



Release Notes for the Cisco FTD Device Package for ACI, 1.0.3

[Supported Versions](#) 2

[Import the Device Package](#) 2

[New Features in Version 1.0\(3\)](#) 2

[Existing Features From Version 1.0\(2\)](#) 5

[Existing Features From Version 1.0\(1\)](#) 5

[Resolved Enhancement Requests in Version 1.0\(3\)](#) 6

[Resolved Caveats in Version 1.0\(3\)](#) 7

[Bug Search](#) 7

[Features Not Supported in Version 1.0\(3\)](#) 7

[Known Issues](#) 7

[Related Documentation](#) 11

Revised: September 16, 2025

Supported Versions

Table 1: Supported Versions of the Cisco FTD Software for Each Supported Platform

FTD Device Package Version	Platform	FTD/FMC Version	ACI/APIC Version
1.0.3	Firepower-93xx	6.2.3	2.3(1f) 3.0(1k) 3.2(1l)
1.0.3	Firepower-41xx	6.2.3	2.3(1f) 3.0(1k) 3.2(1l)
1.0.3	Firepower-21xx	6.2.3	2.3(1f) 3.0(1k) 3.2(1l)
1.0.3	vFTD	6.2.3	2.3(1f) 3.0(1k) 3.2(1l)

Import the Device Package

Sign in on Cisco.com to download and install the device package software. For instructions, see the [Cisco FTD for ACI Quick Start Guide](#).

New Features in Version 1.0(3)

- IPv4 static route support
- FTD clustering support
- Ether-channel sub-interface support

IPv4 Static Route Support

The following fields are supported:

- network (required)
- gateway (required)

- metric (optional)
- isTunneled (optional)



Note The SLA monitor option is not supported

Example of an IPv4 static route configured on the APIC:

The screenshot shows the Cisco APIC interface for configuring L4-L7 Service Parameters. The left sidebar displays the navigation tree, and the main panel shows the 'Edit L4-L7 Service Parameters' form. The 'All Parameters' tab is active, showing a table of parameters for the 'StaticRoute' folder. A red box highlights the 'IPv4 Static Route' section, which includes parameters for Gateway, Metric, Network, and isTunneled.

Folder/Param	Name	Value
☒ > IPv4 Address Configuration	IPv4Config	
☒ > Interface Security Zone	int_security_zone	
☐ > Interface inline set configuration		
☒ > Static Routes List	StaticRoute	
☒ > IPv4 Static Route	IPv4StaticRoute	
☒ Gateway	gateway	192.168.7.1
☒ Metric	metric	2
☒ Network	network	192.168.7.0/24
☒ isTunneled	isTunneled	false
☒ Enabled	enabled	true
☒ Logical Name	ifname	Consumer
☐ MTU		

Example of the IPv4 static route pushed to the FMC by the FTD-DP:

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy 6 System Help ▾

Device Management NAT VPN ▾ QoS Platform Settings FlexConfig Certificates

cluster3

Cisco Firepower 4110 Threat Defense

Cluster Device **Routing** Interfaces Inline Sets DHCP

OSPF
OSPFv3
RIP
BGP
Static Route
Multicast Routing

Add Route

Network	Interface	Gateway	Tunneled	Metric	Tracked
▼ IPv4 Routes					
NET-192.168.7.0-24	Consumer_ed_static_route_cluster2	HOST-192.168.7.1	false	2	 
NET-192.168.9.0-24	Provider_ed_static_route_cluster2	HOST-192.168.9.1	false	1	 

FTD Clustering Support

FTD cluster must be pre-configured on the FMC. For example:

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy 3 System Help ▾ **aciadmin** ▾

Device Management NAT VPN ▾ QoS Platform Settings FlexConfig Certificates

Device Management

List of all the devices currently registered on the Firepower Management Center.

