



Configure the Cisco APIC Integration with ASA

The following topics discuss how to configure the Cisco APIC Integration with ASA.

- [Give the Cisco Secure Dynamic Attributes Connector Access to ASA, on page 1](#)
- [Get Required Information for the Cisco APIC Integration with ASA, on page 1](#)
- [Create a Connector, on page 3](#)
- [Create an ASA Adapter, on page 6](#)
- [Manually Get a Certificate Authority \(CA\) Chain, on page 9](#)

Give the Cisco Secure Dynamic Attributes Connector Access to ASA

This topic discusses how to give the dynamic attributes connector HTTPS access to ASA.

Before you can configure the integration, you must allow the dynamic attributes connector HTTPS access to the ASA using the **http server enable**, **aaa authentication console**, and **route** commands.

An example follows:

```
http server enable
http 0.0.0.0 0.0.0.0 management
aaa authentication http console LOCAL
route management 10.1.0.0 255.255.255.0 192.0.2.100
```

For more information, see:


- [http server enable](#)
- [aaa authentication console](#)
- [route](#)

Get Required Information for the Cisco APIC Integration with ASA

To use the Cisco APIC integration with ASA, you must get all of the following information.

Cisco ACI Endpoint Update App site prefix and update interval

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**.

Cisco APIC application profile name

To find the application profile name:

1. Log in to Cisco APIC.
2. Click **Tenants**.
3. Expand **Application Profiles**.
4. Write down the name of the application profile that contains EPGs and ESGs to integrate with ASA.

EPG name

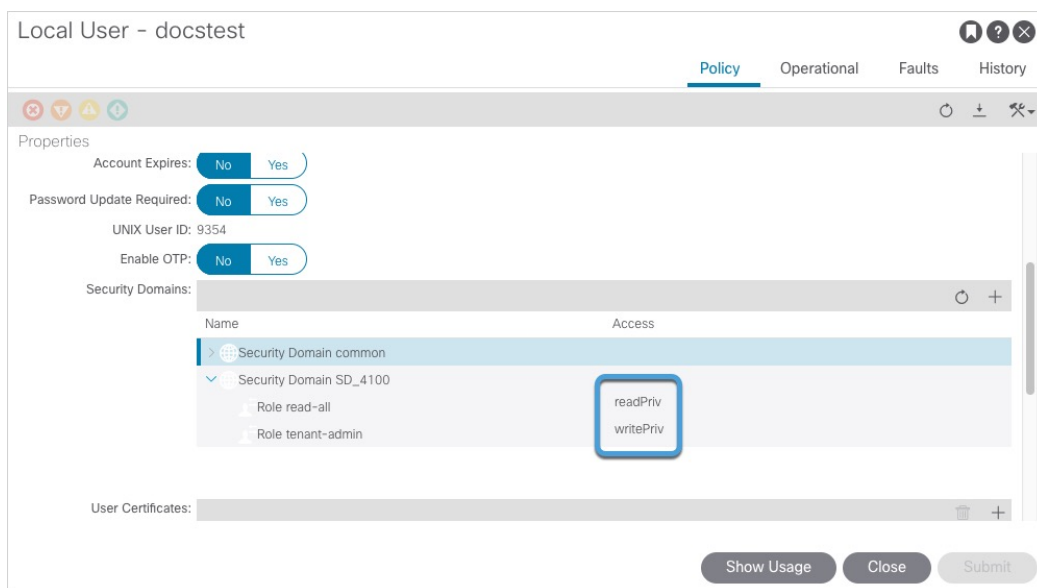
To find the EPG name:

1. Log in to Cisco APIC.
2. Click **Tenants**.
3. Expand **Application Profiles**.
4. Write down the name of the application profile that contains EPGs and ESGs to integrate with ASA.
5. Write down the name of the EPG or ESG that has network object groups to send to ASA.

