FPR4125 /ssa #

```

Operational state progressed to Started

App-Instance Operational State is switched to **Online**. At this point, the FTD Native logical instance has been completely installed in the FPR4125 Chassis and you can perform the initial configuration of FTD.

```

FPR4125 /ssa # show app-instance
App Name Identifier Slot ID Admin State Oper State Running Version Startup Version Deploy Type Turbo Mode Profile Name Cluster State Cluster Role
-----
ftd FTD 1 Enabled Online 7.2.5.208 7.2.5.208 Native No Not Applicable None
FPR4125 /ssa #
FPR4125 /ssa #

```

Operational State is switched to Online

The screenshot shows the FCM interface with the 'Logical Devices' tab selected. The 'Logical Device List' section displays one instance: 'FTD', which is 'Standalone' and has a 'Status: ok'. Below this, a detailed table shows the instance's configuration:

Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status
FTD	7.2.5.208		1.1.1.1	1.1.1.254	Ethernet1/8	Online

FCM shows FTD Logical instance is Online.

Verify

Finally, you can validate that the access to the FTD Logical Device is successful from FXOS CLI with these commands:

```
<#root>
```

```
FPR4125# connect module 1 console
```

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

Connecting to ftd(FTD) console... enter exit to return to bootCLI

> show version

```
FPR4125# 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
Connecting to ftd(FTD) console... enter exit to return to bootCLI
>
> show version
-----[ firepower ]-----
Model          : Cisco Firepower 4125 Threat Defense (76) Version 7.2.5 (Build 208)
UUID           : 4e5405da-5d80-11ee-b433-dcd3e27b0363
VDB version    : 353
-----
```


FTD Show version output

Manage Logical Instance

The **Edit** and **Options** icons are available within the **Logical Device List** tab on the right side.

Choosing options displays:

- Delete
- Set version
- Enable Link State

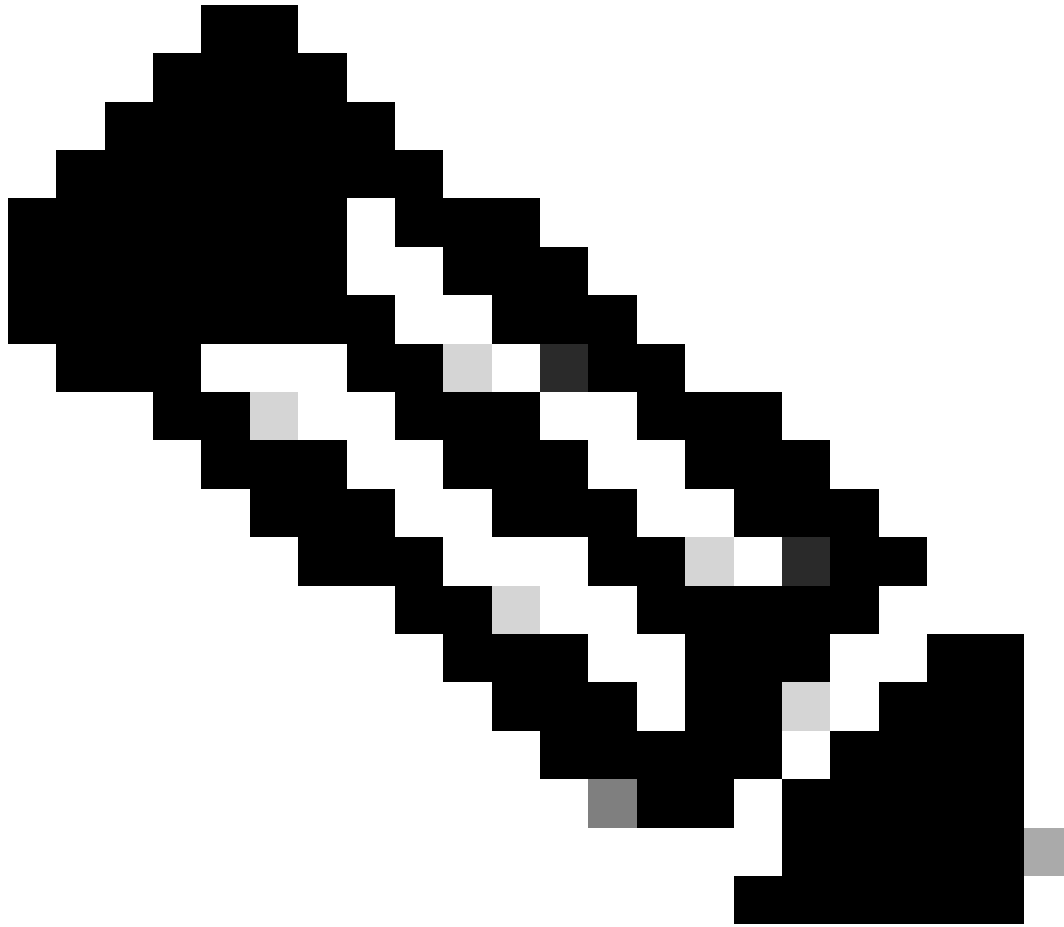
 Refresh Add ▾

Select Options Icon.

