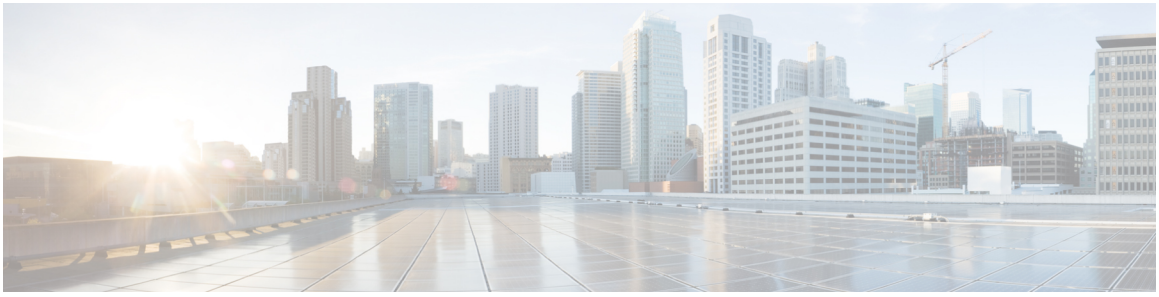
Cisco ACI Endpoint Update App, Version 2.3 Quick Start Guide

First Published: 2021-07-21

Last Modified: 2022-06-24

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



CONTENTS

CHAPTER 1 **Introducing the Endpoint Update App for the Cisco Application Centric Infrastructure (ACI)** 1

Introduction 1

Related Documentation 2

CHAPTER 2 **Install or Upgrade the ACI Endpoint Update App** 3

Install or Upgrade the ACI Endpoint Update App 3

CHAPTER 3 **Configure the ACI Endpoint Update App** 5

Prerequisites for Configuration 5

Configure the Management Center Domains and Subdomains 5

Create Users for the ACI Endpoint Update App 6

Configure the ACI Endpoint Update App 7

JSON Configuration Reference 9

Disable Learning Reference 10

Global and Device-Specific Options 10

CHAPTER 4 **Verify the ACI Endpoint Update App** 15

Verify the ACI Endpoint Update App in the Management Center 15

Verify the Endpoint Update App in the ASA 17

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.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

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.

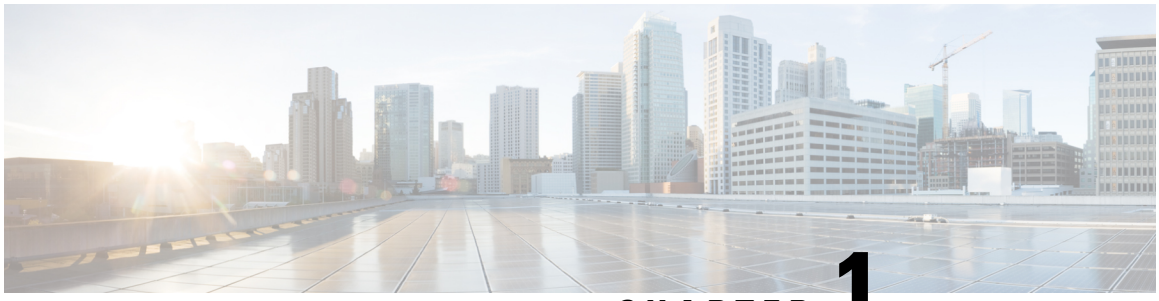
All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

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

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2022 Cisco Systems, Inc. All rights reserved.



CHAPTER 1

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

The 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 ACI endpoint update app and related components.

- Introduction, on page 1
- Related Documentation, on page 2

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 ACI endpoint update app discussed in this guide.