Find a user with appropriate access

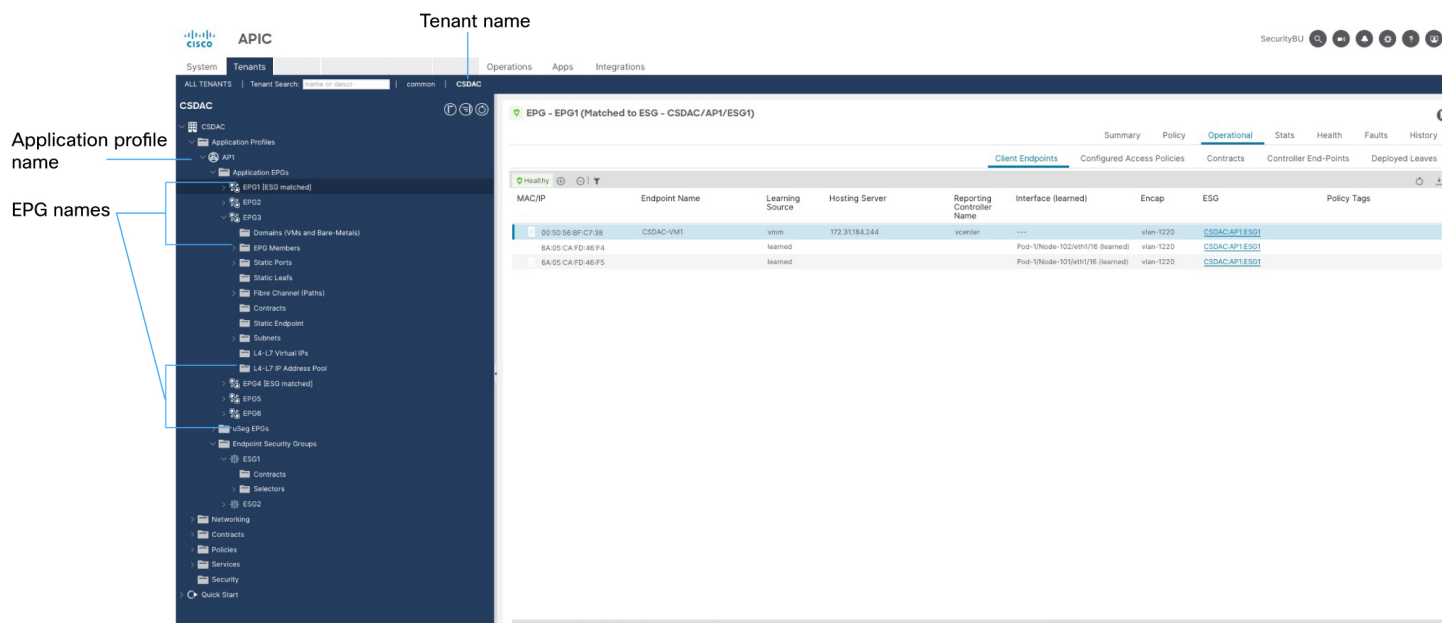
To find a user with at least the `read-all` role with `readPriv` access and the `tenant-admin` role with `writePriv` access for the security domain:

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.



Example

The following figure shows the values in Cisco APIC.



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 access control policies on the Firepower Management Center.

We support the following:

Table 1: List of supported connectors by Cisco Secure Dynamic Attributes Connector version and platform

CSDAC version/platform	AWS	AWS security groups	AWS service tags	Azure	Azure Service Tags	Cisco APIC	Cisco Cyber Vision	Generic Text	GitHub	Google Cloud	Microsoft Office 365	vCenter	Webex	Zoom
Version 1.1 (on-premises)	Yes	No	No	Yes	Yes	No	No	No	No	No	Yes	Yes	No	No
Version 2.0 (on-premises)	Yes	No	No	Yes	Yes	No	No	No	No	Yes	Yes	Yes	No	No
Version 2.2 (on-premises)	Yes	No	No	Yes	Yes	No	No	No	Yes	Yes	Yes	Yes	No	No
Version 2.3 (on-premises)	Yes	No	No	Yes	Yes	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes
Version 3.0 (on-premises)	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Version 3.1 (on-premises)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	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 network object groups from a configured endpoint group (EPG) on Cisco APIC.

Before you begin



Review the information discussed in [About the Cisco APIC Integration with ASA](#) and [Get Required Information for the Cisco APIC Integration with ASA, on page 1](#).

Procedure

Step 1 Log in to the dynamic attributes connector.

Step 2 Click **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.

