Release Notes for the Cisco FTD Device Package for ACI, 1.0.4

Revised: June 12, 2019

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
1.0.4	Firepower-93xx	6.3.0 6.4.0	2.3(1f) 3.0(1k) 3.2(1l) 4.0(1h) 4.1(1j)
1.0.4	Firepower-41xx	6.3.0 6.4.0	2.3(1f) 3.0(1k) 3.2(1l) 4.0(1h) 4.1(1j)
1.0.4	Firepower-21xx	6.3.0 6.4.0	2.3(1f) 3.0(1k) 3.2(1l) 4.0(1h) 4.1(1j)
1.0.4	vFTD	6.3.0 6.4.0	2.3(1f) 3.0(1k) 3.2(1l) 4.0(1h) 4.1(1j)

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.

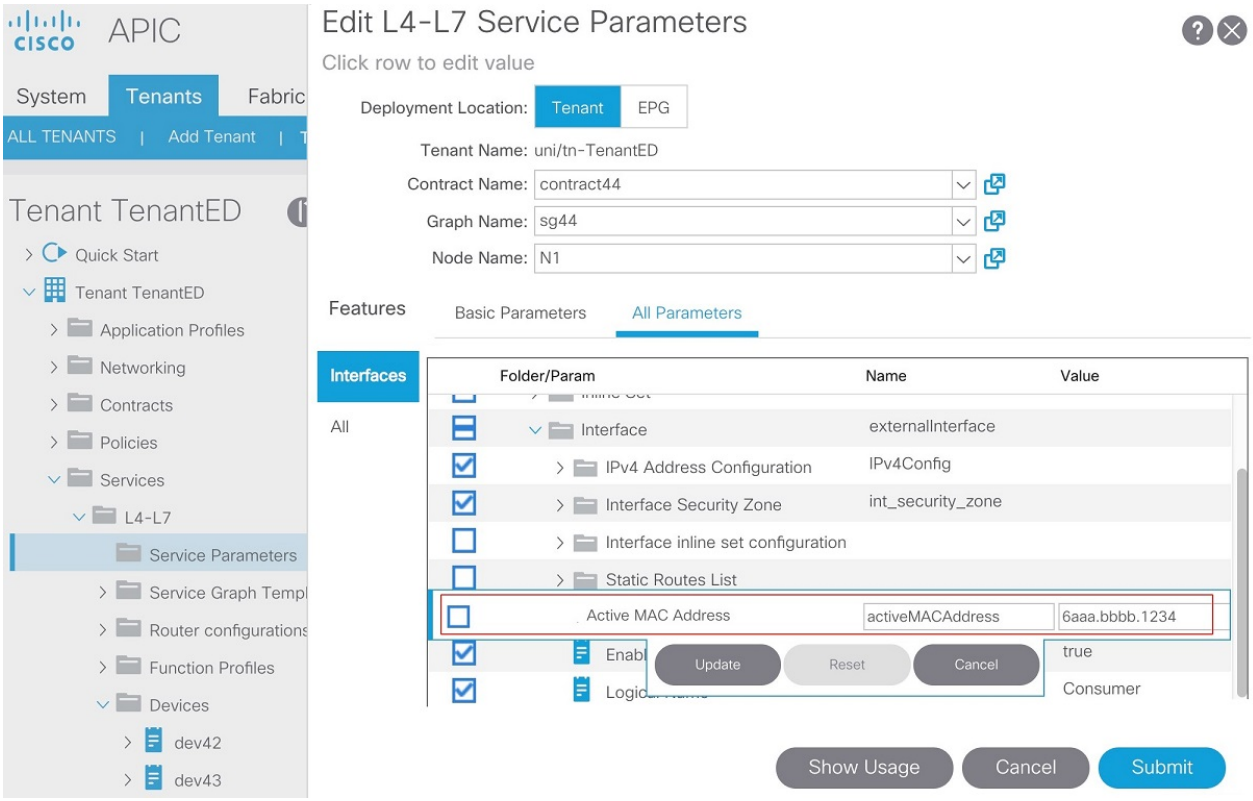
New Features in Version 1.0(4)

- Active MAC address support
- Multi-instance FTD support
- Multi FMC/tenant support

Active MAC Address Support

Active MAC address support includes important functionality in order to support policy-based routing (PBR).

