Cisco APIC Integration with the Secure Firewall Management Center Solution Guide

First Published: 2025-05-07

Last Modified: 2025-12-03

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

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.

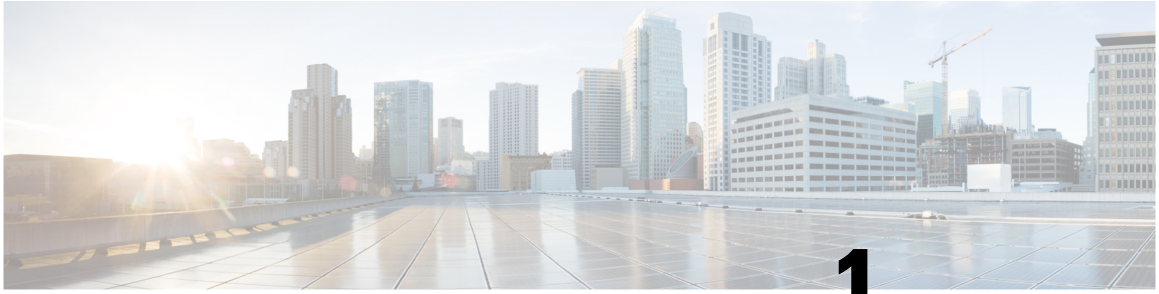
NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE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



CHAPTER 1

About the Cisco APIC Integration with the Secure Firewall Management Center

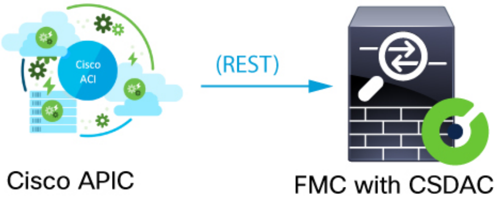
This chapter discusses the integration between Cisco APIC and the Secure Firewall Management Center.

About the Cisco APIC integration with the Secure Firewall Management Center

The dynamic attributes connector enables you to send Cisco APIC dynamic endpoint group (EPG) and endpoint security group (ESG) data from Cisco APIC tenants to the Secure Firewall Management Center.

Cisco APIC defines endpoint groups (EPGs) and endpoint security groups (ESGs) that have network object groups. Create a connector in the dynamic attributes connector that pulls that data from Cisco APIC tenants to the Secure Firewall Management Center on which you can use those objects in access control rules.

The following figure shows how the integration works.



Sample configuration

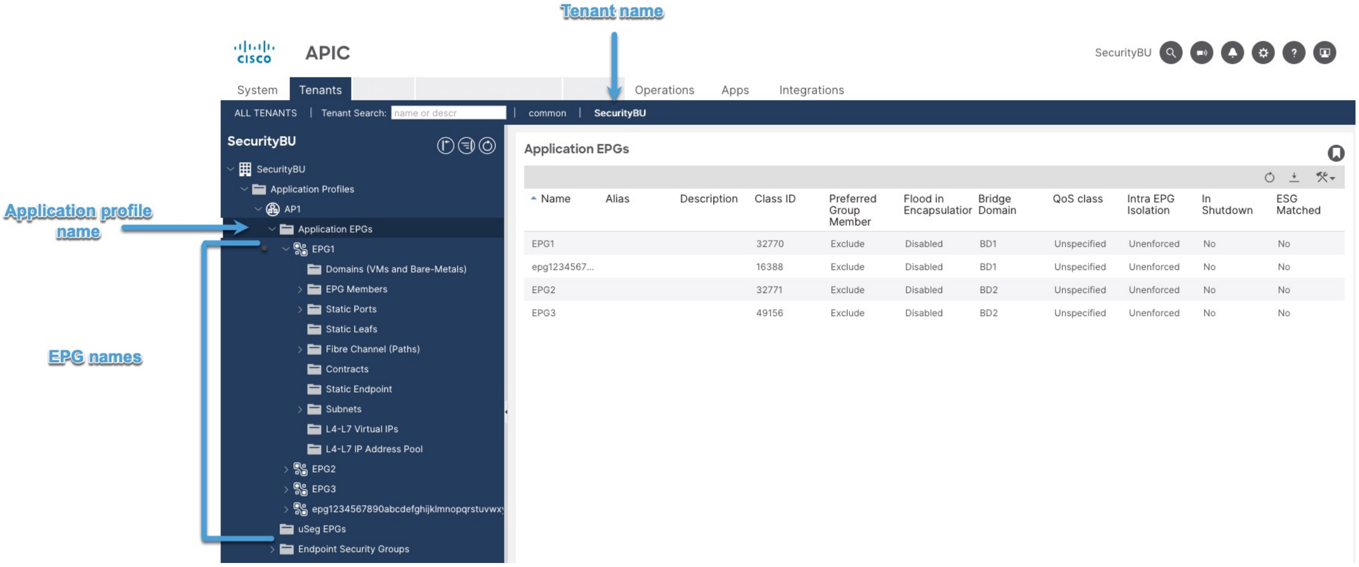
The following sample configuration shows how network object groups are named in the Secure Firewall Management Center based on names in APIC and the APIC connector (not shown).

Network object group names are a concatenation of (in order):

- Cisco ACI Endpoint Update App **Site Prefix** value

Cisco APIC tenant name); in this example, `CSDAC`.

