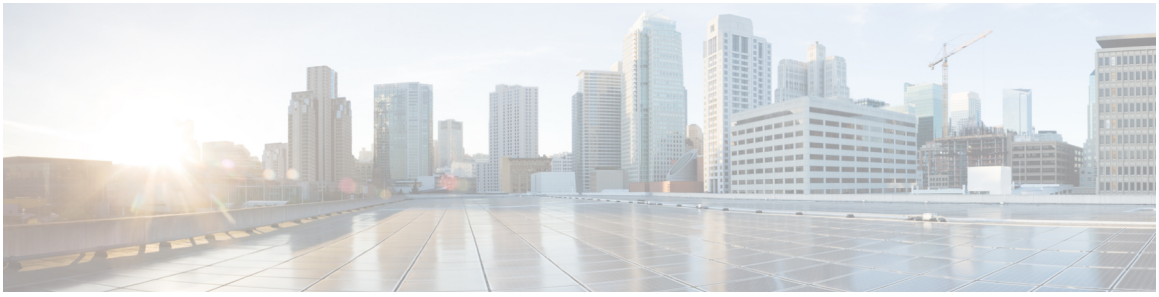


Cisco Secure Dynamic Attributes Connector Configuration Guide 3.1

First Published: 2025-01-31

Last Modified: 2026-05-20

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

Full Cisco Trademarks with Software License ?

CHAPTER 1 **About the Dynamic Attributes Connector** 1

About the dynamic attributes connector 1

How it works 2

About the Cisco APIC integration with ASA 3

How to use network object groups from Cisco APIC in ASA access rules 6

CHAPTER 2 **Install and Upgrade the Dynamic Attributes Connector** 9

Supported operating systems and third-party software 9

Install prerequisite software 10

Install prerequisite software—RHEL 11

Install prerequisite software—Ubuntu 12

Install the dynamic attributes connector 13

Upgrade the dynamic attributes connector 17

CHAPTER 3 **Configure the Dynamic Attributes Connector** 19

Create a connector 19

Amazon Web Services connector—About user permissions and imported data 20

Create an AWS user with minimal permissions for the dynamic attributes connector 20

Create an AWS connector 21

Amazon Web Services Security Groups connector—About user permissions 22

Create an AWS user with minimal permissions for the dynamic attributes connector 22

Create an AWS Security Groups connector 24

Create an AWS service tags connector 25

Azure connector—About user permissions and imported data 26
Create an Azure user with minimal permissions for the dynamic attributes connector 26
Create an Azure connector 28
Create an Azure Service Tags connector 29
Cisco APIC connector 30
Requirements and prerequisites for 30
System requirements for the integration with Cisco APIC 31
Get required information for the integration 31
Create a Cisco APIC connector 35
Manually get a certificate authority (CA) chain 36
Create a Cisco Cyber Vision connector 40
Create a generic text connector 41
Create a GitHub connector 42
Google Cloud connector—About user permissions and imported data 43
Create a Google Cloud user with minimal permissions for the dynamic attributes connector 43
Create a Google Cloud connector 44
Create an Office 365 connector 45
vCenter connector—About user permissions and imported data 46
Create a vCenter user with minimal permissions for the dynamic attributes connector 47
Create a vCenter connector 48
Create a Webex connector 50
Create a Zoom Connector 51
Create an adapter 51
Create an ASA adapter 52
Edit or delete an ASA adapter 54
Create a user for the dynamic attributes connector 55
How to create an On-Prem Firewall Management Center adapter 57
Create a Cloud-Delivered Firewall Management Center adapter 60
Get your base URL and API token 60
How to create a Cloud-Delivered Firewall Management Center adapter 61
Manually get a certificate authority (CA) chain 62
Create dynamic attributes filters 66
Dynamic attribute filter examples 67
Manually get a certificate authority (CA) chain 69

CHAPTER 4 **Use Dynamic Objects in Access Control Policies or DNS Policies** 73

About dynamic objects in access control rules or DNS rules 73

Create dynamic attributes filters 73

Dynamic attributes rule conditions 75

View dynamic objects in the 75

Create access control rules or DNS rules using dynamic attributes filters 77

Use dynamic objects in DNS policies 78

How to use network object groups from Cisco APIC in ASA access rules 79

Add network object groups to access rules 79

View network object groups in ASDM 81

CHAPTER 5 **Troubleshoot the Dynamic Attributes Connector** 85

Troubleshoot error messages 85

Troubleshoot using the command line 87

Manually get a certificate authority (CA) chain 89

CHAPTER 6 **Migrate from the Cisco ACI Endpoint Update App to the Cisco APIC Integration with ASA** 93

About the migration 93

Migration step 1: Set up the dynamic attributes connector 94

Migration step 2: Prepare Cisco APIC 94

Migration step 3: Configure the dynamic attributes connector 95

Migration final step: Verify network object groups in ASDM 95

APPENDIX A **Security and Internet Access** 97

Security requirements 97

Internet access requirements 97

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.

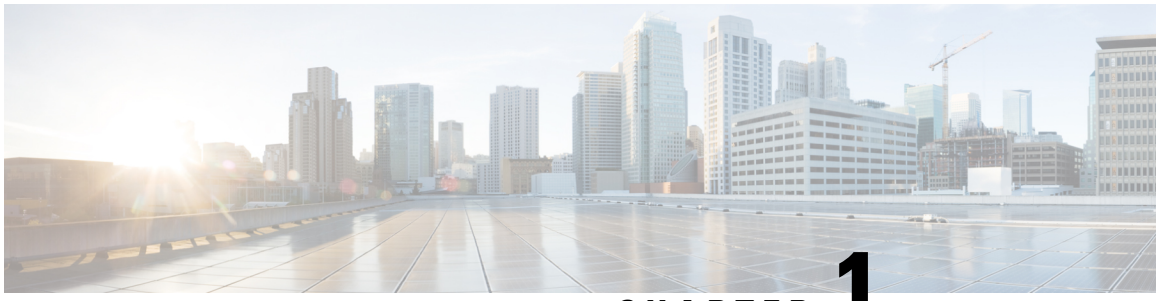
Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual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

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

© 2025 Cisco Systems, Inc. All rights reserved.



CHAPTER 1

About 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 they can be used in access control rules.

The following topics provide background about the dynamic attributes connector:

- About the dynamic attributes connector , on page 1

About the dynamic attributes connector

The dynamic attributes connector enables your access control and DNS policy to adapt in real time to the changes in public and private cloud workloads and business-critical software-as-a-service (SaaS) applications. It simplifies policy management by keeping rules up to date without tedious manual updates and policy deployment. Customers require policy rules to be defined based on non-network constructs such as VM name or security group, so that firewall policy is persistent even when the IP address or VLAN changes.

Supported connectors

We currently support the following connectors:

Table 1: 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	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

Related Topics

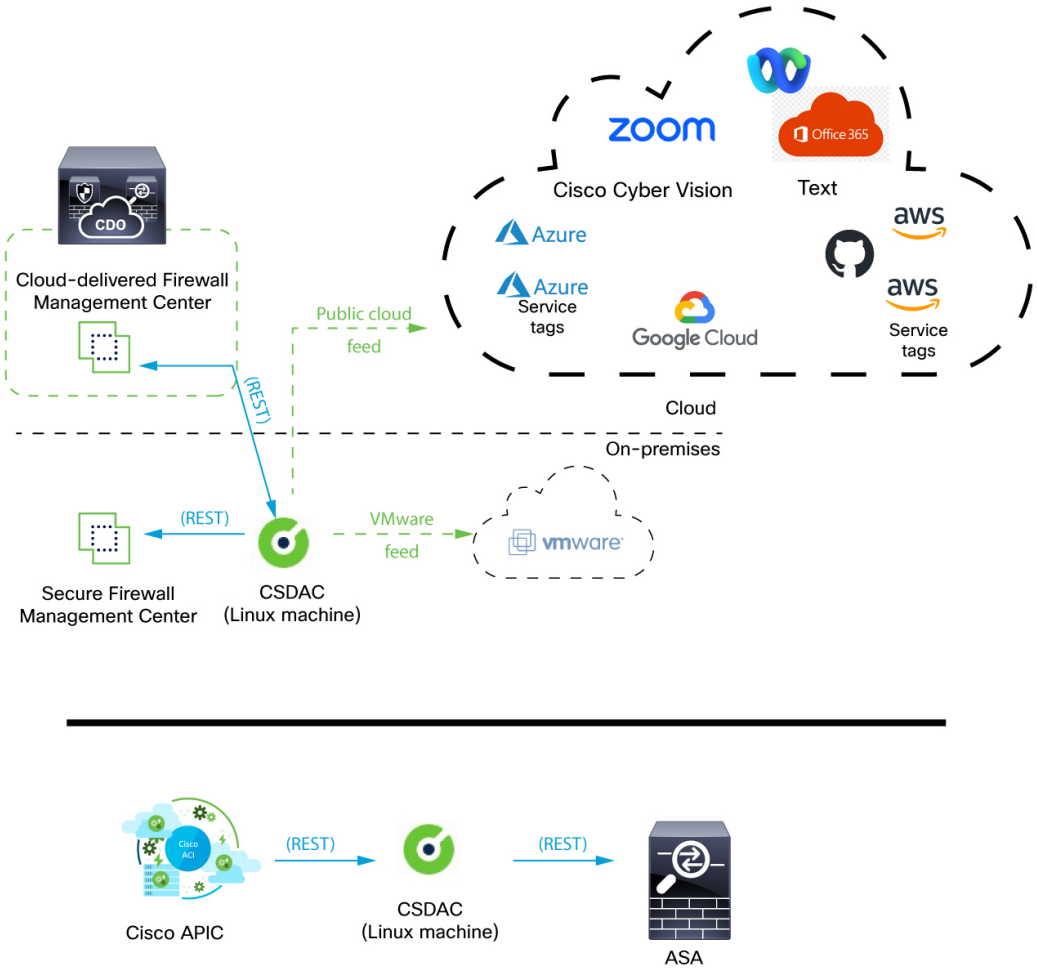
Install prerequisite software, on page 10

How it works

This topic discusses the architecture of the dynamic attributes connector.

You can collect these tags and attributes using Docker containers running on an Ubuntu, CentOS, or Red Hat Enterprise Linux virtual machine. Install the Dynamic Attributes Connector on the Ubuntu host using an Ansible collection.

The following figure shows how the system functions at a high level.



- Install the dynamic attributes connector on a supported Linux virtual machine.

  For more information, see Supported operating systems and third-party software, on page 9.

- The system supports certain public cloud providers.

  This topic discusses supported *connectors* (which are the connections to those providers).

- The *adapter* defined by the dynamic attributes connector receives those dynamic attributes filters as *dynamic objects* and enables you to use them in access control rules.

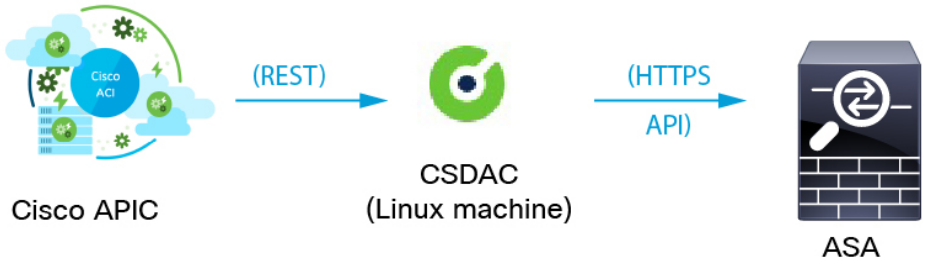
  You can create the following types of adapters:

  - ASA adapter used only by the Cisco APIC connector.
  - *On-Prem Firewall Management Center* for an on-premises Management Center device.

    This type of Management Center device might be managed by Security Cloud Control or it might be a standalone.
  - *Cloud-Delivered Firewall Management Center* for devices managed by Security Cloud Control.

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 . 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

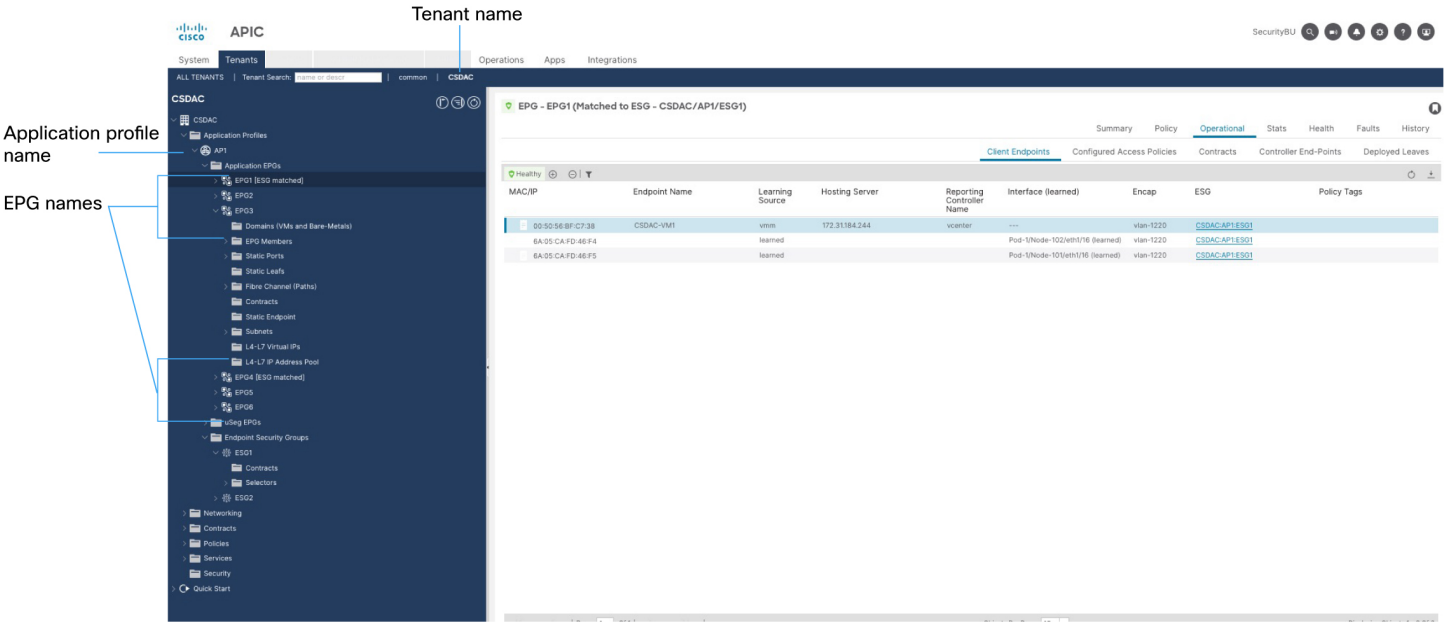
The following sample configuration shows how network object groups are named in ASA based on names in APIC and the APIC connector (not shown).

