Cisco FMC Endpoint Update App for ACI, Version 1.2 Quick Start Guide

First Published: 2021-05-19

Last Modified: 2021-05-19

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

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

CHAPTER 1

Introducing the FMC Endpoint Update App for the Cisco Application Centric Infrastructure (ACI)

The Firepower Management Center Endpoint Update App for the Cisco Application Centric Infrastructure (ACI) provides single-click access to all Cisco ACI fabric information, enabling network automation, programmability, and centralized management.

The following topics provide an overview of the FMC endpoint update app for ACI and related components.

Introduction

The Cisco Application Centric Infrastructure (ACI) is a software-defined network solution and application-intelligent fabric that brings application, security, and infrastructure together in the data center. ACI consists of the following:

- The Cisco Application Policy Infrastructure Controller (APIC) provides single-click access to all Cisco ACI fabric information, enabling network automation, programmability, and centralized management.

  To use the system, perform the following tasks in the order shown:

  1. Install and configure APIC as discussed in the Cisco APIC Getting Started Guide.
  2. Install and configure the FMC endpoint update app discussed in this guide.

- The FMC endpoint update app periodically retrieves endpoint information from the APIC and pushes it to the Firepower Management Center using a REST API. This helps when configuring a security policy on the FMC.

  This guide discusses the FMC endpoint update app.

APIC 5.1 introduces a remediation module that quarantines an infected FMC so no more traffic is allowed to go in or out of that FMC. You do not have to configure anything in the to use this module. For more information, see the release notes.

Related Documentation

- Cisco Application Centric Infrastructure Fundamentals, ACI App Center
- Cisco Firepower Management Center Configuration Guides

CHAPTER 2

Install or Upgrade the FMC Endpoint Update App

This chapter discusses how to install or upgrade and enable the FMC endpoint update app.

Install or Upgrade the FMC Endpoint Update App

To download, install, and enable the FMC endpoint update app, complete the following procedure:

Procedure

Step 1 Log in to APIC.

Step 2 Install the FMC endpoint update app:

a) Click **Apps**.

b) Click **Download Application** (⬇). (link to the download)

c) Search for **FMC Endpoint Update**.

d) When you locate it, click **Download** (⬇).

e) Follow the prompts on your screen to complete the download.

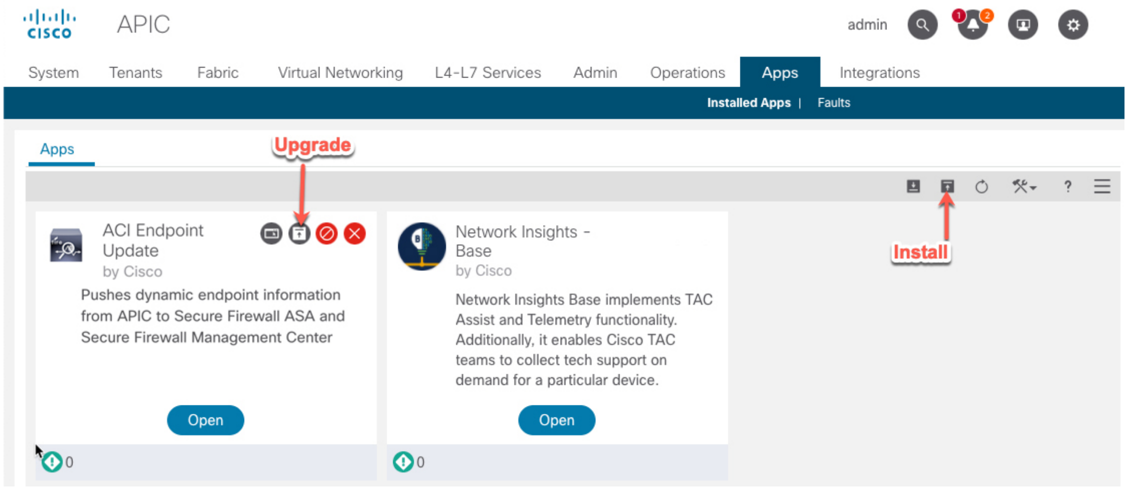
f) Click the APIC tab page in your browser.

