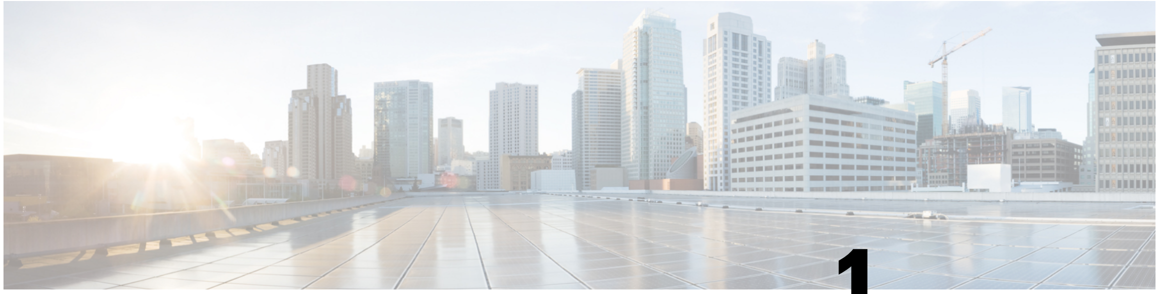
Cisco APIC Integration with ASA Solution Guide

First Published: 2025-01-31

Last Modified: 2025-03-06

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



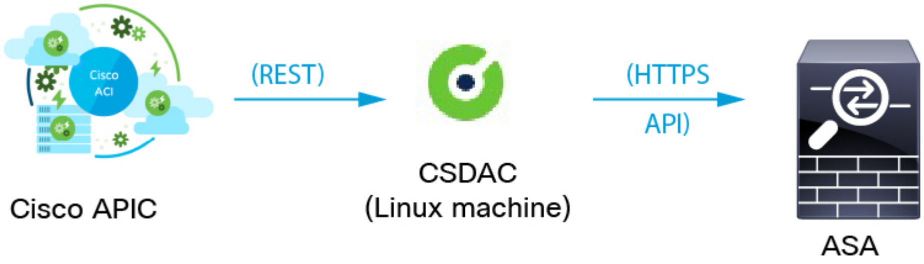
CHAPTER 1

About the Cisco APIC Integration with ASA

This chapter discusses the integration between Cisco Application Policy Infrastructure Controller (APIC) and ASA.

About the Cisco APIC Integration with ASA

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 an ASA. The following figure shows how this works at a high level.



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 ASA on which you can use those objects in access control rules. An ASA adapter pushes network object groups in the configured security context.

(You have the option to specify the tenants from which retrieve EPG and ESG objects when you set up the ASA adapter in the dynamic attributes connector. The Cisco APIC user determines which tenants data can be pulled from.)

You can optionally create an empty network object in the ASA CLI under which to create additional network objects sent from Cisco APIC. For more information, see Access Control Lists.

Note ASDM does not support creating empty network objects at this time.

Sample configuration

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

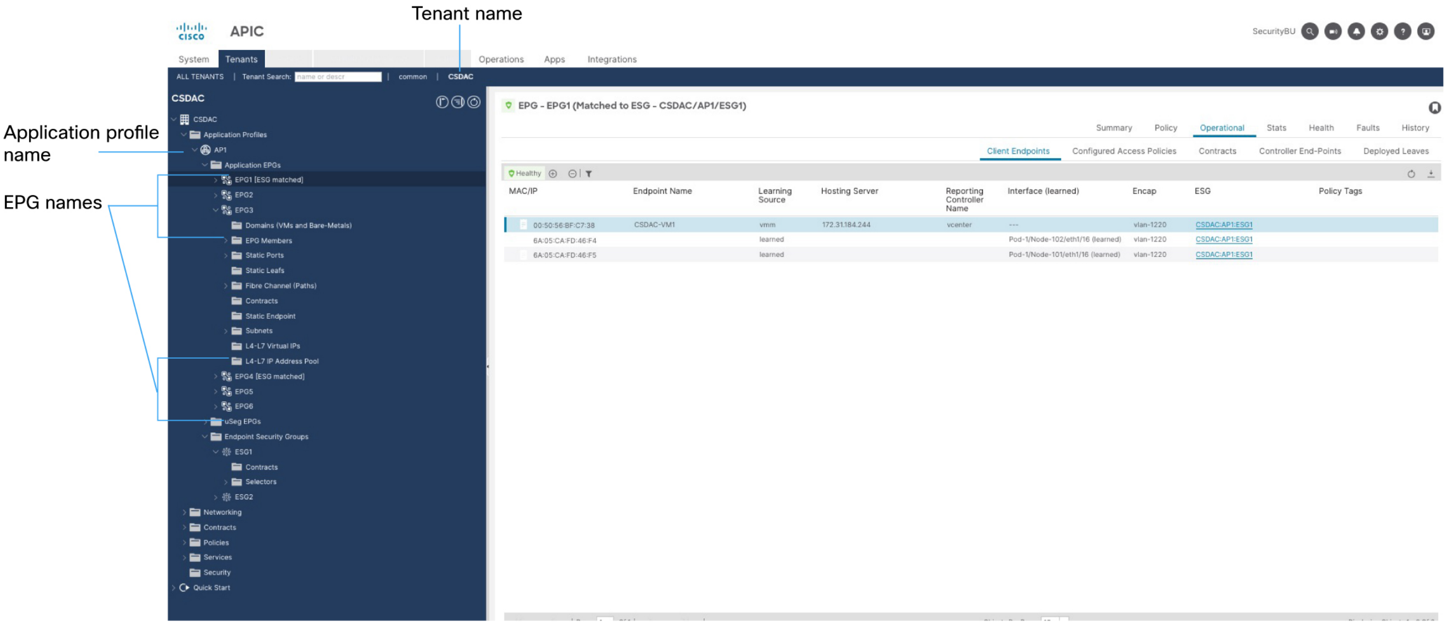
Network object group names are a concatenation of (in order):

- 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`)

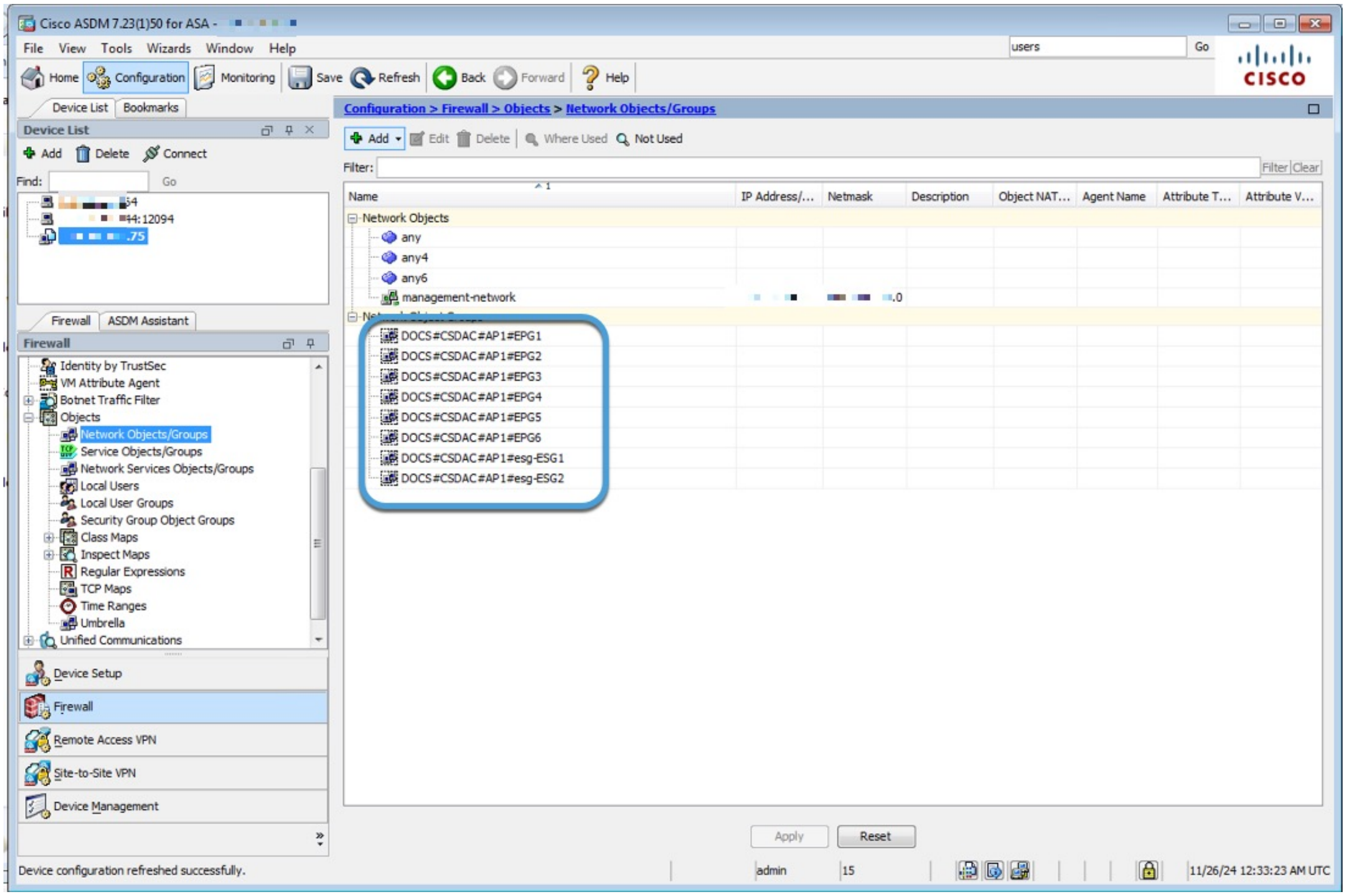
- Cisco APIC EPG name (in this example, `EPG1` through `EPG4`)