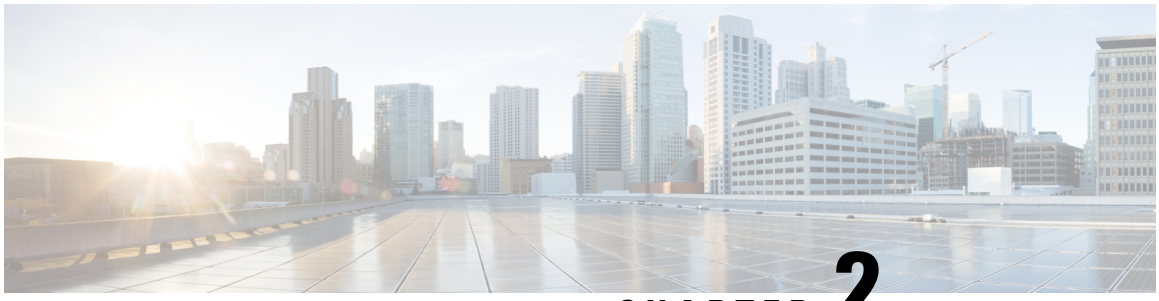
- The ACI endpoint update app periodically retrieves endpoint information from the APIC and pushes it to the Secure Firewall Management Center (formerly Firepower Management Center) and ASA using a REST API. This helps when configuring a security policy on the management center and ASA.

  This guide discusses the ACI endpoint update app.

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

Related Documentation

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



CHAPTER 2

Install or Upgrade the ACI Endpoint Update App

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

- Install or Upgrade the ACI Endpoint Update App, on page 3

Install or Upgrade the ACI Endpoint Update App

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

Step 1 Log in to APIC.

Step 2 Install the ACI endpoint update app:

a) Click **Apps**.

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

c) Search for **ACI 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.

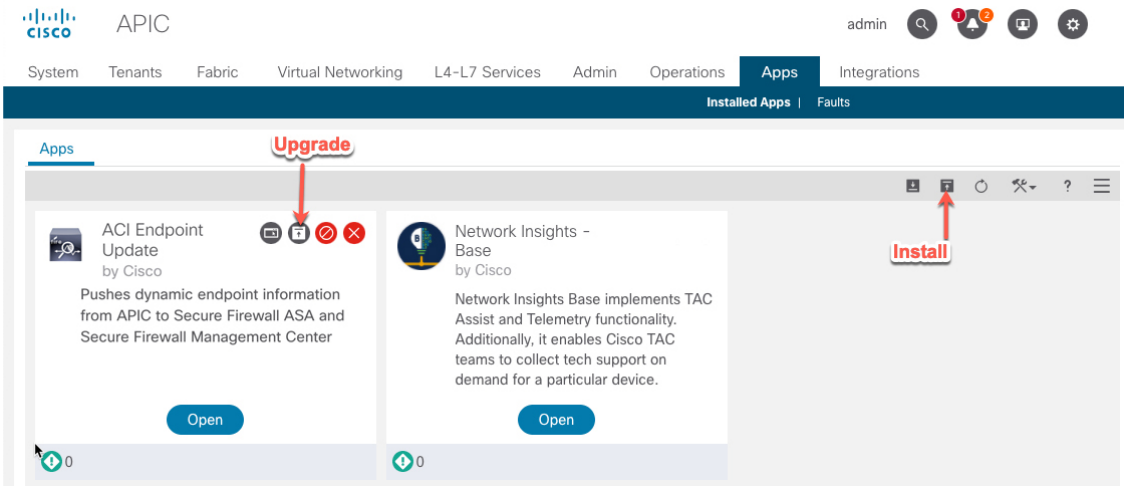
Step 3 Click **Apps** > **Apps**.

Step 4 Do any of the following:

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

The following figure shows both options.