With the **Delete** option, you can completely remove the FTD Logical device instance from the chassis and release all resources dedicated to the FTD instance. This also causes the Security Module to restart.

Choosing the **Set Version** icon shows the Update Image version banner and you can choose the New Version to update FTD. Note that you are required to upload the FTD image file to the FPR4125 chassis beforehand.

Enable Link State is used when FTD is configured with an inline set interface and can enable link state propagation.



Note: For more information, refer to this document, section **Inline Set Link State Propagation for the FTD** -

https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide-v63/firepower_threat_defense_logical_devices.html.

Now, you can see the Disable, Set Version, Restart Instance, and Reinstall Instance icon options as shown in this image:



Disable, Set Version, Restart and Reinstall Icons



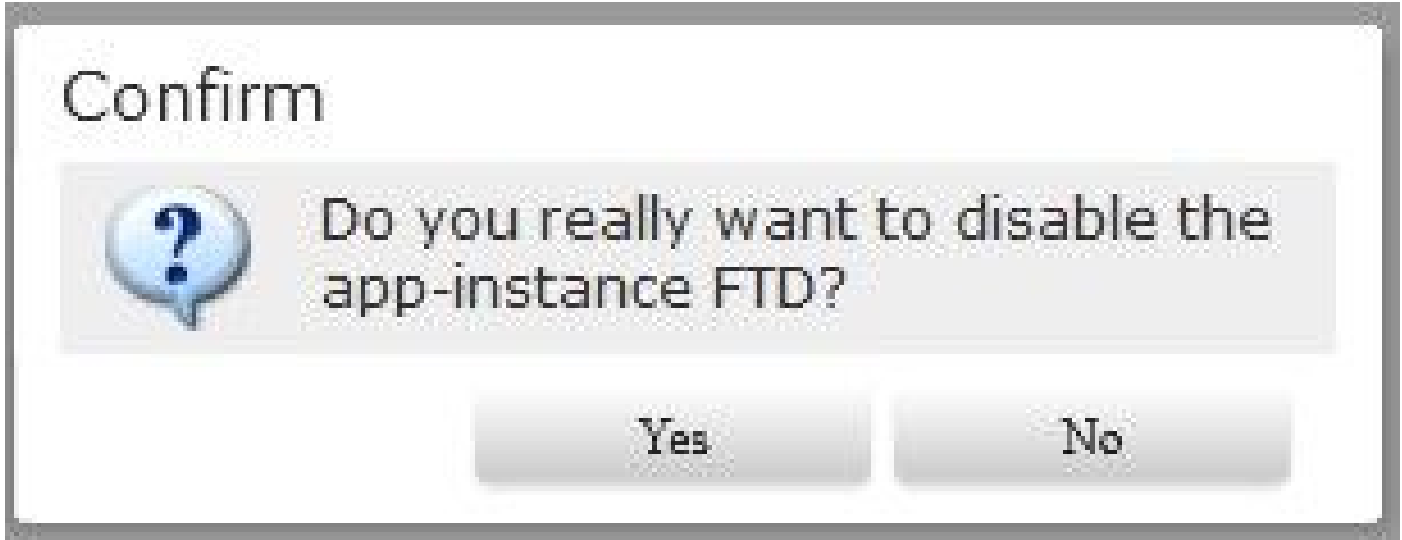
Warning: During normal operation of the FTD device **Disable**, **Restart**, and **Reinstall** options are not advised. If you are planning to perform an FTD reboot or restart, the recommended approach is to perform the said actions from the Cisco Secure Firewall Management Center or FTD CLI (graceful restart).