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

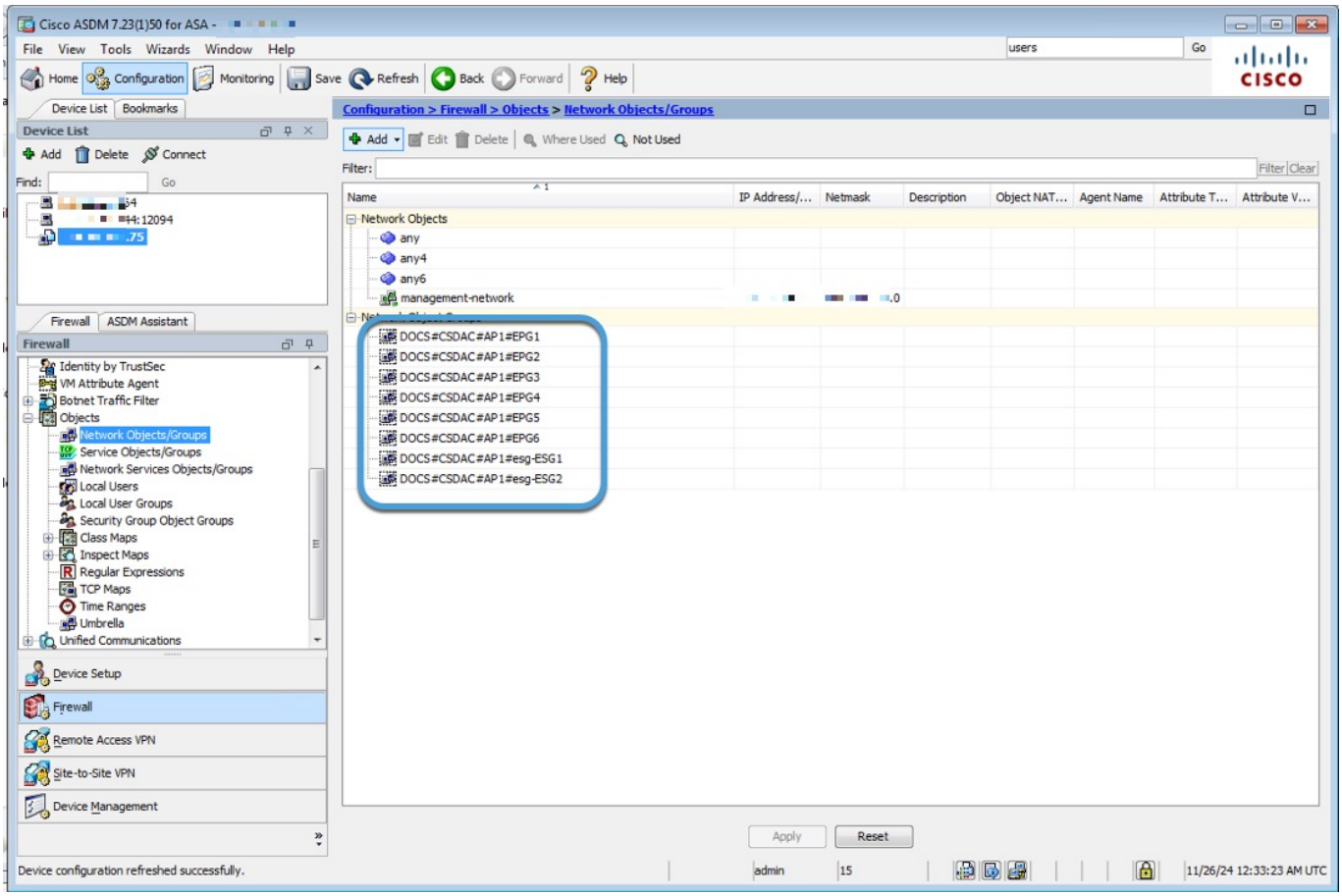
- Cisco ACI Endpoint Update App **Site Prefix** value

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`)



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**):



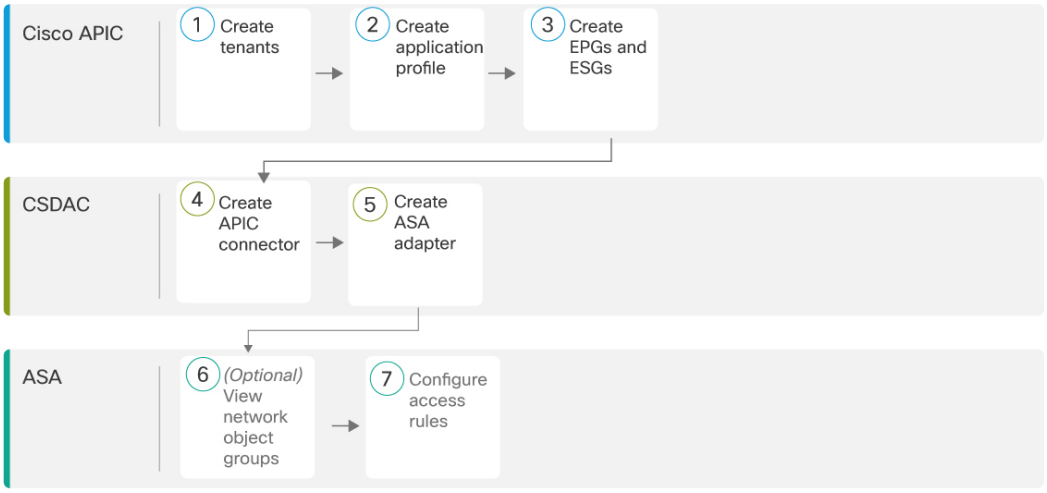
Additional information about Cisco APIC

- Basic User Tenant Configuration
- EPGs
- ESGs

What to do next

See Get required information for the integration, on page 31.

How to use network object groups from Cisco APIC in ASA access rules

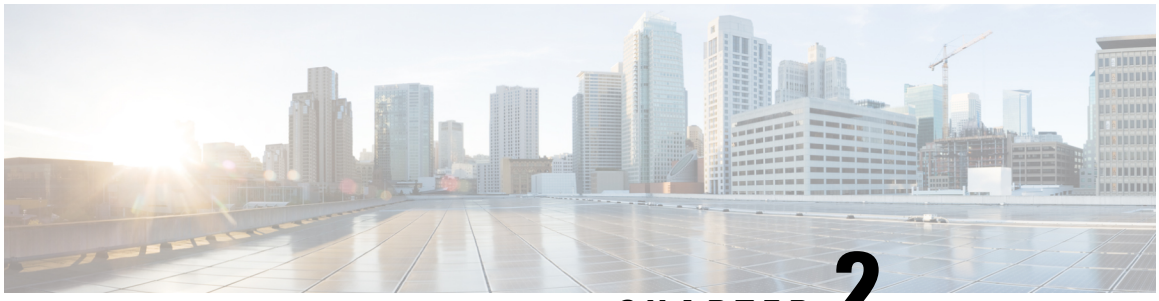


1 https://www.cisco.com/c/en/us/td/docs/dcn/aci/apic/6x/basic-configuration/cisco-apic-basic-configuration-guide-60x/basic-user-tenant-configuration-60x.html
2 https://www.cisco.com/c/en/us/td/docs/dcn/aci/apic/6x/basic-configuration/cisco-apic-basic-configuration-guide-60x/basic-user-tenant-configuration-60x.html
3 https://www.cisco.com/c/en/us/td/docs/dcn/aci/apic/6x/l2-configuration/cisco-apic-layer-2-networking-configuration-guide-61x/epgs-61x.html
4 Create a Cisco APIC connector, on page 35
5 Create an ASA adapter, on page 52
6 View network object groups in ASDM, on page 81
7 Add network object groups to access rules, on page 79

Table 2: 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	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 35
5	Dynamic Attributes Connector	The ASA adapter is responsible for updating objects on ASA. See Create an ASA adapter, on page 52
6	ASA	(Optional.) View the network object groups fetched from Cisco APIC. (Optional). See View network object groups in ASDM, on page 81
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 79



CHAPTER 2

Install and Upgrade the Dynamic Attributes Connector

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

- Supported operating systems and third-party software, on page 9
- Install prerequisite software, on page 10
- Install the dynamic attributes connector, on page 13
- Upgrade the dynamic attributes connector, on page 17

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.

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 12
Install prerequisite software—RHEL, on page 11

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 9.
- (Optional.) If you need proxy access to the dynamic attributes connector, see Install prerequisite software, on page 10.

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 dynamic attributes connector, on page 13.

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 dynamic attributes connector, on page 13.

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

Install the dynamic attributes connector

About the installation

This topic discusses installing the 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 10.

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 10.

- **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 dynamic attributes connector

This topic discusses how to upgrade from any earlier dynamic attributes connector to the current version. These tasks can be performed regardless of 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]
```

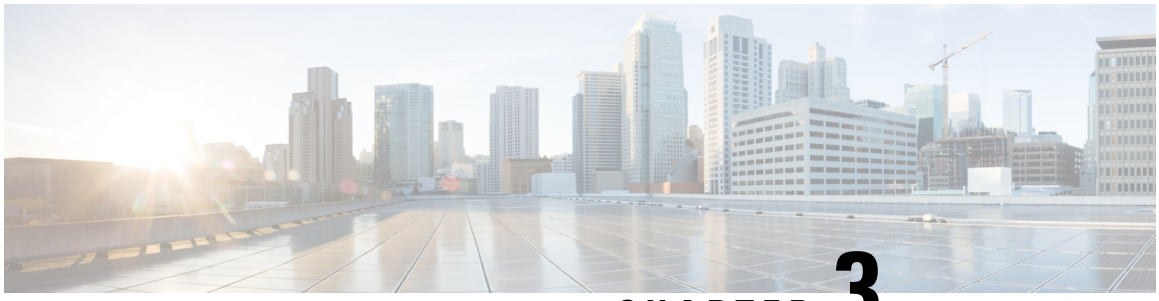
Syntax Description

--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 10. • **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 Dynamic Attributes Connector

Install the dynamic attributes connector and configure connectors, dynamic attributes filters, and adapters to provide or the with dynamic network data that can be used in access control rules.

See the following topics for more information:

- Create a connector, on page 19
- Create an adapter, on page 51
- Create dynamic attributes filters, on page 66
- Manually get a certificate authority (CA) chain, on page 69

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 .

We support the following:

Table 3: 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	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

Amazon Web Services connector—About user permissions and imported data

The dynamic attributes connector imports dynamic attributes from AWS to for use in policies.

Dynamic attributes imported

We import the following dynamic attributes from AWS:

- *Tags*, user-defined key-value pairs you can use to organize your AWS EC2 resources.

  For more information, see Tag your EC2 Resources in the AWS documentation

- *IP addresses* of virtual machines in AWS.

Minimum permissions required

The dynamic attributes connector requires a user at minimum with a policy that permits `ec2:DescribeTags`, `ec2:DescribeVpcs`, and `ec2:DescribeInstances` to be able to import dynamic attributes.

Create an AWS user with minimal permissions for the dynamic attributes connector

This task discusses how to set up a service account with minimum permissions to send dynamic attributes to . For a list of these attributes, see Amazon Web Services connector—About user permissions and imported data, on page 20.

Before you begin

You must already have set up your Amazon Web Services (AWS) account. For more information about doing that, see this article in the AWS documentation.

Procedure

Step 1 Log in to the AWS console as a user with the admin role.

Step 2 From the Dashboard, click **Security, Identity & Compliance** > **IAM**.

Step 3 Click **Access Management** > **Users**.

Step 4 Click **Add Users**.

Step 5 In the **User Name** field, enter a name to identify the user.

Step 6 Click **Access Key - Programmatic Access**.

Step 7 At the Set permissions page, click **Next** without granting the user access to anything. You can grant user access later.

Step 8 Add tags to the user if desired.

Step 9 Click **Create User**.

Step 10 Click **Download .csv** to download the user's key to your computer.

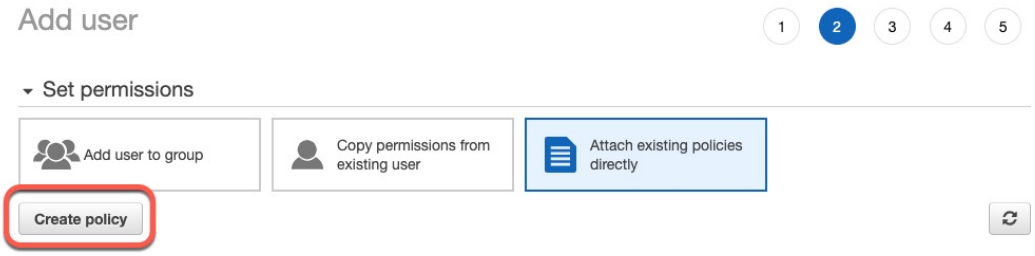
Note
This is the only opportunity you have to retrieve the user's key.

Step 11 Click **Close**.

Step 12 At the Identity and Access Management (IAM) page in the left column, click **Access Management** > **Policies**.

Step 13 Click **Create Policy**.

Step 14 On the Create Policy page, click **JSON**.



Step 15 Enter the following policy in the field:

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "ec2:DescribeTags",
    "ec2:DescribeInstances",
    "ec2:DescribeVpcs"
   ],
   "Resource": "*"
  }
 ]
}
```

Step 16 Click **Next**.

