



Configure

- [Background, on page 1](#)
- [Register the FTD Appliance, on page 1](#)
- [Create a Service Graph, on page 10](#)
- [Apply a Service Graph Template, on page 11](#)
- [Supported Functions, on page 14](#)
- [FTD Deployments, on page 19](#)

Background

The ACI fabric provides for integration of L4-L7 services as an integral part of an application. This is accomplished through the use of an APIC-managed service graph, which requires a L4-L7 device package. The imported device package exposes configuration parameters in APIC, and allows it to orchestrate a given configuration onto the device.

To install the L4-L7 service graph, register a L4-L7 device with the APIC, add its configuration as part of a Function Profile or L4-L7 Service Parameters, and link those two with a service graph. Once you apply this L4-L7 service graph to a contract, the APIC renders it in the fabric by tagging device interfaces and stitching them to appropriate consumer and provider EPGs. The APIC then applies a given configuration to the registered device in an automated fashion. Once all of the configuration is applied to the ACI fabric and the L4-L7 device, the ACI fabric directs traffic defined by the contract to a given device for inspection. The ACI also allows you to chain multiple services together under a single service graph.

Register the FTD Appliance

Before you register the FTD device with the APIC, add its FMC management station as an APIC Device Manager. In this hybrid service graph model, the APIC and the FMC share full responsibility for the FTD configuration. The APIC provisions configuration of the interfaces, IP addresses, security zones, BVIs, and NGIPS inline pairs, while the FMC defines the threat policies and rules that govern communication between EPGs. Add the FMC as a device manager, and register your FTD appliance with the APIC in order to utilize it in a service graph.



Note One FMC can be used as a device manager for multiple FTD devices provisioned for multiple service graphs.

Before you begin

- Configure the APIC Communication Policy to allow HTTP communication.
- Configure either a Virtual Machine Manager or Physical Domain.
- Configure a tenant. The steps in this section require an existing tenant.

- Step 1** Sign in to the APIC.
- Step 2** On the menu bar, click **Tenants**.
- Step 3** In the navigation pane, expand the **Tenant** branch, expand the **L4-L7 Services** branch, and click **Device Managers**.
- Step 4** Select **Actions > Create Device Manager**.
- Step 5** Complete the following options:

Option	Description
Device Manager Name	Name of the device manager.
Device Manager Type	Select CISCO-FTDmgr_FI-1.0 .
Management	Click "+" to add an FMC, which manages an FTD appliance, and complete the Host and Port fields. Click Update .
Username	Username of the FMC.
Password	Password of the FMC.
Confirm Password	Password of the FMC.

The screenshot displays the 'Device Managers' configuration page. On the left, the navigation tree is expanded to 'L4-L7 Services' > 'L4-L7 Devices'. The main content area shows a 'Create Device Manager' modal window. The form fields are as follows:

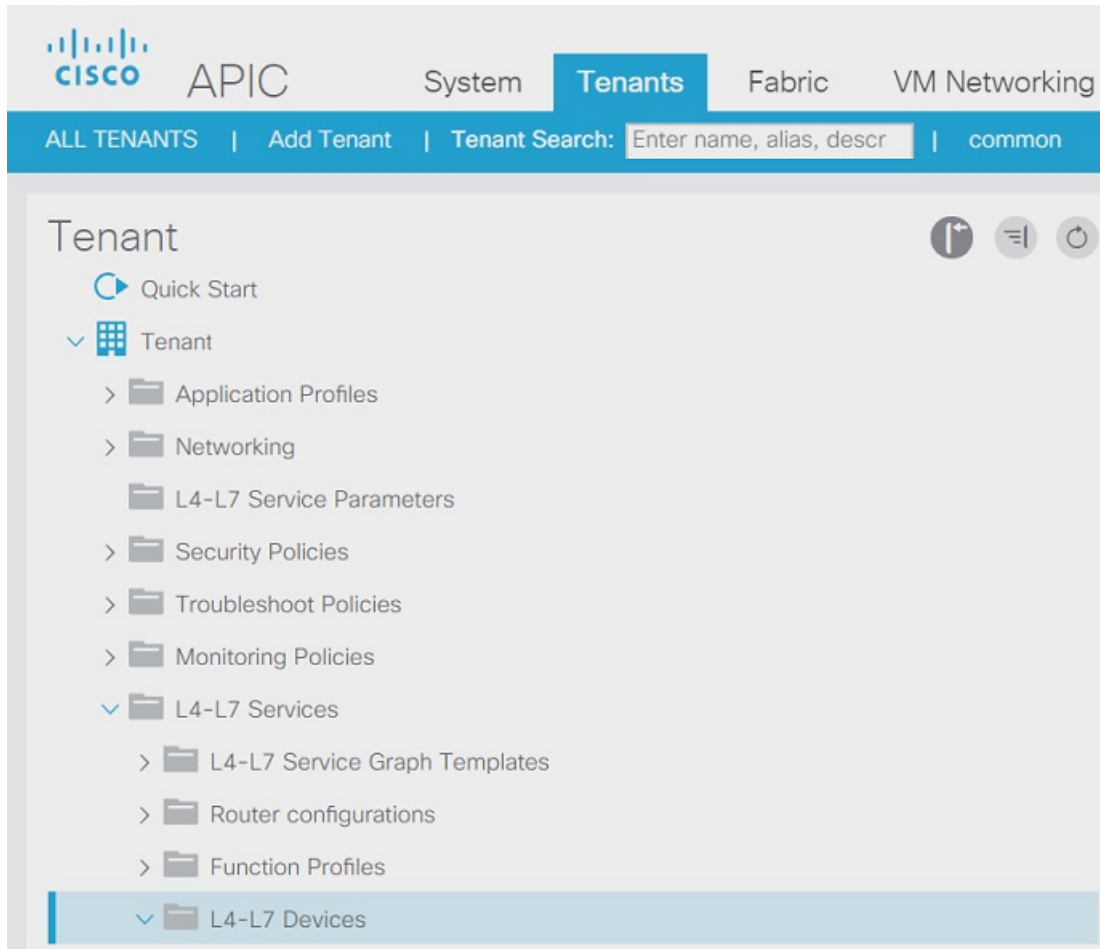
- Device Manager Name: StrictFMC
- Management EPG: select an option (with a note: 'This is required only for inband management.')
- Device Manager Type: CISCO-FTDmgr_FI-1.0
- Management:

Host	Port
10.254.6.84	443
- Username: aciadmin
- Password:
- Confirm Password:

Buttons for 'SUBMIT' and 'CANCEL' are located at the bottom right of the modal.

Step 6 Click **Submit** to create the device manager.

Step 7 In the navigation pane, expand the **Tenant** branch, expand the **L4-L7 Services** branch, and click **L4-L7 Devices**.



Step 8 Right-click and select **Create L4-L7 Devices**. The **Create L4-L7 Devices** dialog box appears, showing the **General** page.

Step 9 Complete the following:

Option	Description
Name	Name of the FTD appliance. Note FMC fields are limited to 48 characters and are saved on the FMC as "<Field Value> _<Tenant Name> _<L4-L7 Device Name>" so we recommend you reduce your tenant and device name lengths to accommodate this limit.
Service Type	Select Firewall .
Device Type	Select PHYSICAL or VIRTUAL .
Device Package	Select the device package you've uploaded.
Model	Select the model of the FTD appliance.
Context Aware	Allocate an appliance to a tenant.

