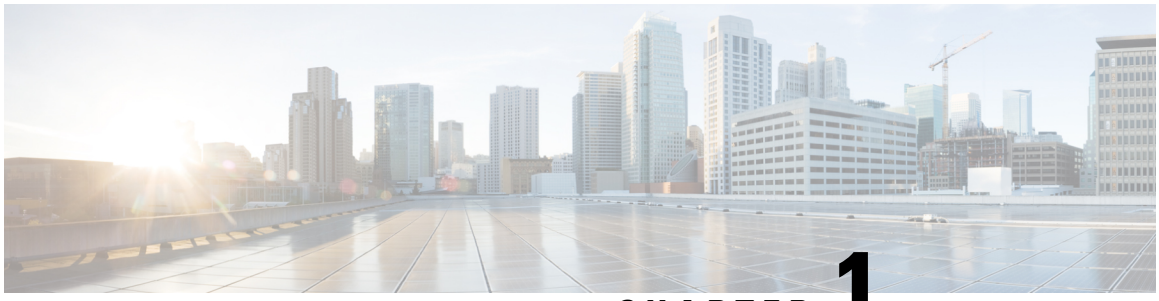
# Cisco Firepower Threat Defense Device Package Quick Start Guide for APIC Integration, 1.0.5

**First Published:** 2019-11-13

**Last Modified:** 2019-11-13

**Americas Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CHAPTER 1

# Introduction



## Overview

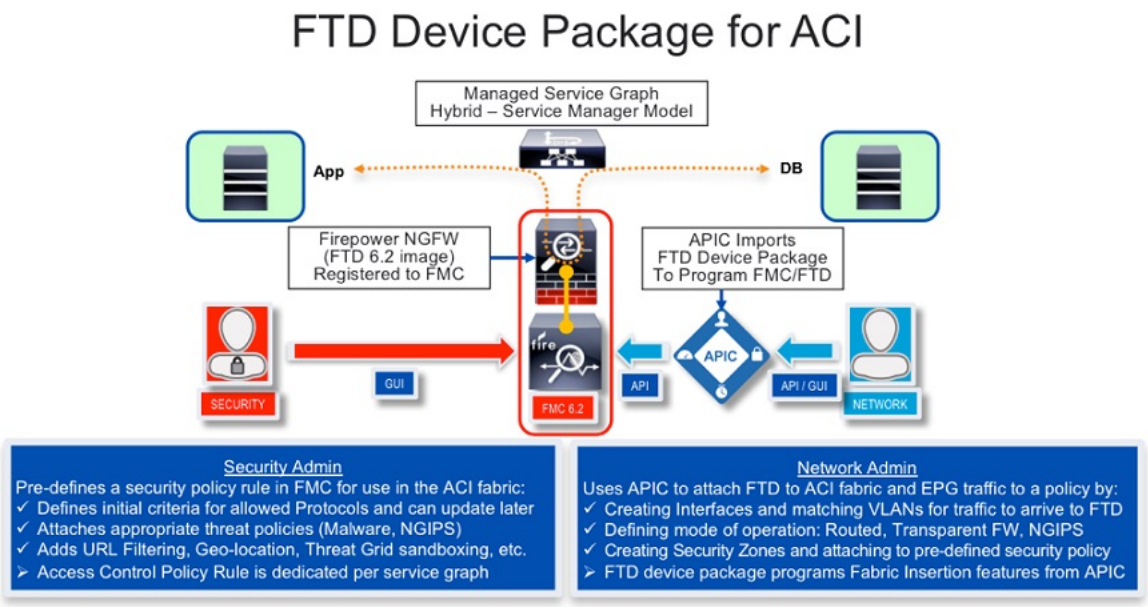
The Cisco Application Policy Infrastructure Controller (APIC) is a single point of control for centralized functions on the Cisco Application Centric Infrastructure (ACI). The APIC can automate the insertion of services such as a Cisco Firepower Threat Defense (FTD) northbound between applications, also called endpoint groups (EPGs). The APIC uses northbound Application Programming Interfaces (APIs) for configuring the network and services. You use these APIs to create, delete, and modify a configuration using managed objects.

To configure and monitor service devices, the APIC requires a device package. A device package manages a class of service device and provides the APIC with information about the device so that the APIC knows what the device can do. By using a device package, you can insert and configure network service functions on a service device such as an FTD appliance.

The FTD Fabric Insertion (FI) Device Package is based on a hybrid model (Service Manager, in ACI terminology) where the responsibility of the full-device configuration is shared between security and network administrators:

- Security administrator. Uses the FMC to pre-define a security policy for the new service graph, leaving Security Zone criteria unset. The new policy rule(s) defines appropriate access (allowed protocols) and an advanced set of protections such as NGIPS and malware policy, URL filtering, Threat Grid, and more.
- Network admininistrator. Uses the APIC to orchestrate a service graph, insert an FTD device into the ACI fabric, and attach directed traffic to this pre-defined security policy. Inside the APIC's L4-L7 Device Parameters or Function profile, the network administrator sets parameters defined in this guide, including matching a pre-defined FMC Access Control Policy and Rule(s).

When the APIC matches the name of the Access Control Policy Rule in the FMC, it simply inserts newly created security zones into the rule(s). If a rule is not found, the APIC creates a new rule by that name, attaches security zones to it, and sets the Action to Deny. This forces the security administrator to update the new Rule(s) criteria and appropriate set of protections before traffic can be allowed for a given service graph.




This document describes how to integrate FTD with the ACI and configure the APIC to utilize capabilities of the FTD:

- Enable the REST API in the Firepower Management Center (FMC)
- Download the FTD for ACI device package software from CCO
- Import the FTD for ACI device package into the APIC
- Register the FTD appliance
- Define a network service graph that utilizes the FTD appliance

**Note** The screenshots of the examples used in this document show a pre-existing tenant named **SampleTenant**. When following the steps in this guide and using provided templates, use the actual name of your tenant.

### Service Function Insertion

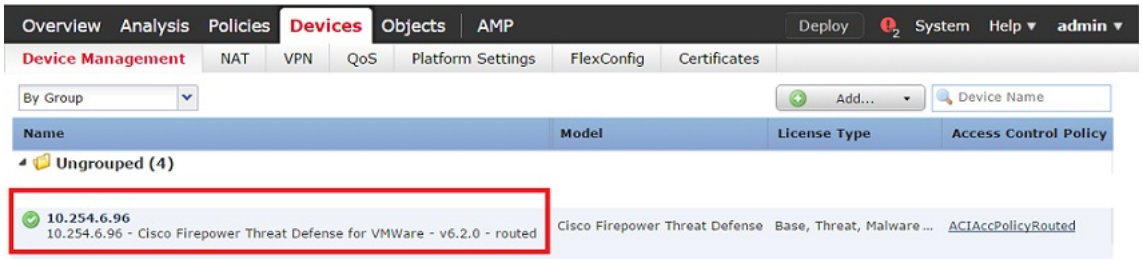
When a service function is inserted in the service graph between applications, traffic from these applications is classified by the APIC and identified using a tag in the overlay network. Service functions use the tag to apply policies to the traffic. For the FTD integration with the APIC, the service function forwards traffic using either routed, transparent, or inline firewall operation.

### Available APIC Products

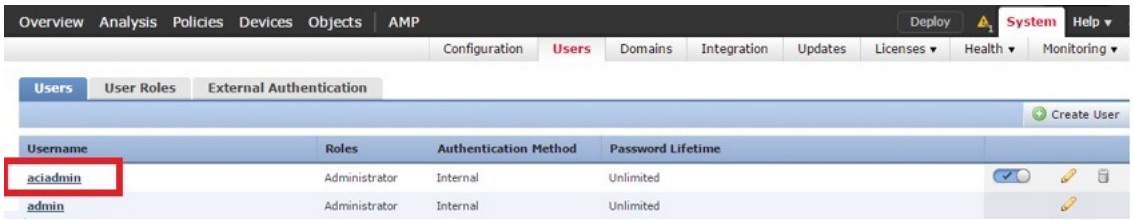
The initial software release contains the Cisco FTD Device Package Fabric Insertion software for ACI.