Step 17 Click **Review**.

Step 18 On the Review Policy page, enter the requested information and click **Create Policy**.

Step 19 On the Policies page, enter all or part of the policy name in the search field and press Enter.

Step 20 Click the policy you just created.

Step 21 Click **Actions** > **Attach**.

Step 22 If necessary, enter all or part of the user name in the search field and press Enter.

Step 23 Click **Attach Policy**.

What to do next

Create an AWS connector, on page 21.

Create an AWS connector

This task discusses how to configure a connector that sends data from AWS to the for use in policies.

Before you begin

Create a user with at least the privileges discussed in Create an AWS user with minimal permissions for the dynamic attributes connector, on page 20.

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.
Pull Interval	(Default 30 seconds.) Interval at which IP mappings are retrieved from AWS.
Region	(Required.) Enter your AWS region code.
Access Key	(Required.) Enter your access key.
Secret Key	(Required.) Enter your secret key.

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.

Amazon Web Services Security Groups connector—About user permissions

The dynamic attributes connector imports dynamic attributes from AWS to for use in policies.

Minimum permissions required

The dynamic attributes connector requires a user at minimum with a policy that permits `ec2:DescribeTags`, `ec2:DescribeVpcs`, and `ec2:DescribeInstances` to be able to import dynamic attributes.

Create an AWS user with minimal permissions for the dynamic attributes connector

This task discusses how to set up a service account with minimum permissions to send dynamic attributes to . For a list of these attributes, see Amazon Web Services connector—About user permissions and imported data, on page 20.

Before you begin

You must already have set up your Amazon Web Services (AWS) account. For more information about doing that, see this article in the AWS documentation.

Procedure

Step 1 Log in to the AWS console as a user with the admin role.

Step 2 From the Dashboard, click **Security, Identity & Compliance** > **IAM**.

Step 3 Click **Access Management** > **Users**.

Step 4 Click **Add Users**.

Step 5 In the **User Name** field, enter a name to identify the user.

Step 6 Click **Access Key - Programmatic Access**.

Step 7 At the Set permissions page, click **Next** without granting the user access to anything. You can grant user access later.

Step 8 Add tags to the user if desired.

Step 9 Click **Create User**.

Step 10 Click **Download .csv** to download the user's key to your computer.

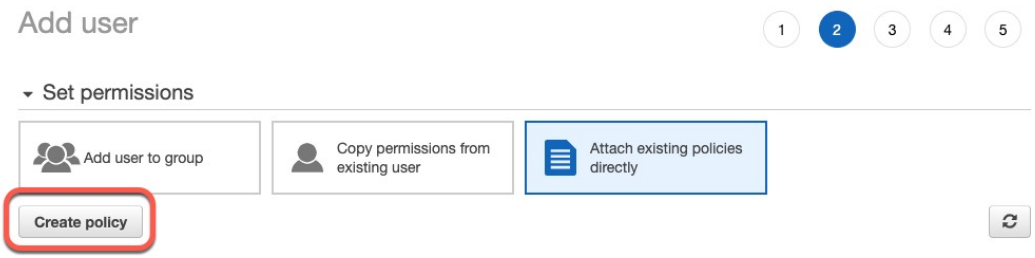
Note
This is the only opportunity you have to retrieve the user's key.

Step 11 Click **Close**.

Step 12 At the Identity and Access Management (IAM) page in the left column, click **Access Management** > **Policies**.

Step 13 Click **Create Policy**.

Step 14 On the Create Policy page, click **JSON**.



Step 15 Enter the following policy in the field:

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "ec2:DescribeTags",
    "ec2:DescribeInstances",
    "ec2:DescribeVpcs"
   ],
   "Resource": "*"
  }
 ]
}
```

Step 16 Click **Next**.

Step 17 Click **Review**.

Step 18 On the Review Policy page, enter the requested information and click **Create Policy**.

Step 19 On the Policies page, enter all or part of the policy name in the search field and press Enter.

Step 20 Click the policy you just created.

Step 21 Click **Actions** > **Attach**.

Step 22 If necessary, enter all or part of the user name in the search field and press Enter.

Step 23 Click **Attach Policy**.

What to do next

Create an AWS connector, on page 21.

Create an AWS Security Groups connector

This task discusses how to configure a connector that sends AWS security groups data to the for use in policies.

Before you begin

Do all of the following:

- Create AWS security groups as discussed in Work with security groups on the AWS documentation site.
- Create a user with at least the privileges discussed in Create an AWS user with minimal permissions for the dynamic attributes connector, on page 20.

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 30 seconds.) Interval at which IP mappings are retrieved from AWS. The minimum value for **Pull Interval** is 1 second. You can set the maximum to any value you want. We recommend against setting the minimum to a low value because it can generate a lot of traffic, and, when applicable, can result in your being billed for the traffic.
Region	(Required.) Enter your AWS region code.
AWS Access Key	(Required.) Enter your access key.
AWS Secret Key	(Required.) Enter your secret key.

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.

Create an AWS service tags connector

This topic discusses how to create a connector for Amazon Web Services (AWS) service tags to the for use in policies.

For more information, see resources like the following on the AWS documentation site:

- What are tags?
- AWS IP address ranges
- Tagging your AWS resources
- Guidance for Tagging on AWS
- AWS service points

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.
URL	(Required.) Do not change the URL unless advised to do so.

Step 5 Click **Test** and make sure **Test connection succeeded** is displayed before you save the connector.

Step 6 Click **Save**.

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

Azure connector—About user permissions and imported data

The dynamic attributes connector imports dynamic attributes from Azure to for use in policies.

Dynamic attributes imported

We import the following dynamic attributes from Azure:

- *Tags*, key-value pairs associated with resources, resource groups, and subscriptions.

  For more information, see this page in the Microsoft documentation.

- *IP addresses* of virtual machines in Azure.

Minimum permissions required

The dynamic attributes connector requires a user at minimum with the **Reader** permission to be able to import dynamic attributes.

Create an Azure user with minimal permissions for the dynamic attributes connector

This task discusses how to set up a service account with minimum permissions to send dynamic attributes to . For a list of these attributes, see Azure connector—About user permissions and imported data, on page 26.

Before you begin

You must already have a Microsoft Azure account. To set one up, see this page on the Azure documentation site.

Procedure

Step 1 Log in to the Azure Portal as the owner of the subscription.

Step 2 Click **Azure Active Directory**.

Step 3 Find the instance of Azure Active Directory for the application you want to set up.

Step 4 Click **Add** > **App registration**.

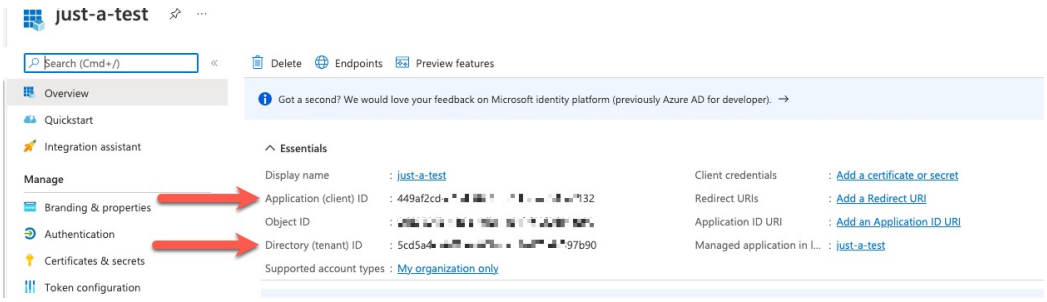
Step 5 In the **Name** field, enter a name to identify this application.

Step 6 Enter other information on this page as required by your organization.

Step 7 Click **Register**.

Step 8 On the next page, write down or copy the Client ID (also referred to as *application ID*) and the tenant ID (also referred to as the *directory ID*).

A sample follows.

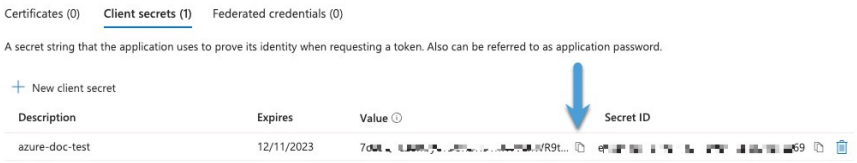


Step 9 Next to Client Credentials, click **Add a certificate or secret**.

Step 10 Click **New Client Secret**.

Step 11 Enter the requested information and click **Add**.

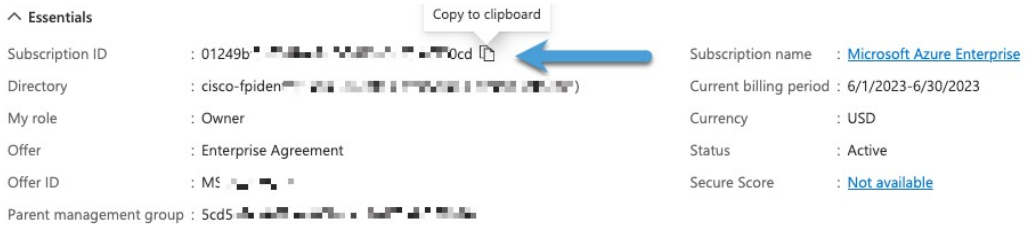
Step 12 Copy the value of the **Value** field to the clipboard. This value, *and not the **Secret ID***, is the client secret.



Step 13 Go back to the main Azure Portal page and click **Subscriptions**.

Step 14 Click the name of your subscription.

Step 15 Copy the subscription ID to the clipboard.



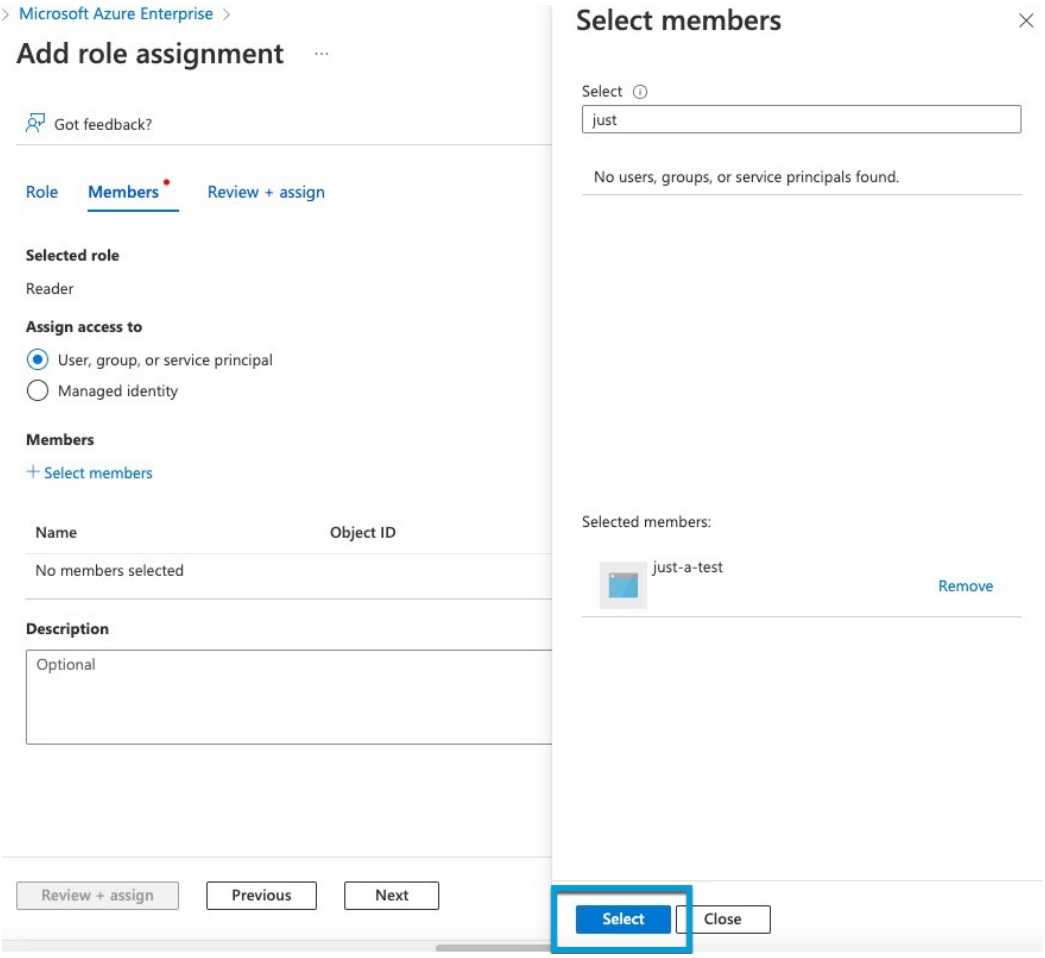
Step 16 Click **Access Control (IAM)**.

Step 17 Click **Add** > **Add role assignment**.

Step 18 Click **Reader** and click **Next**.

Step 19 Click **Select Members**.

Step 20 On the right side of the page, click the name of the app you registered and click **Select**.



Step 21 Click **Review + Assign** and follow the prompts to complete the action.

What to do next

See Create an Azure connector, on page 28.

Create an Azure connector

This task discusses how to create a connector to send data from Azure to for use in policies.

Before you begin

Create an Azure user with at least the privileges discussed in Create an Azure user with minimal permissions for the dynamic attributes connector, on page 26.

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.
Pull Interval	(Default 30 seconds.) Interval at which IP mappings are retrieved from Azure. The minimum value for **Pull Interval** is 1 second. You can set the maximum to any value you want. We recommend against setting the minimum to a low value because it can generate a lot of traffic, and, when applicable, can result in your being billed for the traffic.
Subscription Id	(Required.) Enter your Azure subscription ID.
Tenant Id	(Required.) Enter your tenant ID.
Client Id	(Required.) Enter your client ID.
Client Secret	(Required.) Enter your client secret.

Step 5 Click **Test** and make sure **Test connection succeeded** is displayed before you save the connector.

Step 6 Click **Save**.

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

Create an Azure Service Tags connector

This topic discusses how to create a connector for Azure service tags to the for use in policies. The IP addresses associated with these tags are updated every week by Microsoft.

For more information, see Virtual network service tags on Microsoft TechNet.

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.
Pull Interval	(Default 30 seconds.) Interval at which IP mappings are retrieved from Azure. The minimum value for **Pull Interval** is 1 second. You can set the maximum to any value you want. We recommend against setting the minimum to a low value because it can generate a lot of traffic, and, when applicable, can result in your being billed for the traffic.
Subscription Id	(Required.) Enter your Azure subscription ID.
Tenant Id	(Required.) Enter your tenant ID.
Client Id	(Required.) Enter your client ID.
Client Secret	(Required.) Enter your client secret.

Step 5 Click **Test** and make sure **Test connection succeeded** is displayed before you save the connector.

Step 6 Click **Save**.

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

Cisco APIC connector

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

Related Topics

System requirements for the integration with Cisco APIC, on page 31
Get required information for the integration, on page 31
Create a Cisco APIC connector, on page 35
Manually get a certificate authority (CA) chain, on page 36

Requirements and prerequisites for

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
  - 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 , see About the integration with ASA.

Related Topics

System requirements for the integration with Cisco APIC, on page 31
Get required information for the integration, on page 31
Create a Cisco APIC connector, on page 35
Manually get a certificate authority (CA) chain, on page 36

System requirements for the integration with Cisco APIC

Your system must meet the following requirements:

- 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.

Related Topics

System requirements for the integration with Cisco APIC, on page 31
Get required information for the integration, on page 31
Create a Cisco APIC connector, on page 35
Manually get a certificate authority (CA) chain, on page 36

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:

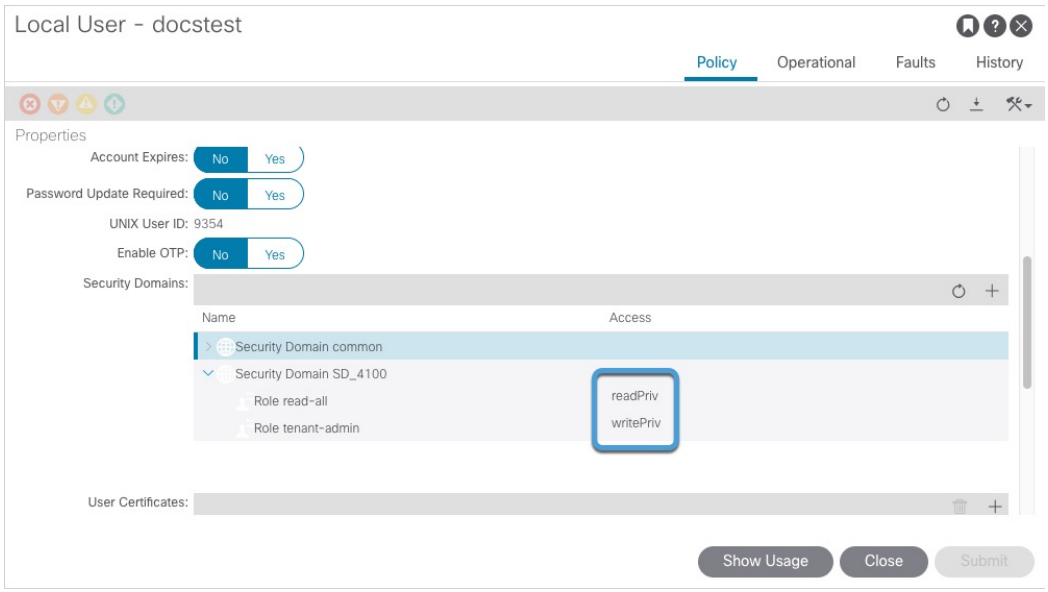
1. Log in to Cisco APIC as a user with `admin` privileges.

   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.



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 .

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 ASA.

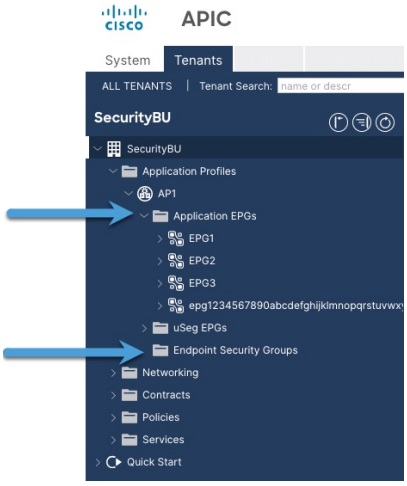
EPG name

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.

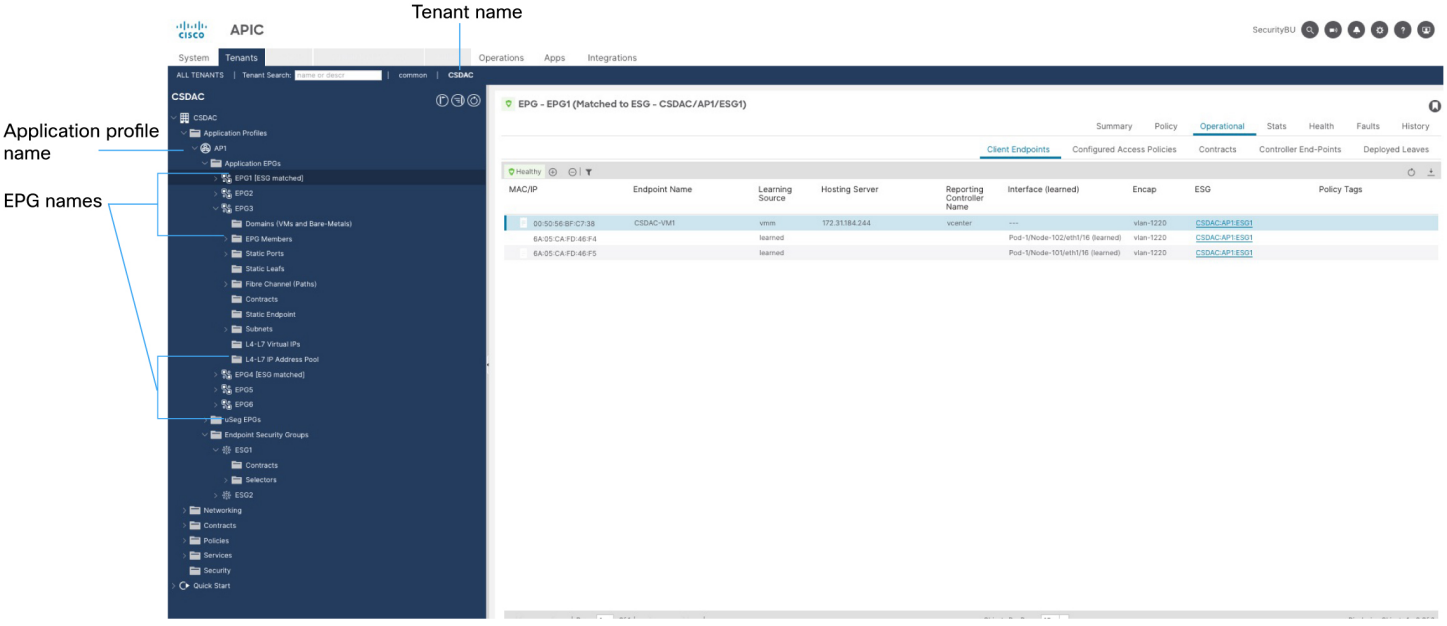
4. Expand your tenant.
5. Expand **Application Profiles**.
6. Expand the name of the application profile.
7. Expand **Application EPGs**.
8. Write down the name of the EPG or ESG that has network object groups to send to ASA.

   The following figure shows an example.



Example

The following figure shows the values in Cisco APIC.



Related Topics

System requirements for the integration with Cisco APIC, on page 31
Get required information for the integration, on page 31