Example of where and how to configure this on the APIC:

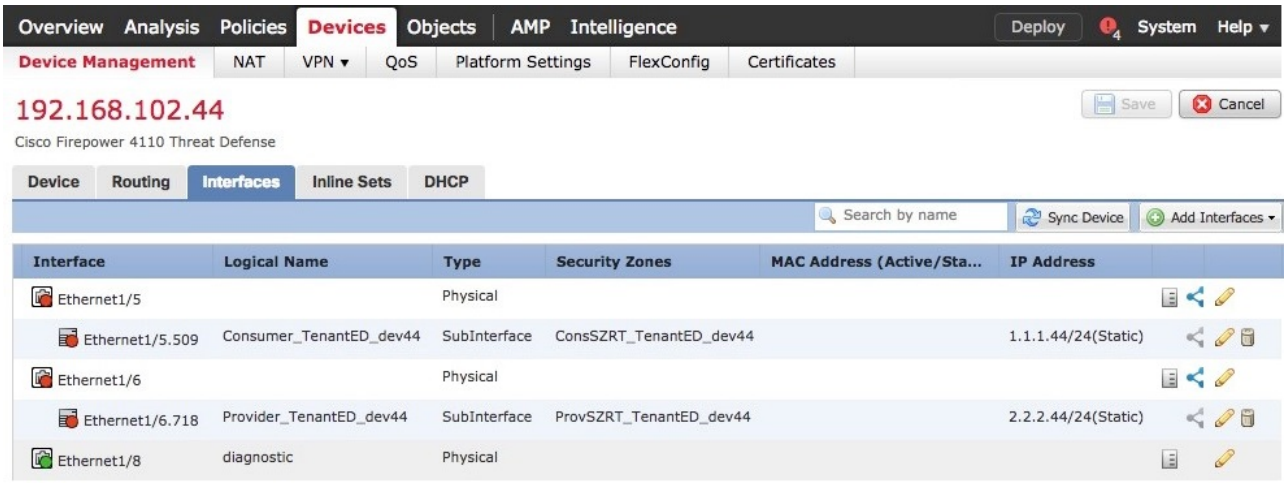


Multi-Instance FTD Support

With support for multiple instances of FTD, we can now support shared interfaces in addition to dedicated physical interfaces and dedicated port-channels.

Note Multi-instance is not currently supported on the Firepower-21xx platform.

Example of a shared interface configuration which was successfully pushed by the FTD DP to the FMC:



Multi FMC/Tenant Support

The enhancement of supporting multiple FMCs and multiple APIC tenants is achieved by leveraging multi-threading APIC service calls. The idea is to allow multiple service calls to run at the same time if the FMC and/or APIC tenant is different, instead of running them serially. As they can be run concurrently, this helps horizontal scalability in terms of overall performance when the deployment involves multiple FMCs and/or multiple APIC tenants.

Existing Features From Version 1.0(3)

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

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(4)

Table 2: Enhancement Requests Resolved in the Cisco FTD Device Package, Version 1.0(4)

Caveat	Description
CSCvm73837	Enhancement: horizontal scaling up of multiple FMCs support in FTD-DP
CSCvn25212	Enhancement: add active MAC address support in FTD-DP

Resolved Caveats in Version 1.0(4)

Table 3: Caveats Resolved in the Cisco FTD Device Package, Version 1.0(4)

Caveat	Description
CSCvn58411	If multi-graph in the same tenant, DP deletes SZs belonging to other graphs if using the same access policy
CSCvn67874	Unable to update IP address on existing bridge group interface
CSCvn67917	Workaround to identify active peer in HA deployment
CSCvn93943	FTD-DP deletes interface configuration if 2 contracts use the same graph and one graph gets removed
CSCvo45961	Graph interfaces are not associated with security zones after changing BVI ID from APIC

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(4)

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:

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

Only occurs when using FMC versions older than 6.3. One solution is to upgrade the FMC to version 6.3 or newer.