Option	Description
	<p>Note Multiple is not recommended.</p> <p>Single means that the appliance cluster cannot be shared across multiple tenants of a given type which are hosted on the provider network.</p> <p>Multiple means that the appliance cluster can be shared across multiple tenants of a given type which you are hosting on this provider network. For example, there could be two hosting companies that share the same appliance. The tenancy assignment is implicitly based on the endpoint group (EPG) to which the package is bound. If you created a cluster, you must specify the management EPG, which determines the network through which the appliance would be managed.</p>
Function Type	<p>Select GoThrough or GoTo.</p> <p>A GoThrough appliance is a transparent firewall (uses BVIs) or NGIPS mode (uses IPS-only ports) appliance. Network packets traverse the appliance with being modified and endpoints are not aware of that appliance. A GoTo appliance is a routed firewall mode and acts as a specific L3 destination to L2-attached EPGs.</p>
Physical Domain	<p>For physical FTD appliances, select the domain to use when allocating network resources for the graphs that use this appliance cluster. Select an existing physical domain or configure a new one.</p> <p>Note This is not required for a virtual FTD appliance.</p>
View	<p>Defaults to Single Node. Shows you Device 1 to configure.</p> <p>Note Starting in 1.0.2, HA Node is supported. When HA Node is selected, both Device 1 and Device 2 in the HA device pair are shown for you to configure.</p> <p>Note Starting in 1.0.3, clustering is supported. When Cluster is selected, multiple devices can be added with its own management addresses.</p>
VMM Domain	<p>For a virtual FTD appliance, select the Virtual Machine Manager (VMM) domain (vCenter domain). Select an existing VMM domain or configure a new one.</p> <p>Note This is not required for a physical FTD appliance.</p>
Username	Username of the FMC.
Password	Password of the FMC.
Confirm Password	Password of the FMC.

Step 10 In the **Device 1** section, complete the following options:

Option	Description
Management IP Address	IP address of the management interface for the concrete appliance in the appliance cluster.
Management Port	Select HTTP or HTTPS.
VM	For a virtual FTD, name of the virtual machine on which the appliance is hosted. Note This is not required for a physical FTD appliance.

Step 11 For Device Interfaces, click "+" to enter information for a concrete interface, which is the interface on the concrete appliance. The information that you enter specifies how the concrete interfaces are connected to the fabric and how the concrete interfaces are mapped to the logical interfaces. Click Update to add the interface. Complete the following options:

Option	Description
Name	Name field identifies an interface on the concrete appliance. For example, GigabitEthernet0/1 or GigabitEthernet0/2.
Path	For physical appliances, specify how the concrete interface attaches to the fabric. For example, the leaf node/slot/port to which the concrete interface is attached.
vNIC	For virtual appliances, the network adapter name that was assigned on the vCenter for identifying the corresponding interface of a concrete appliance. Usually on the vCenter, a vNIC is labeled Network adapter x , where x = 1, 2, 3... Note You can check the interface MAC address on the appliance, and then identify the corresponding vNIC on the vCenter by matching the MAC address field.

Step 12 If **View: HA Node** is selected, then also complete the corresponding options in the **Device 2** section. Devices 1 and 2 form the HA failover pair.

For example:

Device 1

Management IP Address:

VM: 

Chassis:

Management Port:

Device Interfaces:

Name	VNIC	Path (Only For Route Peering)
GigabitEthernet0/0	Network adapter 2	
GigabitEthernet0/1	Network adapter 3	

Device 2

Management IP Address:

VM: 

Chassis:

Management Port:

Device Interfaces:

Name	VNIC	Path (Only For Route Peering)
GigabitEthernet0/0	Network adapter 2	
GigabitEthernet0/1	Network adapter 3	

If **View: Cluster** is selected:

General

Managed:

Name:

Service Type:

Device Type: PHYSICAL VIRTUAL

Physical Domain:

View: Single Node HA Node Cluster

Device Package:

Model:

Promiscuous Mode:

Context Aware: Multiple Single

Function Type: GoThrough GoTo

Connectivity

APIC to Device: Out-Of-Band In-Band

Credentials

Username:

Password:

Confirm Password:

Devices

Name	Management Address	Management Port	Interfaces
FTDmaster	192.168.102.152	443	Port-channel1 (Pod-1), Port-channel2 (Pod-1)
FTDslave	192.168.102.153	443	Port-channel1 (Pod-1), Port-channel2 (Pod-1)

Cluster

Management IP Address:

Management Port:

Device Manager:

Cluster Interfaces:

Type	Name	Concrete Interfaces
consumer	outside	FTDmaster/Port-channel1,FTDslave/F
provider	inside	FTDmaster/Port-channel2,FTDslave/F

Step 13 In the **Cluster** section, complete the following options:

Option	Description
Management IP Address	IP address of the FMC.
Management Port	Port number of the FMC.
Device Manager	Select the device manager.