Create a Cisco APIC connector, on page 35
Manually get a certificate authority (CA) chain, on page 36

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.

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.
Pull Interval	(Default 60 seconds.) Interval at which IP mappings are retrieved from Cisco APIC. We recommend setting this to 15 seconds.
IP or Hostname	Enter the fully-qualified domain name or IP address of the Cisco APIC server from which to retrieve network object groups 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 .
Password	Enter the user's password.

Value	Description
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.

What to do next

Create an ASA adapter, on page 52

Related Topics

System requirements for the integration with Cisco APIC, on page 31
Get required information for the integration, on page 31
Create a Cisco APIC connector, on page 35
Manually get a certificate authority (CA) chain, on page 36

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, , Cisco APIC, or .

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
-
- 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 Cisco APIC, or . For example:

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

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

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

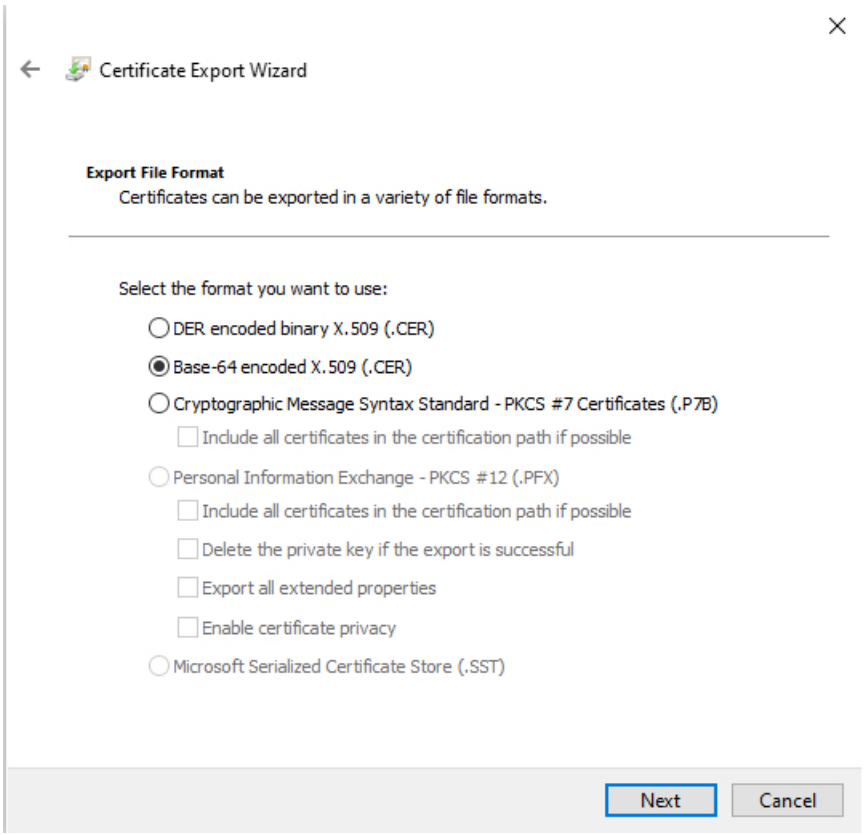
3. Save the entire certificate chain to a plaintext file.
   - *Include* all `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` delimiters.
   - *Exclude* any extraneous text (for example, the name of the certificate and any text contained in angle brackets (< and >) as well as the angle brackets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

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, , Cisco APIC, or 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.



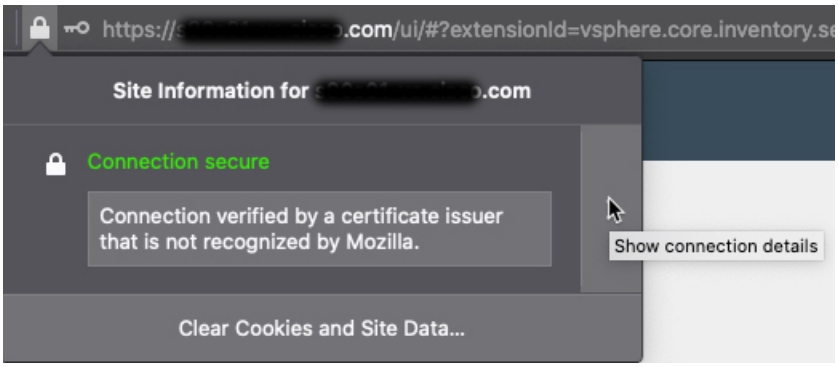
10. Follow the prompts to complete the export.
11. Open the certificate in a text editor.
12. Repeat the process for all certificates in the chain.

    You must paste each certificate in the text editor in order, first to last.
13. Repeat these tasks for vCenter, , Cisco APIC, or .

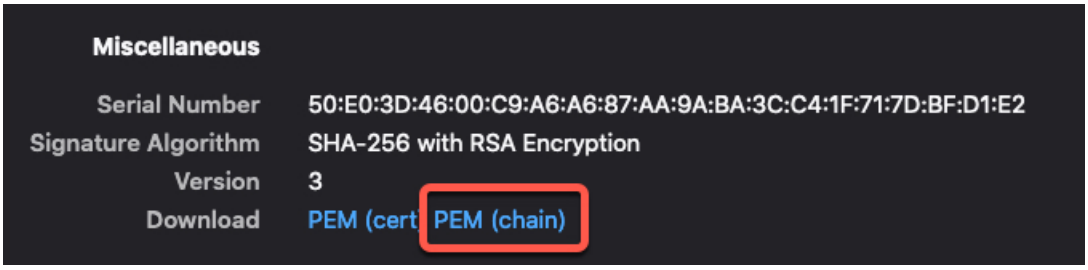
Get a Certificate Chain—Windows Firefox

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

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

Related Topics

How to create an On-Prem Firewall Management Center adapter, on page 57
How to create a Cloud-Delivered Firewall Management Center adapter, on page 61
Create an adapter, on page 51
Create an ASA adapter, on page 52
Edit or delete an ASA adapter, on page 54
Create a user for the dynamic attributes connector, on page 55
Create a Cloud-Delivered Firewall Management Center adapter, on page 60
Get your base URL and API token, on page 60
Manually get a certificate authority (CA) chain, on page 36
System requirements for the integration with Cisco APIC, on page 31
Get required information for the integration, on page 31
Create a Cisco APIC connector, on page 35
Cisco APIC connector, on page 30
Requirements and prerequisites for, on page 30

Create a Cisco Cyber Vision connector

This task discusses how to send data from Cisco Cyber Vision to the .

Before you begin

Cisco Cyber Vision must be reachable from the machine on which the dynamic attributes connector is running. You must know its IP address, port, and API key.

To find the API key in the Cyber Vision management console, click **Admin** > **API** > **Token**, then click **Show** to display the token and  to copy the token to the clipboard.

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.
Cyber Vision Prefix	Enter an alphanumeric string to identify dynamic objects from this Cyber Vision's IP address when objects are sent to . If you have one Cyber Vision IP address, you can enter any value such as **1**.
Pull Interval	(Default 60 seconds.) Interval at which data mappings are retrieved from Cyber Vision. The minimum value for **Pull Interval** is 1 second. You can set the maximum to any value you want. We recommend against setting the minimum to a low value because it can generate a lot of traffic, and, when applicable, can result in your being billed for the traffic.
Host	(Required.) Enter the Cyber Vision fully qualified host name or IP address.
Port	(Required.) Enter the Cyber Vision listen port.
Token	(Required.) Enter the API token.

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.

Create a generic text connector

This task discusses how to create an ad hoc list of IP addresses you maintain manually and retrieve at an interval you select (30 seconds by default). You can update the list of addresses anytime you want.

Before you begin

Create text files with IP addresses and put it on a web server that is accessible from the . IP addresses can include CIDR notation. The text file must have only one IP address per line.

For example, you might have a list of IP addresses for an "allow list" in access control rules and another list of IP addresses for a "block list" in access control rules.

You can specify up to 10,000 IP addresses per text file.

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:

Item	Description
Name	Enter a name to identify the connector.
Description	(Optional.) Enter a description
Pull Interval	Change the frequency, in seconds, at which the dynamic attributes connector retrieves IP addresses from the text file. The default is 30 seconds. The minimum value for **Pull Interval** is 1 second. You can set the maximum to any value you want. We recommend against setting the minimum to a low value because it can generate a lot of traffic, and, when applicable, can result in your being billed for the traffic.
URLs	Enter a URL from which to retrieve IP addresses.
Add another URL	(Optional.) Click the link to add more URLs to an existing list.

Item	Description
Username	(Optional.) If the server on which the text file is located uses authentication, enter the user's name in this field. We use Basic authentication.
Password	(Optional.) Enter the user's password.
Certificate	(Optional.) If a certificate chain is required for a secure connection to the web server, you have the following options: • 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 36. • 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.

Create a GitHub connector

This section discusses how to create a GitHub connector that sends data to the for use in policies. The IP addresses associated with these tags are maintained by GitHub. You do not have to create a dynamic attributes filters.

For more information, see About GitHub's IP addresses.

Note Do not change the URL because doing so will fail to retrieve any IP addresses.

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 a **Name** and an optional description.

Step 5 (Optional.) In the **Pull Interval** field, change the frequency, in seconds, at which the dynamic attributes connector retrieves IP addresses from GitHub. The default is 21,600 seconds (6 hours).

Step 6 Click **Test** and make sure the test succeeds before you save the connector.

Step 7 Click **Save**.

Step 8 Make sure **Ok** is displayed in the Status column.

Google Cloud connector—About user permissions and imported data

The dynamic attributes connector imports dynamic attributes from Google Cloud to for use in policies.

Dynamic attributes imported

We import the following dynamic attributes from Google Cloud:

- *Labels*, key-value pairs you can use to organize your Google Cloud resources.

  For more information, see Creating and Managing Labels in the Google Cloud documentation.

- *Network tags*, key-value pairs associated with an organization, folder, or project.

  For more information, see Creating and Managing Tags in the Google Cloud documentation.

- *IP addresses* of virtual machines in Google Cloud.

Minimum permissions required

The dynamic attributes connector requires a user at minimum with the **Basic** > **Viewer** permission to be able to import dynamic attributes.

Create a Google Cloud user with minimal permissions for the dynamic attributes connector

This task discusses how to set up a service account with minimum permissions to send dynamic attributes to . For a list of these attributes, see Google Cloud connector—About user permissions and imported data, on page 43.

Before you begin

You must already have set up your Google Cloud account. For more information about doing that, see Setting Up Your Environment in the Google Cloud documentation.

Procedure

Step 1 Log in to your Google Cloud account as a user with the owner role.

Step 2 Click **IAM & Admin** > **Service Accounts** > **Create Service Account**.

Step 3 Enter the following information:

- **Service account name**: A name to identify this account; for example, `CSDAC`.
- **Service account ID**: Should be populated with a unique value after you enter the service account name.

- **Service account description**: Enter an optional description.

For more information about service accounts, see Understanding Service Accounts in the Google Cloud documentation.

Step 4 Click **Create and Continue**.

Step 5 Follow the prompts on your screen until the Grant users access to this service account section is displayed.

Step 6 Grant the user the **Basic** > **Viewer** role.

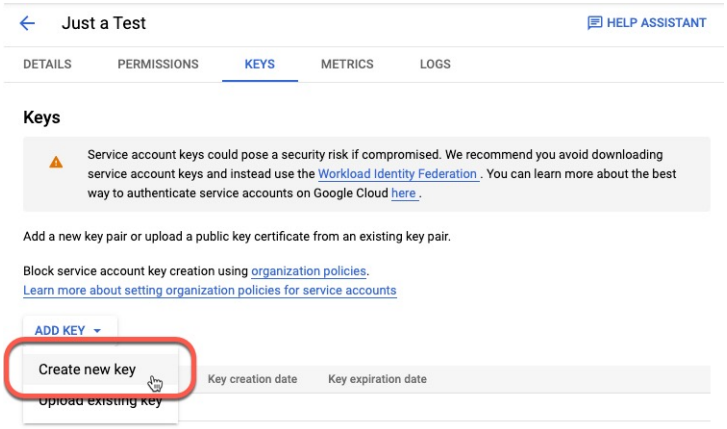
Step 7 Click **Done**.

A list of service accounts is displayed.