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

If the deployment fails:

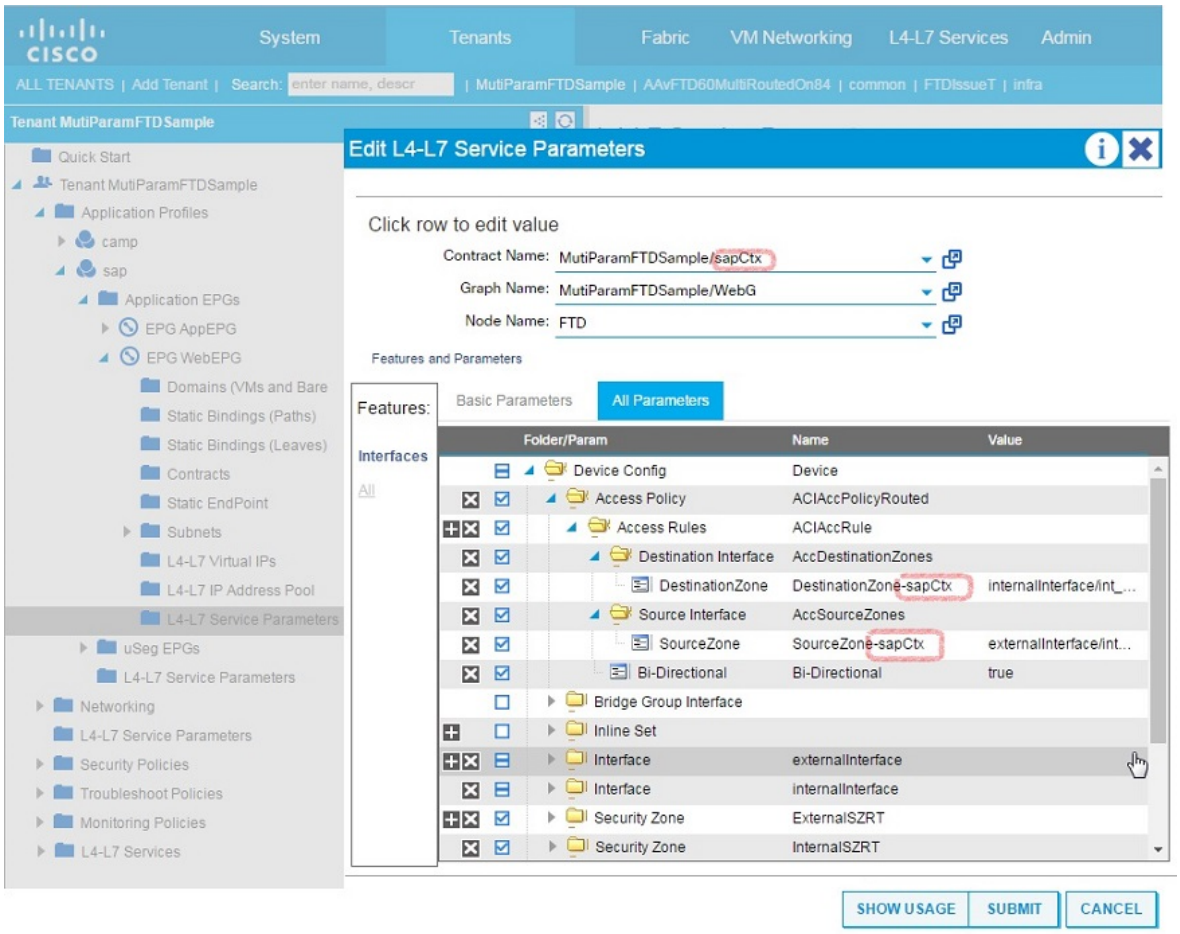
1. On the FMC:
    1. Navigate to **Devices**, and select the FTD.
    2. Delete the new BVI and the associated sub-interfaces. Click **Save**. Click **Deploy**.
    3. Wait for the FMC to complete the deployment.
2. On the APIC:
    1. In the node tree on the left, navigate to **L4-L7 Devices**, and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