View By : Group ▾ All (4) | Error (1) | Warning (0) | Offline (0) | Normal (3) | Deployment Search Device Add ▾

Name	Model	Vers...	Licenses	Access Control Pol...
Ungrouped (3)				
cg Cisco Firepower 4110 Threat Defense Cluste				
✓ 192.168.60.13(Master) 192.168.60.13 - Routed	Cisco Firepower 4110 Threat Defense	6.2.3	Base, Threat, Malware, URL Filtering	None
✓ 192.168.60.3 192.168.60.3 - Routed	Cisco Firepower 4110 Threat Defense	6.2.3	Base, Threat, Malware, URL Filtering	None
✗ ftd110 192.168.60.110 - Routed	Cisco Firepower Threat Defense for VMWare	6.2.3	Base, Threat, Malware, URL Filtering	ACIAccPolicyInline
✓ ftd120 192.168.60.120 - Routed	Cisco Firepower Threat Defense for VMWare	6.2.3	Base, Threat, Malware, URL Filtering	policy1

Register the FTD cluster on the APIC. For example:

The screenshot displays the Cisco APIC web interface. The top navigation bar includes tabs for System, Tenants, Fabric, Virtual Networking, L4-L7 Services, Admin, Operations, and Apps. The 'Tenants' tab is active, showing a list of tenants including 'tenant_cluster'. The left sidebar shows a tree view of the configuration hierarchy, with 'L4-L7' and 'my_cluster' selected. The main content area is titled 'L4-L7 Devices - my_cluster' and contains several sections:

- General:** Includes fields for Name (my_cluster), Alias, Device Package (Cisco-FTD_FF-1.0), Service Type (Firewall), Device Type (PHYSICAL), Physical Domain (ScaleFTDPhy), Promiscuous Mode (unchecked), Context Aware (Multiple/Single), and Function Type (GoThrough/GoTo).
- Credentials:** Includes fields for Username (admin), Password, and Confirm Password.
- Configuration State:** Shows Configuration Issues and Devices State (stable).
- Devices:** A table listing devices and their interfaces.

Name	Management Address	Management Port	Interfaces
dev1	192.168.60.13	443	Port-channel5 (Pod-1/Node-101/jeth1/5) Port-channel7 (Pod-1/Node-101/jeth1/7)
dev2	192.168.60.3	443	Port-channel5 (Pod-1/Node-101/jeth1/8) Port-channel7 (Pod-1/Node-101/jeth1/9)
- Cluster:** Includes fields for Management IP Address (192.168.60.5), Device Manager (common/DM_5_FF_10), and Management Port (443). It also shows a table for Cluster Interfaces.

Type	Name	Concrete Interfaces
consumer	c	dev1.[Port-channel5], dev2.[Port-channel5]
provider	p	dev1.[Port-channel7], dev2.[Port-channel7]

The logical cluster device is used the same way as a normal single device in the APIC.

When a serviceAudit is triggered on the APIC, such as Re-Query for Device Validation, or when a configuration is changed, such as the IP address of the externalInterface of the service graph, which causes a serviceModify, the FTD-DP can use the new FMC etherchannel REST API to push the corresponding configuration to the FMC, and ensure the changes are automatically deployed to the FTD cluster.

Existing Features From Version 1.0(2)

- Virtual FTD VLAN trunking support
- FTD High Availability (HA) support
- Dynamic EPG update
- Firepower 21xx support
- Performance enhancements (FTD-DP scalability)

Existing Features From Version 1.0(1)

- Create interface configuration for FTD

- Configure enabled
- Configure logical name
- Configure MTU
- Configure security zone
- Configure inline set
- Configure static IPv4 addresses
- Create new bridge group interface for Transparent mode
 - Configure bridge group ID
 - Configure static IPv4 addresses
 - Configure interface reference
- Create new inline set
 - Configure snort fail open down
 - Configure snort fail open busy
 - Configure MTU
 - FTD physical appliance with Inline Set requires a specially designed ACI service graph with the same VLAN ID on both interfaces
- Create new or update existing access rule
 - Configure source and destination security zones
- Create new or update existing access policy
 - Configure name
- Create new security zone
 - Configure type

Resolved Enhancement Requests in Version 1.0(3)

Table 2: Enhancement Requests Resolved in the Cisco FTD Device Package, Version 1.0(3)

Caveat	Description
CSCvh58404	Enhancement: add IPv4 static route support in FTD-DP
CSCvh58431	Enhancement: add cluster support in FTD-DP (pre-configured)
CSCvh58443	Enhancement: add etherchannel support in FTD-DP

Resolved Caveats in Version 1.0(3)

Table 3: Caveats Resolved in the Cisco FTD Device Package, Version 1.0(3)

Caveat	Description
CSCvg73120	Associated interfaces deleted if BVI interface ID changed

Bug Search

As a registered Cisco.com user, sign in to view more information about each bug or caveat using the [Cisco Bug Search Tool](#).