-
- Disable



Disable Icon.

This option disables and shuts down the FTD logical instance without removing any configuration. When you choose **Disable**, you see the confirmation banner as shown in this image:



Confirm Disable.

The Logical Instance Status is changed to **Stopping**:



The screenshot shows the 'Logical Devices' page in a management console. The breadcrumb navigation includes 'Overview', 'Interfaces', 'Logical Devices', 'Security Engine', and 'Platform Settings'. The page title is 'Logical Device List' and it indicates '(1 Native Instance) 0% (0 of 62) Cores Available'. A table lists the logical devices with columns for Application, Version, Resource Profile, Management IP, Gateway, Management Port, and Status. The FTD instance is shown with a status of 'Stopping'.

FTD	Standalone	Status					
Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status	
FTD			1.1.1.1	1.1.1.254	Ethernet1/8	Stopping	

Operational state is Stopping.

The FTD Logical Instance Status is switched to **Offline**:

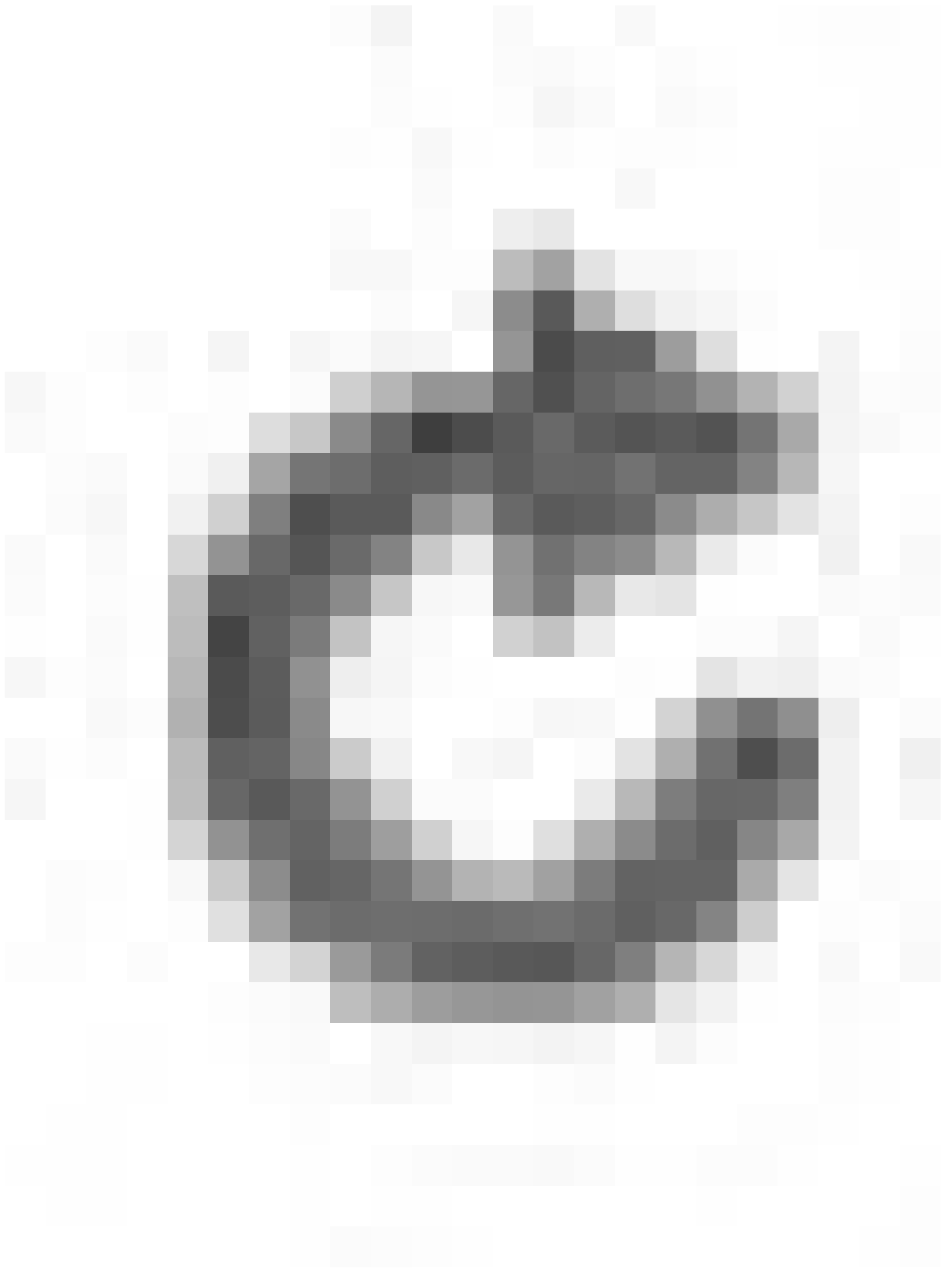


The screenshot shows the 'Logical Devices' page in a management console. The breadcrumb navigation includes 'Overview', 'Interfaces', 'Logical Devices', 'Security Engine', and 'Platform Settings'. The page title is 'Logical Device List' and it indicates '(1 Native Instance) 0% (0 of 62) Cores Available'. A table lists the logical devices with columns for Application, Version, Resource Profile, Management IP, Gateway, Management Port, and Status. The FTD instance is shown with a status of 'Offline'.

FTD	Standalone	Status					
Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status	
FTD			1.1.1.1	1.1.1.254	Ethernet1/8	Offline	