Step 14 For Cluster Interfaces, click "+" to enter information for a cluster interface, which is the cluster logical interface. The information that you enter specifies how the logical interfaces are connected to the fabric and how the logical interfaces are mapped to the appliance concrete interfaces. Click Update to add the interface. Complete the following options:

Option	Description
Type	Type of cluster logical interface. For example, consumer or provider .
Name	Name field identifies an interface on the graph. For example, external or internal .

Option	Description
Concrete Interfaces	Specify how the logical interface attaches to the appliance concrete interface.

Step 15 For Cluster Interfaces, specify the interfaces for both members of the HA device pair.
For example:

Cluster

Management IP Address: Management Port:

Device Manager:

Cluster Interfaces:

Type	Name	Concrete Interfaces
<input type="text" value="consumer"/>	<input type="text" value="external"/>	<input type="text" value="Device2/GigabitEthernet0/0"/> Device1/GigabitEthernet0/0 Device1/GigabitEthernet0/1 Device2/GigabitEthernet0/0 Device2/GigabitEthernet0/1

Cluster

Management IP Address: Management Port:

Device Manager:

Cluster Interfaces:

Type	Name	Concrete Interfaces
consumer	external	Device1/GigabitEthernet0/0,Device2/GigabitEthernet0/0
provider	internal	Device1/GigabitEthernet0/1,Device2/GigabitEthernet0/1

Step 16 Click **Next**.

Step 17 (Optional) Add configuration parameters. The configuration parameters are for the concrete appliance and are used during the one-time configuration at the time of initialization.

Step 18 Click **Finish** to create the appliance.

What to do next

If you select your FTD device under L4-L7 Devices, it should show a 'stable' state if the APIC was able to register it properly. If it was unable to reach your FMC or find a registered FTD with a given IP address on the FMC, an error is displayed. Refer to the **Troubleshoot** chapter to understand and resolve L4-L7 device faults. Ensure that your FTD device is in a 'stable' state before creating a service graph with its L4-L7 configuration.

Create a Service Graph

A service graph is an ordered set of function nodes between a set of terminals, which identifies a set of network service functions that are required by an application. Service functions within a graph are automatically provisioned on a service device that is based on an application's requirements.

After you register an appliance, you can create service graphs using that appliance and all the functions that appliance has exposed. The service graph can be created under the common tenant or can be tenant-specific. This can be done by the provider administrator or by the tenant administrator within its own tenancy.

To insert an FTD as a service function, the service graph template needs to be created using the FTD Function Node.

-
- Step 1** Sign in to the APIC.
 - Step 2** Navigate to a common tenant or specific tenant.
 - Step 3** In the navigation pane, expand the **L4-L7 Services** branch, and click **L4-L7 Service Graph Templates**.
 - Step 4** Select **Actions > Create L4-L7 Service Graph Template**.

Note The **Create L4-L7 Service Graph Template** dialog box appears. The left pane lists the service devices that the APIC knows about and the service functions that are provided by those devices. The APIC obtained this information from the FTD for ACI device package you previously imported.

Create L4-L7 Service Graph Template
i X

Drag device clusters to create graph nodes.