- Cisco APIC application profile name (in this example, `AP1`)
- Cisco APIC EPG name (in this example, `EPG1` through `EPG4`)



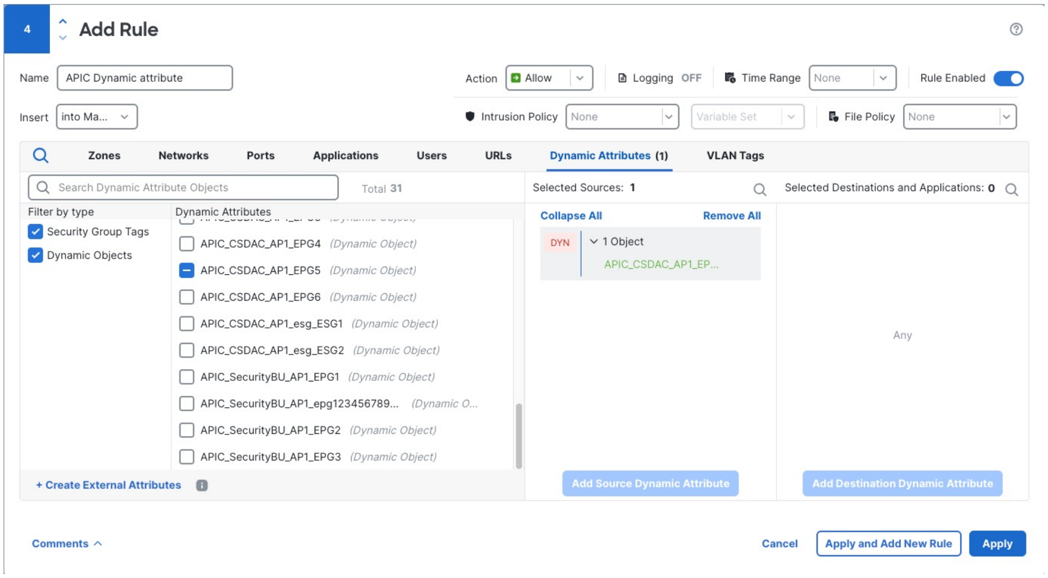
Application EPGs

Name	Alias	Description	Class ID	Preferred Group Member	Flood in Encapsulatior	Bridge Domain	QoS class	Intra EPG Isolation	In Shutdown	ESG Matched
EPG1			32770	Exclude	Disabled	BD1	Unspecified	Unenforced	No	No
epg1234567...			16388	Exclude	Disabled	BD1	Unspecified	Unenforced	No	No
EPG2			32771	Exclude	Disabled	BD2	Unspecified	Unenforced	No	No
EPG3			49156	Exclude	Disabled	BD2	Unspecified	Unenforced	No	No

The following figure shows sample Cisco APIC dynamic object names used in an access control rule.

Dynamic objects created by the integration with Cisco APIC have names matching the pattern:

```
APIC-site-name_tenant-name_application-profile-name_EPG-or-ESG-name
```



Name: APIC Dynamic attribute

Action: Allow

Logging: OFF

Time Range: None

Rule Enabled

Insert: into Ma...

Intrusion Policy: None

Variable Set

File Policy: None

Total 31

Selected Sources: 1

Selected Destinations and Applications: 0

Filter by type

☑ Security Group Tags

☑ Dynamic Objects

Dynamic Attributes

□ APIC_CSDAC_AP1_EPG4 *(Dynamic Object)*

▣ APIC_CSDAC_AP1_EPG5 *(Dynamic Object)*

□ APIC_CSDAC_AP1_EPG6 *(Dynamic Object)*

□ APIC_CSDAC_AP1_esg_ESG1 *(Dynamic Object)*

□ APIC_CSDAC_AP1_esg_ESG2 *(Dynamic Object)*

□ APIC_SecurityBU_AP1_EPG1 *(Dynamic Object)*

□ APIC_SecurityBU_AP1_epg123456789... *(Dynamic O...*

□ APIC_SecurityBU_AP1_EPG2 *(Dynamic Object)*

□ APIC_SecurityBU_AP1_EPG3 *(Dynamic Object)*

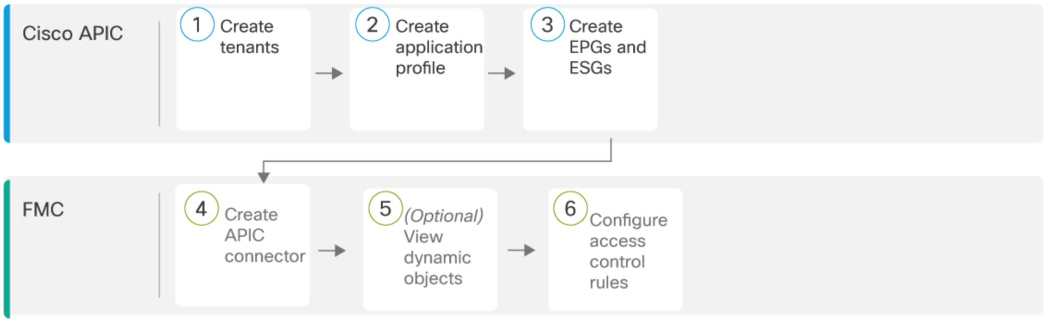
DYN 1 Object
APIC_CSDAC_AP1_EP...

Any

More information

- For more information about the dynamic attributes connector in the Secure Firewall Management Center, see Secure Firewall Management Center Device Configuration Guide.
- APIC Roles and Privileges Matrix
- Endpoint Security Groups
- Basic User Tenant Configuration

How to use dynamic objects from Cisco APIC in Secure Firewall Management Center access control rules or DNS Rules


Cisco APIC
1 Create tenants
2 Create application profile
3 Create EPGs and ESGs
FMC
4 Create APIC connector
5 (Optional) View dynamic objects
6 Configure access control rules

1 Basic User Tenant Configuration
2 Basic User Tenant Configuration
3 EPGs
4 Create a Cisco APIC connector, on page 9
5 View dynamic objects in the Secure Firewall Management Center, on page 17
6 Create access control rules using dynamic attributes filters, on page 18

Table 1: Configure Secure Firewall Management Center access control rules or DNS rules using network object groups

1	Cisco APIC	A tenant allows a Cisco APIC administrator to set up domain-based access control. See Basic User Tenant Configuration
2	Cisco APIC	An application profile is a container for other objects, such as an endpoint group (EPG). See Basic User Tenant Configuration
3	Cisco APIC	An EPG is a container for network objects that serves as the way that devices connect to the network. An ESG is a logical entity that contains a collection of physical or virtual network endpoints. See EPGs and ESGs
	Secure Firewall Management Center	If you haven't done so already, Enable the dynamic attributes connector.

