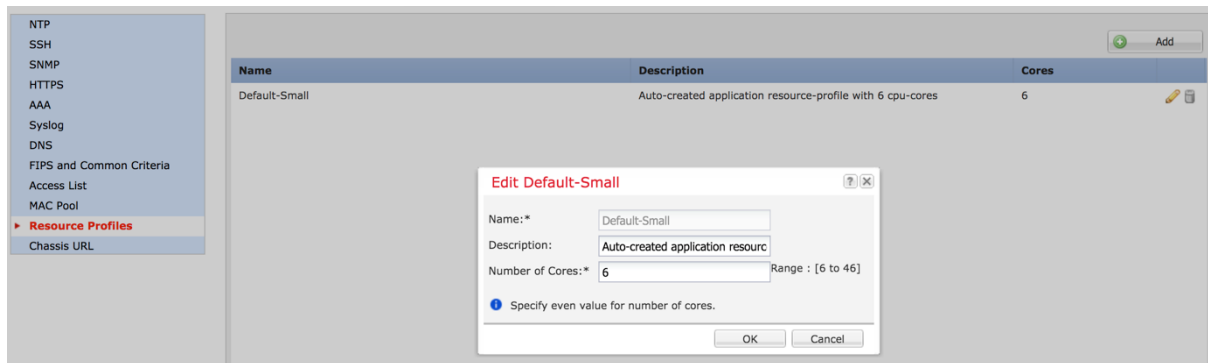


Firepower 4100/9300 FTD 6.3 Multi-instance Configuration Example


Introduction

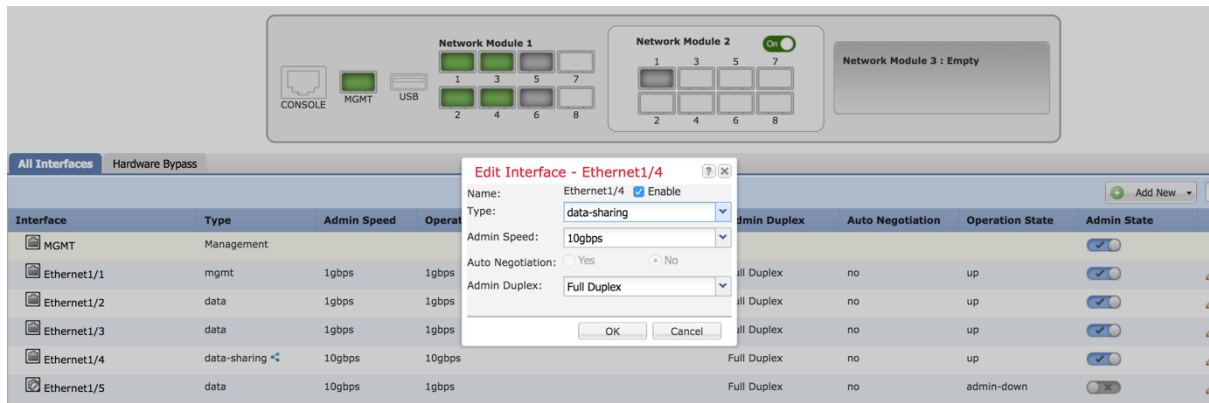
Multi-instance capability is similar to ASA multiple context mode, although the implementation is different. Multiple context mode partitions a single application instance, while multi-instance capability allows independent container instances. Container instances allow hard resource separation, separate configuration management, separate reloads, separate software updates, and full Firepower Threat Defense feature support. Multiple context mode, due to shared resources, supports more contexts on a given platform. Multiple context mode is not available on the Firepower Threat Defense.

Step 1. Add a Resource Profile for Container Instances



Step 2. Edit interfaces

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 ().