# Prerequisites

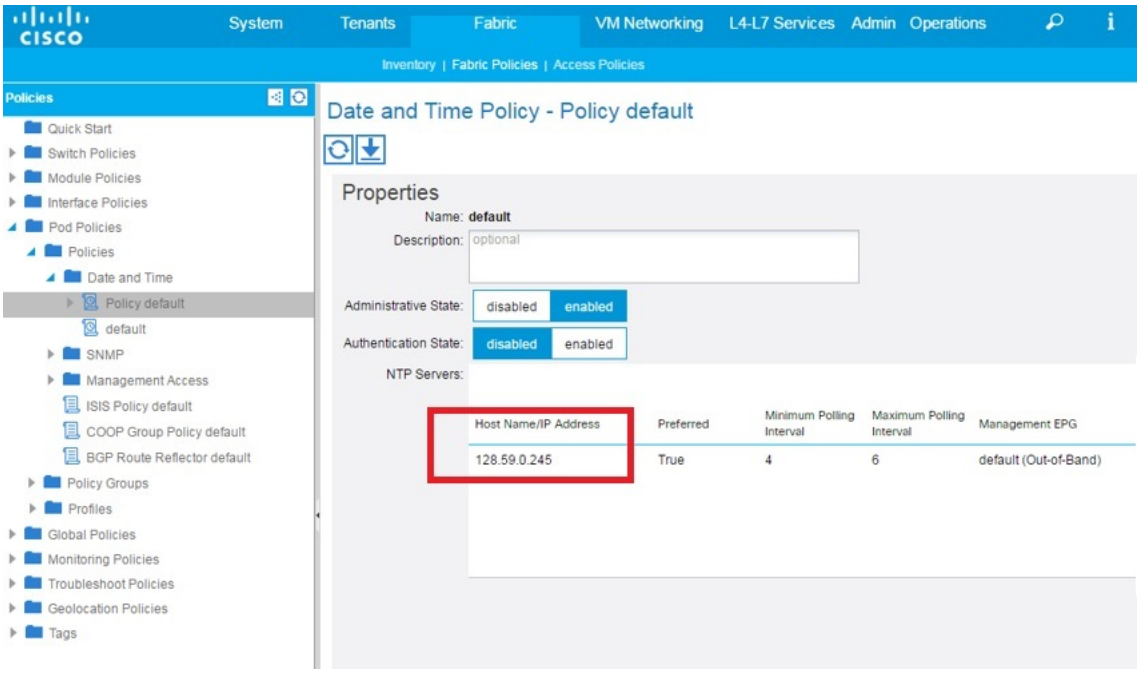
- FMC version 6.3.0; it includes REST API support for FTD.
- FTD version 6.3.0.
- APIC version 4.0(1h); its Device Manager is used to register a device. The FTD device package uses the Device Manager to allow the network portion of the FMC configuration to be instantiated by the APIC.
- Ensure that the FTD appliance you are trying to insert and configure as a network service is bootstrapped with a base configuration and registered with the FMC. For example, check the Device Management page in the FMC for the FTD:



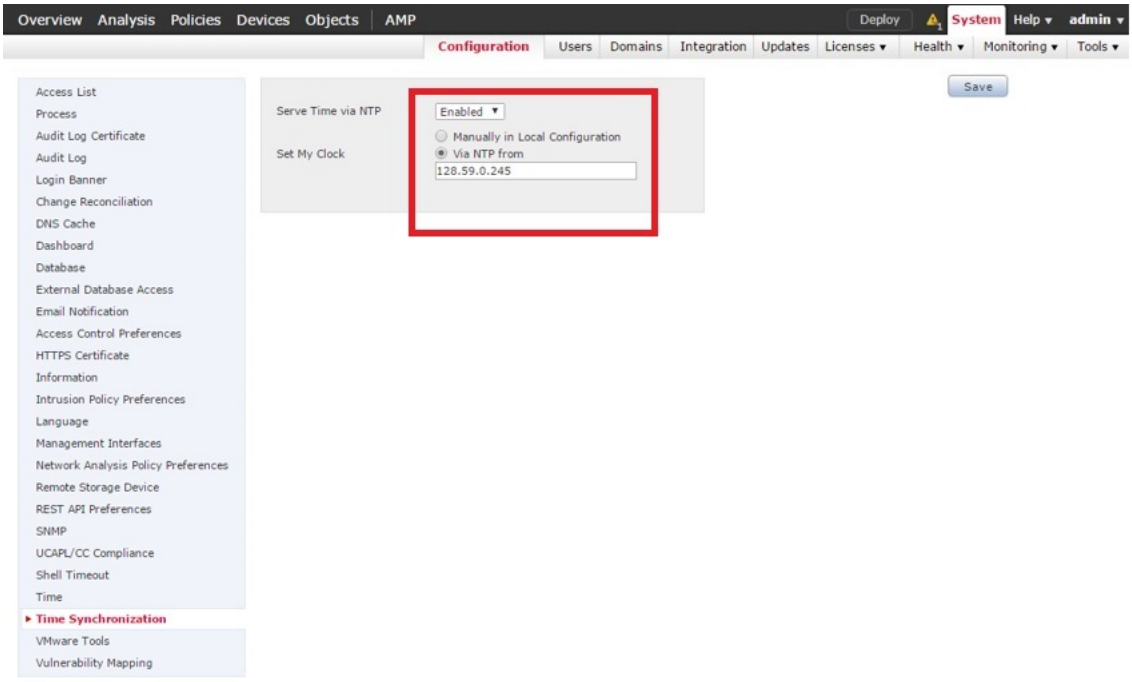

- To avoid REST API token generation race conditions, create an FMC administrator dedicated for use on the ACI. For example:



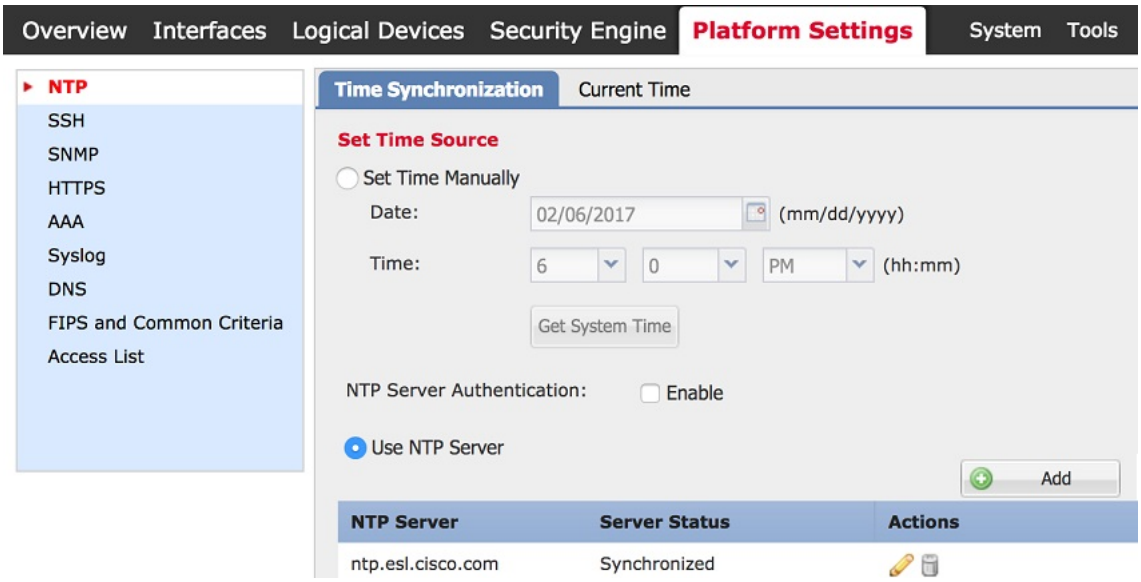

- To avoid both deployment failure and a gap in time between the servers, configure the APIC and FMC to use the same Network Time Protocol (NTP) server. With FTD on the Firepower 41xx and 93xx Series appliance, the Chassis Manager must also be configured.
  - In the APIC, navigate to **Fabric > Fabric Policies > Pod Policies > Policies > Date and Time**. Use the Create Date and Time Policy Wizard to configure the same NTP server:




- In the FMC, navigate to **System > Configuration > Time Synchronization** and configure the same NTP server:



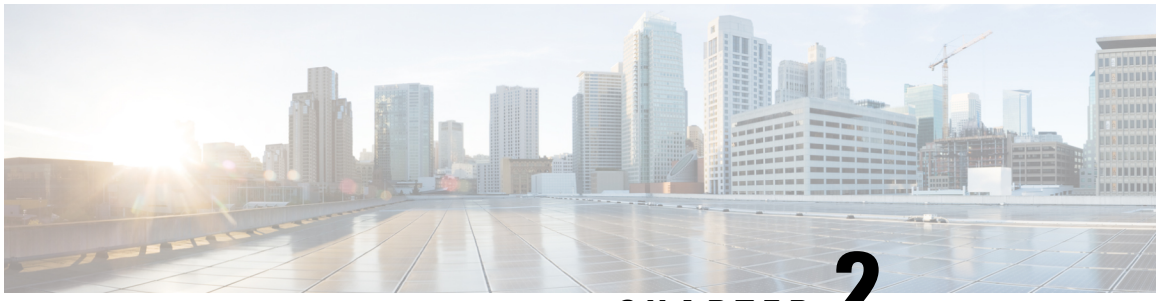

- In the Chassis Manager of the Firepower 41xx and 93xx series appliance, navigate to **Platform Settings > NTP > Time Synchronization** and add the same NTP server:




**Note** If you try to create a configuration that is not supported on your current FMC or FTD version, an error similar to the following may appear on the APIC: "Major script error: Configuration error: …. ERROR: % Invalid input detected at '^' marker."

# Related Documentation

- Cisco Application Centric Infrastructure Fundamentals
- Cisco APIC Layer 4 to Layer 7 Services Deployment Guide
- Cisco Firepower Threat Defense NGFW
- Cisco Firepower Management Center



CHAPTER 2

# Install



# Validate that the FMC REST API is Enabled

The APIC uses a REST API to connect with Firepower devices. By default, the REST API is enabled. Before the APIC can set up and manage any Firepower device, ensure that the FMC REST API is enabled by completing the following steps:

### Before you begin

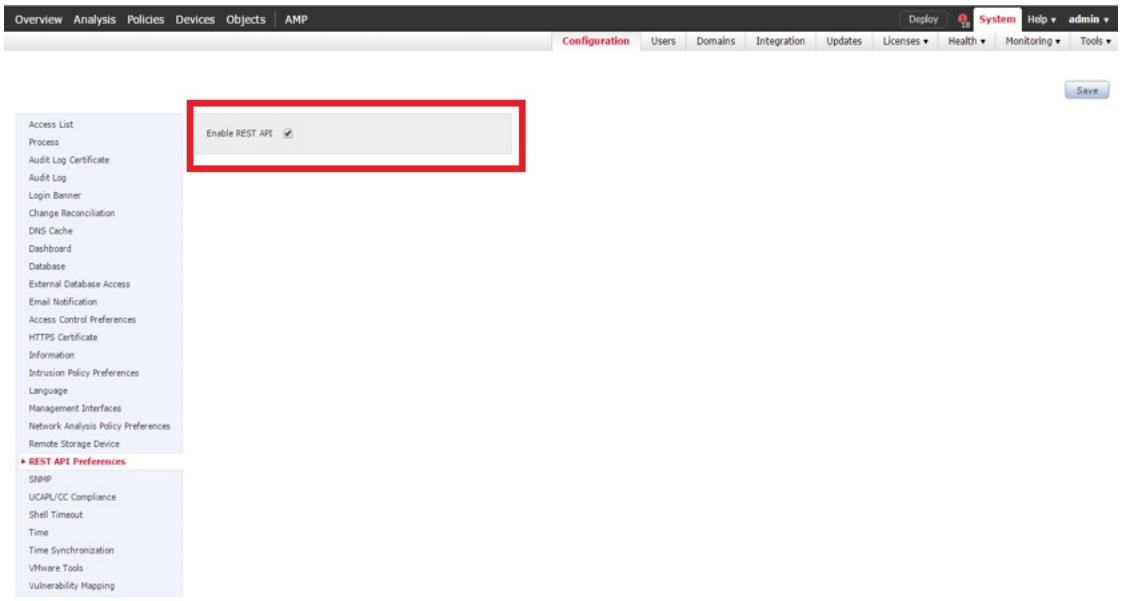
The FMC must be running version 6.2.0 or newer.

**Note** The REST API is already packaged with the FMC software; there is no license required.

**Step 1** Sign in to the FMC using your administrator credentials.

**Step 2** Navigate to **System > Configuration > REST API Preferences**.

**Step 3** If the **Enable REST API** check box is not already selected, check the box and click **Save**.




### What to do next

Once the REST API is enabled, the FMC is ready to support the FTD for ACI device package.

Create an account other than admin to use with the APIC.

# Import the Device Package

The APIC requires a device package in order to configure and monitor a service device. Import the FTD for ACI device package into the APIC so that the APIC knows you have an FTD appliance and what the FTD appliance can do.

**Step 1** Download the device package from http://www.cisco.com/go/software and save it onto your local drive.

**Note** The device package is downloaded as a .zip file. Do not unzip the file.

**Step 2** Sign in to the APIC as the provider administrator.

**Step 3** On the menu bar, click **L4-L7 Services**.

**Step 4** On the submenu bar, click **Packages**.

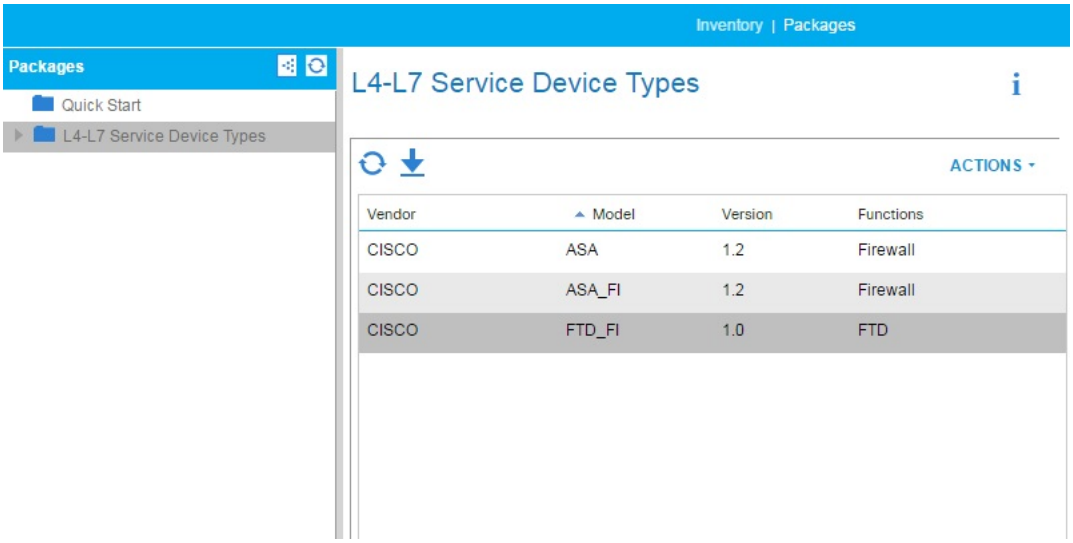
**Step 5** In the navigation pane, click **L4-L7 Service Device Types**.