Step 3 Click **Apps** > **Apps**.

Step 4 Do any of the following:

- Install: Click **Add Application** (⬆) in the toolbar.
- Upgrade: **Upgrade** (⬆) next to FMC endpoint update app.

The following figure shows both options.


APIC
admin
System
Tenants
Fabric
Virtual Networking
L4-L7 Services
Admin
Operations
Apps
Integrations
Installed Apps |
Faults
Apps
Upgrade
Install
ACI Endpoint Update
by Cisco
Pushes dynamic endpoint information from APIC to Secure Firewall ASA and Secure Firewall Management Center
Open
Network Insights - Base
by Cisco
Network Insights Base implements TAC Assist and Telemetry functionality. Additionally, it enables Cisco TAC teams to collect tech support on demand for a particular device.
Open
0
0

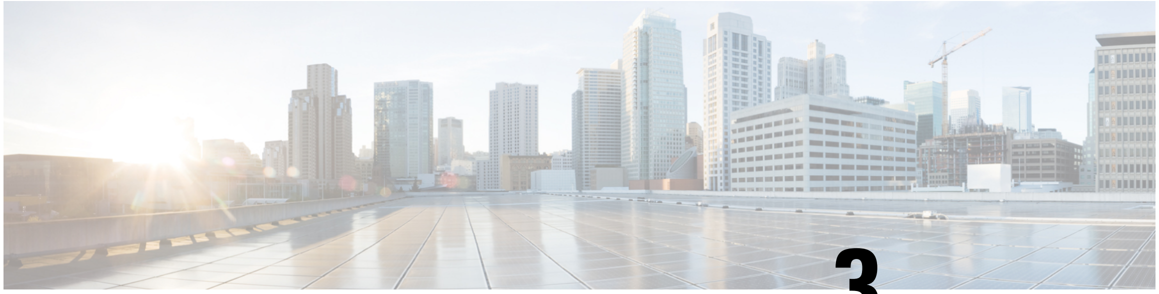
Step 5 Follow the prompts on your screen to upload the app.

Step 6 Wait for the app to be installed or upgraded.

Step 7 Click **Enable**.

Step 8 When prompted, click the name of a security zone from the list.

Step 9 Click **Enable** to enable the app.



CHAPTER 3

Configure the FMC Endpoint Update App

The following task enables you to configure the FMC endpoint update app to communicate with the FMC.

Prerequisites for Configuration

The following topics discuss prerequisite tasks you must complete before configuring the FMC Endpoint Update App.

Related Topics

Configure the FMC Domains and Subdomains, on page 5
Create Users for the FMC Endpoint Update App, on page 6

Configure the FMC Domains and Subdomains

Data in one APIC tenant is pushed and merged to one particular FMC domain you configure. APIC does *not* modify or delete any other object in another FMC domain. Note that objects defined in a domain are visible and usable in an FMC's subdomains, and that can be a way to share an object across subdomains.

For more information about domains, see the chapter on domain management in the Cisco Firepower Management Center Configuration Guide.

Create domains and subdomains

Before you continue, make sure you have created all users, domains, and subdomains on the FMC. Subdomain users must be created in the correct domain (**System** (⚙) > **Users** > **Create User**. If necessary, click **Add Domain** to add the user to the desired domain.)

To create a domain on the FMC:

1. Log in to the FMC.
2. Click **System** (⚙) > **Domains** > **Add Domain**.
3. Enter the required information.

4. Click **Save**.

5. Click **Save**.

Examples

When you create a device in the FMC Endpoint Update App:

- Enter a username only to push and merge the configuration to the default Global domain on the FMC.

- Enter a domain and username in the format *domain\user* to get dynamic data from the tenant and access the FMC as *user*and update the objects of the subdomain named *domain* of the Global domain.