4	Secure Firewall Management Center	Create the Cisco APIC connector which retrieves EPGs and ESGs from Cisco APIC and enables them to be used in Secure Firewall Management Center access control policies or DNS policies. See Cisco APIC connector.
5	Secure Firewall Management Center	(Optional.) View the dynamic objects fetched from Cisco APIC. (Optional.) See View dynamic objects in the Cisco Secure Firewall Management Center.
6	Secure Firewall Management Center	To use dynamic objects in access control policies or DNS policies, you must add them as dynamic objects to those rules. See Create access control rules or DNS rules using dynamic attributes filters.

CHAPTER 2

Configure the Cisco APIC Integration with the Secure Firewall Management Center

The following topics discuss how to configure the Cisco APIC Integration with the Secure Firewall Management Center.

System requirements for the integration with Cisco APIC

Your system must meet the following requirements:

- Secure Firewall Management Center version: 10.0.0 and later.

  Essentials license or better required; high availability is supported.

- Firewall Threat Defense version: 7.2 and later.
- Cisco APIC version: 3.0(1k) or later.
- If you use the ACI Endpoint Update App, it must be version 2.6.

Get required information for the integration

This section discusses:

- Information required to configure the integration
- Information used in dynamic object names

Cisco ACI Endpoint Update App site prefix and update interval

This information applies to you only if you're currently using the Cisco ACI Endpoint Update App; otherwise, you can skip it.

To find the Cisco ACI Endpoint Update App site prefix and update interval:

1. Log in to Cisco APIC as a user with `admin` privileges.

   For more information, see *APIC Roles and Privileges Matrix*.

2. Click **Apps**.

3. Under ACI Endpoint Update app, click **Open**.

4. Click **Edit** (🖉).

5. Write down the values of **Update Interval (In seconds)** and **Site Prefix**.

Required to configure the integration: Find a user with appropriate access

To find a user with at least the `read-all` role with `readPriv` access and the `tenant-admin` role with `writePriv` access for the security domain:

1. Log in to Cisco APIC.

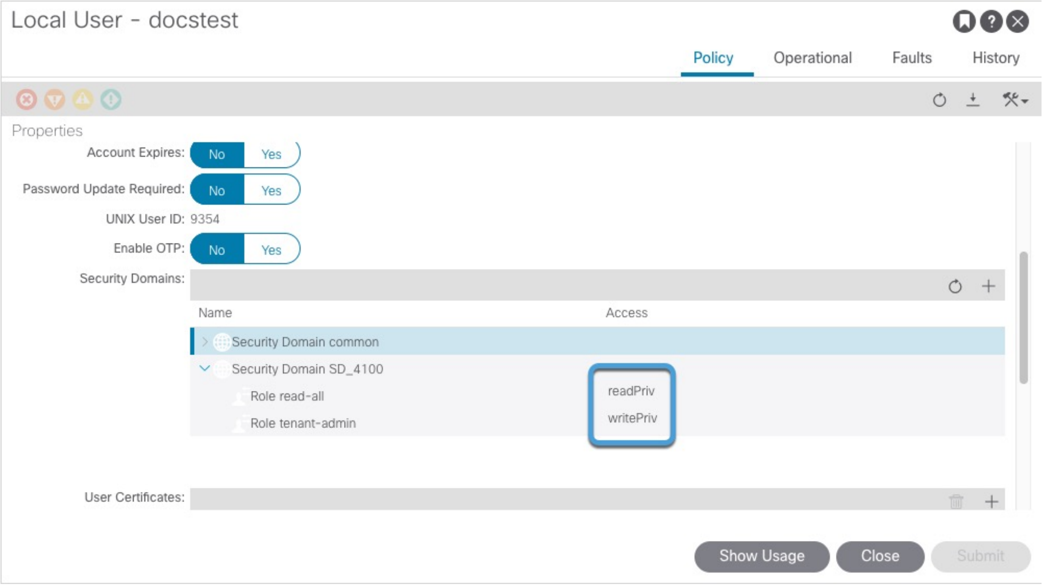
2. Click **Admin**.

3. In the left pane, click **Users**.

4. In the right pane, double-click the name of a user.

5. Scroll to Security Domains.

6. For the relevant security domain, make sure the user has at least the `read-all` role with `readPriv` access and the `tenant-admin` role with `writePriv` access for the security domain, as the following figure shows.



Local User - docstest

Properties

Account Expires: [✓ No] Yes

Password Update Required: [✓ No] Yes

UNIX User ID: 9354

Enable OTP: [✓ No] Yes

Security Domains:

Name	Access
Security Domain common	
Security Domain SD_4100	
Role read-all	readPriv
Role tenant-admin	writePriv

User Certificates:

Cisco APIC tenant name

The Cisco APIC tenant name is used in the names of dynamic objects created by this integration. To find it:

1. Log in to Cisco APIC.

2. Click **Tenants**.

3. Write down the name of the tenant that contains objects to send to the Secure Firewall Management Center.

Cisco APIC application profile name

The Cisco APIC application profile name is used in the names of dynamic objects created by this integration. To find it:

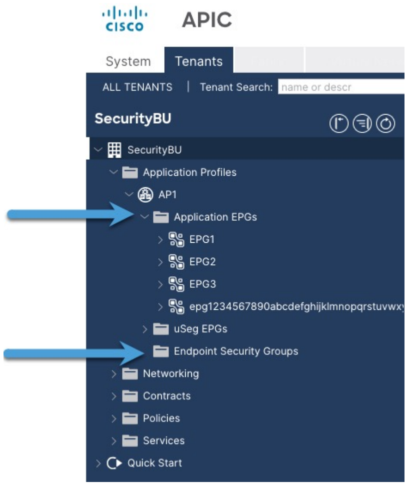
1. Log in to Cisco APIC.
2. Click **Tenants**.
3. Double-click the name of your tenant.
4. Expand your tenant.
5. Expand **Application Profiles**.
6. Write down the name of the application profile that contains EPGs and ESGs to integrate with the Secure Firewall Management Center.