**Step 6** Select **Actions > Import Device Package**.

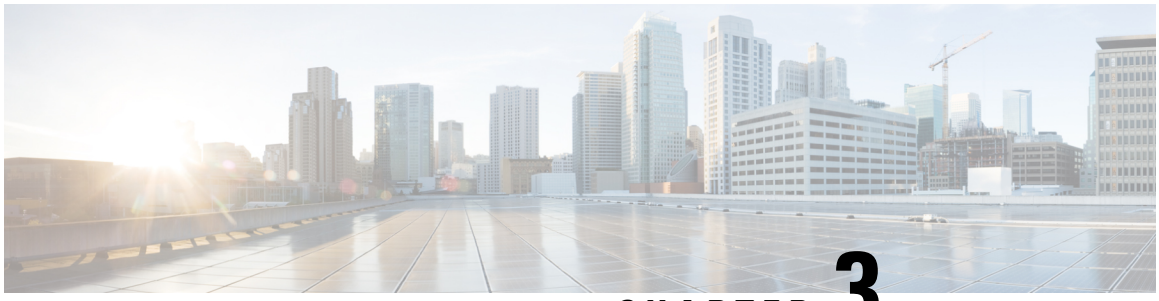
**Step 7** In the **File Name** field, specify the device package that you downloaded in **Step 1**, and click **Submit**.

### What to do next

Refresh the **Device Types** window. The new device appears in the list of device types.




(Optional) In the navigation pane, expand **Device Types** to see the function parameters for the device package.



CHAPTER 3

# Configure



## 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.

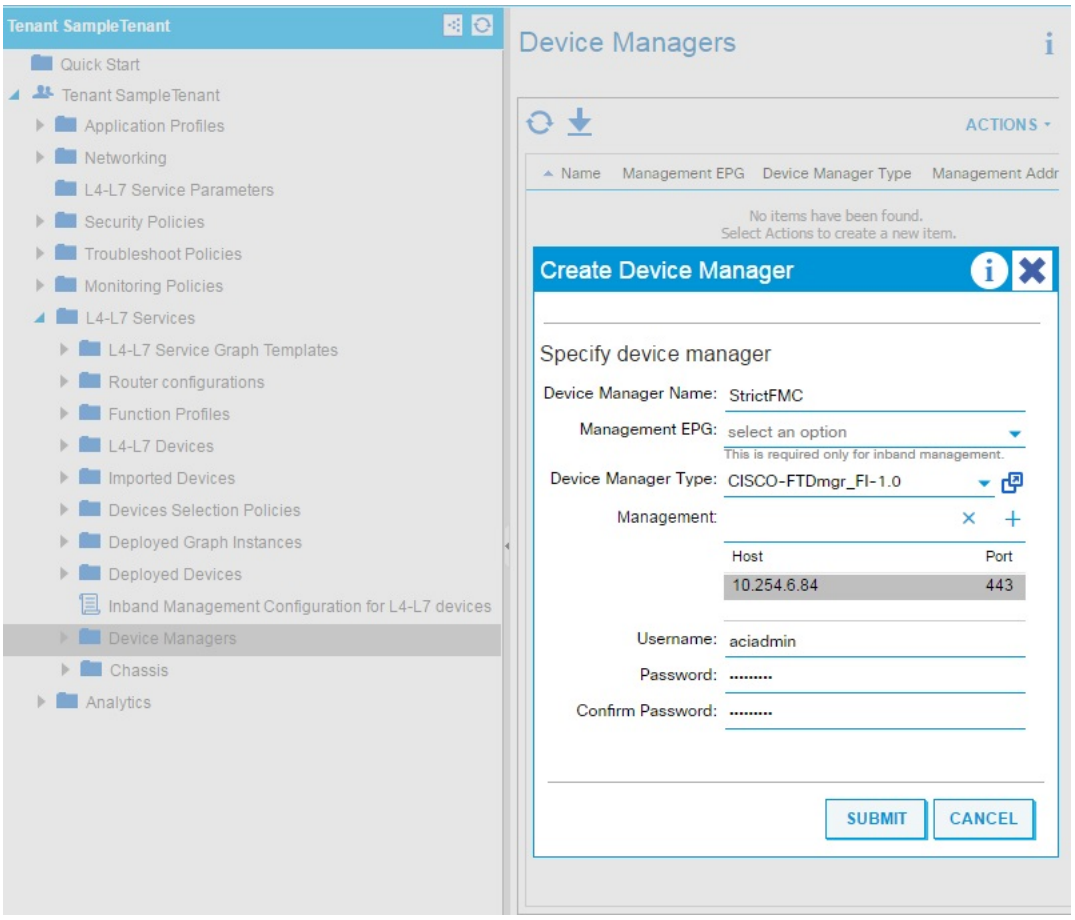
**Step 2** On the menu bar, click **Tenants**.

**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**.

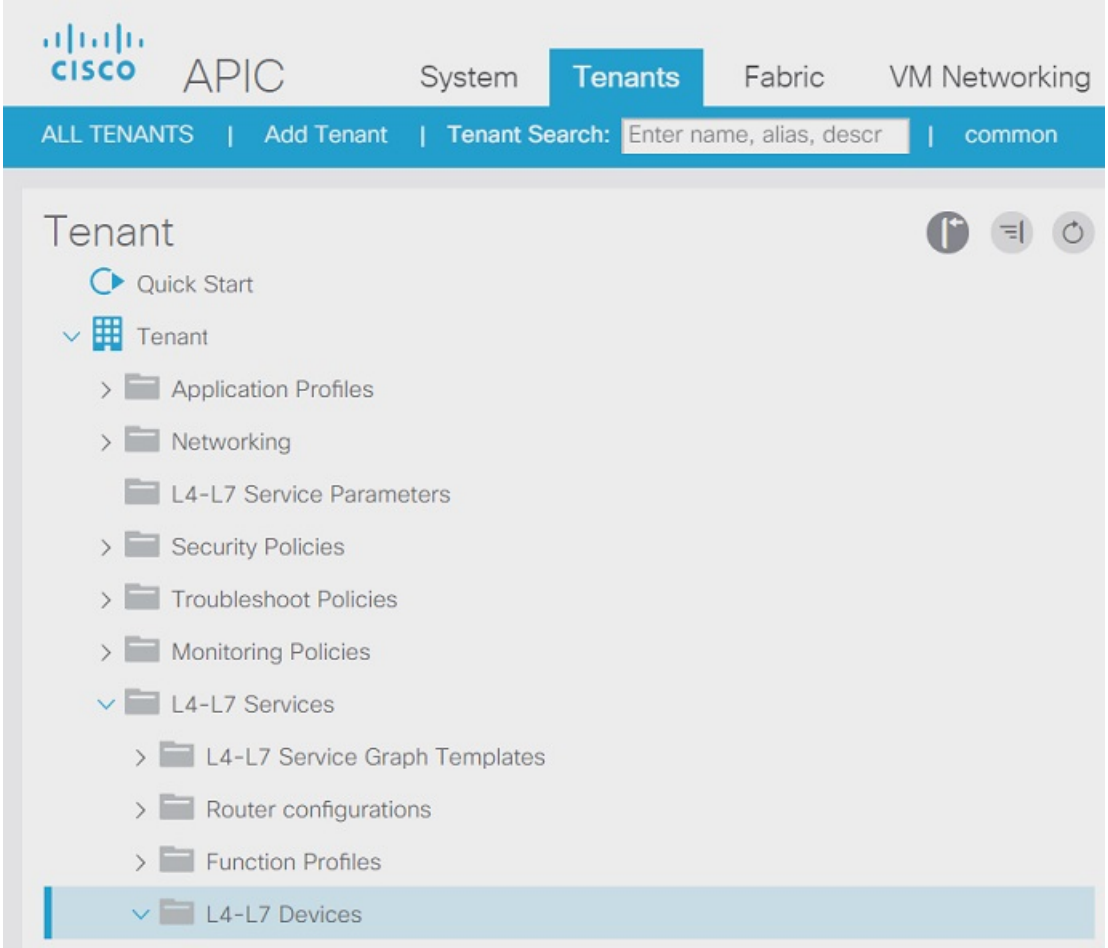
**Step 5** Complete the following options:

| 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. |




**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.<br>**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 |
|---|---|
| | **Note** Multiple is not recommended.<br><br>Single means that the appliance cluster cannot be shared across multiple tenants of a given type which are hosted on the provider network.<br><br>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. |
| Function Type | Select **GoThrough** or **GoTo**.<br><br>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. |
| Physical Domain | 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.<br><br>**Note** This is not required for a virtual FTD appliance. |
| View | Defaults to Single Node. Shows you Device 1 to configure.<br><br>**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.<br><br>**Note** Starting in 1.0.3, clustering is supported. When **Cluster** is selected, multiple devices can be added with its own management addresses. |
| VMM Domain | For a virtual FTD appliance, select the Virtual Machine Manager (VMM) domain (vCenter domain). Select an existing VMM domain or configure a new one.<br><br>**Note** This is not required for a physical FTD appliance. |
| 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:

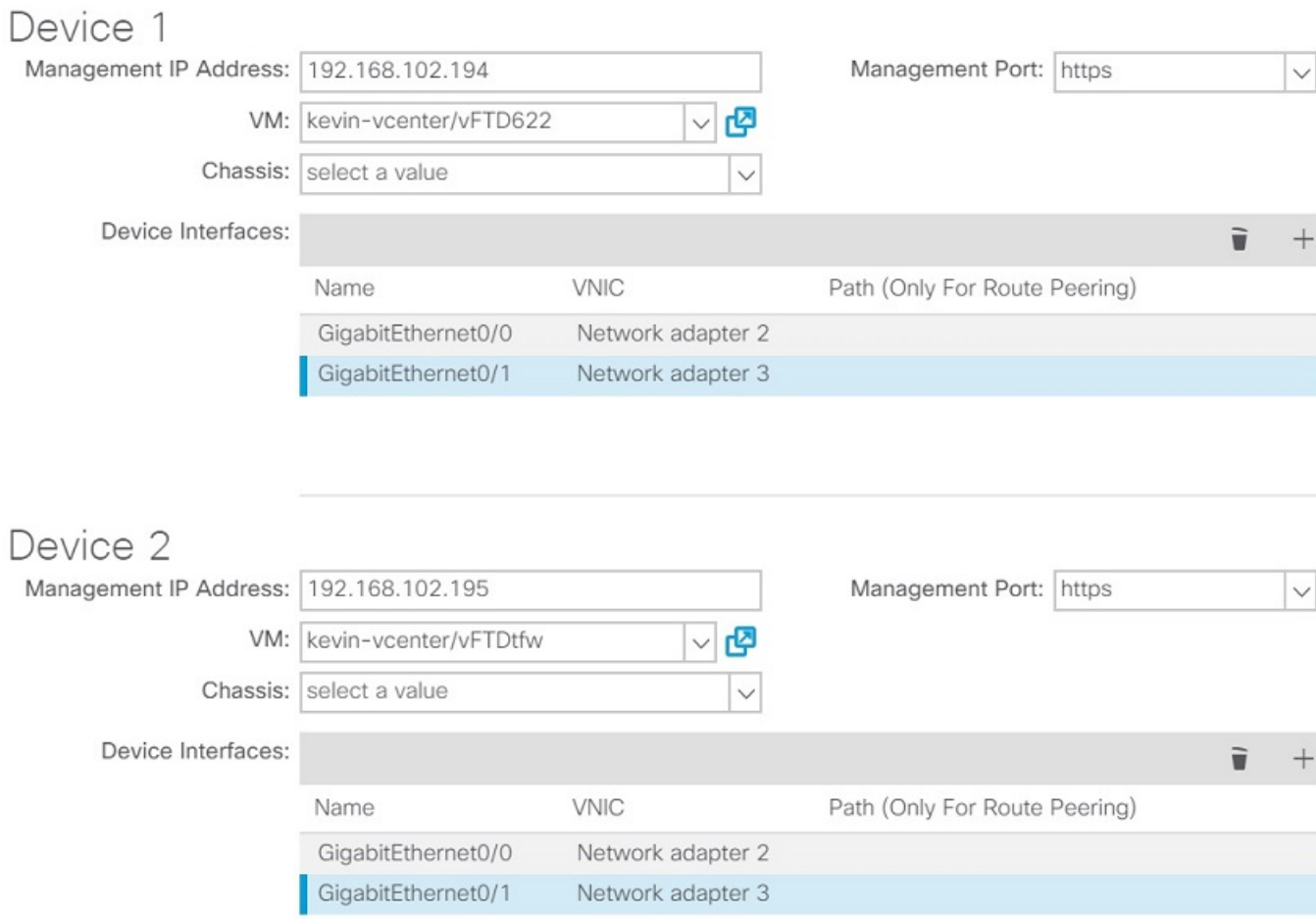
| Option | Description |
|---|---|
| Management IP Address | IP address of the management interface for the concrete appliance in the appliance cluster. |
| Management Port | Select HTTP or HTTPS. |
| VM | For a virtual FTD, name of the virtual machine on which the appliance is hosted.<br>**Note** This 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:

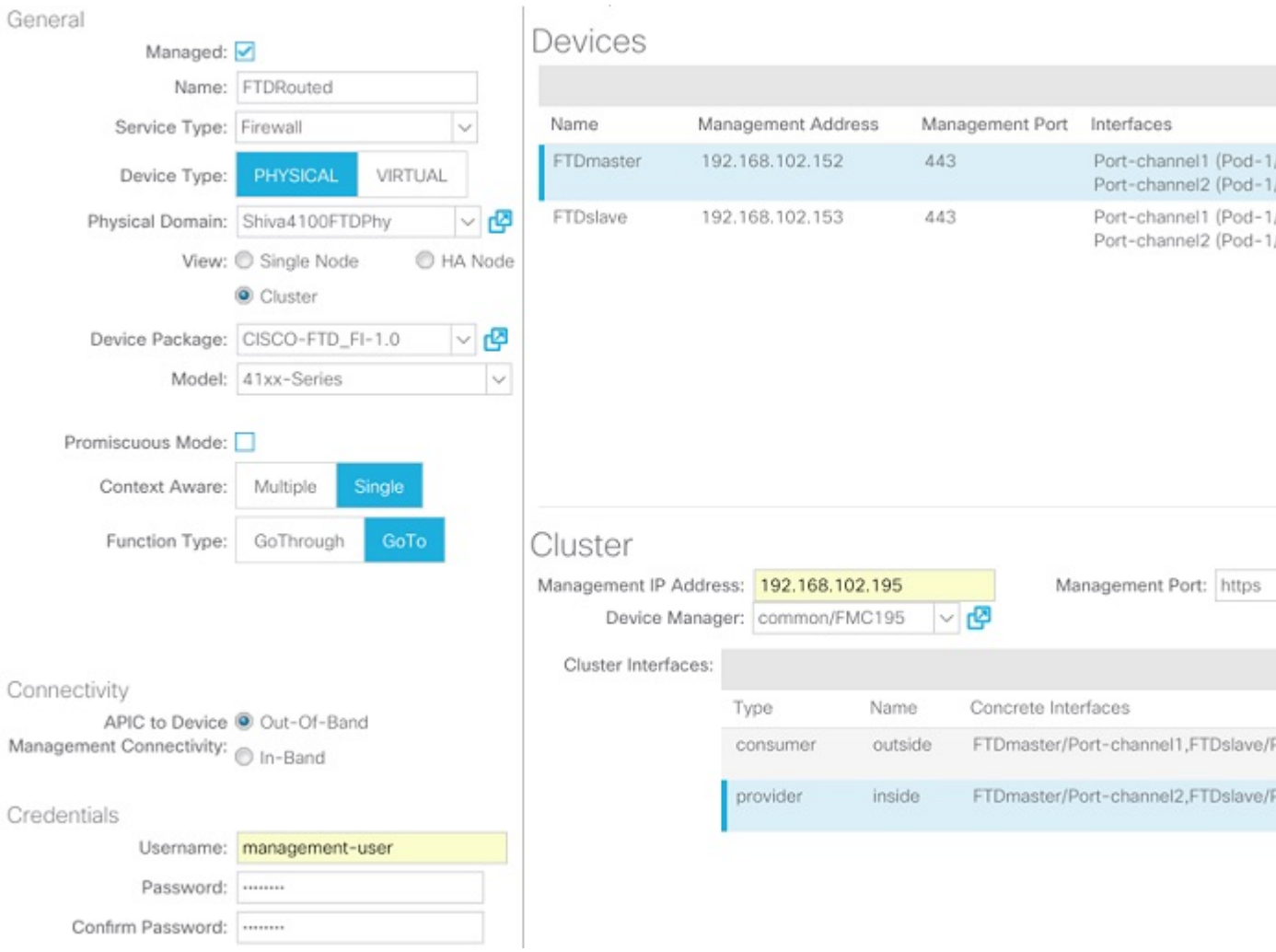
| Option | Description |
|---|---|
| Name | Name field identifies an interface on the concrete appliance. For example, GigabitEthernet0/1 or GigabitEthernet0/2. |
| Path | For physical appliances, specify how the concrete interface attaches to the fabric. For example, the leaf node/slot/port to which 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…<br>**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:




If **View: Cluster** is selected:




**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. |

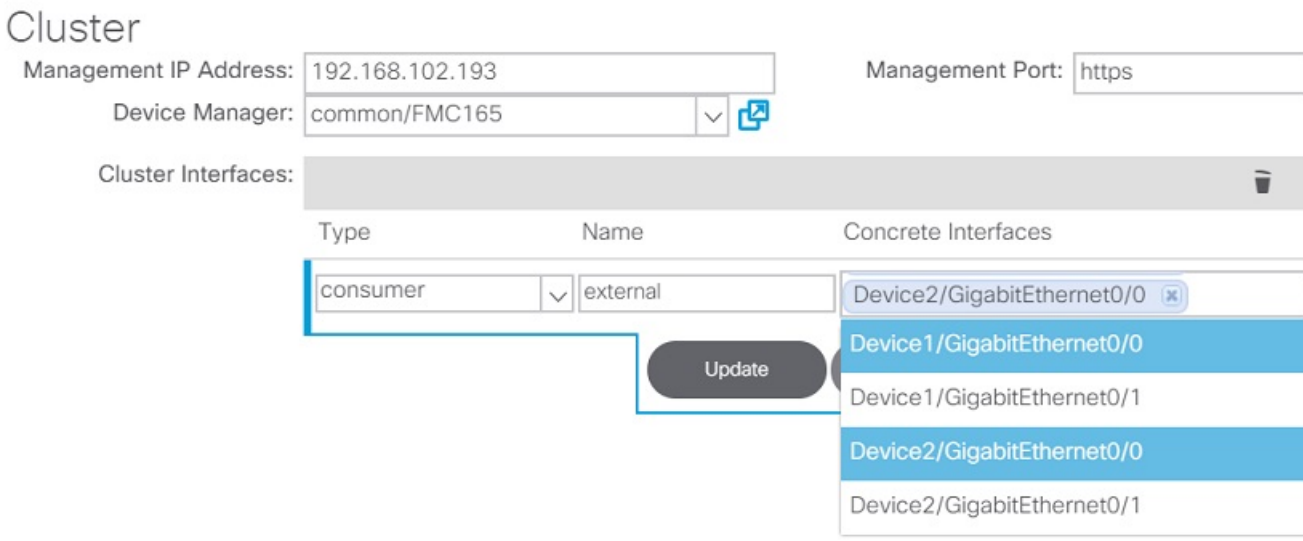
**Step 14** For Cluster Interfaces, click "+" to enter information for a cluster interface, which is the cluster logical interface. The information that you enter specifies how the logical interfaces are connected to the fabric and how the logical interfaces are mapped to the appliance concrete interfaces.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

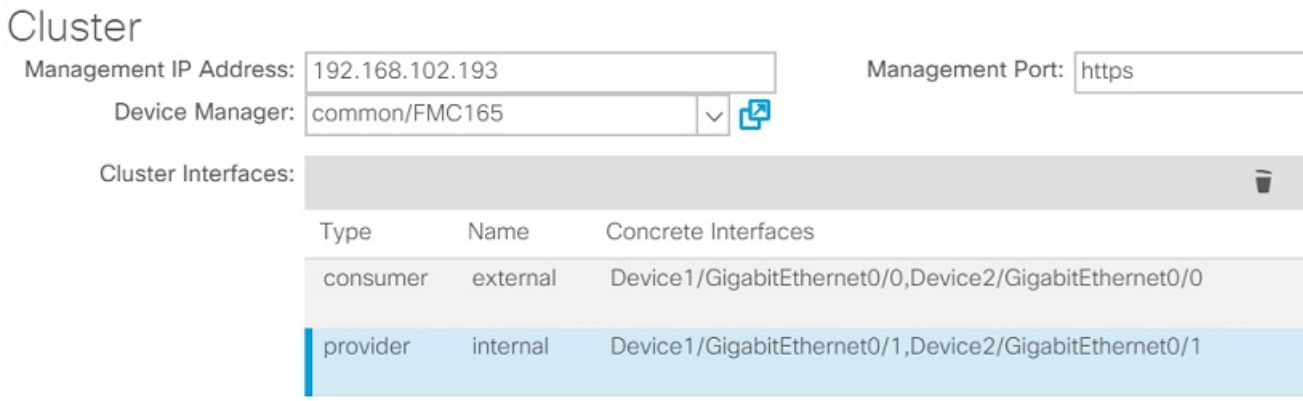
| Option | Description |
|---|---|
| Type | Type of cluster logical interface. For example, **consumer** or **provider**. |
| Name | Name field identifies an interface on the graph. For example, **external** or **internal**. |

| 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:




**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 adress 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.

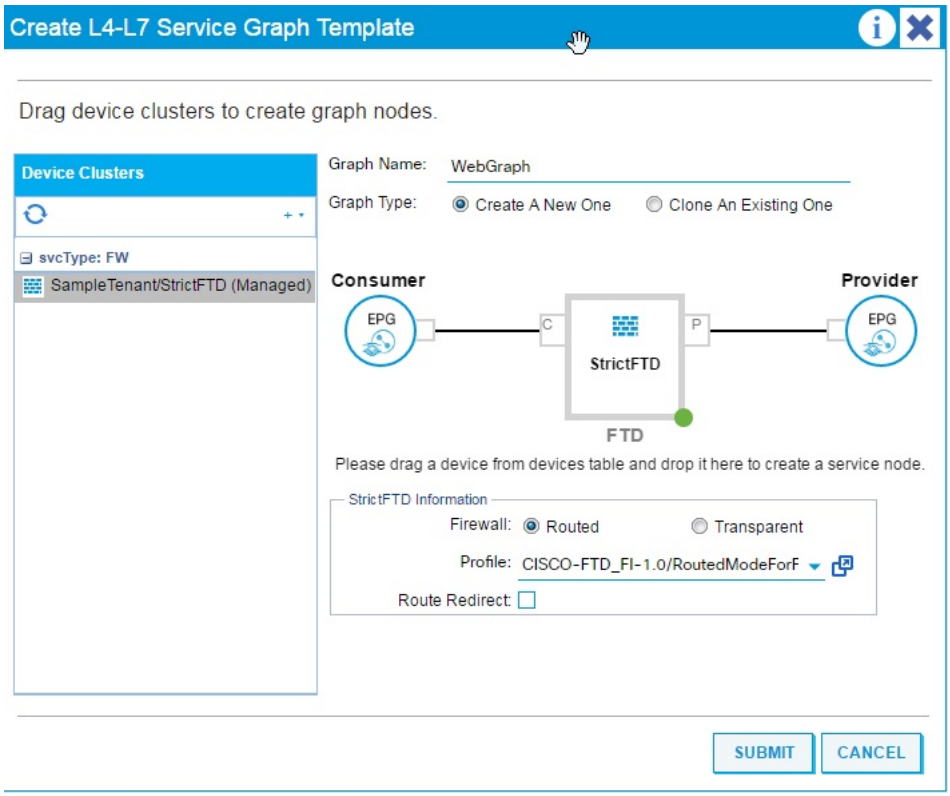
**Step 1** Sign in to the APIC.