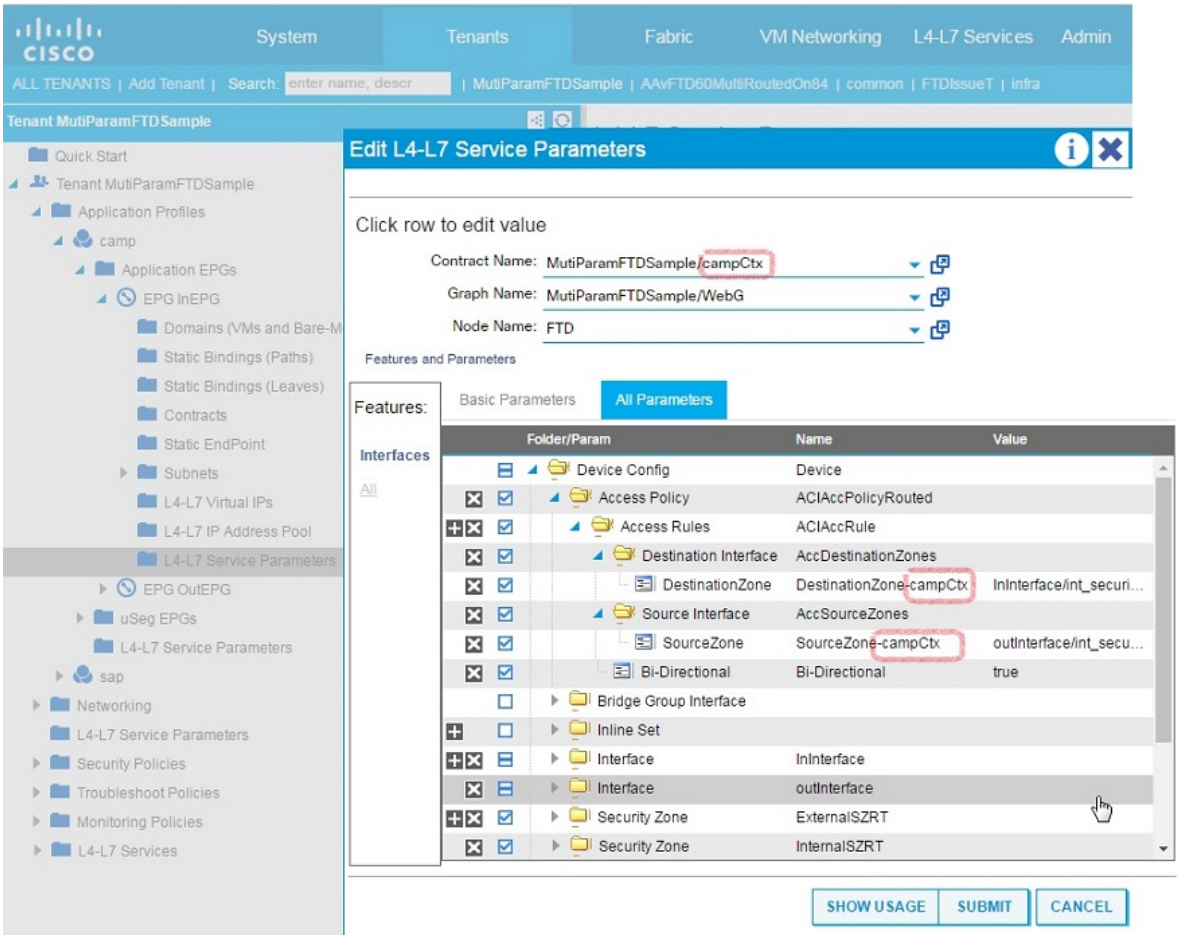
CSCvc46536

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 MutiParamFTDSample
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:
Interfaces
All
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



For more information, see the FMC Configuration Guide in Related Documentation, on page 10.

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.