EPG name

The Cisco APIC EPG name is used in the names of dynamic objects created by this integration. To find it:

1. Log in to Cisco APIC.
2. Click **Tenants**.
3. Double-click the name of your tenant.
4. Expand your tenant.
5. Expand **Application Profiles**.
6. Expand the name of the application profile.
7. Expand **Application EPGs**.
8. Write down the name of the EPG or ESG that has network object groups to send to the Secure Firewall Management Center.

   The following figure shows an example.



Create a connector

A *connector* is an interface with a cloud service. The connector retrieves network information from the cloud service so the network information can be used in policies on the Secure Firewall Management Center.

We support the following:

Table 2: List of supported connectors by Dynamic Attributes Connector version and platform

CSDAC version	AWS	AWS Security Groups	AWS Service Tags	Azure	Azure Service Tags	Cisco APIC	Cisco Cyber Vision	Cisco Multicl. Defense	Generic text	GitHub	Google Cloud	Microsoft Office 365	Tenable	vCenter	Webex	Zoom
Version 1.1 (on-premises)	Yes	No	No	Yes	Yes	No	No	No	No	No	No	Yes	No	Yes	No	No
Version 2.0 (on-premises)	Yes	No	No	Yes	Yes	No	No	No	No	No	Yes	Yes	No	Yes	No	No
Version 2.2 (on-premises)	Yes	No	No	Yes	Yes	No	No	No	No	Yes	Yes	Yes	No	Yes	No	No
Version 2.3 (on-premises)	Yes	No	No	Yes	Yes	No	No	No	No	Yes	Yes	Yes	No	Yes	Yes	Yes
Version 3.0 (on-premises)	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Version 3.1 (on-premises)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Cloud-delivered (Cisco Defense Orchestrator)	Yes	No	No	Yes	Yes	No	No	Yes	No	Yes	Yes	Yes	Yes	No	No	No
Secure Firewall Management Center 7.4.1	Yes	No	No	Yes	Yes	No	No	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes

CSDAC version	AWS	AWS Security Groups	AWS Service Tags	Azure	Azure Service Tags	Cisco APIC	Cisco Cyber Vision	Cisco Multicl. Defense	Generic text	GitHub	Google Cloud	Microsoft Office 365	Tenable	vCenter	Webex	Zoom
Secure Firewall Management Center 7.6	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Secure Firewall Management Center 7.7	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Secure Firewall Management Center 10.0.0	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes

For more information about connectors, see the configuration guide.

Create a Cisco APIC connector

This topic discusses creating a Cisco APIC connector that gets dynamic objects from a configured endpoint group (EPG) on Cisco APIC.

Before you begin

Review the information discussed in .

Procedure

Step 1 Log in to the Secure Firewall Management Center.

Step 2 Click **Integration** > **Dynamic Attributes Connector** > **Connectors**.

Step 3 Do any of the following:

- Add a new connector: click Add icon (+⌄), then click the name of the connector.
- Edit or delete a connector: Click **More** (⋮), then click **Edit** or **Delete** at the end of the row.

Step 4 Enter the following information.

Value	Description
Name	(Required.) Enter a name to uniquely identify this connector.
Description	Optional description.
Pull Interval	(Default 60 seconds.) Interval at which IP mappings are retrieved from Cisco APIC. We recommend setting this to 15 seconds.

Value	Description
Site Prefix	Do any of the following: • If you're not currently using the Cisco ACI Endpoint Update App, enter a value to be used in dynamic objects created by this integration (for example, **`APIC`**). • If you're currently using the Cisco ACI Endpoint Update App, enter a **Site Prefix** value that exactly matches the Cisco ACI Endpoint Update App **Site Prefix** value you found as discussed in Get required information for the integration.
Site Prefix	Enter a name to identify this connector with the corresponding ASA adapter. **Note** The **Site Prefix** name you enter here must exactly match all of the following: • The Cisco ACI Endpoint Update App **Site Prefix** value you found as discussed in Get required information for the integration. This value is *not* case-sensitive.
IP or Hostname	Enter the fully-qualified domain name or IP address of the Cisco APIC server from which to retrieve dynamic objects from EPGs and ESGs. *Do not* enter a scheme (such as **`https://`**) and *do not* include a trailing slash.
Add another cluster IP	(Optional.) Enter the IP address of other servers in the Cisco APIC cluster.
Username	Enter the name of a Cisco APIC user with at least at least the `read-all` role with `readPriv` access and the `tenant-admin` role with `writePriv` access for the security domain. Objects from all tenants the user has privileges to can be pushed to Secure Firewall Management Center.
Password	Enter the user's password.
Server Certificate	(Recommended if using fully-qualified domain name.) You have the following options: • Paste the certificate authority (CA) chain you got as discussed in . • Click **Get Certificate** > **Fetch** to automatically fetch the certificate or, if that is not possible, get the certificate manually as discussed in . • Click **Get Certificate** > **Browse from file** to upload a certificate chain you downloaded previously.

Step 5 Click **Test** and make sure the test succeeds before you save the connector.

Step 6 Click **Save**.

Step 7 Make sure **Ok** is displayed in the Status column.

Manually get a certificate authority (CA) chain

In the event you cannot automatically fetch the certificate authority chain, use one of the following browser-specific procedures to get a certificate chain used to connect securely to vCenter or, or Firewall Management Center.

The *certificate chain* is the root certificate and all subordinate certificates.