Install or Upgrade the ACI Endpoint Update App



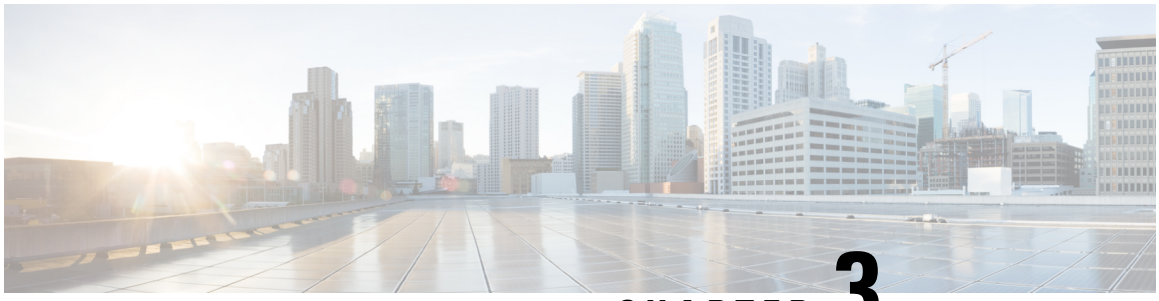
Step 5 Follow the prompts on your screen to upload the app.

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 ACI Endpoint Update App

The following task enables you to configure the ACI endpoint update app to communicate with the management center, ASA, and dynamic objects.

- Prerequisites for Configuration, on page 5
- Configure the ACI Endpoint Update App, on page 7
- JSON Configuration Reference, on page 9
- Disable Learning Reference, on page 10
- Global and Device-Specific Options, on page 10

Prerequisites for Configuration

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

Related Topics

Configure the Management Center Domains and Subdomains, on page 5

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

Configure the Management Center Domains and Subdomains

This section applies to management center devices only. ASA devices don't have domains.

Data in one APIC tenant is pushed and merged to one particular management center domain you configure. APIC does *not* modify or delete any other object in another management center domain. Note that objects defined in a domain are visible and usable in an management center'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 Secure Firewall Management Center Configuration Guide.

Create domains and subdomains

Before you continue, make sure you have created all users, domains, and subdomains on the management center. 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 management center:

1. Log in to the management center.
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 ACI Endpoint Update App:

- Enter a username only to push and merge the configuration to the default Global domain on the management center.
- In the **FMC Domain Name** field, enter a domain in the format *domain1\domain2* to get dynamic data from the tenant and access the management center and update the objects of the subdomain named *domain1\domain2* of the Global domain..
- In the **FMC Username** field, enter the username of a user with privileges to update objects in the management center.

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

1. Log in to APIC.
2. Click **Apps** > **Apps**.
3. Under management center Endpoint Update, click **Open**.
4. Click (Config Devices) > **Add Device > FMC**.
5. Add the device as discussed in Configure the ACI Endpoint Update App, on page 7; the following figure shows an example of adding an management center.
6. Add the following row to the table.

Related Topics

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

Create Users for the ACI Endpoint Update App

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

- The dedicated user is exclusively for the ACI endpoint update app to update the network object and dynamic object configuration

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

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

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

Step 1 Log in to the management center 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 management center 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 ACI Endpoint Update App, on page 7.

Configure the ACI Endpoint Update App

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

Before you begin

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

- Configure the APIC application at minimum with:
  - A tenant for the management center or ASA
  - 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 user with the Administrator role.

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

Step 1 Log in to APIC.

Configure the ACI Endpoint Update App

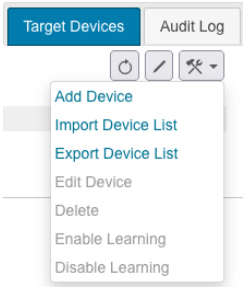
Step 2 Click **Apps** > **Apps** > **ACI Endpoint Update**.

Step 3 Locate the ACI 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
Tenant Name	Click the name of a tenant to which to add the device. (To select multiple tenants, hold down the Control key while clicking.)
IP	Enter the management center's or ASA's IP address or fully-qualified host name. If your management center or ASA is behind a NAT device, separate the IP address from the port with a colon character; for example, `192.2.0.9:5001`.
Username	Enter the user name of an management center or ASA user that is an Administrator in the domain (management center) or user context (ASA).
Password	Enter the user's password.
Confirm Password	Re-enter the user's password.
Domain	(Management Center only.) Enter the alphanumeric username used by the app to sign in to the management center. The username must be different than the username you use to sign in to the management center. 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 Management Center Domains and Subdomains, on page 5.