**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.




**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.

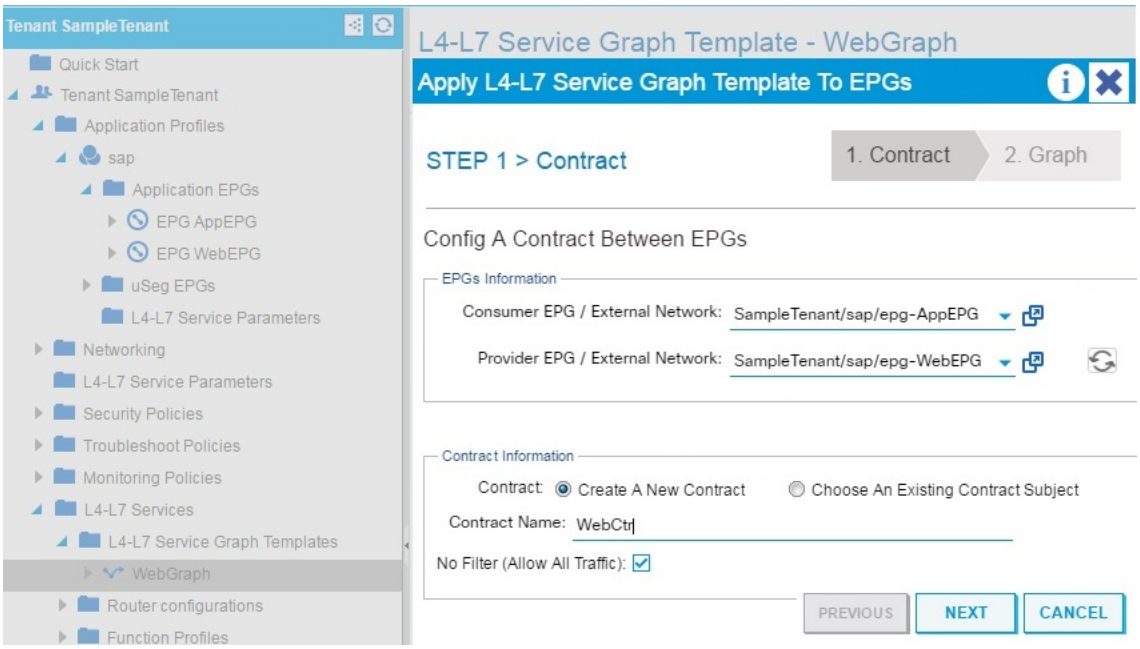
**Step 2** On the menu bar, click **Tenants**.

**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.

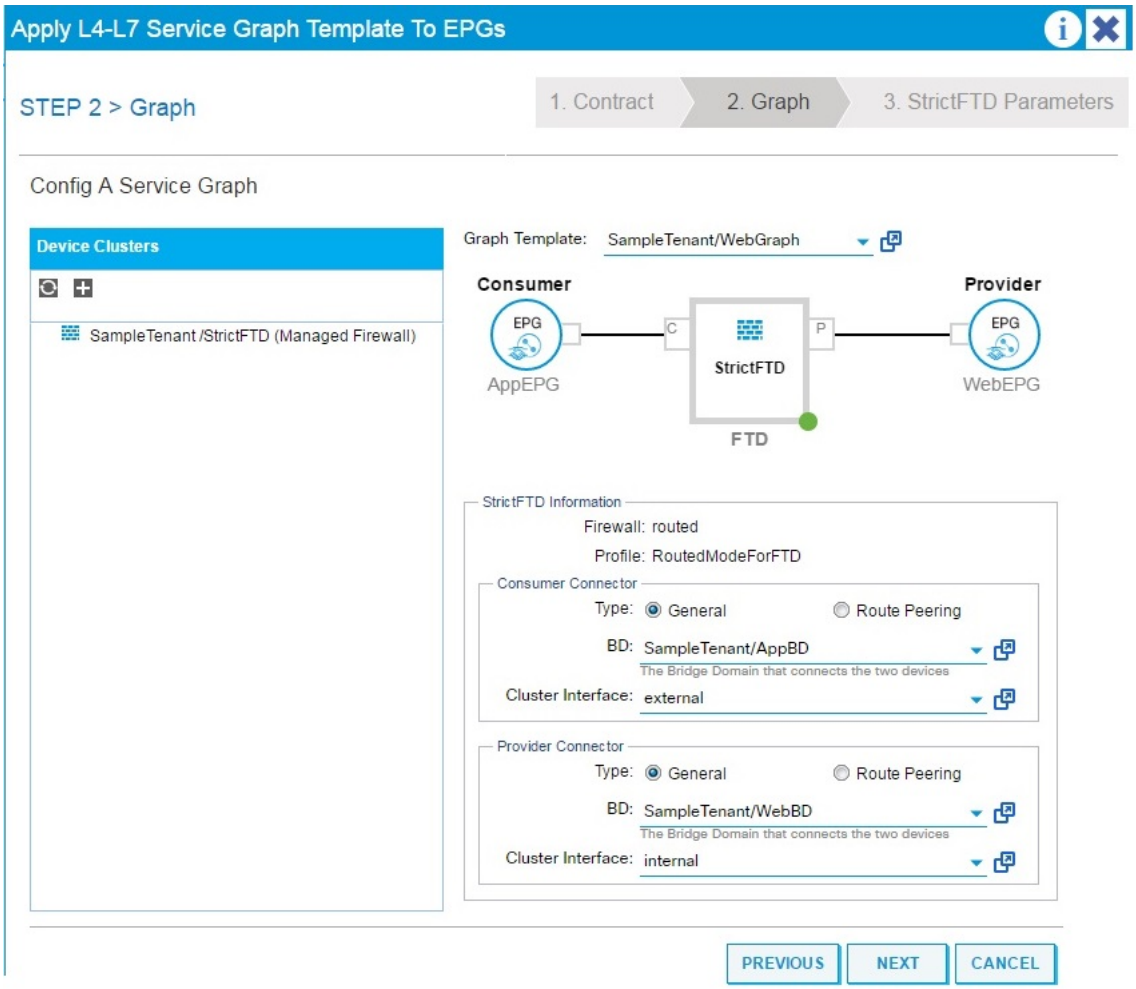
**Step 5** Right-click the service graph template of your choice, and in the pop-up menu that appears, click **Apply L4-L7 Service Graph Template**.