EPG - EPG1 (Matched to ESG - CSDAC/AP1/ESG1)

MAC/IP	Endpoint Name	Learning Source	Hosting Server	Reporting Controller Name	Interface (learned)	Encap	ESG	Policy Tags
00:50:56:BF:C7:38	CSDAC-VM1	vmm	172.31.184.244	vcenter	---	vlan-1220	CSDAC:AP1:ESG1	
6A:05:CA:FD:46:F4		learned			Pod-1/Node-102/eth1/16 (learned)	vlan-1220	CSDAC:AP1:ESG1	
6A:05:CA:FD:46:F5		learned			Pod-1/Node-101/eth1/16 (learned)	vlan-1220	CSDAC:AP1:ESG1	

Assuming the connector's Site Prefix is DOCS and the Cisco APIC tenant name the `CSDAC` user has rights to is CSDAC, network object groups on ASA are named as follows (in ASDM, **Configuration** > **Firewall** > **Objects** > **Network Objects/Groups**):



Name	IP Address/...	Netmask	Description	Object NAT...	Agent Name	Attribute T...	Attribute V...
Network Objects							
any							
any4							
any6							
management-network	[redacted]	[redacted].0					
Ne[redacted]							
DOCS#CSDAC#AP1#EPG1							
DOCS#CSDAC#AP1#EPG2							
DOCS#CSDAC#AP1#EPG3							
DOCS#CSDAC#AP1#EPG4							
DOCS#CSDAC#AP1#EPG5							
DOCS#CSDAC#AP1#EPG6							
DOCS#CSDAC#AP1#esg-ESG1							
DOCS#CSDAC#AP1#esg-ESG2							

Device configuration refreshed successfully.

Additional information about Cisco APIC

- Basic User Tenant Configuration
- EPGs
- ESGs

Additional information about the Cisco Secure Dynamic Attributes Connector

Cisco%20Secure%20Dynamic%20Attributes%20Connector%20Configuration%20Guide.

What to do next

See Get Required Information for the Cisco APIC Integration with ASA, on page 19.

How to Use Network Object Groups from Cisco APIC in ASA Access Rules

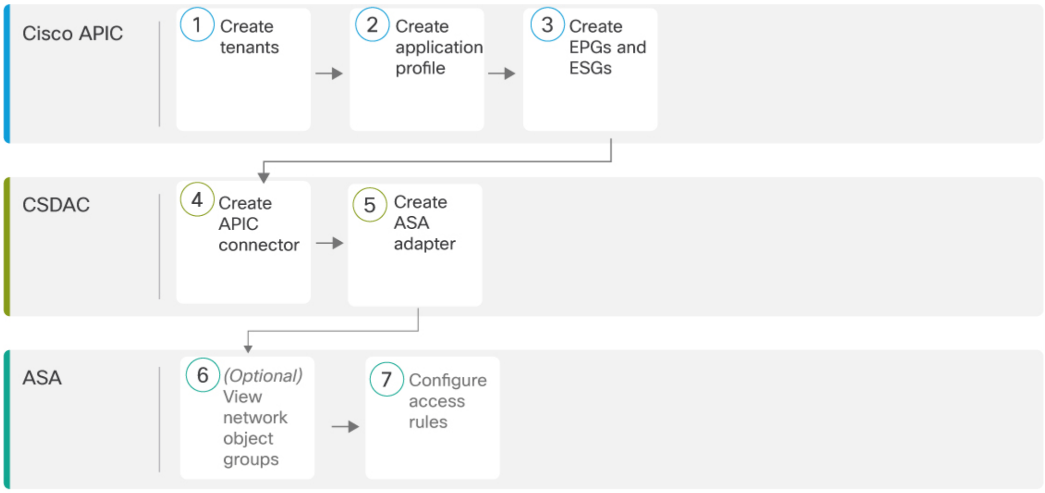


Table 1: Configure ASA access control policies using network object groups

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
4	Cisco Secure Dynamic Attributes Connector	The Cisco APIC connector retrieves network object groups from Cisco APIC periodically. As the objects or the IP addresses in them change, ASA is updated dynamically without the need to redeploy access rules. See Create a Cisco APIC Connector, on page 22
5	Cisco Secure Dynamic Attributes Connector	The ASA adapter is responsible for updating objects on ASA. See Create an ASA Adapter, on page 24

6	ASA	(Optional.) View the network object groups fetched from Cisco APIC. (Optional). See View Network Object Groups in ASDM, on page 33
7	ASA	To use network object groups in access rules, you must add them as source criteria to those rules. See Add Network Object Groups to Access Rules, on page 31

CHAPTER 2

Install and Upgrade the Cisco Secure Dynamic Attributes Connector

This chapter discusses how to install and upgrade the Cisco Secure Dynamic Attributes Connector on all supported operating systems.

Supported Operating Systems and Third-Party Software

The dynamic attributes connector requires the following:

- Ubuntu 18.04 to 22.04.2
- Red Hat Enterprise Linux (RHEL) 7 or 8
- Python 3.6.x or later
- Ansible 2.9 or later

Minimum requirements for all operating systems:

- 4 CPUs
- 8 GB RAM
- For new installations, 100 GB available disk space to install the dynamic attributes connector

If you use a hypervisor:

VMware ESX or ESXi up to 8

If you wish to use vCenter attributes, we also require:

- vCenter up to 8
- VMware Tools must be installed on the virtual machine

Virtual machine sizing

We recommend you size your virtual machines as follows:

- 50 connectors, assuming 5 filters per connector and 20,000 workloads: 4 CPUs; 8 GB RAM; 100 GB available disk space
- 125 connectors, assuming 5 filters per connector and 50,000 workloads: 8 CPUs, 16 GB RAM, 100 GB available disk space

Note Failure to size your virtual machines properly can cause the dynamic attributes connector to fail or not to start.

Requirements and Prerequisites for the Cisco APIC Integration with ASA

Following are requirements and prerequisits to use Cisco APIC to send dynamic objects to ASA:

- Network communication: All of the following must be able to communicate with each other securely:
  - ASA 9.16 and later
  - Cisco APIC 4.2(7q) and later
  - Cisco Secure Dynamic Attributes Connector virtual machine, version 3.1 and later
- ASA requirements
  - License: Essentials

    For more information about licensing, see Smart Software Licensing.
  - FQDN: Supported
  - Multi-context: Supported
  - Multi-instance: Supported
  - High availability: Supported
  - Clustering: Supported
- Permissions required:
  - ASA: privilege 15
  - Cisco APIC: at least the `read-all` role with `readPriv` access and the `tenant-admin` role with `writePriv` access for the security domain

More information

For more information about the the Cisco APIC Integration with ASA, see About the Cisco APIC Integration with ASA, on page 1.