Item	Description
Network Groups	(Management Center only.) Check the box to deploy the network object configuration to the management center at the interval you select. (Management Center only.) Uncheck the box if you don't want to push dynamic EPG data as network objects. Dynamic objects will be pushed to the configured management center if the management center version is 7.0 and later.
Automatic Deploy	Management Center Check the box to start an management center policy deployment after the app completes a periodic endpoint update. Consider disabling this option during periods of desired manual control of management center configuration, such as during a maintenance window for management center policy changes.

Step 8 After you've configured all your management centers or ASAs, click **Submit**.

Related Topics

Global and Device-Specific Options, on page 10

JSON Configuration Reference

You can optionally upload and download the ACI 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.

All devices are exported when you request it but for easier reading, the following formats are split between management center and ASA.

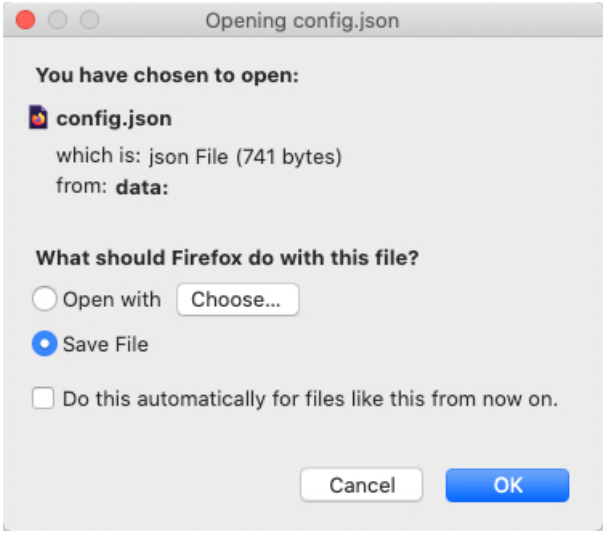
Management Center:

```
{"interval":"value","site_prefix":"prefix","ip_1":"host or
ip","user_1":"username","password_1":"<hidden>","tenant_1":"tenant
name","type_1":"FMC","networkgroup_1":true,
"deploy_1":true|false,"status_1":"enabled|unreachable|Connectivity is not
OK","domain_1":"name"}
```

ASA:

```
{"interval":"value","site_prefix":"prefix","ip_1":host or
ip","user_1":"name","password_1":"<hidden>","tenant_1":"tenant
name","type_1":"ASA","networkgroup_1":null,deploy_1":null,
"status_1":"enabled|reachable|Connectivity is OK","domain_1":null}
```

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



Disable Learning Reference

You can optionally clean up the APIC configuration pushed to the management center or ASA in the event any of the following occur:

- You remove the APIC application entirely.
- You move the APIC configuration to another management center or ASA.

The ACI endpoint update app cleans up the management center 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.

Note Domains are supported on the management center only.

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 management center or ASA 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 management center or ASA, the following happens:

- The management center network object or ASA network object group is not deleted.
- The IP address is replaced by 127.0.0.1.

Global and Device-Specific Options

This topic discusses how to set device-specific options for all configured devices.

Test connections to devices

You can test the connectivity to your configured devices; devices with connection issues have an orange background in the Status column.

To perform a connection test:

1. Log in to APIC.
2. Click **Apps** > **Apps** > **ACI Endpoint Update**.
3. Locate the ACI endpoint update app.
4. Click **Open**.
5. On the right side of the page, click (Test Connectivity).

   Devices that have connectivity issues have an orange background in the Status column; the following figure shows an example.