Features Not Supported in Version 1.0(3)

The APIC cannot configure the following features using the FTD device package:

- Dynamic routing
- Port-channels
- Access control policy rule ports, IPs, or inspections
- Network Address Translation (NAT)



Note

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

Known Issues

This section describes known issues and their workarounds.

CSCvj29517

In some circumstances, the FMC may be too busy to complete a service call from the APIC, which causes the same request to be made to the FMC again and again. This may occur when:

- Using the FTD device package, version 1.0.3
- Clustering deployment with Inline mode

Workaround

You can use the Cisco-provided Python script (attached to CSCvj29517) to access the APIC REST API and modify the timeout values:

1. Run the script to change the timeout value to its maximum number:

```
set_timeout.py <APIC_IP> <USERNAME> <PASSWORD> maximum
```

2. Monitor the debug.log from the APIC to verify that the service call has completed. Or check the the FMC to verify that the intended changes have been pushed down to the FMC and the deployment to the FTD is complete.
3. Run the script again to change the timeout value back to its default number. Otherwise, unexpected behavior may occur.

```
set_timeout.py <APIC_IP> <USERNAME> <PASSWORD> default
```

CSCvf88494

When deleting a tenant with a large configuration, the device package process is killed before it can finish the service call, resulting in a configuration that may not be completely cleaned up on the FMC. This may occur when:

- Using the FTD device package, version 1.0.2
- The tenant contains a device that has more than 50 service graphs deployed
- Deleting the tenant directly before detaching the service graphs

Workaround

Detach the service graphs before deleting the tenant, or increase various timeout values on the APIC using its REST API. The REST payload is like this:

```
<polUni>
  <infraInfra>
    <vnsMDev vendor=CISCO model=FTD_FI version=1.0>
      <vnsDevScript auditTimeout=10800 modifyTimeout=10800 watchdogTimeout=10800/>
    </vnsMDev>
  </infraInfra>
</polUni>
```

You can use the Cisco-provided Python script (attached to CSCvf88494) to access the APIC REST API and modify the timeout values:

1. Before deleting the tenant, run the script to change the timeout value to its maximum number:
2. Delete the tenant from the APIC.
3. Monitor the debug.log from the APIC to verify that the service call has completed. Or check the FMC to verify that all relevant configuration data has been cleaned up (such as access rules, security zones, sub-interfaces, and inline sets).
4. Run the script again to change the timeout value back to its default number. Otherwise, unexpected behavior may occur.

```
set_timeout.py <APIC_IP> <USERNAME> <PASSWORD> default
```



Note Note: If the “CISCO-FTD_FI-1.0” device package is not installed on the APIC, running the script results in a “Bad Request” error. This error message can be safely ignored, as the script is designed to affect this particular device package only.

For more information, see CSCvg00515, opened to track this issue.

CSCvg06100

VLAN trunking fails in Transparent mode on a virtual FTD.

Workaround

Opened to track the FMC issue in CSCvf90086.

Enable the trunking port after creating the L4-L7 device. Then, apply the service graph.

If the deployment fails:

1. On the FMC:
 - a. Navigate to **Devices**, and select the FTD.
 - b. Delete the new BVI and the associated sub-interfaces. Click **Save**. Click **Deploy**.
 - c. Wait for the FMC to complete the deployment.
2. On the APIC:
 - a. In the node tree on the left, navigate to **L4-L7 Devices**, and select the device.
 - b. Verify that the **Trunking Port** check box is selected.
 - c. Right-click the device, and select **Re-Query For Device Validation**.