Install Prerequisite Software

Before you begin

Make sure you have physical or virtual set up and that the system that can communicate with your the On-Prem Firewall Management Center or Cloud-delivered Firewall Management Center.

Procedure

Step 1 (Optional.) Use a text editor to edit `/etc/environment` to export the following variables to enable communication with the internet if your Ubuntu machine is behind an internet proxy.

Variable	Value
export http_proxy	Use with an HTTP proxy. *user***:***pass@host-or-ip***:***port*
export https_proxy	Use this with an HTTPS proxy. *user***:***pass@host-or-ip***:***port*
export no_proxy	Remove the proxy configuration. **export no_proxy="localhost,127.0.0.1"**

Examples:

HTTP proxy without authentication:

```
vi /etc/environment
export http_proxy="myproxy.example.com:8181"
```

HTTPS proxy with authentication:

```
vi /etc/environment
export https_proxy="ben.smith:bens-password@myproxy.example.com:8181"
```

Step 2 Use a different command window to confirm the settings:

```
env | grep proxy
```

Example result:

```
http_proxy=myproxy.example.com:8181
```

Step 3 Continue with one of the following sections.

Related Topics

Install Prerequisite Software—Ubuntu, on page 11

Install Prerequisite Software—RHEL, on page 10

Install Prerequisite Software—RHEL

Before you begin

Do all of the following:

- Make sure your system meets the prerequisites discussed in Supported Operating Systems and Third-Party Software, on page 7.
- (Optional.) If you need proxy access to the dynamic attributes connector, see Install Prerequisite Software, on page 9.

Procedure

Step 1 Make sure Docker is not installed and uninstall it if it is.

```
docker --version
```

If Docker is installed, uninstall it as discussed in Uninstall Docker Engine on Ubuntu.

Step 2 Update your repositories.

RHEL 7:

```
sudo yum -y update && sudo yum -y upgrade
```

RHEL 8:

```
sudo dnf -y update && sudo dnf -y upgrade
```

Step 3 Install the epel repository.

RHEL 7:

```
sudo yum -y install https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
```

RHEL 8:

```
sudo dnf -y install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

Step 4 (RHEL 7 only.) Install Python 3.

```
sudo yum install -y python3 libselinux-python3
```

Step 5 Install Ansible.

RHEL 7:

```
sudo yum -y install ansible
```

RHEL 8:

```
sudo dnf install -y ansible
```

Step 6 Verify the Ansible version.

```
ansible --version
```

An example follows.

RHEL 7:

```
ansible 2.9.24
  config file = /etc/ansible/ansible.cfg
  configured module search path = [u'/home/stevej/.ansible/plugins/modules',
u'/usr/share/ansible/plugins/modules']
  ansible python module location = /usr/lib/python2.7/site-packages/ansible
  executable location = /usr/bin/ansible
  python version = 2.7.5 (default, Mar 20 2020, 17:08:22) [GCC 4.8.5 20150623 (Red Hat 4.8.5-39)]
```

Note
It's normal for Ansible to reference Python 2.x as the preceding output shows. The connector will still use Python 3.

RHEL 8:

```
ansible 2.9.24
  config file = /etc/ansible/ansible.cfg
  configured module search path = ['/home/stevej/.ansible/plugins/modules',
'/usr/share/ansible/plugins/modules']
  ansible python module location = /usr/lib/python3.6/site-packages/ansible
  executable location = /usr/bin/ansible
  python version = 3.6.8 (default, Mar 18 2021, 08:58:41) [GCC 8.4.1 20200928 (Red Hat 8.4.1-1)]
```

What to do next

Install the connector as discussed in Install the Cisco Secure Dynamic Attributes Connector, on page 12.

To optionally stop using a proxy with the dynamic attributes connector, edit `/etc/environment` and remove the proxy configuration.

Install Prerequisite Software—Ubuntu

This task discusses how to install prerequisite software on Ubuntu.

Procedure

Step 1 Make sure Docker is not installed and uninstall it if it is.

```
docker --version
```

If Docker is installed, uninstall it as discussed in Uninstall Docker Engine on Ubuntu.

Step 2 Update your repositories.

```
sudo apt -y update && sudo apt -y upgrade
```

Step 3 Confirm your Python version.

```
/usr/bin/python3 --version
```

If the version is earlier than 3.6, you must install version 3.6 or later.

Step 4 Install Python 3.6.

```
sudo apt -y install python3.6
```

Step 5 Install the common libraries.

```
sudo apt -y install software-properties-common
```

Step 6 Install Ansible.

```
sudo apt-add-repository -y -u ppa:ansible/ansible && sudo apt -y install ansible
```

Step 7 Verify the Ansible version.

```
ansible --version
```

An example follows.

```
ansible --version
ansible 2.9.19
  config file = /etc/ansible/ansible.cfg
  configured module search path = [u'/home/admin/.ansible/plugins/modules',
u'/usr/share/ansible/plugins/modules']
  ansible python module location = /usr/lib/python2.7/dist-packages/ansible
  executable location = /usr/bin/ansible
  python version = 2.7.17 (default, Feb 27 2021, 15:10:58) [GCC 7.5.0]
```

Note
It's normal for Ansible to reference Python 2.x as the preceding output shows. The connector will still use Python 3.6.

What to do next

Install the connector as discussed in Install the Cisco Secure Dynamic Attributes Connector, on page 12.

To optionally stop using a proxy with the dynamic attributes connector, edit `/etc/environment` and remove the proxy configuration.

Install the Cisco Secure Dynamic Attributes Connector

About the installation

This topic discusses installing the Cisco Secure Dynamic Attributes Connector. You must install the dynamic attributes connector as a user with `sudo` privileges but you can run the connector as a non-privileged user.

Before you begin

Make sure your system has the following prerequisite software:

- Ubuntu 18.04 to 22.04.2
- Red Hat Enterprise Linux (RHEL) 7 or 8
- Python 3.6.x or later
- Ansible 2.9 or later

Minimum requirements for all operating systems:

- 4 CPUs
- 8 GB RAM
- For new installations, 100 GB available disk space to install the dynamic attributes connector

We recommend you size your virtual machines as follows:

- 50 connectors, assuming 5 filters per connector and 20,000 workloads: 4 CPUs; 8 GB RAM; 100 GB available disk space
- 125 connectors, assuming 5 filters per connector and 50,000 workloads: 8 CPUs, 16 GB RAM, 100 GB available disk space

Note Failure to size your virtual machines properly can cause the dynamic attributes connector to fail or not to start.

If you wish to use vCenter attributes, we also require:

- vCenter up to 8
- VMware Tools must be installed on the virtual machine

To install prerequisite software, see Install Prerequisite Software, on page 9.

View the Readme and Release Notes

For the latest installation information, see the following:

Readme: https://galaxy.ansible.com/cisco/csdac

Release Notes: Release Notes

Install the muster service

The muster service is another name for the dynamic attributes connector.

Run the following command from the `~/.ansible/collections/ansible_collections/cisco/csdac` directory.

ansible-playbook default_playbook.yml [--ask-become-pass] [--extra-vars " *vars* "]

Syntax Description		
	--ask-become-pass	Prompts you to enter the **sudo** password. Required if sudo is enabled on your machine.

--extra-vars	The following optional extra variables enable the dynamic attributes connector to use a proxy. The value you use must match the value in /etc/environment, which you configured as discussed in Install Prerequisite Software, on page 9. • **csdac_proxy_enabled=true** • **csdac_http_proxy_url=http://***PROXY_URL* **csdac_https_proxy_url=***PROXY_URL* The following optional extra variables create a self-signed certificate you can use to securely connect to the dynamic attributes connector. If you omit these parameters, the dynamic attributes connector uses a default certificate. • **csdac_certificate_domain** domain name for autogenerated certificate. Default value is autodetected hostname of the host (detected by ansible) • **csdac_certificate_country_name** Two-letter country code. (Default is `US`) • **csdac_certificate_organization_name** Organization name. (Default is `Cisco`) • **csdac_certificate_organization_unit_name** • Organizational unit name (Default is `Cisco`) The following optional extra variables enable you to skip validation checks. • **skip_disk_space_check=true** Skip the available disk space check when installing the dynamic attributes connector. We recommend doing this if your system has less than 100GB free disk space; however, you could experience unpredictable performance if the disk fills up. • **skip_all_verifications=true** Skip the available disk space and internet verifications when installing the dynamic attributes connector. The following optional extra variable enables you to set group ownership for TBD files and directories after installation: **user_group=***any_existing_user_group*

Example installation with a default certificate

For example, to install the software with default options:

```
ansible-galaxy collection install cisco.csdac
cd ~/.ansible/collections/ansible_collections/cisco/csdac
ansible-playbook default_playbook.yml --ask-become-pass
```

Example installation with optional certificate

For example, to install the software with an optional certificate:

```
ansible-galaxy collection install cisco.csdac
cd ~/.ansible/collections/ansible_collections/cisco/csdac
ansible-playbook default_playbook.yml --ask-become-pass --extra-vars
"csdac_certificate_domain=domain.example.com csdac_certificate_country_name=US
csdac_certificate_organization_name=Cisco
csdac_certificate_organization_unit_name=Engineering"
```

After you create the certificate, import it into the web browser you'll use to access the connector. The certificate is created in the `~/csdac/app/config/certs` directory.

Example: Example installation skipping the disk space check

```
ansible-galaxy collection install cisco.csdac
cd ~/.ansible/collections/ansible_collections/cisco/csdac
ansible-playbook default_playbook.yml --ask-become-pass --extra-vars
"skip_disk_space_check=true"
```

Example: Example installation skipping all verification checks and assigning group ownership to mygroup

```
ansible-galaxy collection install cisco.csdac
cd ~/.ansible/collections/ansible_collections/cisco/csdac
ansible-playbook default_playbook.yml --ask-become-pass --extra-vars
"skip_all_verifications=true user_group=mygroup"
```

View the installation log

The installation log is located as follows:

```
~/.ansible/collections/ansible_collections/cisco/csdac/logs/csdac.log
```

Use your certificate to connect to the dynamic attributes connector

If you have a certificate and key, put them in the `~/csdac/app/config/certs` directory on your virtual machine.

After you perform the preceding task, restart the dynamic attributes connector's Docker container by entering the following command:

```
docker restart muster-ui
```

Log in to the connector

1. Access the dynamic attributes connector at `https://`*`ip-address`*
2. Log in.

   The initial login is username `admin`, password `admin`. You are required to change the password the first time you log in.

Upgrade the Cisco Secure Dynamic Attributes Connector

This topic discusses how to upgrade from any earlier Cisco Secure Dynamic Attributes Connector to the current version. These tasks can be performed regardless of Cisco Secure Dynamic Attributes Connector version or operating system.

Procedure

Step 1 Log in to the machine you want to upgrade.

Step 2 Enter the following commands:

```
cd ~/.ansible/collections/ansible_collections/cisco/csdac
ansible-galaxy collection install cisco.csdac --force
ansible-playbook default_playbook.yml --ask-become-pass [--extra-vars vars]
```

Syntax Description

--ask-become-pass Prompts you to enter the **sudo** password. Required if sudo is enabled on your machine.

--extra-vars The following optional extra variables enable the dynamic attributes connector to use a proxy. The value you use must match the value in /etc/environment, which you configured as discussed in Install Prerequisite Software, on page 9.

- **csdac_proxy_enabled=true**
- **csdac_http_proxy_url=http://***PROXY_URL*

  csdac_https_proxy_url=*PROXY_URL*

The following optional extra variables create a self-signed certificate you can use to securely connect to the dynamic attributes connector. If you omit these parameters, the dynamic attributes connector uses a default certificate.

- **csdac_certificate_domain**

  domain name for autogenerated certificate. Default value is autodetected hostname of the host (detected by ansible)

- **csdac_certificate_country_name**

  Two-letter country code. (Default is `US`)

- **csdac_certificate_organization_name**

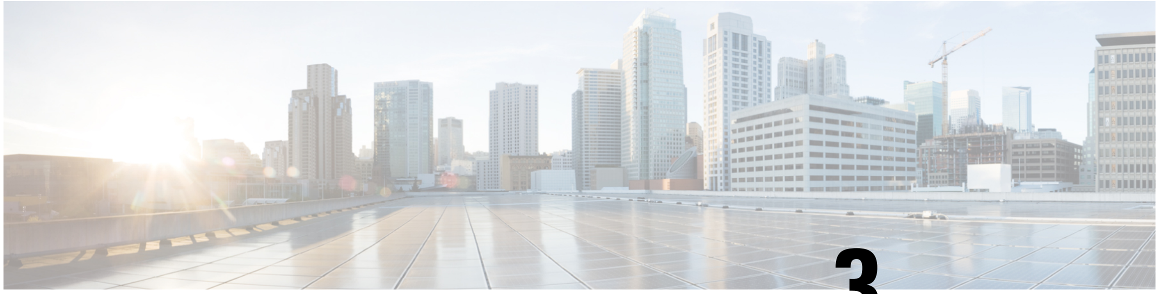
  Organization name. (Default is `Cisco`)

- **csdac_certificate_organization_unit_name**
- Organizational unit name (Default is `Cisco`)

Step 3 Wait for the upgrade to complete.

Step 4 Upgrade logs are available in the following location:

```
~/.ansible/collections/ansible_collections/cisco/csdac/logs/csdac.log
```



CHAPTER 3

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

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

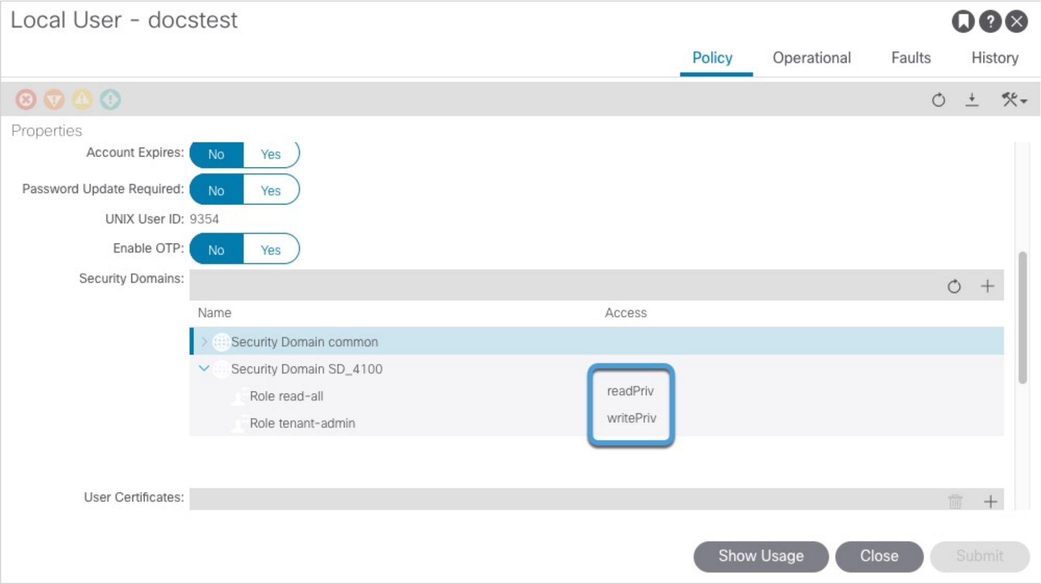
To find the EPG name:

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, nake 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

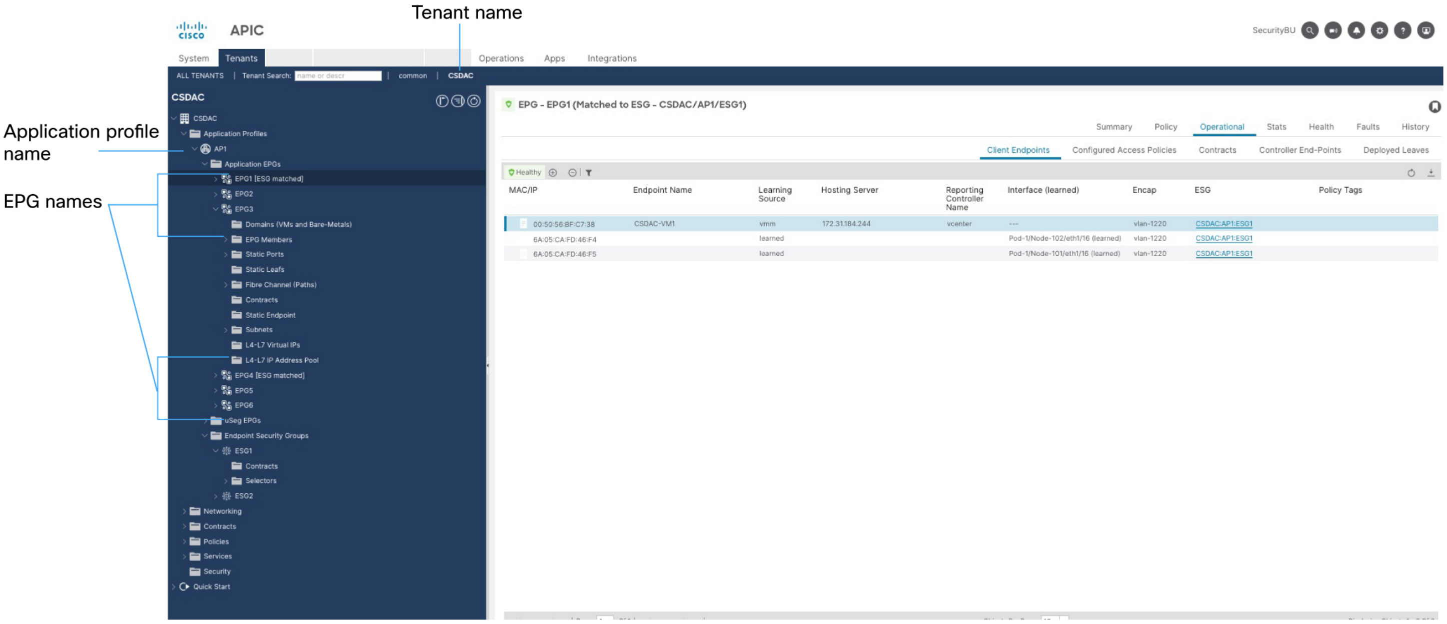
Security Domains:

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

User Certificates:

Example

The following figure shows the values in Cisco APIC.



EPG - EPG1 (Matched to ESG - CSDAC/AP1/ESG1)

MAC/IP	Endpoint Name	Learning Source	Hosting Server	Reporting Controller Name	Interface (learned)	Encap	ESG	Policy Tags
00:50:56:BF:C7:38	CSDAC-VM1	vmm	172.31.184.244	vcenter	---	vlan-1220	CSDAC:AP1:ESG1	
6A:05:CA:FD:46:F4		learned			Pod-1/Node-102/eth1/16 (learned)	vlan-1220	CSDAC:AP1:ESG1	
6A:05:CA:FD:46:F5		learned			Pod-1/Node-101/eth1/16 (learned)	vlan-1220	CSDAC:AP1:ESG1	

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 2: 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, on page 1 and Get Required Information for the Cisco APIC Integration with ASA, on page 19.

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	(Required.) 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 Cisco APIC Integration with ASA, on page 19. • 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 24. This value is *not* case-sensitive.
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	(Required.) 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 ASA. You can filter the tenants using the **Tenants** field in the ASA adapter, which you'll configure later in this guide.
Password	(Required.) 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 Manually Get a Certificate Authority (CA) Chain, on page 27. • 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 27. • 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 24

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 22.

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	From the list, click one of the following: - **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	(Required.) Enter a name to use as the prefix for the objects created on ASA. We strongly recommend you use a unique name. This value must match all of the following: - 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 19. - The value of the **APIC Site Prefix** you specified for the Cisco APIC connector as discussed in Create a Cisco APIC Connector, on page 22. This value is *not* case-sensitive.
Tenants	(Required.) Specify the names of one or more Cisco APIC tenants the `readPriv` user has access to. Objects from only the tenants you specify will be pushed to ASA. To specify more than one tenant, separate them with a comma character.
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 *Cisco Security Appliance Command Line Configuration Guide*.

Value	Description
Server Certificate	(Optional.) You have the following options: • Paste the certificate authority (CA) chain you got as discussed in Manually Get a Certificate Authority (CA) Chain, on page 27. • 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 27. • 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 24.

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:

a) Click **More** (⋮), then click **Delete**.
b) Follow the prompts to complete the action.
c) Create another ASA adapter as discussed in Create an ASA Adapter, on page 24.

Step 4 To delete an adapter:

a) Click **More** (⋮), then click **Delete**.
b) 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
   ```

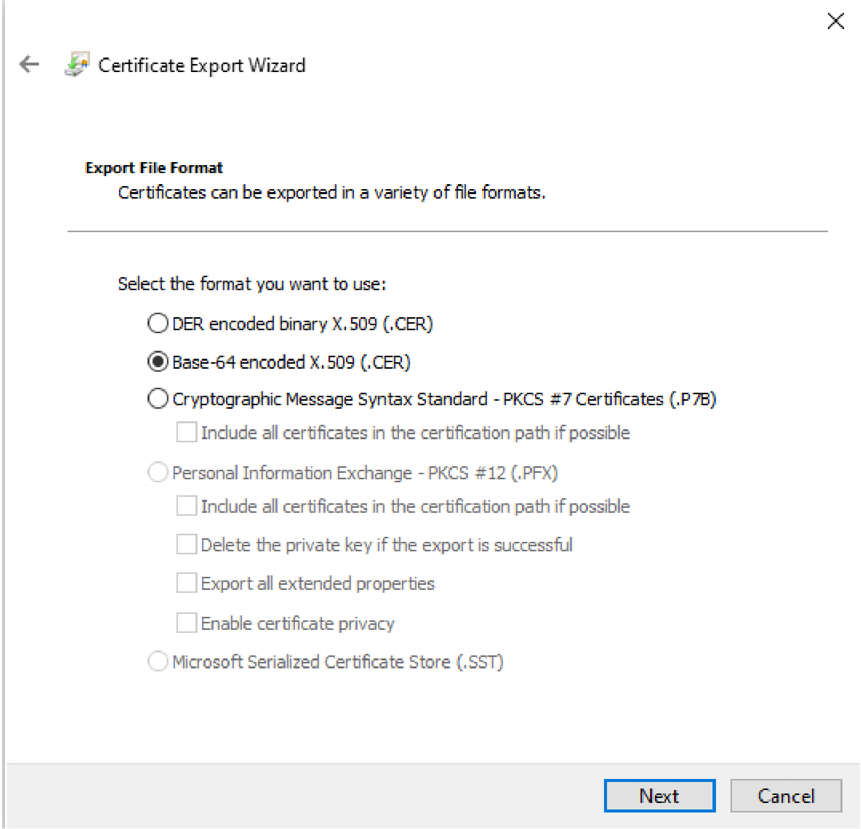
3. Save the entire certificate chain to a plaintext file.
   - *Include* all `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` delimiters.
   - *Exclude* any extraneous text (for example, the name of the certificate and any text contained in angle brackets (< and >) as well as the angle brackets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



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.

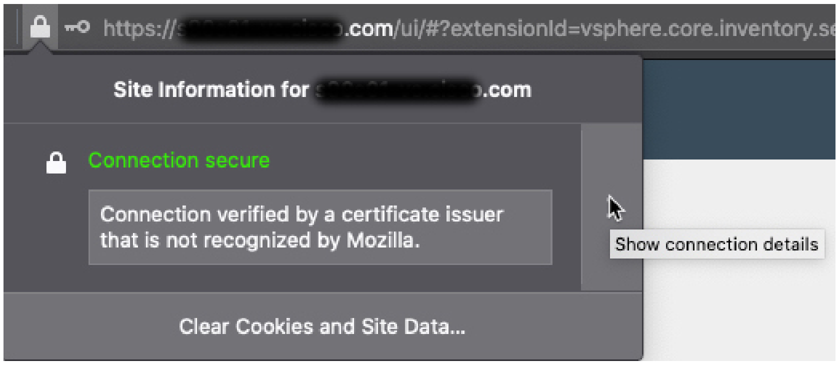
You must paste each certificate in the text editor in order, first to last.