Device Clusters


+ -

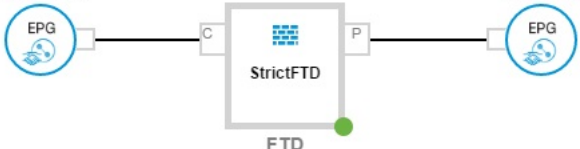
svcType: FW

SampleTenant/StrictFTD (Managed)


Graph Name:

Graph Type: Create A New One Clone An Existing One

Consumer




FTD

Provider


Please drag a device from devices table and drop it here to create a service node.

StrictFTD Information

Firewall:
 Routed
 Transparent

Profile: CISCO-FTD_FI-1.0/RoutedModeForF v +

Route Redirect:

- Step 5** Complete the **Graph Name** field with the name of the service graph.
- Step 6** Drag and drop an FTD service function from the left pane to the right pane to add that function to the service graph.
- Step 7** Change the name of the node.
- Step 8** Select the type of firewall mode, **Routed** or **Transparent**, based on your deployment.
- Step 9** Select a profile for the service node. Select a function profile in the default templates that come with the device package or that you created before.
- Step 10** Click **Submit** to create the graph.
The **Service Graph** dialog box should list the new graph that you created.

Apply a Service Graph Template

The APIC automatically configures services according to the service function requirements that are specified in the service graph. The APIC also automatically configures the network according to the needs of the service function that is specified in the service graph; no change in the service device is required.

The APIC passes the parameters to the appliance script within the device package. The appliance script converts the parameter data to the configuration that is downloaded onto the appliance. It assumes application profile, EPGs, and contract exists under a specific tenant to associate a created service graph.

Complete the following steps to associate a service graph with a contract.

Before you begin

Configure a tenant.

Configure an application profile with EPGs.

Step 1 Sign in to the APIC.

Step 2 On the menu bar, click **Tenants**.

Step 3 In the navigation pane, expand the tenant's folder tree.

Step 4 Expand the **L4-L7 Services > L4-L7 Service Graph Templates** branch to show the service graph templates.

Step 5 Right-click the service graph template of your choice, and in the pop-up menu that appears, click **Apply L4-L7 Service Graph Template**.

Step 6 In the **Step 1 Contract** dialog box, select the Consumer and Provider EPGs.

Step 7 Create a new contract, or choose an existing contract subject. Enter a name for the new contract. Click **Next**.

Step 8 In the **Step 2 Graph** dialog box, select the bridge domains (BDs) and Cluster Interfaces. Click **Next**.

Apply L4-L7 Service Graph Template To EPGs

STEP 2 > Graph

1. Contract 2. Graph 3. StrictFTD Parameters

Config A Service Graph

Device Clusters

SampleTenant/StrictFTD (Managed Firewall)

Graph Template: SampleTenant/WebGraph

StrictFTD Information

Firewall: routed

Profile: RoutedModeForFTD

Consumer Connector

Type: General Route Peering

BD: SampleTenant/AppBD
The Bridge Domain that connects the two devices

Cluster Interface: external

Provider Connector

Type: General Route Peering

BD: SampleTenant/WebBD
The Bridge Domain that connects the two devices

Cluster Interface: internal

PREVIOUS NEXT CANCEL

Step 9 In the **Step 3 Parameters** dialog box, click the **All Parameters** tab.

Apply L4-L7 Service Graph Template To EPGs
i
✕

STEP 3 > StrictFTD Parameters

1. Contract
2. Graph
3. StrictFTD Parameters

config parameters for the selected device

Profile Name:
RoutedModeForFTD

Features:
Required Parameters
All Parameters

	Folder/Param	Name	Value	Write Domain
<div style="font-size: 0.8em; margin-bottom: 5px;">Interfaces</div> <div style="margin-bottom: 5px;">All</div> <div style="font-size: 0.8em;">+</div>	Device Config	Device		
	Access Policy	ACIAccPolicyRouted		
	Bridge Group Interface			
	Inline Set			
	Interface	externalInterface		
	Interface	internalInterface		
	Security Zone	ExternalSZRT		
	Security Zone	InternalSZRT		
	Function Config	Function		
	Access Policy Configuration	AccessPolicyFolder		
	Bridge Group Interface Configuration			
	External Interface Configuration	ExtConfig		
	Internal Interface Configuration	IntConfig		

RED indicators parameters needed to be updated and GREEN indicates parameters will be submitted to the provider EPG.