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

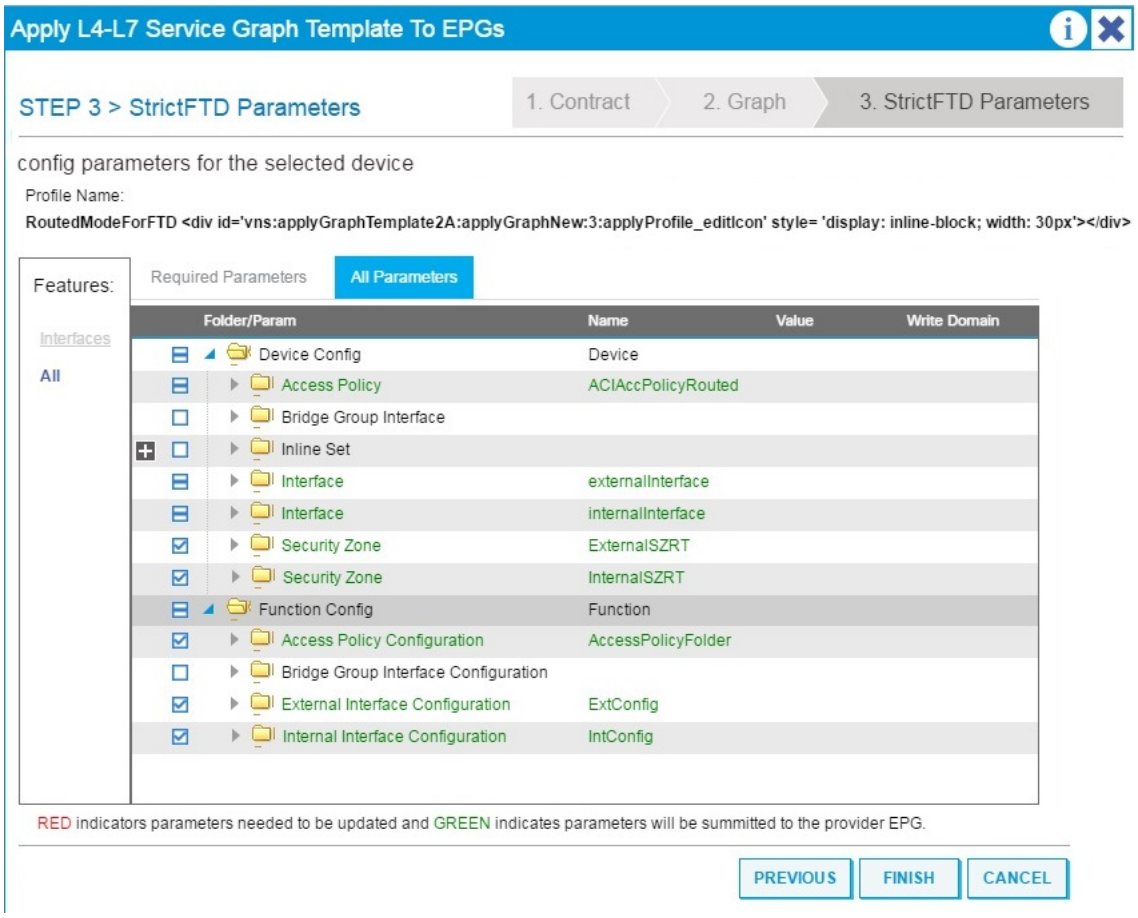



**Step 7** Create a new contract, or choose an existing contract subject. Enter a name for the new contract. Click **Next**.

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




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




**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.<br>• The APIC internally adds a GraphDeploymentSuffix and other information to the Policy description.<br>• Pre-existing FMC Access Policy name must match for the APIC to use. |
| | *Access Rules | *Name | <name> | Name of the access rule.<br>• The APIC internally adds a GraphDeploymentSuffix and other information to the Rule comment.<br>• 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> | Name of the security zone. Also, APIC folder name of the security zone object, so that other APIC objects can reference it.<br>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>.<br>**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. |
| | *Type | INLINE \| ROUTED \| SWITCHED | Type of the security zone.<br>A mismatched security zone type and interface type are not allowed. It's based on deployment mode. |

| | | | |
|---|---|---|---|
| Inline Set | *Name | <name> | Name of the inline set. Also, APIC folder name of the inline set object, so that other APIC objects can reference it.<br>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>.<br>**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. |
| | *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> | | | Logical name of the interface (optional unless Inline).<br>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>.<br>**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. |
| | *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.<br>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 | | | — |
| | • 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.<br>• 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

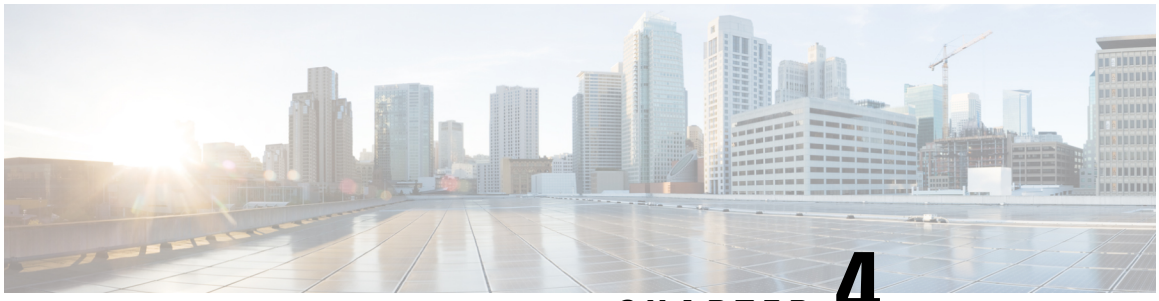
Select the default function profile **CISCO-FTD_FI-1.0/RoutedModeForFTD** and:

- 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.



CHAPTER 4

# Troubleshoot



# Fault Remediation

This section describes some basic troubleshooting including common faults and how to remediate them.

## Parameter Configurations

Any misconfigured configuration parameters for an FTD service node in a network service graph in the APIC may return one of the following faults.

### Fault Format

Graph configuration resulted in *Major script error: Configuration error: <error>* for <parameter-name> in context <context-name> on cluster <cluster-name> in tenant <tenant-name>

### Fault Message

Graph configuration resulted in *Major script error: Configuration error: Specified interface type and security zone type must match* for enabled in context SampleTenantctx1 on cluster StrictFTDvCluster in tenant SampleTenant

### Remediation

Create a new security zone with the correct type, and delete the old zone. The FMC cannot alter a security zone after it is created. Correct the misconfigured configuration parameter in the service graph based on what the FMC is expecting.

### Fault Message

Graph configuration resulted in *Major script error: Configuration error: Item with name DefaultInlineSet already exists. Please choose a different name or delete the current item*

#### Remediation

Verify that the inline set with the name DefaultInlineSet is not configured in the FMC. Inline sets that already exist cannot be used by the device package. The device package wants to create a fresh inline set so that it can delete it without affecting the workflow.

#### Fault Message

Graph configuration resulted in *Major script error : Configuration error : Interface name cannot be more than 48 characters long*

#### Remediation

Verify that the Tenant, Device, and Interface logical or Inline Set names combined with 2 delimiters ("_") is not more than 48 characters.

#### Fault Message

Graph configuration resulted in *Major script error : Configuration error : Name should be less than 48 characters *

#### Remediation

Verify that the Tenant, Device, and Interface Security Zone names combined with 2 delimiters ("_") is not more than 48 characters.

## Appliance Configurations

Any misconfigured appliance login and IP information in the APIC may return one of the following faults.

#### Fault Message

Graph configuration resulted in *Major script error : Configuration error : Can’t login to a appliance, configured login information is wrong.*

#### Remediation

Verify that the configured FMC username and password are correct.

#### Fault Message

Graph configuration resulted in *Major script error : Configuration error : The requested device does not exist.*

#### Remediation

Verify that the configured device is registered with the configured FMC.

#### Fault Message

Graph configuration resulted in * A connection attempt failed because the connected party did not properly respond after a period of time, or established connection failed because connected host has failed to respond.*

### Remediation

Verify that the configured FMC IP address is correct and reachable.

### Fault Message

Graph configuration resulted in *Major script error : Configuration error : Unable to find the requested interface.*

### Remediation

Verify that the concrete interface configured in the device which is in the device cluster is present in the FMC.

### Fault Message

Graph configuration resulted in *Major script error : Configuration error : Unable to deploy configuration changes to device. Possible reasons could be that another deployment is in progress, or APIC and FMC times are out of sync. Please be sure to sync their time to the same NTP service, set up their time zones, and retry by re-attaching the service graph.*

### Remediation

Verify that the ACI and FMC are configured with the same NTP service and that no other deployment is in progress for the same device.

### Fault Message

Graph configuration resulted in *Major script error : Configuration error : Device configuration missing.*

### Remediation

Verify that the device in the device cluster is configured correctly. Also, verify that the Device Manager is configured with information for only one FMC host.

### Fault Message

Graph configuration resulted in *Major script error : Configuration error : Device IP or Port configuration missing.*

### Remediation

Verify that the registered device cluster or appliance IP address and port are configured correctly.

### Fault Message

Graph configuration resulted in *Major script error : Configuration error : Device Username or Password configuration missing.*

### Remediation

Verify that the registered device cluster username and password are configured correctly.

### Fault Message

Graph configuration resulted in *Major script error : Configuration error : Device Username or Password configuration missing.*

### Remediation

Verify that the registered device cluster username and password are configured correctly.

### Fault Message

Graph configuration resulted in *Major script error : Configuration error : FMC fields are limited to 48 characters and are saved on FMC as "<Field Value>_<Tenant Name>_<L4-L7 Device Name>". Your current Tenant and Device names combined with 2 delimiters ("_") are greater than 40 characters, leaving you with an 8-character function profile field. Please reduce your Tenant or Device name lengths to accommodate this limit.*

### Remediation

Verify that the Tenant and Device names combined are not more than 38 characters.