Step 8 Click **More** (⋮) at the end of the row of the service account you created.

Step 9 Click **Manage Keys**.

Step 10 Click **Add Key** > **Create New Key**.



Step 11 Click **JSON**.

Step 12 Click **Create**.

The JSON key is downloaded to your computer.

Step 13 Keep the key handy when you configure the GCP connector.

What to do next

See Create a Google Cloud connector, on page 44.

Create a Google Cloud connector

Before you begin

Have your Google Cloud JSON-formatted service account data ready; it's required to set up the connector.

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.
Pull Interval	(Default 30 seconds.) Interval at which IP mappings are retrieved from AWS. The minimum value for **Pull Interval** is 1 second. You can set the maximum to any value you want. We recommend against setting the minimum to a low value because it can generate a lot of traffic, and, when applicable, can result in your being billed for the traffic.
GCP region	(Required.) Enter the GCP region in which your Google Cloud is located. For more information, see Regions and Zones in the Google Cloud documentation.
Service account	Paste the JSON code for your Google Cloud service account.

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.

Create an Office 365 connector

This task discusses how to create a connector for Office 365 tags to send data to the for use in policies. The IP addresses associated with these tags are updated every week by Microsoft. You do not have to create a dynamic attributes filter to use the data.

For more information, see Office 365 URLs and IP address ranges on docs.microsoft.com.

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.
Pull Interval	(Default 30 seconds.) Interval at which IP mappings are retrieved from Azure. The minimum value for **Pull Interval** is 1 second. You can set the maximum to any value you want. We recommend against setting the minimum to a low value because it can generate a lot of traffic, and, when applicable, can result in your being billed for the traffic.
Base API URL	(Required.) Enter the URL from which to retrieve Office 365 information, if it's different from the default. For more information, see Office 365 IP Address and URL web service on the Microsoft documentation site.
Instance name	(Required.) From the list, click an instance name. For more information, see Office 365 IP Address and URL web service on the Microsoft documentation site.
Disable optional IPs	(Required.) Enter **true** or **false**.

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.

vCenter connector—About user permissions and imported data

The Dynamic Attributes Connector imports dynamic attributes from vCenter to for use in policies.

Dynamic attributes imported

We import the following dynamic attributes from vCenter:

- *Operating system*
- *MAC address*
- *IP addresses*
- *NSX tags*

Minimum permissions required

The Dynamic Attributes Connector requires a user at minimum with the **Read Only** permission to be able to import dynamic attributes.

Create a vCenter user with minimal permissions for the dynamic attributes connector

This task discusses how to set up a service account with minimum permissions to send dynamic attributes to . For a list of these attributes, see vCenter connector—About user permissions and imported data, on page 46.

Before you begin

You must already have set up your vCenter Server account. For more information about doing that, see About vCenter Server Installation and Setup in the vCenter documentation.

Procedure

Step 1 Log into vCenter as an administrator.

Step 2 Click **Menu** > **Administration**.

Step 3 In the left pane, click **Single Sign On** > **Users and Groups**.

Step 4 From the **Domain** list, click the name of a domain to add the user.

Step 5 Click **Add User**.

Step 6 Enter the requested information and click **Add**.

Step 7 In the left pane, click **Access Control** > **Global Permissions**.

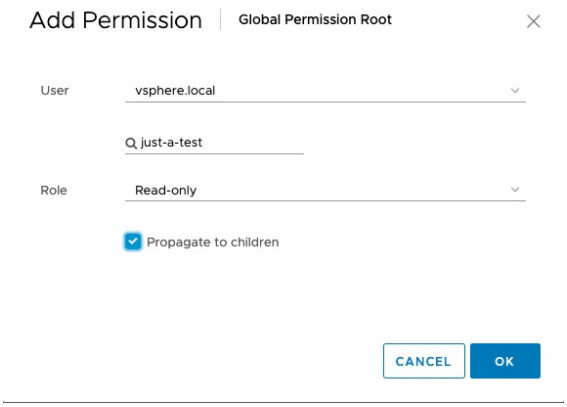
Step 8 Click **Add**(+).

Step 9 From the **User** field, click the name of the vCenter domain in which you created the user.

Step 10 In the search field, enter part of the user's name.

Step 11 From the **Role** list, click **Read-only**.

Step 12 Select the **Propagate to children** check box.



Step 13 Click **OK**.

What to do next

See Create a vCenter connector, on page 48.

Create a vCenter connector

This task discusses how to create a connector for VMware vCenter to send data to the for use in policies.

Before you begin

If you use non-trusted certificates to communicate with vCenter, see Manually get a certificate authority (CA) chain, on page 36.

Procedure

Step 1 Log in to the dynamic attributes connector.

Step 2 Click **Connectors**.

Step 3 Do any of the following:

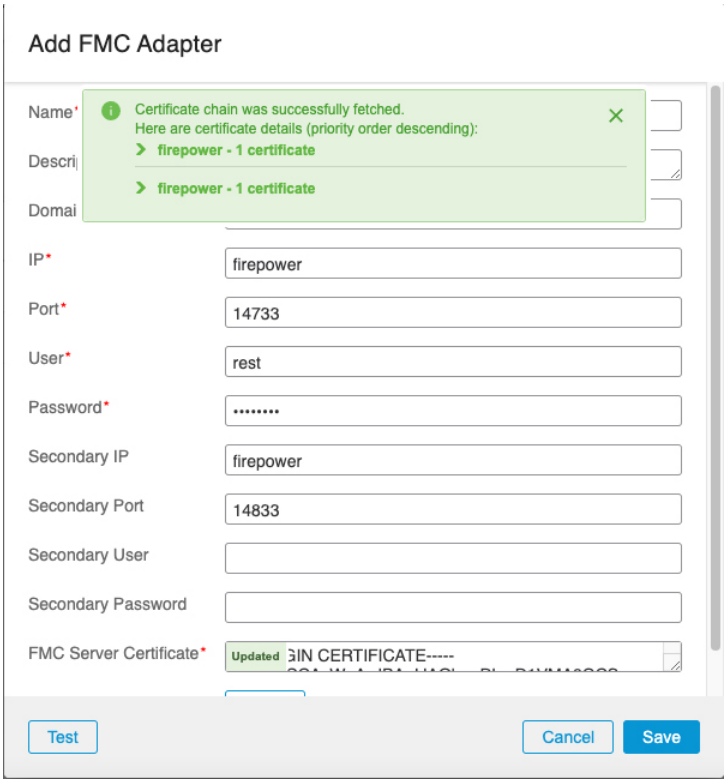
- Add a new connector: click Add icon (), then click the name of the connector.
- Edit or delete a connector: Click **More** (⋮), then click **Edit** or **Delete** at the end of the row.

Step 4 Enter the following information.

Value	Description
Name	(Required.) Enter a name to uniquely identify this connector.
Description	Enter an optional description.
Pull Interval	(Default 30 seconds.) Interval at which IP mappings are retrieved from vCenter. The minimum value for **Pull Interval** is 1 second. You can set the maximum to any value you want. We recommend against setting the minimum to a low value because it can generate a lot of traffic, and, when applicable, can result in your being billed for the traffic.
Host	(Required.) Enter any of the following: • vCenter's fully qualified host name • vCenter's IP address • (Optional.) A port *Do not* enter a scheme (such as `https://`) or trailing slash. For example, `myvcenter.example.com` or `192.0.2.100:9090`
User	(Required.) Enter the user name of a user with the Read-only role at minimum. User names are case-sensitive.
Password	(Required.) Enter the user's password.

Value	Description
NSX IP	If you use vCenter Network Security Visualization (NSX), enter its IP address.
NSX User	Enter the user name of an NSX user with the Auditor role at minimum.
NSX Type	Enter **NSX-T**.
NSX Password	Enter the NSX user's password.
vCenter Certificate	You have the following options: • 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 36. • Click **Get Certificate** > **Browse from file** to upload a certificate chain you downloaded previously.

Following is an example of successfully fetching a certificate chain:



Expanding the certificate CA chain at the top of the dialog box displays the certificates similar to the following.



If it's not possible to fetch the certificate this way, you can get the certificate chain manually as discussed in Manually get a certificate authority (CA) chain, on page 36.

Step 5 Click **Test** and make sure **Test connection succeeded** is displayed before you save the connector.

Step 6 Click **Save**.

Create a Webex connector

This section discusses how to create a Webex connector that sends data to the for use in policies. The IP addresses associated with these tags are maintained by Webex. You do not have to create a dynamic attributes filters.

For more information, see Port Reference for Webex Calling.

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.
Pull Interval	(Default 30 seconds.) Interval at which IP mappings are retrieved from Webex. The minimum value for **Pull Interval** is 1 second. You can set the maximum to any value you want. We recommend against setting the minimum to a low value because it can generate a lot of traffic, and, when applicable, can result in your being billed for the traffic.
Provider Reserved IPs	(Required.) (Required.) Slide to enabled to retrieve any reserved IP addresses.

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.

Create a Zoom Connector

This section discusses how to create a Zoom connector that sends data to the for use in policies. The IP addresses associated with these tags are maintained by Zoom. You do not have to create a dynamic attributes filters.

For more information, see Zoom network firewall or proxy server settings.

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.
Pull Interval	(Default 30 seconds.) Interval at which IP mappings are retrieved from Zoom. The minimum value for **Pull Interval** is 1 second. You can set the maximum to any value you want. We recommend against setting the minimum to a low value because it can generate a lot of traffic, and, when applicable, can result in your being billed for the traffic.
Provider Reserved IPs	(Required.) Slide to enabled to retrieve any reserved IP addresses.

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.

Create an adapter

An *adapter* is a secure connection to to which you push network information from cloud objects for use in access control policies.

First you can optionally fetch the certificate authority chain, which is required to securely connect to the .

Fetching the certificate authority chain requires only the host name; creating the adapter requires a user name, password, and other information.

Related Topics

How to create an On-Prem Firewall Management Center adapter, on page 57
How to create a Cloud-Delivered Firewall Management Center adapter, on page 61
Create an adapter, on page 51
Create an ASA adapter, on page 52
Edit or delete an ASA adapter, on page 54
Create a user for the dynamic attributes connector, on page 55