Value	Description
Pull Interval	(Default 60 seconds.) Interval at which IP mappings are retrieved from Cisco APIC. We recommend setting this to 15 seconds.
Site Prefix	<p>(Required.) Enter a name to identify this connector with the corresponding ASA adapter.</p> <p>Note The Site Prefix name you enter here must exactly match all of the following:</p> <ul style="list-style-type: none"> • The Cisco ACI Endpoint Update App Site Prefix value you found as discussed in Get Required Information for the Cisco APIC Integration with ASA, on page 1. • Later in this guide, the value of the APIC Site Prefix you enter for the ASA adapter as discussed in Create an ASA Adapter, on page 6. <p>This value is <i>not</i> case-sensitive.</p>
IP or Hostname	(Required.) Enter the fully-qualified domain name or IP address of the Cisco APIC server from which to retrieve dynamic network object groups from EPGs and ESGs.
Add another cluster IP	(Optional.) Enter the IP address of other servers in the Cisco APIC cluster.
Username	<p>(Required.) Enter the name of a Cisco APIC user with at least at least the <code>read-all</code> role with <code>readPriv</code> access and the <code>tenant-admin</code> role with <code>writePriv</code> access for the security domain.</p> <p>Objects from all tenants the user has privileges to can be pushed to ASA.</p> <p>You can filter the tenants using the Tenants field in the ASA adapter, which you'll configure later in this guide.</p>
Password	(Required.) Enter the user's password.
Server Certificate	<p>(Recommended if using fully-qualified domain name.)</p> <p>You have the following options:</p> <ul style="list-style-type: none"> • Paste the certificate authority (CA) chain you got as discussed in Manually Get a Certificate Authority (CA) Chain, on page 9. • Click Get Certificate > Fetch to automatically fetch the certificate or, if that is not possible, get the certificate manually as discussed in Manually Get a Certificate Authority (CA) Chain, on page 9. • 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.

What to do next

[Create an ASA Adapter, on page 6](#)

Create an ASA Adapter

This topic discusses how to create an ASA adapter that creates network object groups on ASA. These network object groups can be used in access rules.





Note The ASA adapter creates only Cisco APIC network object groups. You *cannot* create on ASA dynamic objects from other cloud sources, such as Microsoft Outlook 365.

Before you begin

Create a Cisco APIC connector as discussed in [Create a Cisco APIC Connector, on page 4](#).

Procedure

- Step 1** Log in to the dynamic attributes connector.
- Step 2** Click **Adapters**.
- 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.

Note
Deleting an adapter by itself does not delete dynamic objects created by the adapter. If you wish to delete those objects permanently, do so on the device associated with the adapter.

Before deleting the adapter, you can set its **Operative Status** to **Paused and Clear**. Doing this stops sending network object groups to ASA and clears any previously sent objects from ASA.

Editing an adapter does not push updated objects to the associated device. If you must change the adapter's settings, delete the adapter and add it again.

- Step 4** Enter the following information.

Value	Description
Name	(Required.) Enter a unique name to identify this adapter.
Description	Optional description of the adapter.

Value	Description
Operative Status	<p>From the list, click one of the following:</p> <ul style="list-style-type: none"> • Running is the normal running state where the integration sends network object groups to ASA. In the Running state, the adapter's status is displayed as Ok on the dynamic attributes connector Adapters page. • Paused pauses sending network object groups, such as during an upgrade. You can pause and resume sending network object groups at any time; this option preserves the objects already pushed to ASA. To resume sending network object groups, edit this adapter again and click Running. In the Paused state, the adapter's status is displayed as Disabled on the dynamic attributes connector Adapters page. • Paused and Clear stops sending network object groups to ASA and clears any previously sent objects from ASA. After you do this you can delete the adapter if you wish. In the Paused and Clear state, the adapter's status is displayed as Disabled on the dynamic attributes connector Adapters page.
APIC Site Prefix	<p>(Required.) Enter a name to use as the prefix for the objects created on ASA. We strongly recommend you use a unique name.</p> <p>This value must match all of the following:</p> <ul style="list-style-type: none"> • The Cisco ACI Endpoint Update App Site Prefix value you found as discussed in Get Required Information for the Cisco APIC Integration with ASA, on page 1. • The value of the APIC Site Prefix you specified for the Cisco APIC connector as discussed in Create a Cisco APIC Connector, on page 4. <p>This value is <i>not</i> case-sensitive.</p>
Tenants	<p>(Required.) Specify the names of one or more Cisco APIC tenants the <code>readPriv</code> user has access to. Objects from only the tenants you specify will be pushed to ASA.</p> <p>To specify more than one tenant, separate them with a comma character.</p>
IP	(Required.) ASA IP address.
Port	(Required.) ASA TLS/SSL port (default is 443).
User	(Required.) Enter the name of an ASA user with privilege level 15.
Password	(Required.) Enter the user's password.
Security Context	(Optional.) Enter the name of the ASA security context. For more information, see Enabling Multiple Context Mode in the <i>Cisco Security Appliance Command Line Configuration Guide</i> .