Edit global options

Global options consist of:

- Update interval: The interval, in seconds, to update the management center or ASA. Default is 60. The minimum interval is 10 seconds because updating too frequently might negatively impact system performance with a large number of the management centers or ASA.
- Site prefix: Enter a unique alphanumeric string to create a network group object on the management center or ASA. In a multi-tenant environment, different network group objects prevent the configuration sent by APIC from being confused with any other configuration.

To edit global options:

1. Log in to APIC.
2. Click **Apps** > **Apps** > **ACI Endpoint Update**.
3. Locate the ACI endpoint update app.
4. Click **Open**.
5. Click (Global Settings).
6. Enter or edit the following information:

Option	Description
Update interval is	Enter the update interval, in seconds. Default is 60. Minimum is 10.
and Site Prefix	Enter a unique alphanumeric site prefix. Maximum of 10 characters.

7. Click **Submit**.

Edit device-specific options

Device-specific options include the following:

- Import or export a JSON file with device information: see JSON Configuration Reference, on page 9.
- Edit a device's configuration: see Configure the ACI Endpoint Update App, on page 7.
- Enable or disable learning: Endpoint groups (EPGs) or Endpoint Security Groups (ESGs) act as containers for collections of applications, or application components and tiers, that can be used to apply forwarding and policy logic.

  EPG or ESG data includes network objects and dynamic objects.

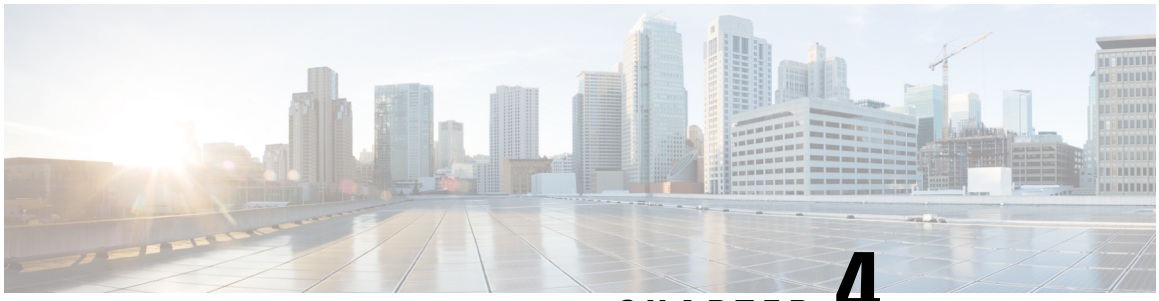
  - Dynamic objects are pushed to management centers with version 7.0 or later.
  - Dynamic objects are pushed to ASAs with version 9.3.1 or later.

Note If you choose to disable learning, you have the option of erasing data on a configured management center or ASA device.

To edit device-specific options:

1. Log in to APIC.
2. Click **Apps** > **Apps** > **ACI Endpoint Update**.
3. Locate the ACI endpoint update app.
4. Click **Open**.
5. Select the check box next to an management center or ASA device.
6. Click (Config Devices) then click one of the following options:
   - **Import Device List:** See JSON Configuration Reference, on page 9.
   - **Export Device List**: See JSON Configuration Reference, on page 9.
   - **Enable Learning**: Start learning on the selected device. You are required to confirm the selection.
   - **Disable Learning**: Stop learning on the selected device. If you click this option, a checkbox is displayed that enables you to optionally erase all existing learning objects on the device.