PREVIOUS
FINISH
CANCEL

Step 10

Configure the parameters based on your deployment. You can define a function profile based on a built-in template and use that in this step. See the sections below on Supported Functions and FTD Deployments. Click **Finish** to attach the contract to the service graph.

What to do next

Once the service graph is instantiated, verify that the APIC pushed the provisioned configurations to the FTD interfaces into the FMC correctly.

Also, verify that end points can communicate to each other using the provisioned FTD.

Supported Functions

This section describes the exposed functionality supported by the FTD for ACI device package.



Note An asterisk ("*") indicates that the option is required. Otherwise, it's optional.



Note The GraphDeploymentSuffix is "_<Tenant Name>_<Device Name>" and gets appended to a value where specified below.



Note For any unsupported FTD feature, we recommended that you clean up the configuration manually before removing a service graph or deleting the tenant.

Function	Parameter	Options		Description
Access Policy	*Name	<name>		Name of the access policy. <ul style="list-style-type: none"> The APIC internally adds a GraphDeploymentSuffix and other information to the Policy description. Pre-existing FMC Access Policy name must match for the APIC to use.
	*Access Rules	*Name	<name>	Name of the access rule. <ul style="list-style-type: none"> The APIC internally adds a GraphDeploymentSuffix and other information to the Rule comment. Pre-existing FMC Access Rule name must match for the APIC to update with the created Service Graph Security Zones.
		Source Interface	Reference to Interface Object Security Zone	—
		Destination Interface	Reference to Interface Object Security Zone	—
		Bi-directional	true false	If set to true, applies both Security Zones under Access Rule Source and Destination Zones. Otherwise, Security Zones are individually applied Source and Destination fields.

Security Zone	*Name	<name>	<p>Name of the security zone. Also, APIC folder name of the security zone object, so that other APIC objects can reference it.</p> <p>The APIC internally adds a GraphDeploymentSuffix to the name. For example, if you select a Security Zone name of External, on the FMC you'll see a Security Zone named External_<Tenant Name>_<Device Name>.</p> <p>Note The name field gets saved as <Field Value>_<Tenant Name>_<Device Name> on the FMC which is limited to a total of 48 characters. Since the GraphDeploymentSuffix can use up to 40 characters, try to limit the name field value to 8 characters.</p>
	*Type	INLINE ROUTED SWITCHED	<p>Type of the security zone.</p> <p>A mismatched security zone type and interface type are not allowed. It's based on deployment mode.</p>

Inline Set	*Name	<name>	<p>Name of the inline set. Also, APIC folder name of the inline set object, so that other APIC objects can reference it.</p> <p>The APIC internally adds a GraphDeploymentSuffix to the name. For example, if you select an Inline Set name of External, on the FMC you'll see an Inline Set named External_<Tenant Name>_<Device Name>.</p> <p>Note The name field gets saved as <Field Value>_<Tenant Name>_<Device Name> on the FMC which is limited to a total of 48 characters. Since the GraphDeploymentSuffix can use up to 40 characters, try to limit the name field value to 8 characters.</p>
	*MTU	<integer>	MTU property of the Inline Set.
	*Snort Fail Open Busy	true false	Snort Fail Open Busy property of an Inline Set.
	*Snort Fail Open Down	true false	Snort Fail Open Down property of an Inline Set.