Value	Description
Server Certificate	<p>(Optional.) You have the following options:</p> <ul style="list-style-type: none"> • Paste the certificate authority (CA) chain you got as discussed in Manually Get a Certificate Authority (CA) Chain, on page 9. • Click Get Certificate > Fetch to automatically fetch the certificate or, if that is not possible, get the certificate manually as discussed in Manually Get a Certificate Authority (CA) Chain, on page 9. • Click Get Certificate > Browse from file to upload a certificate chain you downloaded previously.

Edit or Delete an ASA Adapter

This task discusses the supported way to either edit or delete an ASA adapter. Failure to follow this procedure might mean dynamic objects do not get updated on the ASA device.

Before you begin

Create an ASA adapter as discussed in [Create an ASA Adapter, on page 6](#).



Note Deleting an adapter by itself does not delete dynamic objects created by the adapter. If you wish to delete those objects permanently, do so on the device associated with the adapter.

Before deleting the adapter, you can set its **Operative Status** to **Paused and Clear**. Doing this stops sending network object groups to ASA and clears any previously sent objects from ASA.

Editing an adapter does not push updated objects to the associated device. If you must change the adapter's settings, delete the adapter and add it again.

Procedure

-
- Step 1** Log in to the dynamic attributes connector.
- Step 2** Click **Adapters**.
- Step 3** To change an adapter's configuration:
- Click **More** (⋮), then click **Delete**.
 - Follow the prompts to complete the action.
 - Create another ASA adapter as discussed in [Create an ASA Adapter, on page 6](#).
- Step 4** To delete an adapter:
- Click **More** (⋮), then click **Delete**.
 - Follow the prompts to complete the action.

Note

Deleting an adapter by itself does not delete dynamic objects created by the adapter. If you wish to delete those objects permanently, do so on the device associated with the adapter.

Before deleting the adapter, you can set its **Operative Status** to **Paused and Clear**. Doing this stops sending network object groups to ASA and clears any previously sent objects from ASA.

Editing an adapter does not push updated objects to the associated device. If you must change the adapter's settings, delete the adapter and add it again.

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, FMC, Cisco APIC, or ASA.

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
- FMC
- Cisco APIC
- ASA

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, FMC, Cisco APIC, or ASA. For example:

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

If you access vCenter, FMC, Cisco APIC, or ASA using NAT or PAT, you can add a port as follows:

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

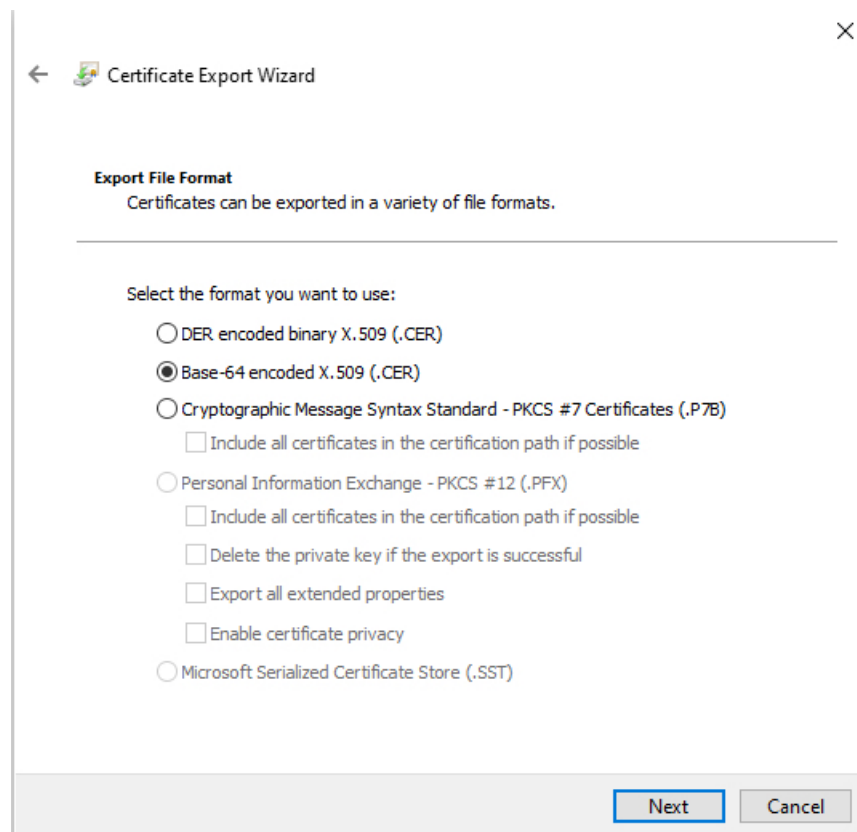
3. Save the entire certificate chain to a plaintext file.
 - *Include* all -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- delimiters.
 - *Exclude* any extraneous text (for example, the name of the certificate and any text contained in angle brackets (< and >) as well as the angle brackets themselves.
4. Repeat these tasks for vCenter, FMC, Cisco APIC, or ASA.

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, FMC, Cisco APIC, or ASA 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.



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.

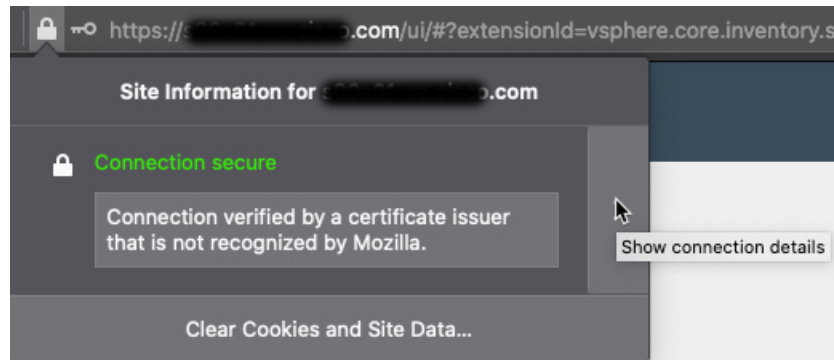
You must paste each certificate in the text editor in order, first to last.

13. Repeat these tasks for vCenter, FMC, Cisco APIC, or ASA.

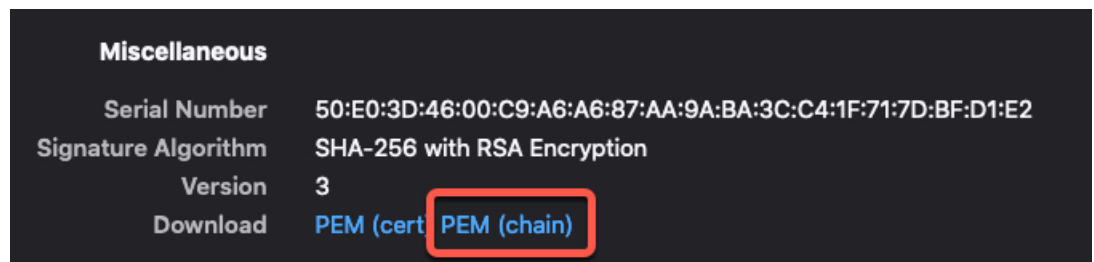
Get a Certificate Chain—Windows Firefox

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

1. Log in to vCenter, FMC, Cisco APIC, or ASA 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.



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.



9. Save the file.
10. Repeat these tasks for vCenter, FMC, Cisco APIC, or ASA.