- Enter a domain and username in the format *domain1/domain2\user2* to get dynamic data from the APIC tenant and access the FMC as *user2* and update the objects of the subdomain *domain2*, which is a subdomain of *domain1*, which is a subdomain of Global.

For example, to push the APIC configuration for a tenant named ExampleTenant to the **`Global \ domain1 \ domain2`** domain on an FMC with IP address 192.0.2.25 as a user named SampleUser:

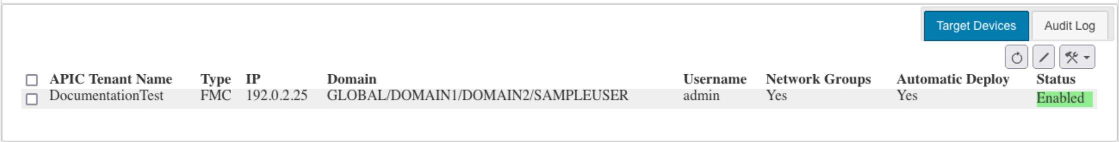
1. Log in to APIC.

2. Click **Apps** > **Apps**.

3. Under FMC Endpoint Update, click **Open**.

4. Click **Add Tenant/FMC**.

5. Add the following row to the table.



□	APIC Tenant Name	Type	IP	Domain	Username	Network Groups	Automatic Deploy	Status
□	DocumentationTest	FMC	192.0.2.25	GLOBAL/DOMAIN1/DOMAIN2/SAMPLEUSER	admin	Yes	Yes	Enabled

Related Topics

Create Users for the FMC Endpoint Update App, on page 6

Create Users for the FMC Endpoint Update App

You must create one dedicated FMC user for the FMC Endpoint Update App to update network object and dynamic object configuration:

- The dedicated user is exclusively for the FMC endpoint update app to update the FMC network object configuration

- In addition, you must have a second administative user that can be shared between the FMC endpoint update app and other FMC functions. (This can be an existing user or a new user.)

Each user must have the Administrator role. Each ASA user must have privilege level 15. It's necessary to have to users to avoid the FMC endpoint update app logging out the administrator unexpectedly.

The task that follows discusses how to create users on the FMC only. To create ASA users, see the *Cisco ASA Series General Operations ASDM Configuration Guide*.

Procedure

Step 1 Log in to the FMC if you haven't done so already.

Step 2 Click **System** > **Users** > **Users**.

Step 3 Click **Create User**.

Step 4 Under User Role Configuration, check **Administrator**.

Step 5 (Optional.) Click **Add Domain** to give the user access to a particular domain.

Both FMC users must be administrators in the same domains.

Step 6 Enter the other information required to configure the user; consult the online help for assistance.

What to do next

See Configure the FMC Endpoint Update App, on page 7.

Configure the FMC Endpoint Update App

To configure the FMC endpoint update app, complete the following procedure:

Before you begin

Before you configure and use the FMC Endpoint Update App, complete all of the following tasks:

- Configure the APIC application at minimum with:
  - A tenant for the FMC
  - In the tenant configuration, an application profile and an endpoint group (EPG)

  For more information about configuring APIC, see the chapter on Basic User Tenant Configuration in the Cisco APIC Basic Configuration Guide.
- Create one dedicated FMC user with the Administrator role.

  For more information, see Create Users for the FMC Endpoint Update App, on page 6.
- (Optional.) Create domains on the FMC as discussed in Configure the FMC Domains and Subdomains, on page 5.

Procedure

Step 1 Log in to APIC.

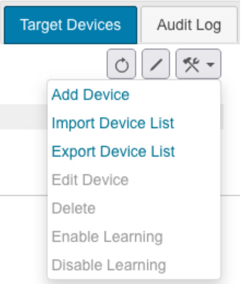
Step 2 Click **Apps** > **Apps** > **FMC Endpoint Update**.

Step 3 Locate the FMC endpoint update app.

Step 4 Click **Open**.