13. Repeat these tasks for vCenter, 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.



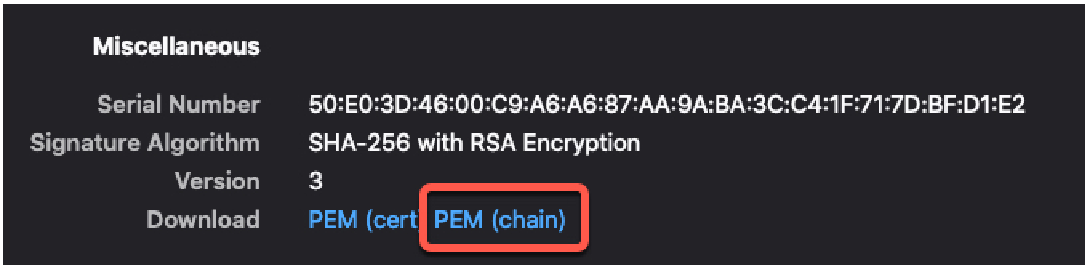
https://[redacted].com/ui/#?extensionId=vsphere.core.inventory.se

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, FMC, Cisco APIC, or ASA.

CHAPTER 4

Use Network Object Groups from Cisco APIC in ASA Access Rules

The following topics discuss the basics of using network object groups from Cisco APIC in ASA access rules.

- Add Network Object Groups to Access Rules, on page 31
- View Network Object Groups in ASDM, on page 33

Add Network Object Groups to Access Rules

To use dynamic network object groups from Cisco APIC to ASA access rules, you must add those objects as discussed in this task.

Before you begin

Complete all of the following tasks:

- Create a Cisco APIC Connector, on page 22
- Create an ASA Adapter, on page 24

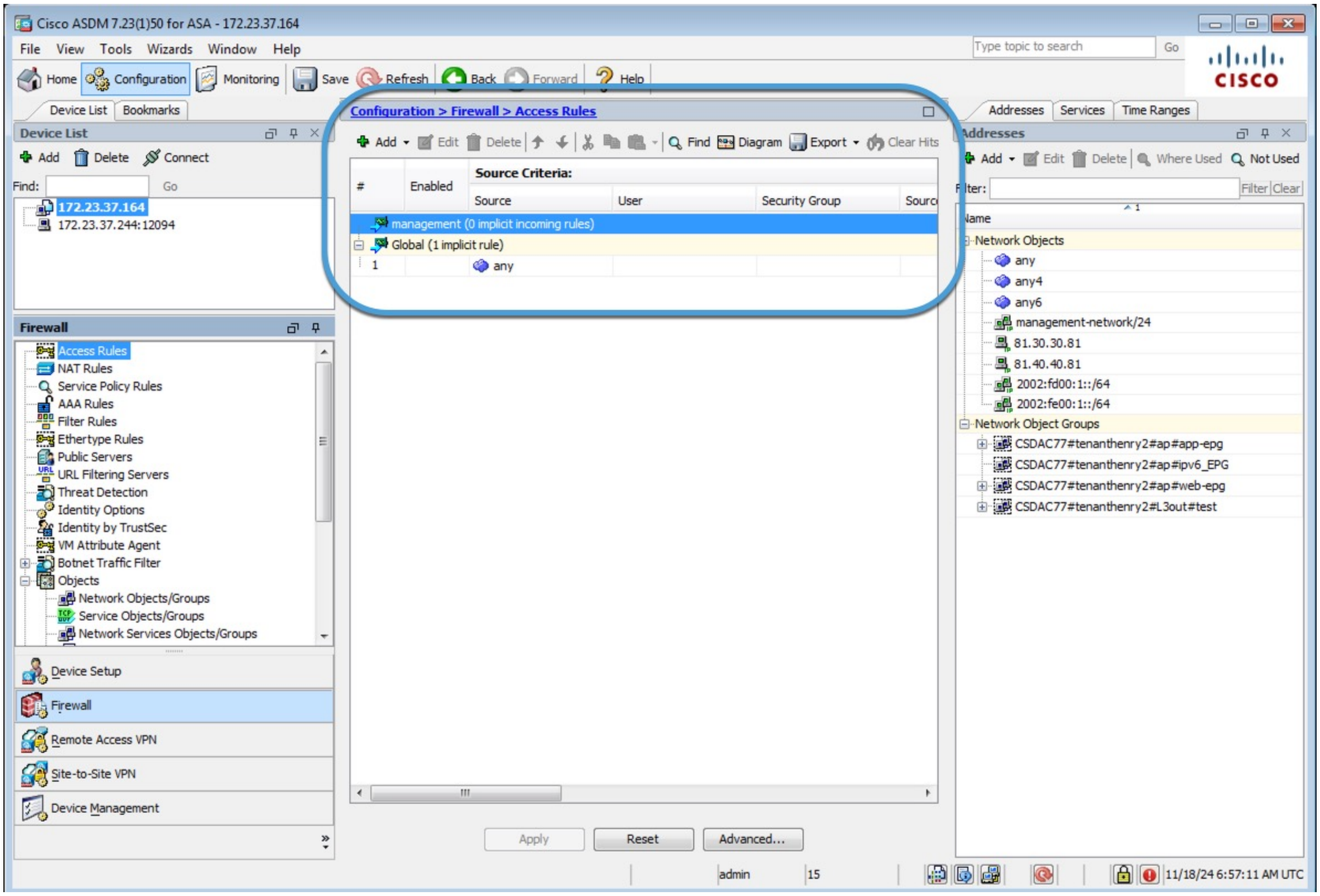
Procedure

Step 1 Log in to ASDM as a user with level 15 (administrator) privilege.

For more information about starting ASDM, see Start ASDM.

For more information about permissions, see Configure Management Remote Access.

Step 2 Click **Configuration** > **Firewall** > **Access Rules** > **Network Objects/Groups**.
Access rules are displayed in the center pane as the following figure shows.