7. Follow the prompts on your screen to complete the action.



CHAPTER 4

Verify the ACI Endpoint Update App

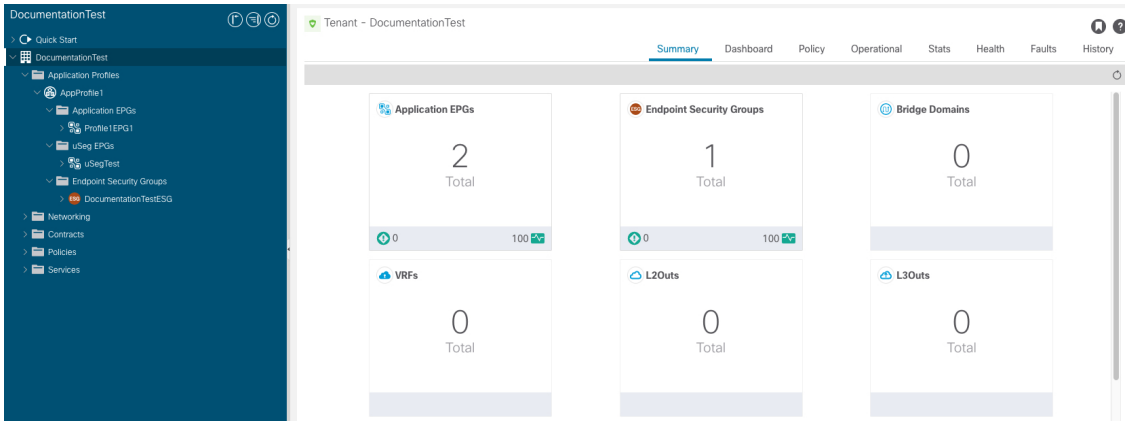
Verify the ACI endpoint update app is working properly by checking the network objects in the management center.

- Verify the ACI Endpoint Update App in the Management Center, on page 15
- Verify the Endpoint Update App in the ASA, on page 17

Verify the ACI Endpoint Update App in the Management Center

When an APIC endpoint is pulled and pushed to the management center, it's put into either a dynamic object or a network object. The object is named *SitePrefix_TenantName_ApplicationProfileName_ApplicationEPGName*.

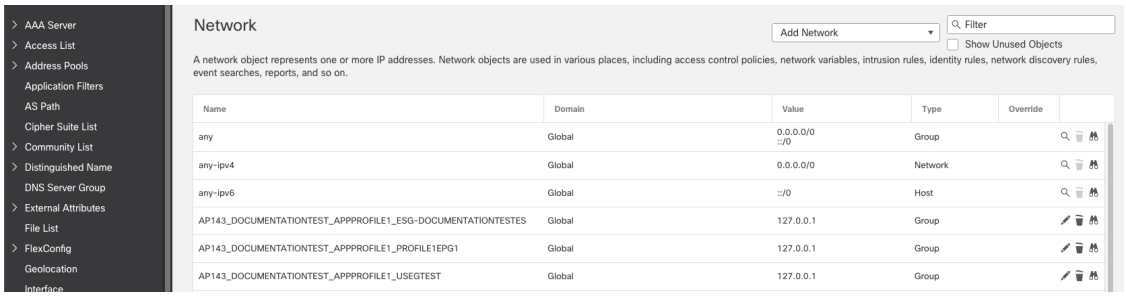
Following is an example APIC tenant on which the information in this section is based.



Step 1 Log in to the management center.

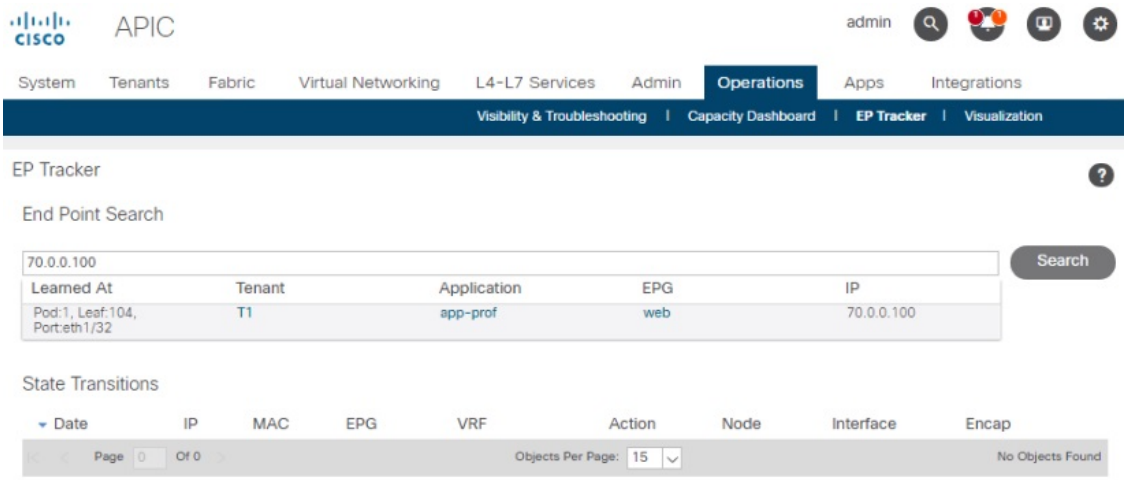
Step 2 Click one of the following:

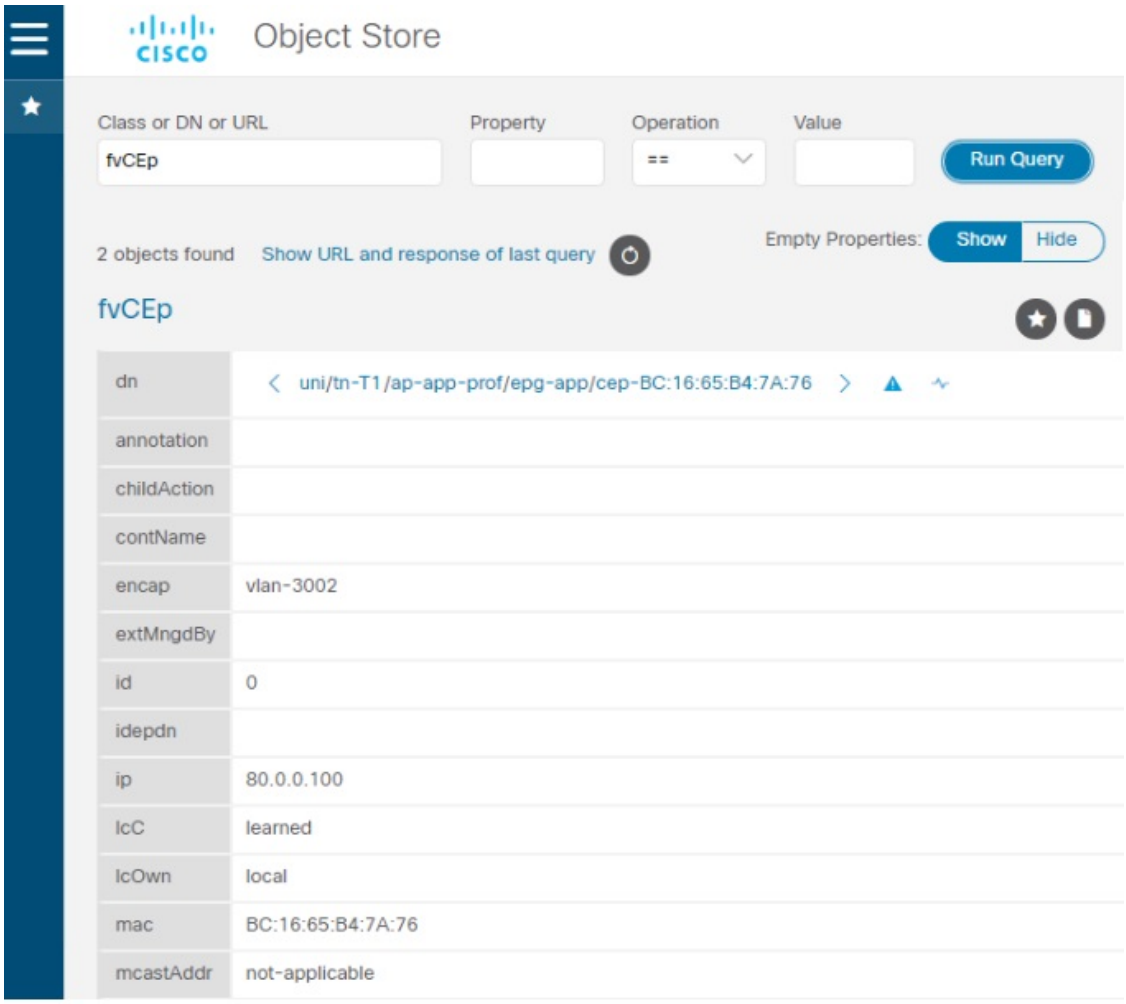
- Network object: Click **Objects > Object Management > Network**.
- Dynamic object: Click **Objects > Object Management > External Attributes** > **Dynamic Objects**.