Step 5 Click 🛠▾ (Config Devices) > **Add Device**.

The following figure shows an example.



Step 6 For **Type**, click either **FMC** or **ASA**.

Step 7 Enter or edit the following information.

Item	Description
Update Interval	Enter the interval, in seconds, to update the FMC. Default is 60. The minimum interval is 30 seconds because updating too frequently might negatively impact system performance with a large number of FMCs.
Add Tenant/FMC	Click to add a row to the table and enter the following information: • **APIC Tenant Name**: Enter the name of an existing tenant. • **FMC IP**: Enter the FMC's IP address or fully-qualified host name. If your FMC is behind a NAT device, separate the IP address from the port with a colon character; for example, `192.2.0.9:5001`. • **FMC Domain/Username**: Enter the alphanumeric username used by the app to sign in to the FMC. The username must be different than the username you use to sign in to the FMC. Otherwise, if they're the same, your sessions might get disconnected. Enter the domain and subdomain name, if any, to which to push data. Domain names can consist of alphanumeric characters or the \ and / characters only. For more information, see Configure the FMC Domains and Subdomains, on page 5. • **FMC Password**: Enter the FMC user's password. Click **Remove** at the end of the row to remove an FMC tenant.
Site Prefix	Enter a unique alphanumeric string to create a network group object on the FMC. In a multi-tenant environment,

Item	Description
	different network group objects prevent the configuration sent by APIC from being confused with any other configuration.
Automatic Deploy	FMC Check the box to start an FMC policy deployment after the app completes a periodic endpoint update. Consider disabling this option during periods of desired manual control of FMC configuration, such as during a maintenance window for FMC policy changes.
Download Config to JSON File	See JSON Configuration Reference, on page 9.
Cleanup FMC Objects	(FMC only.) See FMC Cleanup Reference, on page 10.
Failed Logins	Validates the configured FMC user name and password. The app displays login information with a UTC timestamp to identify each one.

Step 8 After you’ve configured all your FMCs, click **Submit Data**.

JSON Configuration Reference

You can optionally upload and download the FMC endpoint update app in JSON format. This might be useful to create a large configuration at once and then to back up that configuration later.

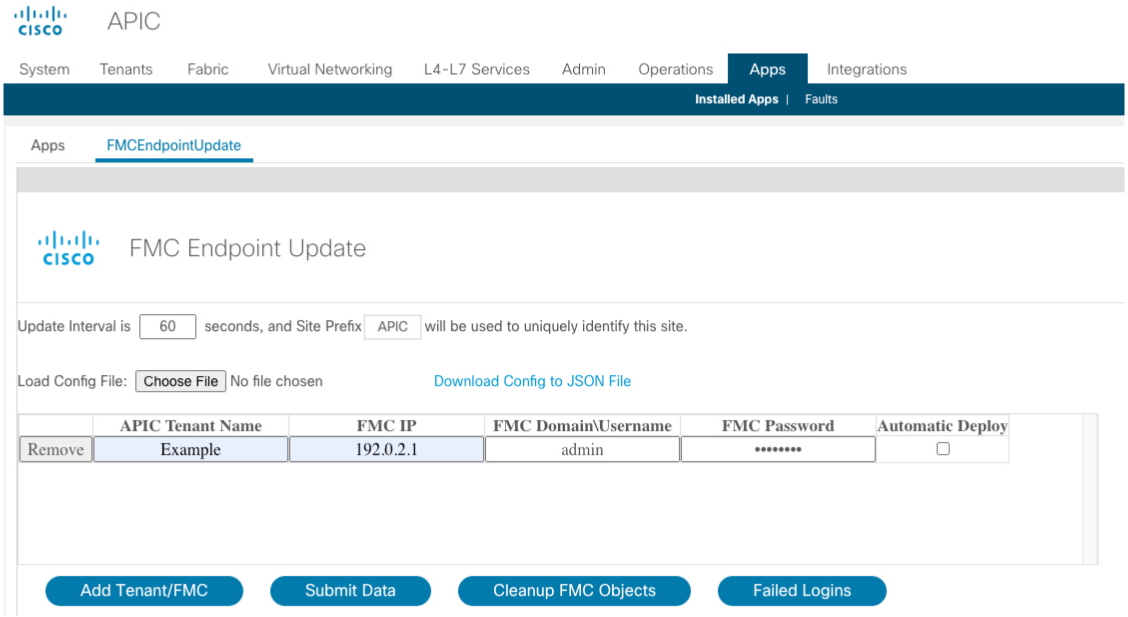
The JSON format follows:

```
{"interval":"value","site_prefix":"prefix","tenant_1":"name", "user_1": "username",
"password_1":
"<hidden>","deploy_n":"{true|false}","status_n":"enabled|reachable|Connectivity is
OK","domain_n":domain name}
```