Interface	Type	Admin Speed	Operational Speed	Instances	VLAN	Admin Duplex	Auto Negotiation	Operation State	Admin State
MGMT	Management								Enabled
Ethernet1/1	mgmt	1gbps	1gbps			Full Duplex	no	up	Enabled
Ethernet1/2	data	1gbps	1gbps			Full Duplex	no	up	Enabled
Ethernet1/2.10	data				10				Enabled
Ethernet1/2.20	data				20				Enabled
Ethernet1/3	data	1gbps	1gbps			Full Duplex	no	up	Enabled
Ethernet1/4	data-sharing	10gbps	10gbps			Full Duplex	no	up	Enabled

Step 3. Add 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 module/engine, so you can only install one native instance.
- Container instance—A container instance uses a subset of resources of the security module/engine, so you can install multiple container instances. Multi-instance capability is only supported for the Firepower Threat Defense; it is not supported for the ASA.

Add Device

Device Name:

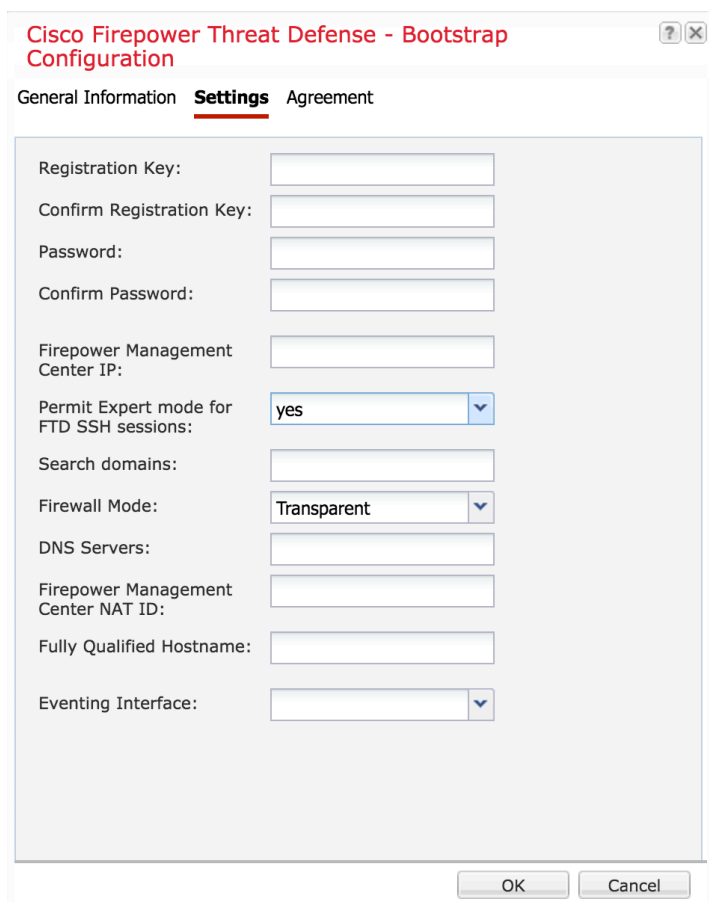
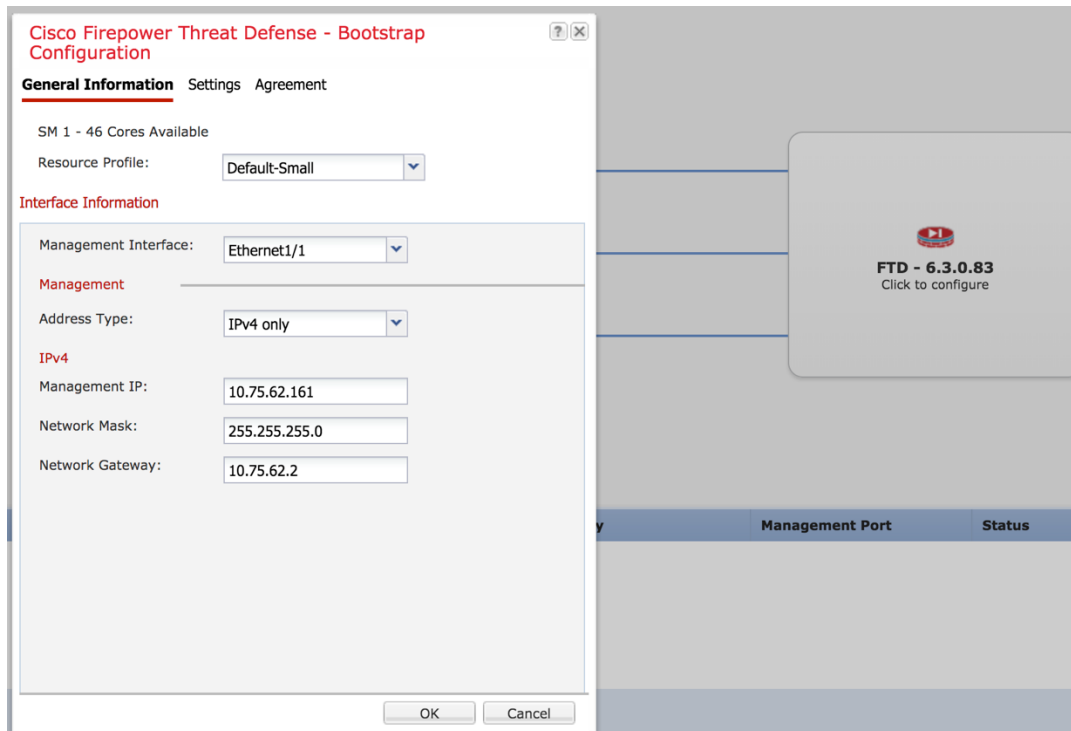
Template:

Image Version:

Instance Type:

Usage: Standalone Cluster

i 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.



Permit Expert mode from FTD SSH sessions

Expert Mode provides FTD 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.

Click **OK**. FTD installation starts automatically.

FTD-instance		Standalone	Status:ok				
Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status	
FTD	6.3.0.83	Default-Small	10.75.62.161	10.75.62.2	Ethernet1/1	Installing	

For the Firepower 9300, you can use a native instance on some modules, and container instances on the other module(s).

For the Firepower 4100, if a Native FTD application is installed, you need to delete it first. And when installing instances, you may get an error message:

Application installation failed. Reason: container support requires Blade reinitialization (Disk Format).

FTD-instance		Standalone	Status:ok				
Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status	
FTD	6.3.0.83	Default-Small	10.75.62.161	10.75.62.2	Ethernet1/1	Install-failed	Application installation failed. Reason: Container support requires Blade reinitialization (Disk Format)

FPR4100 /ssa # show app-instance de

```

App Name: ftd
Identifier: FTD-instance
Slot ID: 1
Admin State: Disabled
Oper State: Install Failed
Running Version:
Startup Version: 6.3.0.83
Deploy Type: Container
Profile Name: Default-Small
Cluster State: Not Applicable
Cluster Role: None
Current Job Type: Install
Current Job Progress: 0
Current Job State: Failed
Clear Log Data: Available
Error Msg: Container support requires Blade reinitialization (Disk Format)
Hotfixes:
Externally Upgraded: No
  
```

- Reinitialize the security engine

Hardware State	Service State	Power	Application
Up	Offline	On	Cisco Firepower Threat Defense

- Check reinitialization progress

```
FPR4100 /ssa # show slot 1 de
```

Slot:

```
Slot ID: 1
Log Level: Info
Admin State: Ok
Oper State: Offline
Disk Format State: Formatting
Disk Format Status: 97%
Clear Log Data: Available
Error Msg:
```

```
[FPR4100 /ssa # show slot 1 de
```

Slot:

```
Slot ID: 1
Log Level: Info
Admin State: Ok
Oper State: Offline
Disk Format State: Ok
Disk Format Status: 100%
Clear Log Data: Available
Error Msg: _
```

Hardware State	Service State	Power	Application
Up	Online	On	Cisco Firepower Threat Defense

Once the security engine is online, FTD installation starts automatically.

Step 4. Register FTD instances to FMC

Name	Model	Version	Chassis	Licenses	Access Control Policy
Ungrouped (2)					
FTD-Instance 10.75.62.161 - Routed	FTD on Firepower 4120	6.3.0	FPR4100-443 Security Module - 1 (Container)	Base, Threat (2 more...)	None
FTD-Instance1 10.75.62.162 - Transparent	FTD on Firepower 4120	6.3.0	FPR4100-443 Security Module - 1 (Container)	Base, Threat (2 more...)	None