Create a Cloud-Delivered Firewall Management Center adapter, on page 60
Get your base URL and API token, on page 60
Manually get a certificate authority (CA) chain, on page 36

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 35.

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.
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 integration, on page 31. • The value of the **APIC Site Prefix** you specified for the Cisco APIC connector as discussed in Create a Cisco APIC connector, on page 35. 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 36. • 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 36. • Click **Get Certificate** > **Browse from file** to upload a certificate chain you downloaded previously.

Related Topics

How to create an On-Prem Firewall Management Center adapter, on page 57
How to create a Cloud-Delivered Firewall Management Center adapter, on page 61
Create an adapter, on page 51
Create an ASA adapter, on page 52
Edit or delete an ASA adapter, on page 54
Create a user for the dynamic attributes connector, on page 55
Create a Cloud-Delivered Firewall Management Center adapter, on page 60
Get your base URL and API token, on page 60
Manually get a certificate authority (CA) chain, on page 36

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 52.

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 52.

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.

Related Topics

How to create an On-Prem Firewall Management Center adapter, on page 57
How to create a Cloud-Delivered Firewall Management Center adapter, on page 61
Create an adapter, on page 51
Create an ASA adapter, on page 52
Edit or delete an ASA adapter, on page 54
Create a user for the dynamic attributes connector, on page 55
Create a Cloud-Delivered Firewall Management Center adapter, on page 60
Get your base URL and API token, on page 60
Manually get a certificate authority (CA) chain, on page 36

Create a user for the dynamic attributes connector

We recommend you create a dedicated user for the dynamic attributes connector adapter. Creating a dedicated user avoids issues like unexpected logouts from the because the dynamic attributes connector periodically logs in using a REST API to update the with new and updated dynamic objects.

The user must have Access Admin privileges at least.

Procedure

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

Step 2 Click **System** (⚙) > **Users**.

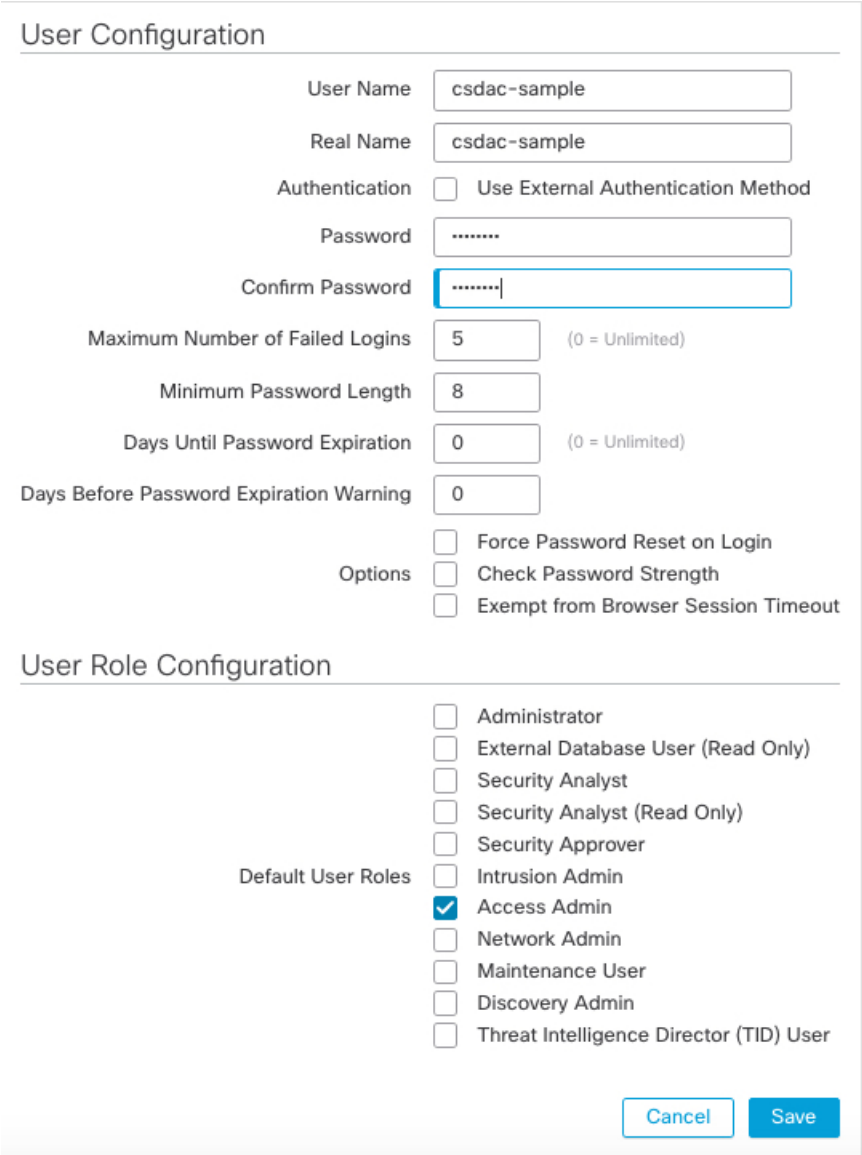
Step 3 Click **Create User**.

Step 4 Enter the information required to create the user.

Step 5 Under User Role Configuration, check any of the following default roles or a custom role with the same privilege level:

- **Administrator**
- **Access Admin**
- **Network Admin**

The following figure shows an example.



You can also choose a custom role with sufficient privileges to allow REST actions or a different default role with sufficient privileges. For more information about default roles, see the User Roles section in the chapter on user accounts.

What to do next

Create an adapter, on page 51

Related Topics

How to create an On-Prem Firewall Management Center adapter, on page 57
How to create a Cloud-Delivered Firewall Management Center adapter, on page 61
Create an adapter, on page 51
Create an ASA adapter, on page 52
Edit or delete an ASA adapter, on page 54
Create a user for the dynamic attributes connector, on page 55
Create a Cloud-Delivered Firewall Management Center adapter, on page 60
Get your base URL and API token, on page 60
Manually get a certificate authority (CA) chain, on page 36

How to create an On-Prem Firewall Management Center adapter

This topic discusses how to create an adapter to push dynamic objects from the dynamic attributes connector to the .

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.

Before you begin

See Create a user for the dynamic attributes connector, on page 55.

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.

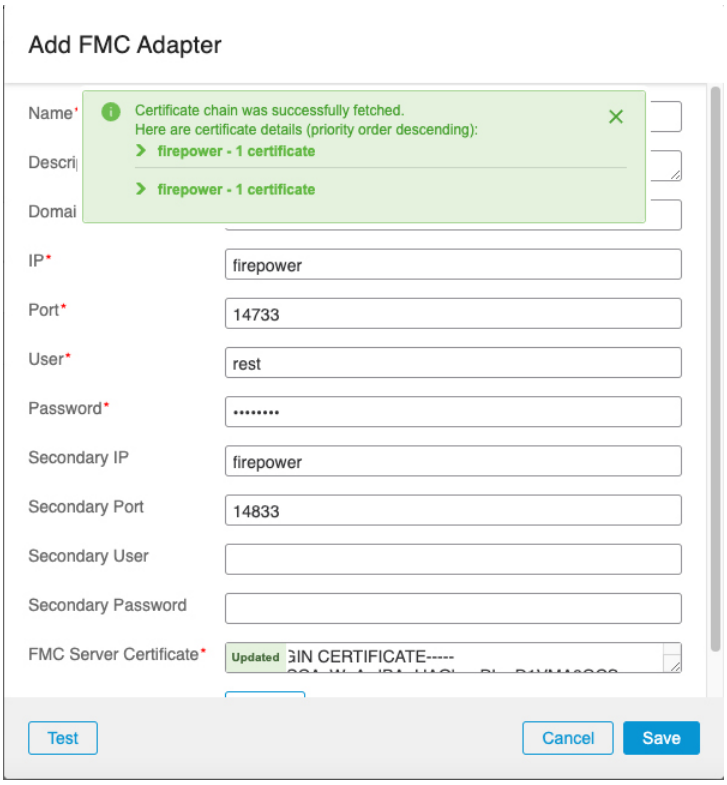
Before deleting the adapter, you can set its **Operative Status** to **Paused and Clear**. Doing this stops sending network object groups to ASA and clears any previously sent objects from ASA.

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.
Domain	Enter the domain in which to create dynamic objects. Leave the field blank to create dynamic objects in the Global domain. For example, `Global/MySubdomain`
IP	(Required.) Enter your 's host name or IP address. The host name or IP you enter must exactly match the Common Name of the CA certificate used to securely connect to it.
Port	(Required.) Enter the TLS port used by your .
User	(Required.) Enter the name of an user with the Network Admin role at minimum.
Password	(Required.) Enter the user's password.
Secondary IP	(High availability only.) Enter the secondary s host name or IP address. The host name or IP you enter must exactly match the Common Name of the CA certificate used to securely connect to it.
Secondary Port	(High availability only.) Enter the TLS port used by your secondary .
Secondary User	(High availability only.) Enter the name of a secondary user with the Network Admin role at minimum.
Secondary Password	(High availability only.) Enter the user's password.
Server Certificate	You have the following options: • 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 36. • Click **Get Certificate** > **Browse from file** to upload a certificate chain you downloaded previously.

Following is an example of successfully fetching a certificate chain:



Expanding the certificate CA chain at the top of the dialog box displays the certificates similar to the following.



If it's not possible to fetch the certificate this way, you can get the certificate chain manually as discussed in Manually get a certificate authority (CA) chain, on page 36.

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

Step 6 Click **Save**.

Related Topics

How to create an On-Prem Firewall Management Center adapter, on page 57
How to create a Cloud-Delivered Firewall Management Center adapter, on page 61
Create an adapter, on page 51
Create an ASA adapter, on page 52
Edit or delete an ASA adapter, on page 54
Create a user for the dynamic attributes connector, on page 55
Create a Cloud-Delivered Firewall Management Center adapter, on page 60
Get your base URL and API token, on page 60
Manually get a certificate authority (CA) chain, on page 36

Create a Cloud-Delivered Firewall Management Center adapter

This topic discusses how to create an adapter to push dynamic objects from the dynamic attributes connector to a managed management center on the .

You can create the following adapters:

- *On-Prem Firewall Management Center* for an on-premises
- *Cloud-Delivered Firewall Management Center* for devices managed by Security Cloud Control

Before you can create a Cloud-Delivered Firewall Management Center, get the following information first: Get your base URL and API token, on page 60.

Related Topics

How to create an On-Prem Firewall Management Center adapter, on page 57
How to create a Cloud-Delivered Firewall Management Center adapter, on page 61
Create an adapter, on page 51
Create an ASA adapter, on page 52
Edit or delete an ASA adapter, on page 54
Create a user for the dynamic attributes connector, on page 55
Create a Cloud-Delivered Firewall Management Center adapter, on page 60
Get your base URL and API token, on page 60
Manually get a certificate authority (CA) chain, on page 36

Get your base URL and API token

This task dicusses how to get the URL and API token from Security Cloud Control that are required to create a Cloud-Delivered Firewall Management Center adapter.

Before you begin

You must be a Security Cloud Control Super Admin to complete the tasks discussed in this section.

Procedure

Step 1 Log in to Security Cloud Control as a user with the Super Admin role.

Step 2 In the upper right corner of the page, click **Settings**.

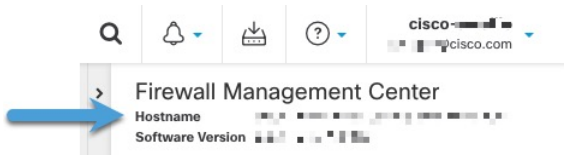
Step 3 Click **General Settings**.

Step 4 Next to API Token, click **Refresh**.

Step 5 Copy the API token to a text file for later use.

Step 6 Click the name of the management center to which to send dynamic attributes connector data.

Step 7 The value of **Hostname**, preceded by **https://**, is the base URL.
An example follows:



What to do next

How to create a Cloud-Delivered Firewall Management Center adapter, on page 61.

Related Topics

How to create an On-Prem Firewall Management Center adapter, on page 57
How to create a Cloud-Delivered Firewall Management Center adapter, on page 61
Create an adapter, on page 51
Create an ASA adapter, on page 52
Edit or delete an ASA adapter, on page 54
Create a user for the dynamic attributes connector, on page 55
Create a Cloud-Delivered Firewall Management Center adapter, on page 60
Get your base URL and API token, on page 60
Manually get a certificate authority (CA) chain, on page 36

How to create a Cloud-Delivered Firewall Management Center adapter

This task discusses how to create a Cloud-Delivered Firewall Management Center adpater that sends data from the dynamic attributes connector to a device managed by Security Cloud Control.

Before you begin

You must get the management center base URL and API token from Security Cloud Control before you can complete this task. For more information, see Get your base URL and API token, on page 60.