Interface	*Name	<name>			APIC folder name of the interface object.
	*Enabled	true false			Enable property of the interface.
	*MTU	<integer>			MTU property of the interface.
	*Logical Name	<name>			<p>Logical name of the interface (optional unless Inline).</p> <p>The APIC internally adds a GraphDeploymentSuffix to the name. For example, if you select a Logical Name of External, on the FMC you'll see a Logical Name of External_<Tenant Name>_<Device Name>.</p> <p>Note The name field gets saved as <Field Value>_<Tenant Name>_<Device Name> on the FMC which is limited to a total of 48 characters. Since the GraphDeploymentSuffix can use up to 40 characters, try to limit the name field value to 8 characters.</p>
	*Inline Set	Inline Set Object			Reference link to the APIC Inline Set folder object.
	*Security Zone	Security Zone Object			Reference link to the APIC Security Zone folder object.
	*IPv4	*static	*address	IPv4 address with subnet mask	Applies only to routed interfaces. Values are the IPv4 address with a subnet mask. For example, 1.1.1.1/24

Bridge Group Interface	*Name	<name>			APIC folder name of the bridge group interface. The APIC internally adds a GraphDeploymentSuffix and other information to the description.
	*IPv4 Address Configuration	*static	*address	IPv4 address with subnet mask	Applies only to transparent interfaces. Values are the IPv4 address with a subnet mask. For example, 1.1.1.1/24
	*Bridge Group ID	<integer>			—
	*Interfaces	—			Reference link to the APIC interface folder object.
IPv4 Static Route	*Network	<network>			The foreign network for this route. Must be in A.B.C.D/prefix format. For example, 192.168.1.0/24
	*Gateway	<gateway>			The IPv4 address of the gateway by which the foreign network is reached. For example, 192.168.1.1
	Metric	<integer>			Distance metric for this route. Valid range is a number between 1 and 255, inclusive.
	isTunneled	true false			—
	<ul style="list-style-type: none"> • For routed-mode FTD, if an IPv4 static route is to be configured, configure it at the physical-interface level. However, if physical interfaces are put into the BVI interface (IRB feature), configure the IPv4 static route at the BVI-interface level. • For transparent-mode FTD, if an IPv4 static route is to be configured, configure it at the physical-interface level, no matter the BVI configuration. 				

FTD Deployments

This section describes the function profile configuration changes required for the various deployment modes. All three modes require you to reference the appropriate access control policy or rules:

- Verify that the Access Policy name is set correctly.
- Verify that the Access Rules under the Access Policy are set correctly, with source and destination Security Zone mappings pointing to the correct interfaces. Ensure that the Bi-directional flag is set to apply both interfaces' Security Zones to Access Rule Source and Destination Zones.

Transparent Mode

Select the default function profile **CISCO-FTD_FI-1.0/TransparentModeForFTD** and:

- Verify that the Bridge Group ID (**Device Config > Bridge Group Interface > Bridge Group ID > Value**) is a unique number. Set the Bridge Group Interface IP address, and ensure the interfaces are configured correctly.
- Verify that the Security Zone name (**Device Config > Security Zone > Name**) is set correctly and its type is set to SWITCHED.
- Verify that the Logical Name of the Interface is unique (**Device Config > Interface (either internal or external) > Logical Name > Value**). Ensure that the Enabled flag is set to true and the Security Zone is mapped correctly.

Routed Mode

Select the default function profile **CISCO-FTD_FI-1.0/RoutedModeForFTD** and:

- Verify that the Security Zone name (**Device Config > Security Zone > Name**) is set correctly and its type is set to ROUTED.
- Verify that the Logical Name of the Interface is unique (**Device Config > Interface (either internal or external) > Logical Name > Value**). Ensure that the Enabled flag is set to true and the Security Zone is mapped correctly. Set the Interface IP address.

Inline Mode

Select the default function profile **CISCO-FTD_FI-1.0/InlineModeForFTD** and verify:

- Verify that the Inline Set name (**Device Config > Inline Set > Name**) is set correctly.
- Verify that the Security Zone name (**Device Config > Security Zone > Name**) is set correctly and its type is set to INLINE.
- Verify that the Logical Name of the Interface is unique (**Device Config > Interface (either internal or external) > Logical Name > Value**). Ensure that the Enabled flag is set to true and the Inline Set and Security Zone are mapped correctly.