Operational State is Offline.

- Restart Instance



Restart Instance Icon.

This option is used to immediately restart the application instance and oftentimes can be used after modifying the bootstrap settings of a logical device.

- Reinstall Instance



Reinsall.

Choosing this option removes all application configurations and resets the factory settings on the FTD logical instance software. A confirmation banner is shown before proceeding:

Confirm



Warning: Application will be removed and reinstalled. All application configuration will be lost. Backing up your application configuration is strongly recommended before continuing.

Yes

No

Confirm Reinstall.

Troubleshoot

During abnormal operations, ungrateful or unexpected reboots of the device, the Operational Status of the logical instance can show abnormal states like 'Security Module not responding':

FTD	Standalone	Status				
Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status
FTD	7.2.5.208		1.1.1.1	1.1.1.254	Ethernet/9	Security module not responding

Operational State is Not Responding.

Navigate to the Security Engine tab. Service State of the Security engine shows Not-responding.

Hardware State	Service State	Power	Application
Up	Not-responding	On	Cisco Secure Firewall Threat Defense

Security Engine state is Not-responding.

You can validate the app-instance operational status from FXOS CLI by issuing this command:

```
<#root>
```

```
# show app-instance detail
```

Security Engine can be reset in case no critical or major security module faults are observed and the operational state of app instance is in *Starting*. CHOOSE *Reinitialize Security Engine*.



Warning: Ensure that you have a FTD configuration backup before proceeding.