You can optionally use one of these procedures to connect to the following:

- vCenter or NSX
- Firewall Management Center
- Cisco APIC

Get a Certificate Chain—Mac (Chrome and Firefox)

Use this procedure to get a certificate chain using the Chrome and Firefox browsers on Mac OS.

1. Open a Terminal window.
2. Enter the following command.

   ```
   security verify-cert -P url[:port]
   ```

   where *url* is the URL (including scheme) to vCenter or, or Firewall Management Center. For example:

   ```
   security verify-cert -P https://myvcenter.example.com
   ```

   If you access vCenter or, or Firewall Management Center using NAT or PAT, you can add a port as follows:

   ```
   security verify-cert -P https://myvcenter.example.com:12345
   ```

3. Save the entire certificate chain to a plaintext file.
   - *Include* all `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` delimiters.
   - *Exclude* any extraneous text (for example, the name of the certificate and any text contained in angle brackets (< and >) as well as the angle brackets themselves.

4. Repeat these tasks for vCenter, or Firewall Management Center.

Get a Certificate Chain—Windows Chrome

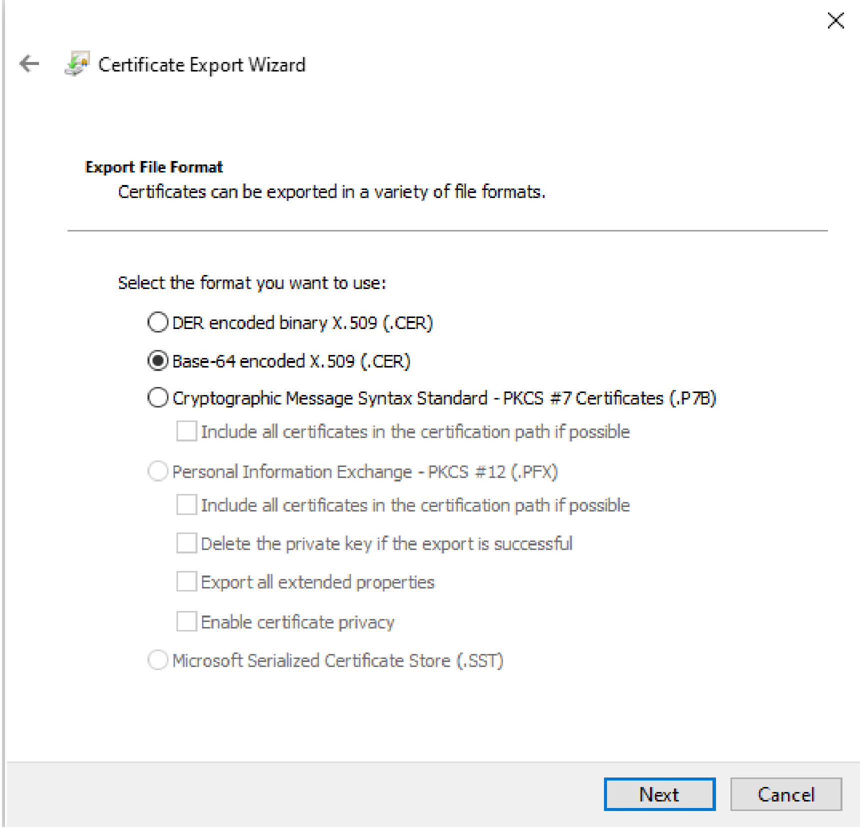
Use this procedure to get a certificate chain using the Chrome browser on Windows.

1. Log in to vCenter or, or Firewall Management Center using Chrome.
2. In the browser address bar, click the lock to the left of the host name.
3. Click **Certificate**.
4. Click the **Certification Path** tab.
5. Click the top (that is, first) certificate in the chain.
6. Click **View Certificate**.
7. Click the **Details** tab.

8. Click **Copy to File**.

9. Follow the prompts to create a CER-formatted certificate file that includes the entire certificate chain.

   When you're prompted to choose an export file format, click **Base 64-Encoded X.509 (.CER)** as the following figure shows.



Certificate Export Wizard

Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

● Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

○ Personal Information Exchange - PKCS #12 (.PFX)

□ Include all certificates in the certification path if possible

□ Delete the private key if the export is successful

□ Export all extended properties

□ Enable certificate privacy

○ Microsoft Serialized Certificate Store (.SST)

10. Follow the prompts to complete the export.

11. Open the certificate in a text editor.

12. Repeat the process for all certificates in the chain.

    You must paste each certificate in the text editor in order, first to last.

13. Repeat these tasks for vCenter or, or Firewall Management Center.

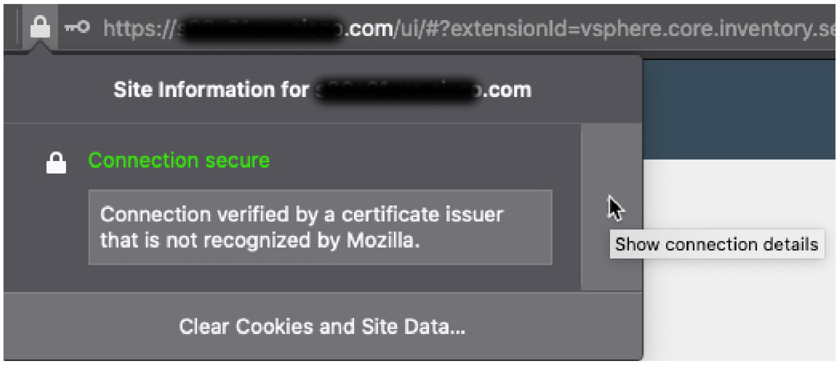
Get a Certificate Chain—Windows Firefox

Use the following procedure to get a certificate chain for the Firefox browser on either Windows or Mac OS.