What to do next

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





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 management center.
- 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 management center gets deleted too. But if the object group is referenced or used in any access rule on the management center, 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.

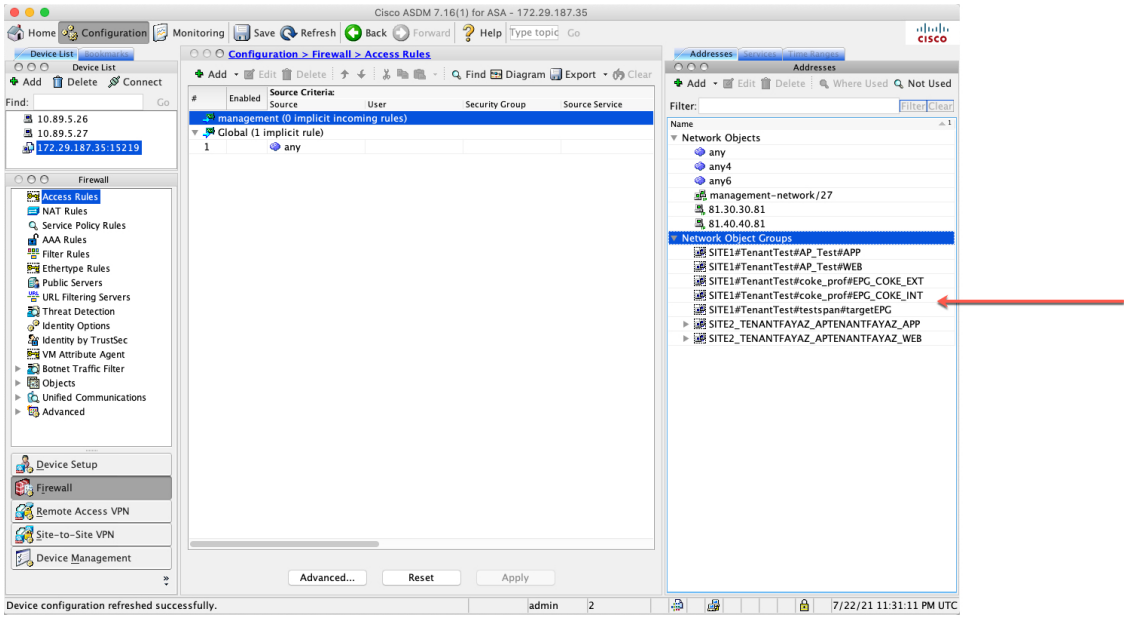
Verify the Endpoint Update App in the ASA

When an APIC endpoint is pushed to the ASA, it's put into a network object group named *SitePrefix#TenantName#ApplicationProfileName#ApplicationEPGName*.

Step 1 Start ASDM.

Step 2 Log in to the ASA.

Step 3 Click **Configuration** > **Firewall**.

Step 4 In the right pane, expand **Network Objects**.

Step 5 Network objects created by the Endpoint Update App are displayed under **Network Object Groups**, similar to the following.