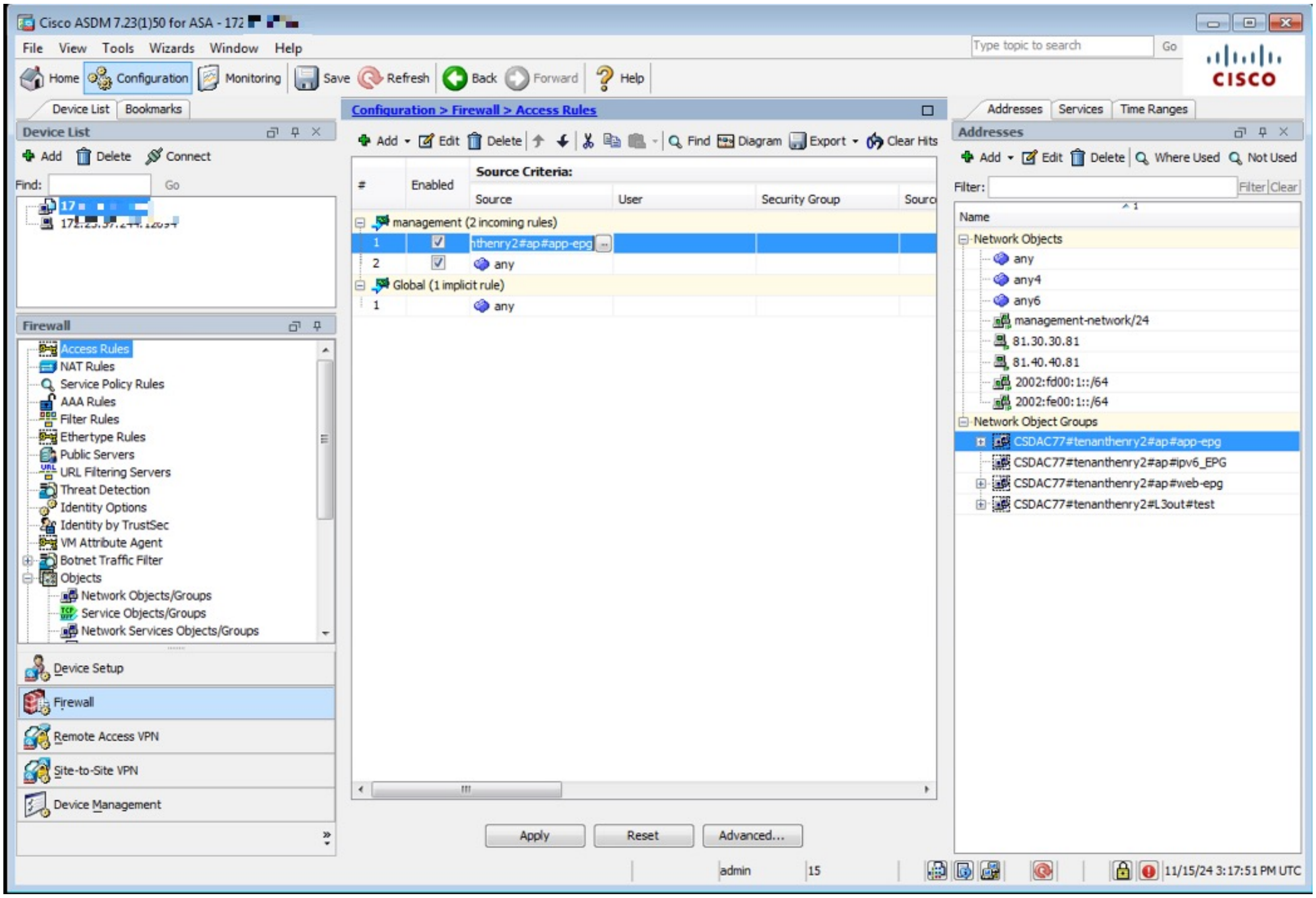


#	Enabled	Source Criteria: Source	User	Security Group	Sourc
management (0 implicit incoming rules)					
Global (1 implicit rule)					
1		any			

Step 3 Specify one or more network object groups as source criteria for the rule.

Double-click the **Source** field, then click ▭ to select a network object group for the rule.

The following figure shows an example.



#	Enabled	Source Criteria: Source	User	Security Group	Sourc
management (2 incoming rules)					
1	☑	nthenry2#ap#app-epg			
2	☑	any			
Global (1 implicit rule)					
1		any			

Name

- Network Objects
  - any
  - any4
  - any6
  - management-network/24
  - 81.30.30.81
  - 81.40.40.81
  - 2002:fd00:1::/64
  - 2002:fe00:1::/64
- Network Object Groups
  - CSDAC77#tenanthenry2#ap#app-epg
  - CSDAC77#tenanthenry2#ap#ipv6_EPG
  - CSDAC77#tenanthenry2#ap#web-epg
  - CSDAC77#tenanthenry2#L3out#test

Network object groups are named as follows: `SiteName#TenantName#ProfileName#EPGName`

Step 4 Follow the prompts on your screen to complete the action.

For more information, see Access Rules.

View Network Object Groups in ASDM

This task is optional. To configure ASA access rules without viewing network object groups, see Add Network Object Groups to Access Rules, on page 31.

Before you begin

Complete all of the following tasks:

- Create a Cisco APIC Connector, on page 22
- Create an ASA Adapter, on page 24

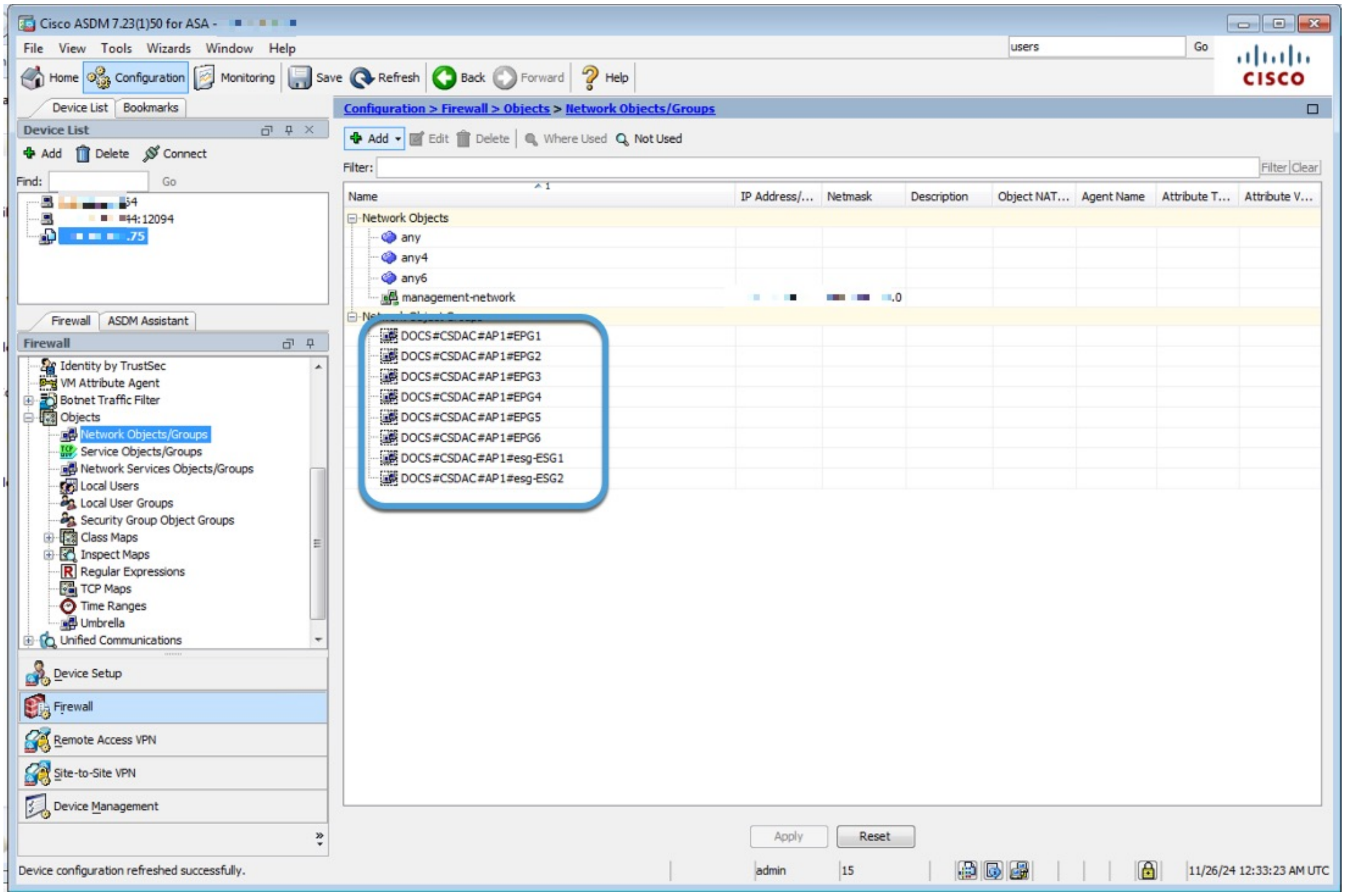
Procedure

Step 1 Log in to ASDM as a user with at least privilege level 15 (administrator).

For more information about starting ASDM, see Start ASDM.

For more information about permissions, see Configure Management Remote Access.

Step 2 Click **Configuration** > **Firewall** > **Objects** > **Network Objects/Groups**.
The network object groups are displayed in the right pane as the following figure shows.



Network object groups are named as follows: `SiteName#TenantName#ProfileName#EPGName`

What to do next

See Add Network Object Groups to Access Rules, on page 31

CHAPTER 5

Migrate from the Cisco API Update App to the Cisco APIC Integration with ASA

The following topics discuss the Cisco API Update App to the Cisco APIC Integration with ASA.