We recommend you download a configuration (even an empty one), edit the JSON file, then upload it.

After you upload a configuration, you must click **Submit Data** to save it.

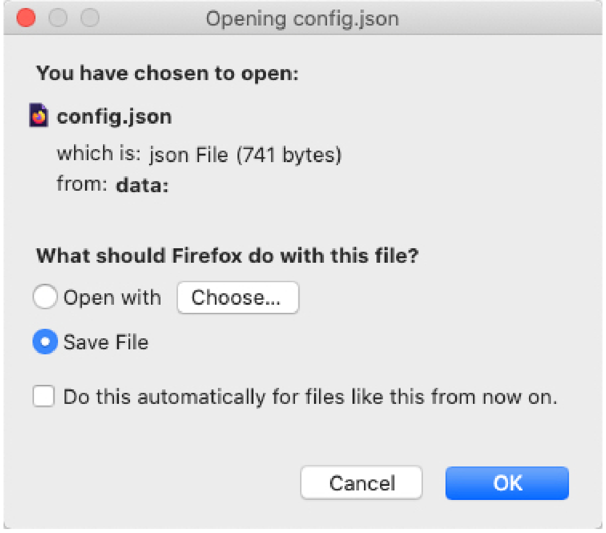
An example follows.



Update Interval is 60 seconds, and Site Prefix APIC will be used to uniquely identify this site.

Load Config File: Choose File No file chosen Download Config to JSON File

	APIC Tenant Name	FMC IP	FMC Domain\Username	FMC Password	Automatic Deploy
Remove	Example	192.0.2.1	admin	••••••••	□



You have chosen to open:

config.json

which is: json File (741 bytes)

from: data:

What should Firefox do with this file?

○ Open with Choose...

● Save File

□ Do this automatically for files like this from now on.

JSON for the preceding configuration:

```
{"interval":"60","site_prefix":"TEST","tenant_1":"Example","ip_1":"192.0.2.1","user_1":
"admin","password_1":"<hidden>","deploy_n":"false"}
```

FMC Cleanup Reference

You can optionally clean up the APIC configuration pushed to the FMC in the event any of the following occur:

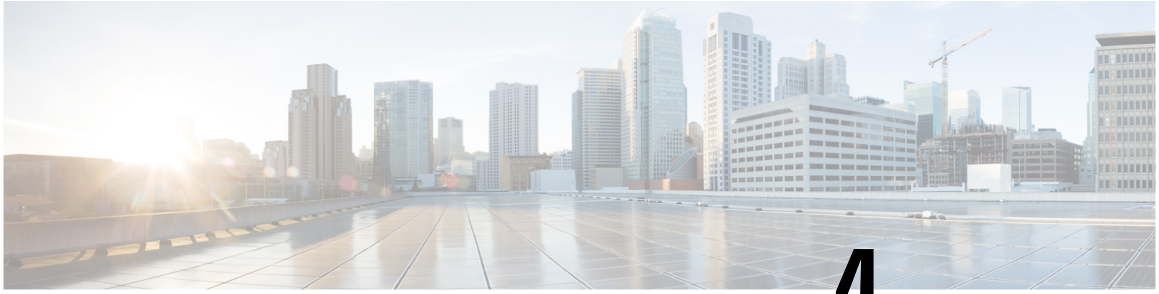
- You remove the APIC application entirely.
- You move the APIC configuration to another FMC.