1. Log in to vCenter or, or Firewall Management Center. using Firefox.

2. Click the lock to the left of the host name.

3. Click the right arrow (**Show connection details**). The following figure shows an example.



https://[redacted].com/ui/#?extensionId=vsphere.core.inventory.se

Site Information for [redacted].com

Connection secure

Connection verified by a certificate issuer that is not recognized by Mozilla.

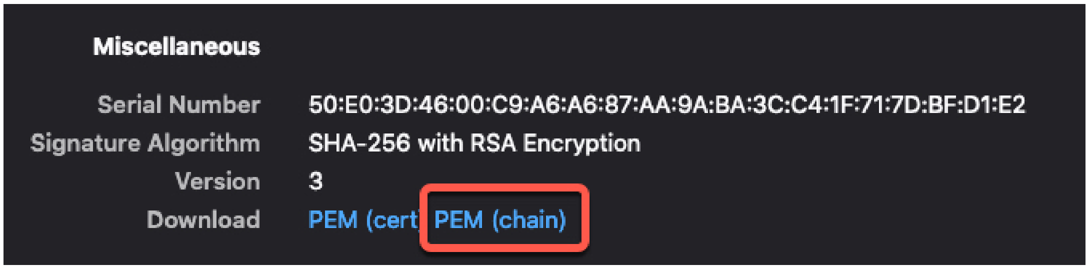
4. Click **More Information**.

5. Click **View Certificate**.

6. If the resulting dialog box has tab pages, click the tab page corresponding to the top-level CA.

7. Scroll to the Miscellaneous section.

8. Click **PEM (chain)** in the Download row. The following figure shows an example.



Miscellaneous

Serial Number	50:E0:3D:46:00:C9:A6:A6:87:AA:9A:BA:3C:C4:1F:71:7D:BF:D1:E2
Signature Algorithm	SHA-256 with RSA Encryption
Version	3
Download	PEM (cert PEM (chain)

9. Save the file.

10. Repeat these tasks for vCenter or, or Firewall Management Center.

CHAPTER 3

Use dynamic objects in access control policies or DNS policies

The dynamic attributes connector enables you to configure dynamic filters, seen in the Secure Firewall Management Center as dynamic objects, in access control rules or DNS policies.

About dynamic objects in access control rules or DNS rules

A *dynamic object* is automatically pushed from the dynamic attributes connector to the Secure Firewall Manager after you create connectors and save a dynamic attributes filter on the connector.

You can use dynamic objects on the access control rule's or DNS rule's **Dynamic Attributes** tab page. You can add dynamic objects as source or destination attributes; for example, in an access control block rule, you can add a Finance dynamic object as a destination attribute to block access to Finance servers by whatever objects match the other criteria in the rule.

Note You cannot create dynamic attributes filters for AWS service tags, AWS service groups, Cisco APIC, Cisco Cyber Vision, Generic Text, GitHub, Office 365, Azure Service Tags, Webex, or Zoom. These types of cloud objects provide their own IP addresses.

Create dynamic attributes filters

Dynamic attributes filters that you define using the Dynamic Attributes Connector are exposed in the Secure Firewall Management Center as dynamic objects that can be used in access control policies. For example, restrict access to an AWS server for the Finance Department to only members of the Finance group defined in Microsoft Active Directory.

Note You cannot create dynamic attributes filters for AWS service tags, AWS service groups, Cisco APIC, Cisco Cyber Vision, Generic Text, GitHub, Office 365, Azure Service Tags, Webex, or Zoom. These types of cloud objects provide their own IP addresses.

For more information about access control or DNS rules, see Create access control rules or DNS rules using dynamic atttributes filters.

Procedure

Step 1 Log in to Secure Firewall Management Center.

Step 2 Click **Integration** > **Dynamic Attributes Connector**.

Step 3 Click **Dynamic Attributes Filters**.

- Add a new filter: click **Add** (+).
- Edit or delete a filter: Click **More** (⋮), then click **Edit** or **Delete** at the end of the row.

Step 4 Enter the following information.

Item	Description
Name	Unique name to identify the dynamic filter (as a dynamic object) in a policy and in the Secure Firewall Management Center Object Manager (**External Attributes** > **Dynamic Object**).
Connector	From the list, click the name of a connector to use.
Query	Click Add ⊞.

Step 5 To add or edit a query, enter the following information.

Item	Description
Key	Click a key from the list. Keys are fetched from the connector.
Operation	Click one of the following: • **Equals** to exactly match the key to the value. • **Contains** to match the key to the value if any part of the value matches.
Values	Click either **Any** or **All** and click one or more values from the list. Click **Add another value** to add values to your query.

Step 6 Click **Show Preview** to display a list of networks or IP addresses returned by your query.

Step 7 When you're finished, click **Save**.

Step 8 (Optional.) Verify the dynamic object in the Secure Firewall Management Center .

a) Log in to the Secure Firewall Management Center as a user with the Network Admin role at minimum.

b) Click **Objects** > **Object Management** > **External Attributes** > **Dynamic Object**.

The dynamic attribute query you created should be displayed as a dynamic object.

Dynamic attributes rule conditions

Dynamic attributes include the following:

- (Source or destination.) Dynamic objects (such as from the Dynamic Attributes Connector)

  The dynamic attributes connector enables you to collect data (such as networks and IP addresses) from cloud providers and send it to the so it can be used in access control rules.

  For more information about the dynamic attributes connector, see About the Dynamic Attributes ConnectorAbout the dynamic attributes connector.

- (Source only.) SGT objects contain tags either manually defined or defined in ISE. For more information, see Source and Destination Security Group Tag (SGT) MatchingSource and Destination Security Group Tag (SGT) Matching and Security Group Tag.

- (Source only.) Location IP objects, defined by Cisco ISE

- (Source only.) Device type objects, defined by Cisco ISE (also referred to as endpoint profile objects)

Dynamic attributes can be used as source criteria and destination criteria in access control rules. Use the following guidelines:

- Objects of different types are ANDd together

- Objects of a similar type are ORd together

For example, if you choose source destination criteria SGT 1, SGT 2, and device type 1; the rule is matched if device type 1 is detected on either SGT 1 or SGT 2. As another example, if you select both a security group tag, and a dynamic object that lists IP addresses, the rule matches if traffic with the tag originates from (or is destined to) one of those IP addresses.