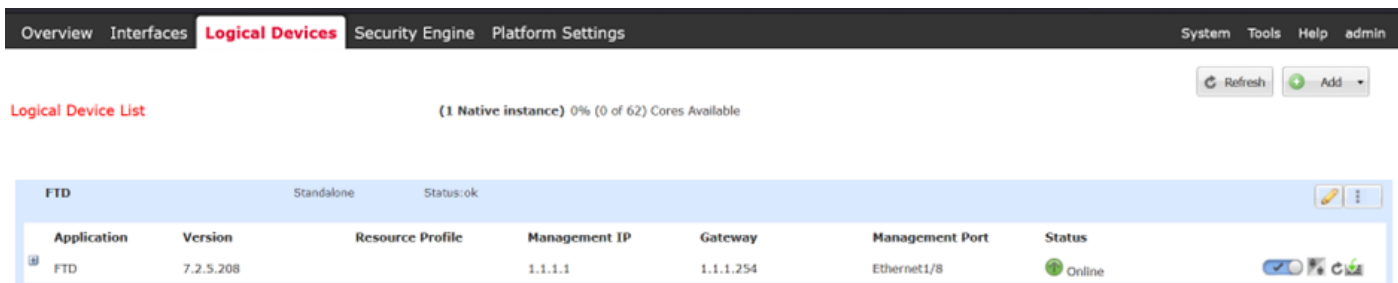
Reinitialize Security Engine

After 3-5 minutes, the Security Engine Service State is back to the **Online** State:

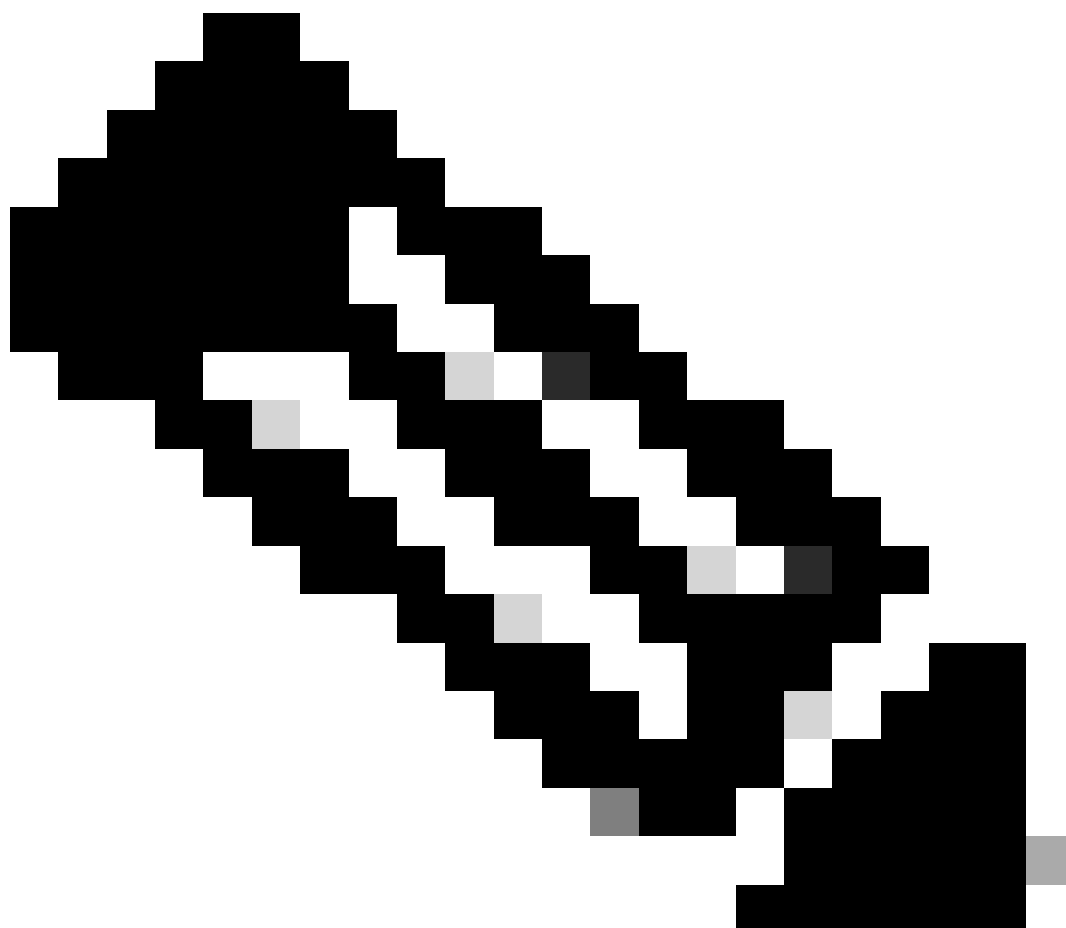


Security Engine State is Online.

Finally, the FTD Logical Instance is back to the **Online** state as well:



Logical Instance State is back to Online



Note: If the reason or scenario of the degraded operational state matches to the described example,

use these steps to fix the issue. For other reasons, it is recommended that you contact TAC.