The FMC endpoint update app cleans up the FMC object group configuration *only* for the site that is displayed in the app. No other configuration is removed either; for examle, if Domain1 is defined for Site 1 and Domain2 is defined for Site 2, if you clean the configuration of Site 2, Domain 1 is not affected.

When disabling learning, check **Erase all objects** to erase the pushed object information on configured devices.To avoid configuration conflicts, we prevent pushing a new configuration to the FMC at the same time as cleaning up an existing configuration.

If the object group you clean up is used in any access control rule on the FMC, the following happens:

- The FMC network object is not deleted.
- The IP address is replaced by 127.0.0.1.



CHAPTER 4

Verify the FMC Endpoint Update App

Verify the FMC endpoint update app for ACI is working properly by checking the network objects in the FMC.

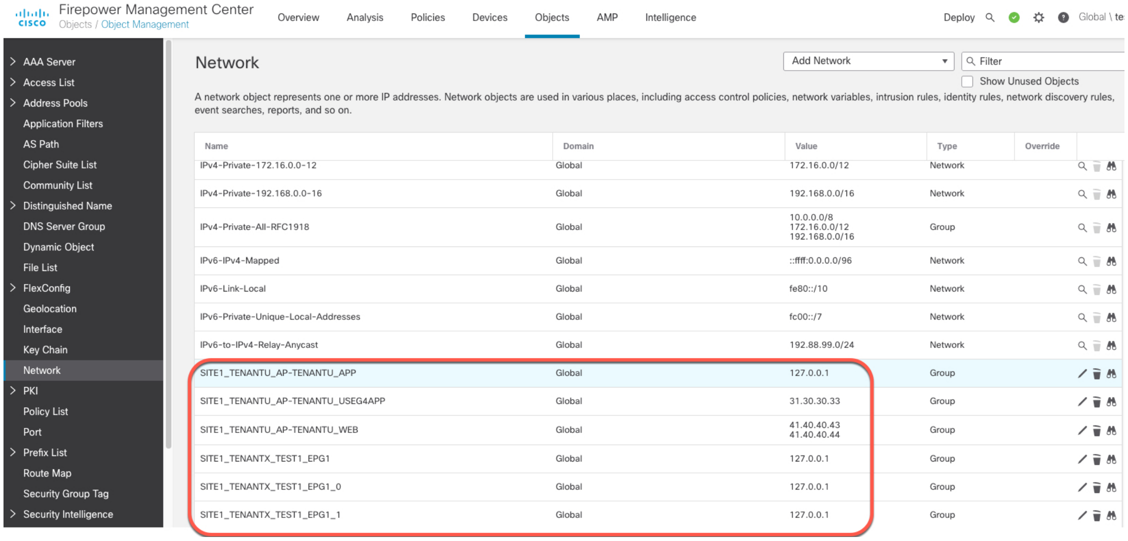
Verify the Endpoint Update in the FMC

When an APIC endpoint is pulled and pushed to the FMC, it's put into a network object named *SitePrefix_TenantName_ApplicationProfileName_ApplicationEPGName*.

Procedure

Step 1 Log in to the FMC.

Step 2 Click **Objects** > **Object Management** > **Network**.