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 ASA. Among the reasons to migrate:

- The Cisco APIC integration with ASA uses the Cisco Secure Dynamic Attributes Connector, which retrieves dynamic objects (that is, network object groups) from Cisco APIC and sends them to ASA.
- You can add more Cisco APIC-ASA integrations to the dynamic attributes connector at any time.

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

To migrate, perform the following tasks:

1. Install the dynamic attributes connector and make sure it, Cisco APIC, and ASA can communicate with each other over the network. The dynamic attributes connector retrieves network object groups from Cisco APIC and pushes them to ASA so all systems must be able to communicate.

   See Migration Step 1: Set up the Cisco Secure Dynamic Attributes Connector, on page 36

2. 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 2: Prepare Cisco APIC, on page 36

3. On the dynamic attributes connector, create a Cisco APIC connector an ASAadapter.

See Migration Step 3: Configure the Cisco Secure Dynamic Attributes Connector, on page 37

4. As a final verification step, make sure you see network group objects on the ASA.

   See Migration Final Step: Verify Network Object Groups in ASDM, on page 38

Migration Step 1: Set up the Cisco Secure Dynamic Attributes Connector

To use the integration, you must install the Cisco Secure Dynamic Attributes Connector on a Ubuntu or Red Hat Enterprise Linux virtual machine and verify it can communicate both with Cisco APIC and ASA.

Following are the minimum requirements for your system:

- Ubuntu 18.04 to 22.04.2
- Red Hat Enterprise Linux (RHEL) 7 or 8
- Python 3.6.x or later
- Ansible 2.9 or later

For more information, SOLUTION GUIDE LINKING

Procedure

Step 1 Set up a virtual machine with the hardware and software prerequisites discussed in Supported Operating Systems and Third-Party Software, on page 7.

Step 2 Get the dynamic attributes connector software as discussed in Install Prerequisite Software, on page 9.

Step 3 Install the dynamic attributes connector as discussed in Install the Cisco Secure Dynamic Attributes Connector, on page 12.

What to do next

See Migration Step 2: Prepare Cisco APIC, on page 36.

Migration Step 2: Prepare Cisco APIC

Get required information

To migrate to the Cisco APIC integration with ASA, 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 Cisco APIC Integration with ASA, on page 19.

Disable learning for the Cisco ACI Endpoint Update App

To prevent the Cisco ACI Endpoint Update App from communicating with TBD, 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 ASA.
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 3: Configure the Cisco Secure Dynamic Attributes Connector

In the dynamic attributes connector, create a Cisco APIC connnector and an ASA adapter.

Before you begin

Complete the tasks discussed in Migration Step 2: Prepare Cisco APIC, on page 36.

Procedure

Step 1 Log in to the dynamic attributes connector.

Step 2 Create the connector: Create a Cisco APIC Connector, on page 22.

Step 3 Create the adapter: Create an ASA Adapter, on page 24.

What to do next

Migration Final Step: Verify Network Object Groups in ASDM, on page 38.

Migration Final Step: Verify Network Object Groups in ASDM

To make sure the integration is working, you can optionally view network object groups retrieved from Cisco APIC in ASDM.

Before you begin

Complete the tasks discussed in Migration Step 3: Configure the Cisco Secure Dynamic Attributes Connector, on page 37.

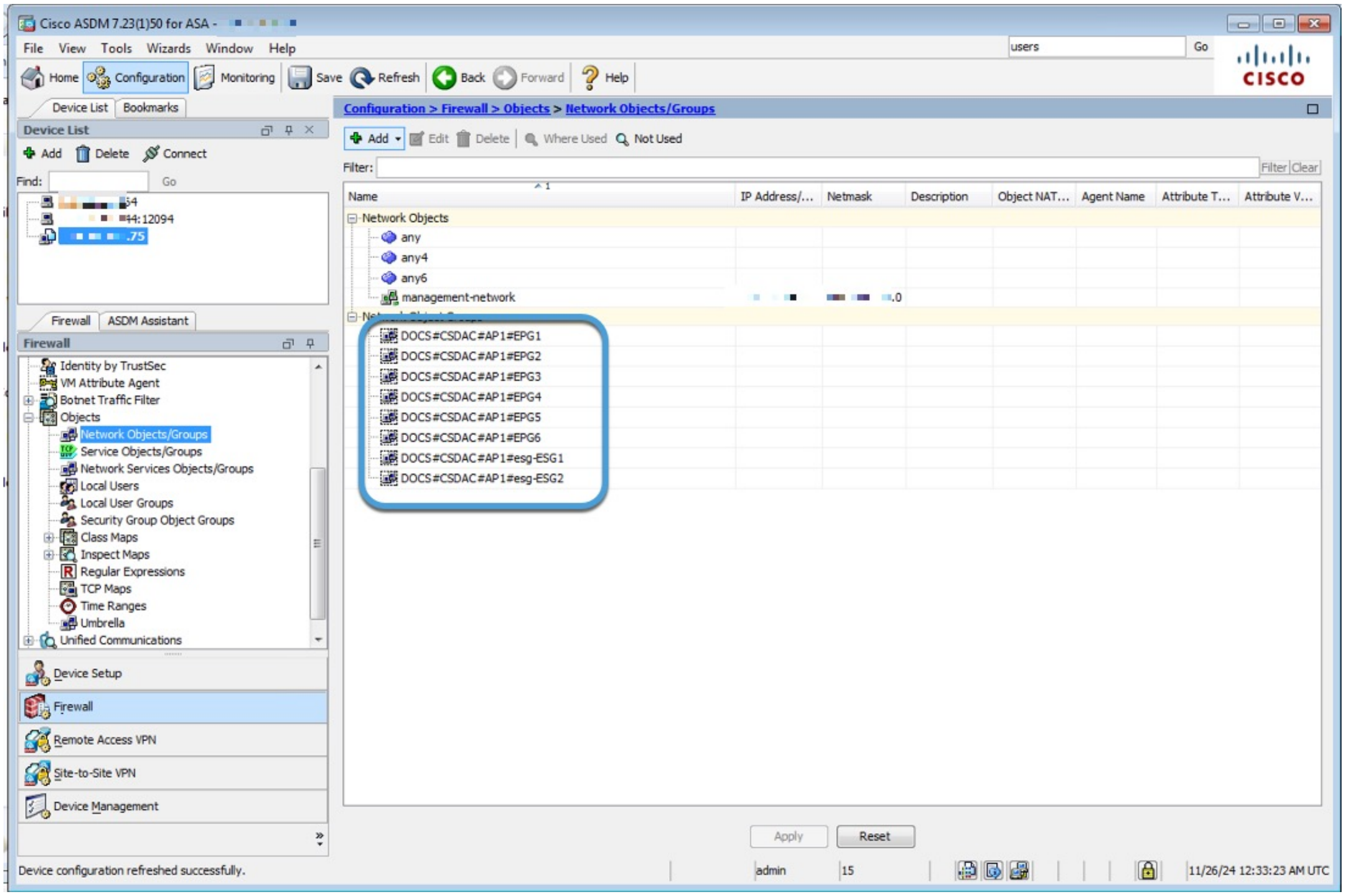
Procedure

Step 1 Log in to ASDM as a user with at least privilege level 15 (administrator).

For more information about starting ASDM, see Start ASDM.

For more information about permissions, see Configure Management Remote Access.

Step 2 Click **Configuration** > **Firewall** > **Objects** > **Network Objects/Groups**.
The network object groups are displayed in the right pane as the following figure shows.



Name	IP Address/...	Netmask	Description	Object NAT...	Agent Name	Attribute T...	Attribute V...
Network Objects							
any							
any4							
any6							
management-network	[redacted]	[redacted].0					
Network Object Groups							
DOCS#CSDAC#AP1#EPG1							
DOCS#CSDAC#AP1#EPG2							
DOCS#CSDAC#AP1#EPG3							
DOCS#CSDAC#AP1#EPG4							
DOCS#CSDAC#AP1#EPG5							
DOCS#CSDAC#AP1#EPG6							
DOCS#CSDAC#AP1#esg-ESG1							
DOCS#CSDAC#AP1#esg-ESG2							

Device configuration refreshed successfully. admin 15 11/26/24 12:33:23 AM UTC

Network object groups are named as follows: `SiteName#TenantName#ProfileName#EPGName`