View dynamic objects in the Secure Firewall Management Center

(Optional.) The following task discusses how you can view Cisco APIC network objects in the **Objects** > **Object Management** > **External Attributes** > **Dynamic Object**.

Before you begin

Complete all of the previous tasks related to integrating Cisco APIC with the Secure Firewall Management Center.

Procedure

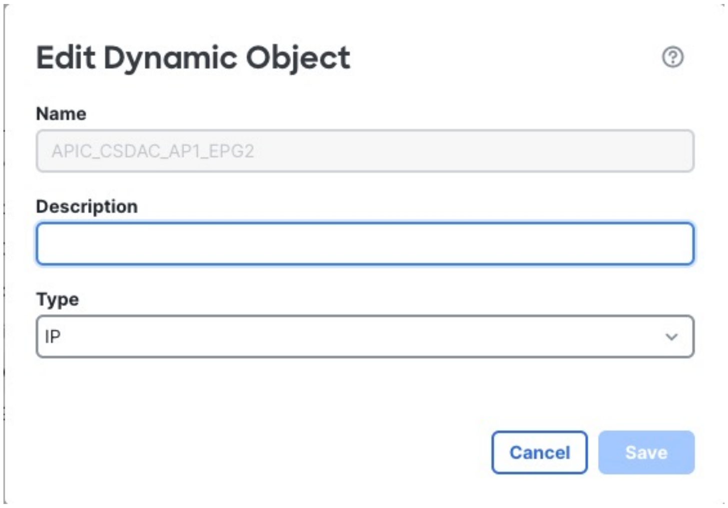
Step 1 Log in to the Secure Firewall Management Center

Step 2 Expand **Objects** > **Object Management** > **External Attributes** > **Dynamic Object**.

Dynamic objects created by the integration with Cisco APIC have names matching the pattern:

`APIC-site-name_tenant-name_application-profile-name_EPG-or-ESG-name`

The following figure shows an example.



Edit Dynamic Object

Name: APIC_CSDAC_AP1_EPG2

Description:

Type: IP

What to do next

See Create access control rules using dynamic attributes filters, on page 18.

Create access control rules using dynamic attributes filters

This topic discusses how to create access control rules using dynamic objects.

To add dynamic attributes filters to DNS policies, see Creating Basic DNS Policies.

Before you begin

Create dynamic attributes filters as discussed in Create dynamic attributes filters.

Note You cannot create dynamic attributes filters for AWS service tags, AWS service groups, Cisco APIC, Cisco Cyber Vision, Generic Text, GitHub, Office 365, Azure Service Tags, Webex, or Zoom. These types of cloud objects provide their own IP addresses.

Procedure

Step 1 Log in to the Secure Firewall Management Center

Step 2 Click **Policies** > **Access Control heading** > **Access Control**.

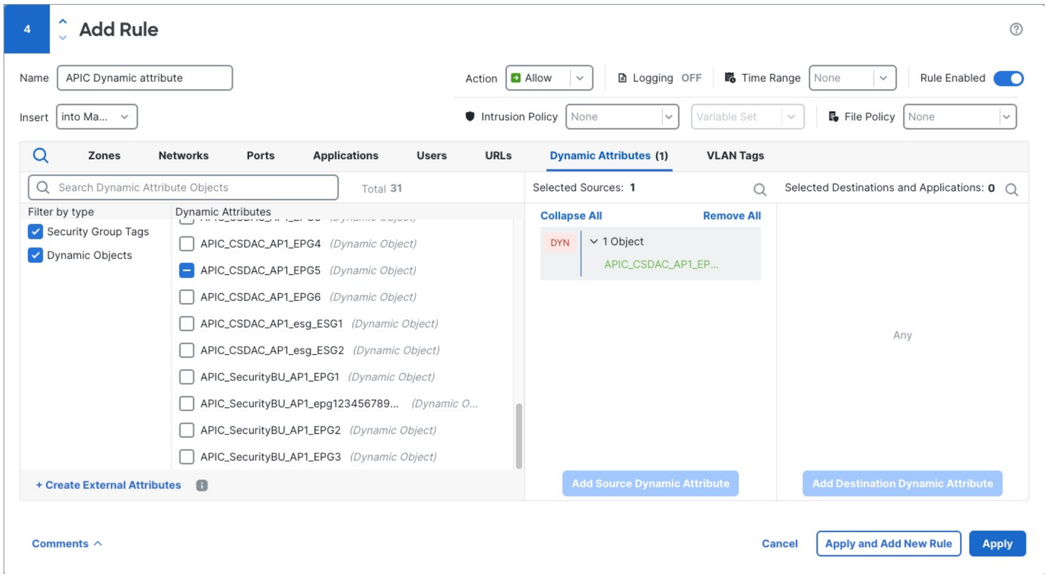
Step 3 Click **Edit** (✎) next to an access control policy.

Step 4 Click **Add Rule**.

Step 5 Click the **Dynamic Attributes** tab.

Step 6 In the Available Attributes section, from the list, click **Dynamic Objects**.

The following figure shows an example.