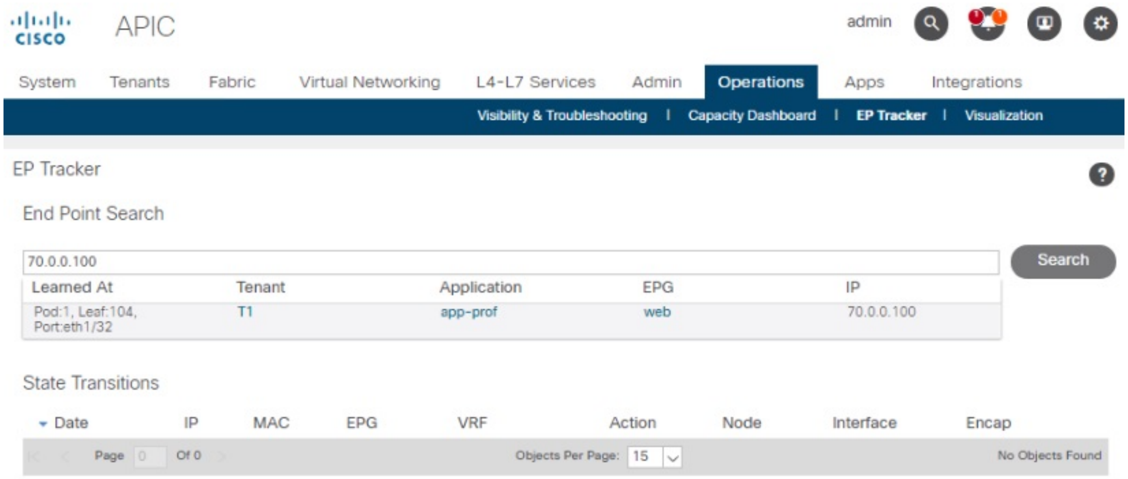
Network

A network object represents one or more IP addresses. Network objects are used in various places, including access control policies, network variables, intrusion rules, identity rules, network discovery rules, event searches, reports, and so on.

Name	Domain	Value	Type	Override
IPv4-Private-172.16.0.0-12	Global	172.16.0.0/12	Network	
IPv4-Private-192.168.0.0-16	Global	192.168.0.0/16	Network	
IPv4-Private-All-RFC1918	Global	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	Group	
IPv6-IPv4-Mapped	Global	::ffff:0.0.0.0/96	Network	
IPv6-Link-Local	Global	fe80::/10	Network	
IPv6-Private-Unique-Local-Addresses	Global	fc00::/7	Network	
IPv6-to-IPv4-Relay-Anycast	Global	192.88.99.0/24	Network	
SITE1_TENANTU_AP-TENANTU_APP	Global	127.0.0.1	Group	
SITE1_TENANTU_AP-TENANTU_USEG4APP	Global	31.30.30.33	Group	
SITE1_TENANTU_AP-TENANTU_WEB	Global	41.40.40.43 41.40.40.44	Group	
SITE1_TENANTX_TEST1_EPG1	Global	127.0.0.1	Group	
SITE1_TENANTX_TEST1_EPG1_0	Global	127.0.0.1	Group	
SITE1_TENANTX_TEST1_EPG1_1	Global	127.0.0.1	Group	