CSCvc46536

Multiple graph deployment needs a different parameter name for an access rule.

Workaround

For instance, Access Rules is a common APIC configuration parameter that can be shared across multiple graph deployments on the same L4-L7 device. In order to attach each graph deployment's interface security zones to a common access rule, provide different names for the SourceZone and DestinationZone parameters. For example, append each parameter with a matching suffix name, such as SourceZone-campCtx and DestinationZone-campCtx in one case and SourceZone-sapCtx and DestinationZone-sapCtx in another.

System
Tenants
Fabric
VM Networking
L4-L7 Services
Admin

ALL TENANTS | Add Tenant | Search: enter name, descr | MutiParamFTDSample | AAvFTD60MultiRoutedOn84 | common | FTDIssueT | infra

Tenant MutiParamFTD Sample

Quick Start

Tenant MutiParamFTDSample

Application Profiles

camp

sap

Application EPGs

EPG AppEPG

EPG WebEPG

Domains (VMs and Bare

Static Bindings (Paths)

Static Bindings (Leaves)

Contracts

Static EndPoint

Subnets

L4-L7 Virtual IPs

L4-L7 IP Address Pool

L4-L7 Service Parameters

uSeg EPGs

L4-L7 Service Parameters

Networking

L4-L7 Service Parameters

Security Policies

Troubleshoot Policies

Monitoring Policies

L4-L7 Services

Edit L4-L7 Service Parameters

Click row to edit value

Contract Name: MutiParamFTDSample/sapCtx

Graph Name: MutiParamFTDSample/WebG

Node Name: FTD

Features and Parameters

Features:

Basic Parameters

All Parameters

Folder/Param	Name	Value
Device Config	Device	
Access Policy	ACIAccPolicyRouted	
Access Rules	ACIAccRule	
Destination Interface	AccDestinationZones	
DestinationZone	DestinationZone-sapCtx	internalInterface/int_...
Source Interface	AccSourceZones	
SourceZone	SourceZone-sapCtx	externalInterface/int...
Bi-Directional	Bi-Directional	true
Bridge Group Interface		
Inline Set		
Interface	externalInterface	
Interface	internalInterface	
Security Zone	ExternalSZRT	
Security Zone	InternalSZRT	

SHOW USAGE

SUBMIT

CANCEL

CISCO System Tenants Fabric VM Networking L4-L7 Services Admin

ALL TENANTS | Add Tenant | Search: enter name, descr | MultiParamFTDSample | AAvFTD60MultiRoutedOn84 | common | FTDIssueT | infra

Tenant MultiParamFTDSample

Quick Start

Tenant MultiParamFTDSample

Application Profiles

camp

Application EPGs

EPG InEPG

Domains (VMs and Bare-M

Static Bindings (Paths)

Static Bindings (Leaves)

Contracts

Static EndPoint

Subnets

L4-L7 Virtual IPs

L4-L7 IP Address Pool

L4-L7 Service Parameters

EPG OutEPG

uSeg EPGs

L4-L7 Service Parameters

sap

Networking

L4-L7 Service Parameters

Security Policies

Troubleshoot Policies

Monitoring Policies

L4-L7 Services

Edit L4-L7 Service Parameters

Click row to edit value

Contract Name: MultiParamFTDSample/campCtx

Graph Name: MultiParamFTDSample/WebG

Node Name: FTD

Features and Parameters

Features: Basic Parameters All Parameters

Folder/Param	Name	Value
Device Config	Device	
Access Policy	ACIAccPolicyRouted	
Access Rules	ACIAccRule	
Destination Interface	AccDestinationZones	
DestinationZone	DestinationZone-campCtx	InInterface/int_securi...
Source Interface	AccSourceZones	
SourceZone	SourceZone-campCtx	outInterface/int_secu...
BI-Directional	BI-Directional	true
Bridge Group Interface		
Inline Set		
Interface	InInterface	
Interface	outInterface	
Security Zone	ExternalSZRT	
Security Zone	InternalSZRT	

SHOW USAGE SUBMIT CANCEL

For more information, see the FMC Configuration Guide in [Related Documentation](#), on page 11.

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](#)



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.