Name: APIC Dynamic attribute
Action: Allow
Logging: OFF
Time Range: None
Rule Enabled
Insert: into Ma...
Intrusion Policy: None
Variable Set
File Policy: None

Total 31

Filter by type
☑ Security Group Tags
☑ Dynamic Objects

Dynamic Attributes
□ APIC_CSDAC_AP1_EPG4 (Dynamic Object)
⊟ APIC_CSDAC_AP1_EPG5 (Dynamic Object)
□ APIC_CSDAC_AP1_EPG6 (Dynamic Object)
□ APIC_CSDAC_AP1_esg_ESG1 (Dynamic Object)
□ APIC_CSDAC_AP1_esg_ESG2 (Dynamic Object)
□ APIC_SecurityBU_AP1_EPG1 (Dynamic Object)
□ APIC_SecurityBU_AP1_epg123456789... (Dynamic O...
□ APIC_SecurityBU_AP1_EPG2 (Dynamic Object)
□ APIC_SecurityBU_AP1_EPG3 (Dynamic Object)

Selected Sources: 1
1 Object
APIC_CSDAC_AP1_EP...

Selected Destinations and Applications: 0

The preceding example shows a dynamic object named `APIC Dynamic Attribute` that corresponds to the dynamic attribute filter created in the Dynamic Attributes Connector.

Step 7 Add the desired object to source or destination attributes.

Step 8 Add other conditions to the rule if desired.

What to do next

See Dynamic attributes rule conditions.

CHAPTER 4

Migrate from the Cisco ACI Endpoint Update App to the Cisco APIC Integration with the Secure Firewall Management Center

The following topics discuss the Cisco ACI Endpoint Update App to the Cisco APIC integration with the Secure Firewall Management Center.

About the migration

This chapter discusses how to migrate your configuration and objects from the Cisco ACI Endpoint Update App to the Cisco APIC integration with Secure Firewall Management Center. Among the reasons to migrate:

- The Cisco APIC integration uses the Dynamic Attributes Connector, which retrieves dynamic objects (that is, network object groups, EPGs, and ESGs) from Cisco APIC and sends them to Secure Firewall Management Center.

Note As an alternative to this migration, you can use the Standalone ACI-Endpoint-Update-App.

To migrate, perform the following tasks:

1. On Cisco APIC, get the site prefix and update interval from the Cisco ACI Endpoint Update App, disable learning, and choose a user with the appropriate privilege level.

   See Migration step 1: Prepare Cisco APIC, on page 22

2. On the dynamic attributes connector, create a Cisco APIC connector.

   See Migration step 2: Configure the Dynamic Attributes Connector, on page 22

3. As a final verification step, make sure you see objects on the Secure Firewall Management Center.

   See Migration final step: View dynamic objects in the Secure Firewall Management Center, on page 23.

Migration step 1: Prepare Cisco APIC

Get required information

To migrate to the Cisco APIC integration with Secure Firewall Management Center, you must get all of the following information:

- Cisco ACI Endpoint Update App site prefix and update interval
- Cisco APIC tenant name
- Cisco APIC application profile name
- EPG name
- User with at least the `read-all` role with `readPriv` access and the `tenant-admin` role with `writePriv` access for the security domain that contains the network object groups to send to ASA.

For more information, see Get required information for the integration, on page 5.

Disable learning for the Cisco ACI Endpoint Update App

To prevent the Cisco ACI Endpoint Update App from communicating with Secure Firewall Management Center, you must disable learning.

1. Log in to Cisco APIC as a user with the `tenant-admin` role with `writePriv` access.
2. Click **Apps**.
3. Under ACI Endpoint Update app, click **Open**.
4. Select the check box next to one or more tenants you're integrating with Secure Firewall Management Center.
5. On the right side of the page, click ⚒▾.
6. From the list, click **Disable Learning**.
7. Select the checkbox to optionally erase all existing learning objects on the Cisco APIC device with which the Cisco ACI Endpoint Update App was previously associated.
8. Click **Submit**.

Migration step 2: Configure the Dynamic Attributes Connector

In the dynamic attributes connector, create a Cisco APIC connnector.

Before you begin

Complete the tasks discussed in Migration step 1: Prepare Cisco APIC, on page 22.

Procedure

Step 1 Log in to the dynamic attributes connector.

Step 2 Create the connector: Create a Cisco APIC connector, on page 9.

What to do next

See Migration final step: View dynamic objects in the Secure Firewall Management Center, on page 23.

Migration final step: View dynamic objects in the Secure Firewall Management Center

(Optional.) The following task enables you to confirm the integration was successful by viewing dynamic objects in the Secure Firewall Management Center.

Before you begin

Create the Cisco APIC connector as discussed in Create a Cisco APIC connector, on page 9.

Procedure

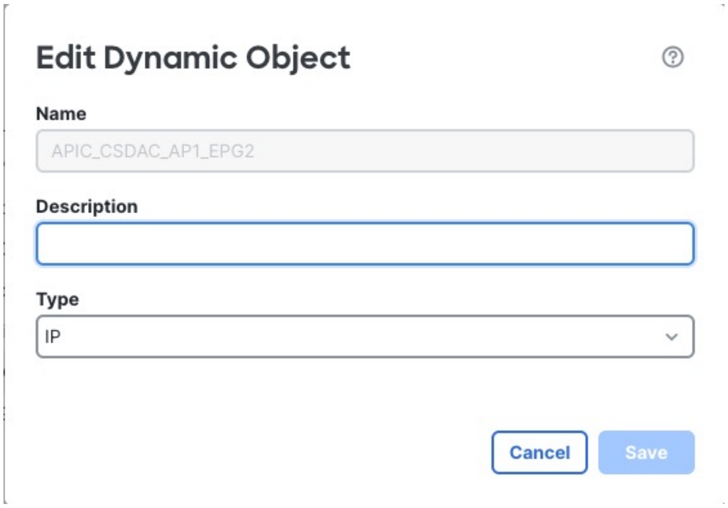
Step 1 Log in to the Secure Firewall Management Center

Step 2 Expand **Objects** > **Object Management** > **External Attributes** > **Dynamic Object**.

Dynamic objects created by the integration with Cisco APIC have names matching the pattern:

```
APIC-site-name_tenant-name_application-profile-name_EPG-or-ESG-name
```

The following figure shows an example.



Edit Dynamic Object

Name

APIC_CSDAC_AP1_EPG2

Description

Type

IP