What to do next

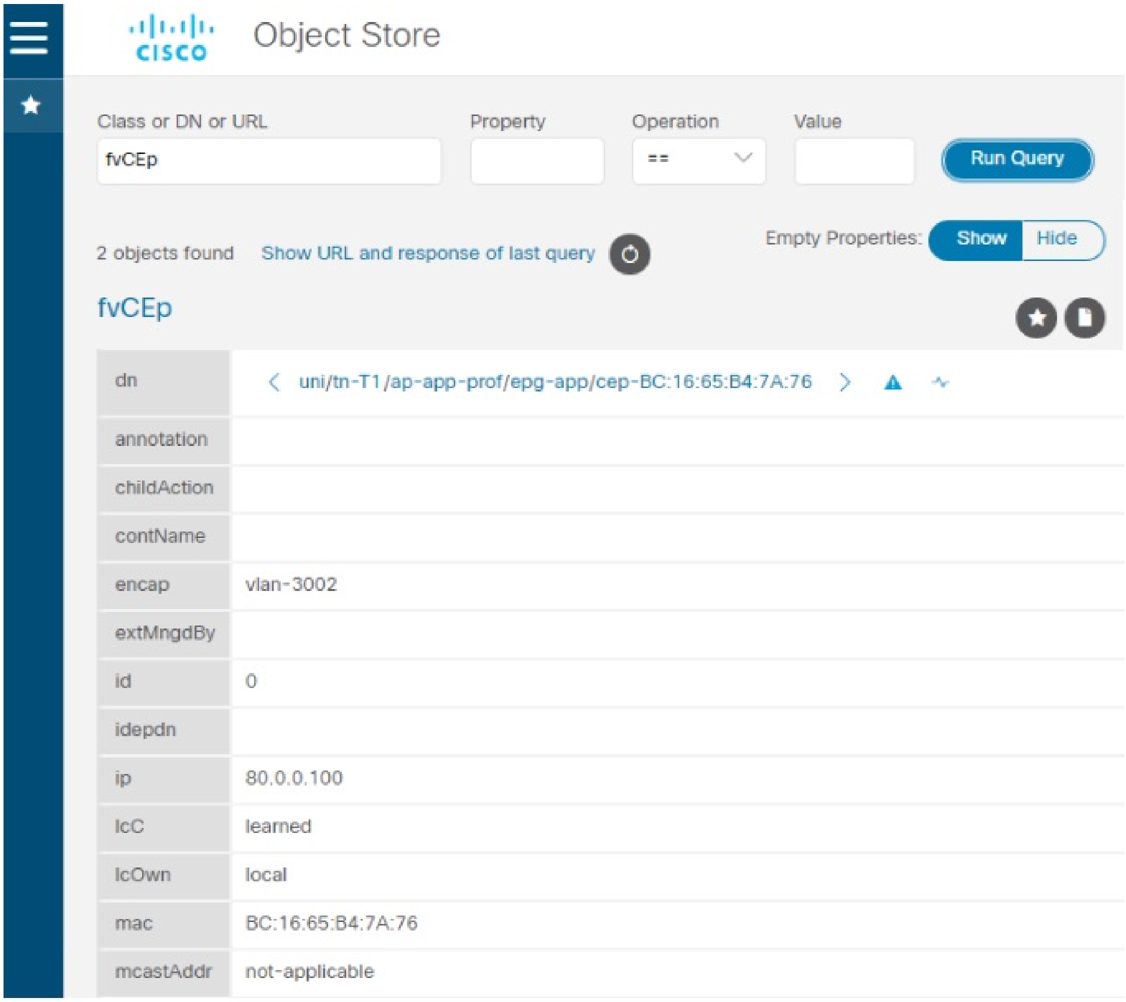
For troubleshooting purposes, you can track endpoints in the APIC's EP Tracker and Object Store Browser:



70.0.0.100

Learned At	Tenant	Application	EPG	IP
Pod:1, Leaf:104, Port:eth1/32	T1	app-prof	web	70.0.0.100

Date	IP	MAC	EPG	VRF	Action	Node	Interface	Encap


Object Store
Run Query
Show URL and response of last query
Empty Properties: Show Hide

Class or DN or URL: fvCEp
Property:
Operation: ==
Value:

2 objects found

fvCEp

dn	uni/tn-T1/ap-app-prof/epg-app/cep-BC:16:65:B4:7A:76
annotation	
childAction	
contName	
encap	vlan-3002
extMngdBy	
id	0
idepdn	
ip	80.0.0.100
lcC	learned
lcOwn	local
mac	BC:16:65:B4:7A:76
mcastAddr	not-applicable

Additional notes:

- During the push process, the REST operation (POST, PUT, or DELETE) is determined based on the comparison of what data is on the APIC and what is on the FMC.
- For diff calculation, each tenant updates only the data of its own tenant.
- When all endpoints are deleted from an APIC endpoint group (EPG), the corresponding object group on the FMC gets deleted too. But if the object group is referenced or used in any access rule on the FMC, because there is a dependency, the object group cannot get deleted. In this case, we keep the group name and put the localhost IP address, 127.0.0.1, inside the group instead.