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.
Base Url	(Required.) Use the Base URL you found in Get your base URL and API token, on page 60.
API Token	(Required.) Use the API token you found in Get your base URL and API token, on page 60.

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

Step 6 Click **Save**.

What to do next

Create dynamic attributes filters, on page 66.

Related Topics

How to create an On-Prem Firewall Management Center adapter, on page 57
How to create a Cloud-Delivered Firewall Management Center adapter, on page 61
Create an adapter, on page 51
Create an ASA adapter, on page 52
Edit or delete an ASA adapter, on page 54
Create a user for the dynamic attributes connector, on page 55
Create a Cloud-Delivered Firewall Management Center adapter, on page 60
Get your base URL and API token, on page 60
Manually get a certificate authority (CA) chain, on page 36

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, , Cisco APIC, or .

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
-
- 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 Cisco APIC, or . For example:

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

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

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

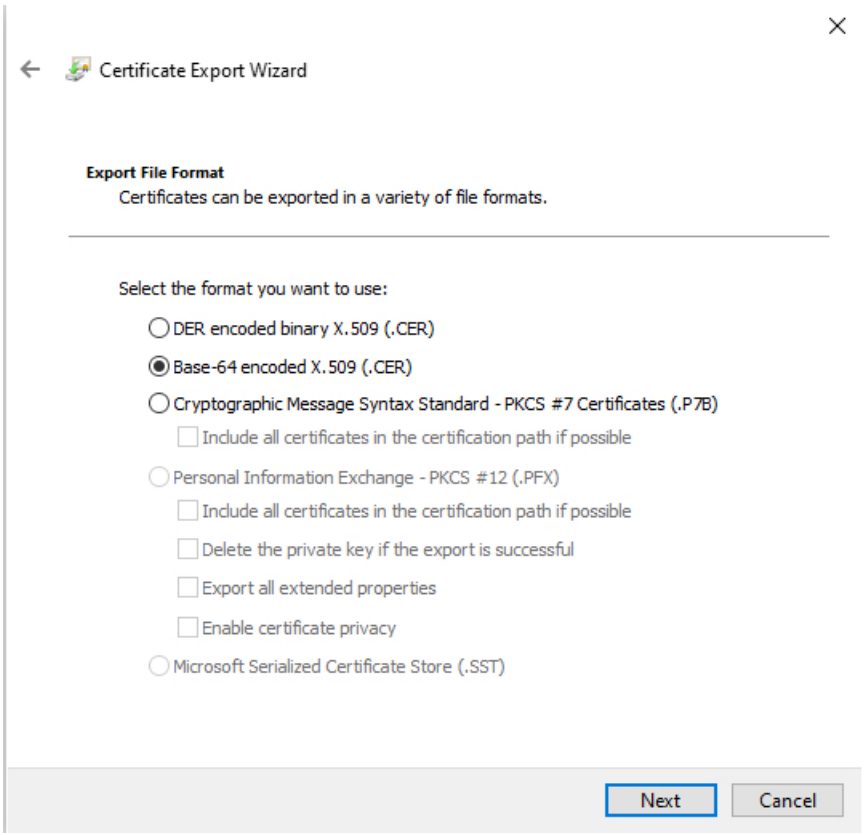
3. Save the entire certificate chain to a plaintext file.
   - *Include* all `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` delimiters.
   - *Exclude* any extraneous text (for example, the name of the certificate and any text contained in angle brackets (< and >) as well as the angle brackets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

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, , Cisco APIC, or 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.



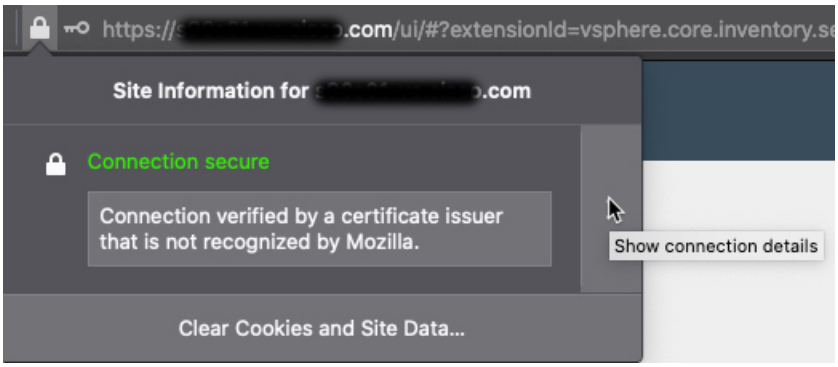
10. Follow the prompts to complete the export.
11. Open the certificate in a text editor.
12. Repeat the process for all certificates in the chain.

    You must paste each certificate in the text editor in order, first to last.
13. Repeat these tasks for vCenter, , Cisco APIC, or .

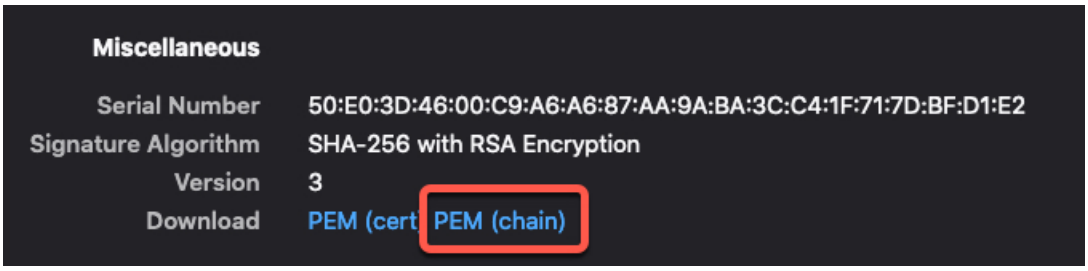
Get a Certificate Chain—Windows Firefox

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

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

Related Topics

How to create an On-Prem Firewall Management Center adapter, on page 57
How to create a Cloud-Delivered Firewall Management Center adapter, on page 61
Create an adapter, on page 51
Create an ASA adapter, on page 52
Edit or delete an ASA adapter, on page 54
Create a user for the dynamic attributes connector, on page 55
Create a Cloud-Delivered Firewall Management Center adapter, on page 60
Get your base URL and API token, on page 60
Manually get a certificate authority (CA) chain, on page 36
System requirements for the integration with Cisco APIC, on page 31
Get required information for the integration, on page 31
Create a Cisco APIC connector, on page 35
Cisco APIC connector, on page 30
Requirements and prerequisites for, on page 30

Create dynamic attributes filters

Dynamic attributes filters that you define using the Dynamic Attributes Connector are exposed in the 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, AWS service tags, AWS service groups, Azure, Azure Service Tags, Cisco Cyber Vision, Generic Text, GitHub, Google Cloud, Office 365, vCenter, Webex, or Zoom. These types of cloud objects provide their own IP addresses.

Before you begin

Create a connector, on page 19

Procedure

Step 1 Log in to the dynamic attributes connector.

Step 2 Click **Dynamic Attributes Filters**.

Step 3 Do any of the following:

- 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 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.

Item	Description
	• **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 .

a) Log in to the as a user with the Network Admin role at minimum.

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

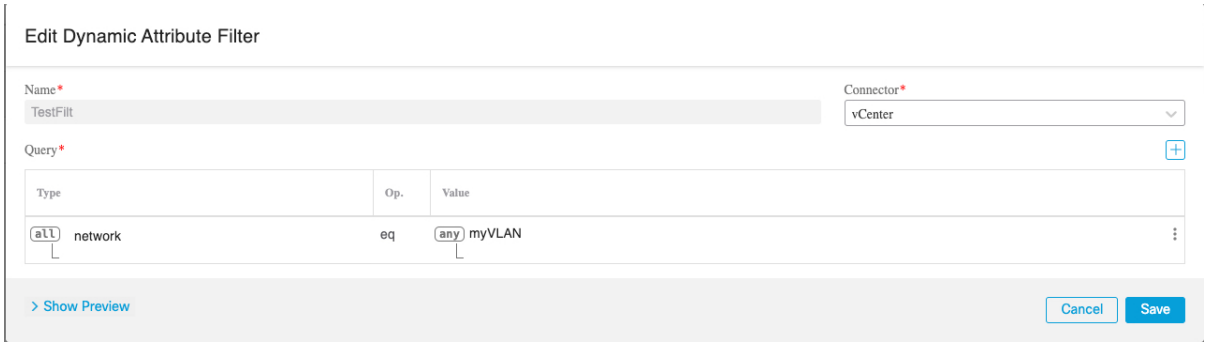
The dynamic attribute query you created should be displayed as a dynamic object.

Dynamic attribute filter examples

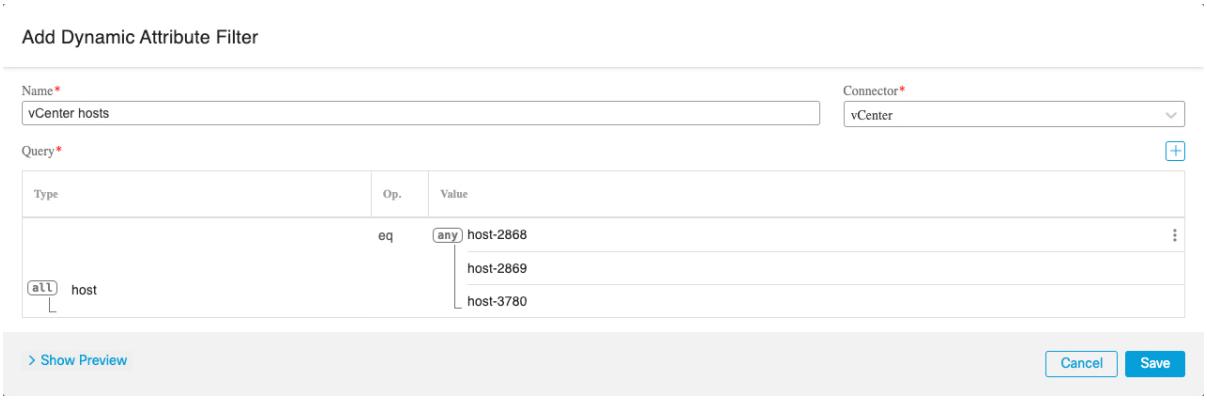
This topic provides some examples of setting up dynamic attribute filters.

Examples: vCenter

The following example shows one criterion: a VLAN.

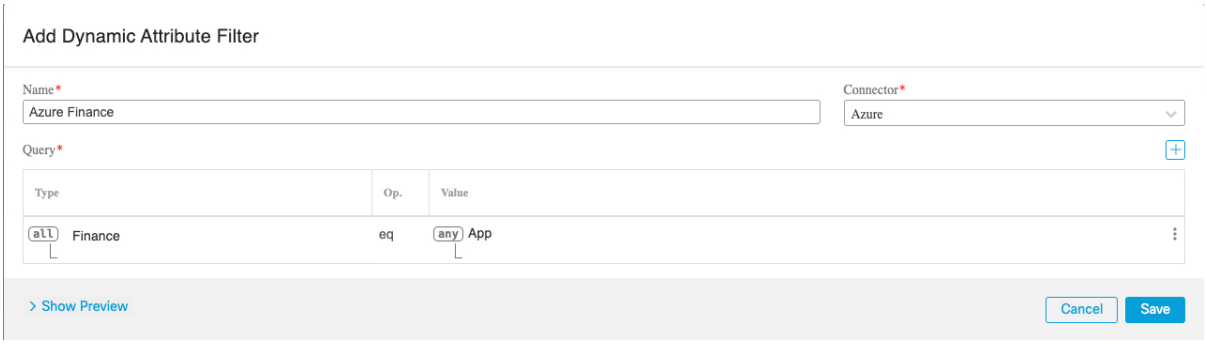


The following example shows three criteria that are joined with OR: the query matches any of three hosts.



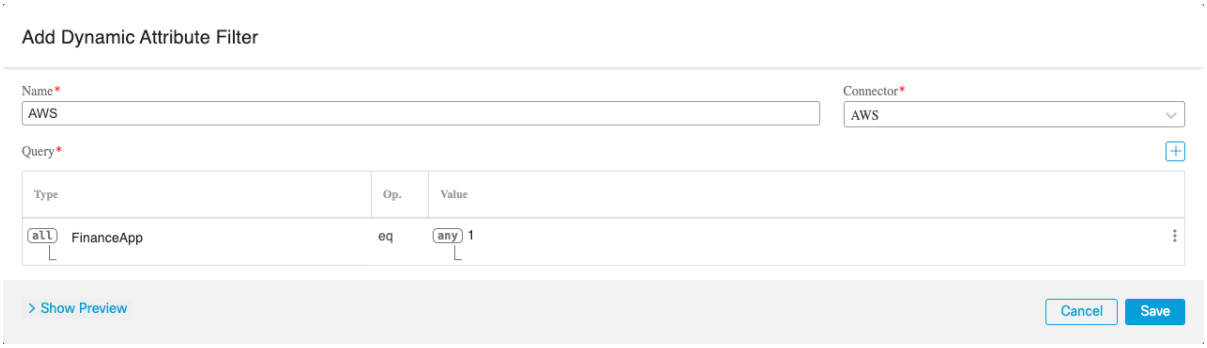
Example: Azure

The following example shows one criterion: a server tagged as a Finance app.



Example: AWS

The following example shows one criterion: a FinanceApp with a value of 1.



Example: pxGrid Cloud

The following example shows one criterion: PostureStatus is NonCompliant.



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, , Cisco APIC, or .

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
-
- 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 Cisco APIC, or . For example:

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

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

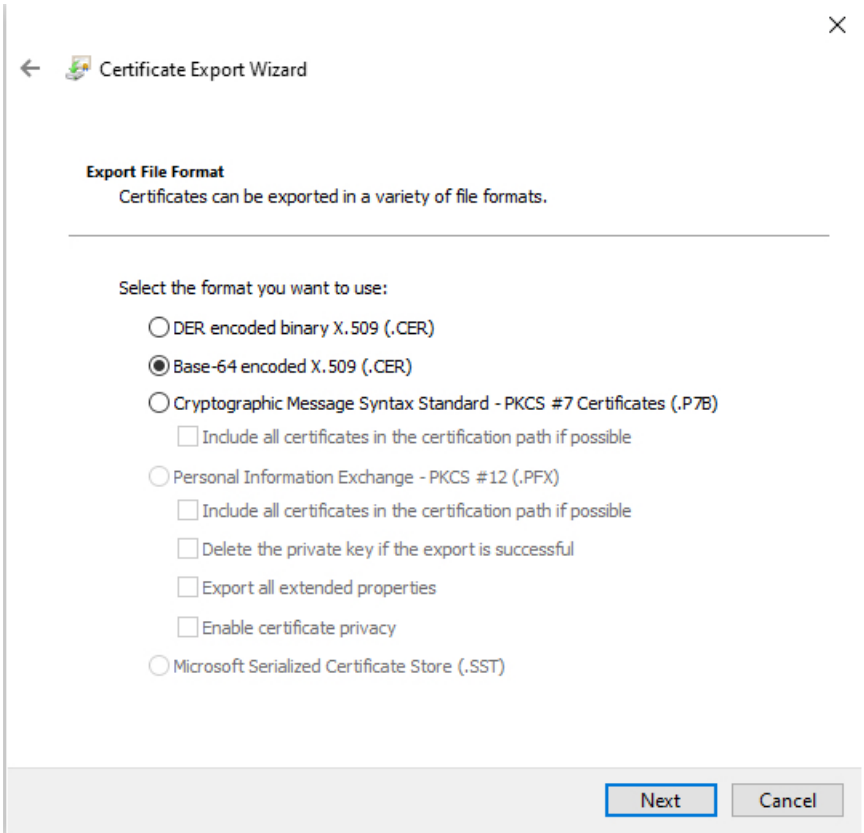
   `security verify-cert -P https://myvcenter.example.com:12345`
3. Save the entire certificate chain to a plaintext file.
   - *Include* all `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` delimiters.
   - *Exclude* any extraneous text (for example, the name of the certificate and any text contained in angle brackets (< and >) as well as the angle brackets themselves.
4. Repeat these tasks for vCenter, , Cisco APIC, or .

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, , Cisco APIC, or 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.



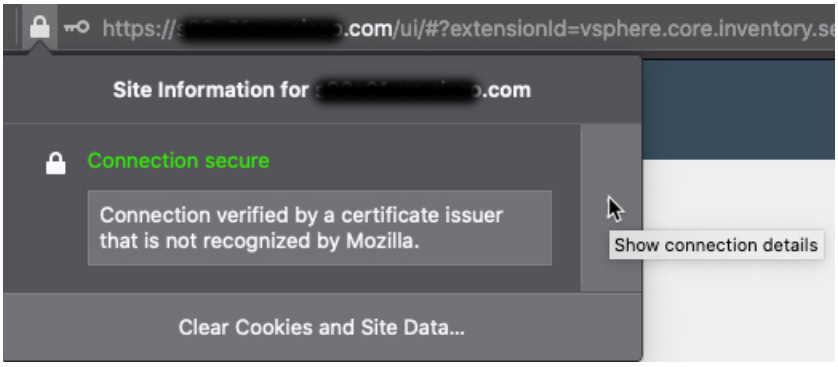
10. Follow the prompts to complete the export.
11. Open the certificate in a text editor.
12. Repeat the process for all certificates in the chain.

    You must paste each certificate in the text editor in order, first to last.
13. Repeat these tasks for vCenter, , Cisco APIC, or .

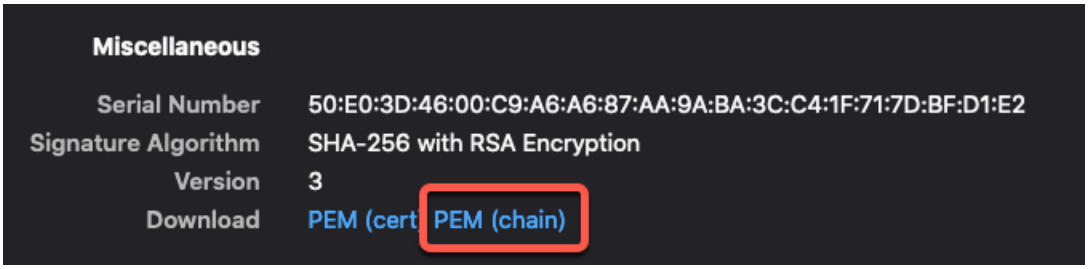
Get a Certificate Chain—Windows Firefox

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

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

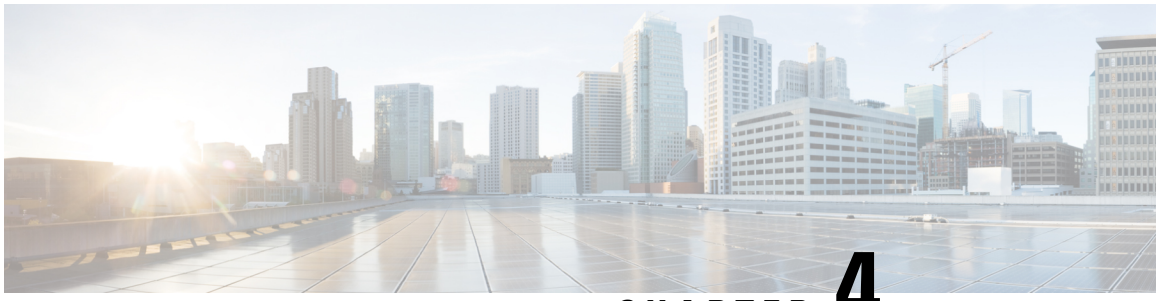


9. Save the file.
10. Repeat these tasks for vCenter, , Cisco APIC, or ASA.

Related Topics

How to create an On-Prem Firewall Management Center adapter, on page 57
How to create a Cloud-Delivered Firewall Management Center adapter, on page 61
Create an adapter, on page 51
Create an ASA adapter, on page 52
Edit or delete an ASA adapter, on page 54
Create a user for the dynamic attributes connector, on page 55
Create a Cloud-Delivered Firewall Management Center adapter, on page 60
Get your base URL and API token, on page 60

Manually get a certificate authority (CA) chain, on page 36
System requirements for the integration with Cisco APIC, on page 31
Get required information for the integration, on page 31
Create a Cisco APIC connector, on page 35
Cisco APIC connector, on page 30
Requirements and prerequisites for, on page 30



CHAPTER 4

Use Dynamic Objects in Access Control Policies or DNS Policies

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

- About dynamic objects in access control rules or DNS rules, on page 73
- Create dynamic attributes filters, on page 73
- Dynamic attributes rule conditions, on page 75
- View dynamic objects in the , on page 75
- Create access control rules or DNS rules using dynamic attributes filters, on page 77
- Use dynamic objects in DNS policies, on page 78
- How to use network object groups from Cisco APIC in ASA access rules, on page 79

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 these 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, AWS service tags, AWS service groups, Azure, Azure Service Tags, Cisco Cyber Vision, Generic Text, GitHub, Google Cloud, Office 365, vCenter, 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 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, AWS service tags, AWS service groups, Azure, Azure Service Tags, Cisco Cyber Vision, Generic Text, GitHub, Google Cloud, Office 365, vCenter, Webex, or Zoom. These types of cloud objects provide their own IP addresses.

Before you begin

Create a connector, on page 19

Procedure

Step 1 Log in to the dynamic attributes connector.

Step 2 Click **Dynamic Attributes Filters**.

Step 3 Do any of the following:

- 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 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 .

a) Log in to the 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:

- (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 they can be used in access control rules.

  For more information about the dynamic attributes connector, see .

- (Source only.) SGT objects contain tags either manually defined or defined in ISE. For more information, see Source 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

(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 .

Procedure

Step 1 Log in to the

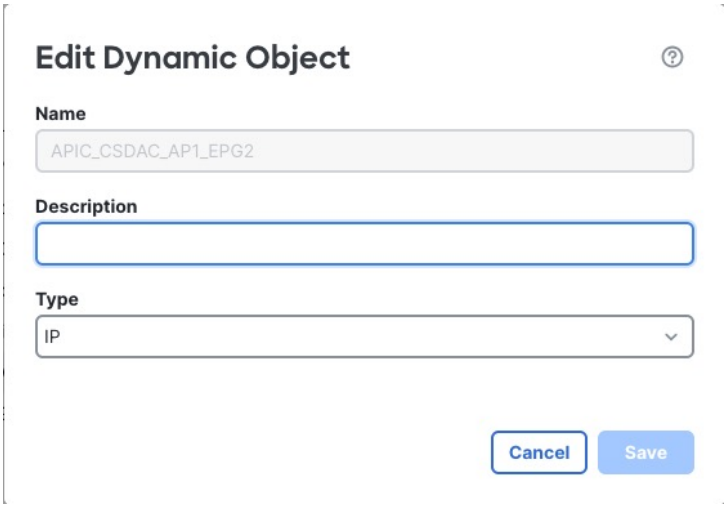
Step 2 Expand **Objects** > **Object Management** > **External Attributes** > **Dynamic Object**.

Dynamic objects have their own naming conventions; for example, AWS dynamic objects have names like `aws_AMAZON`.

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

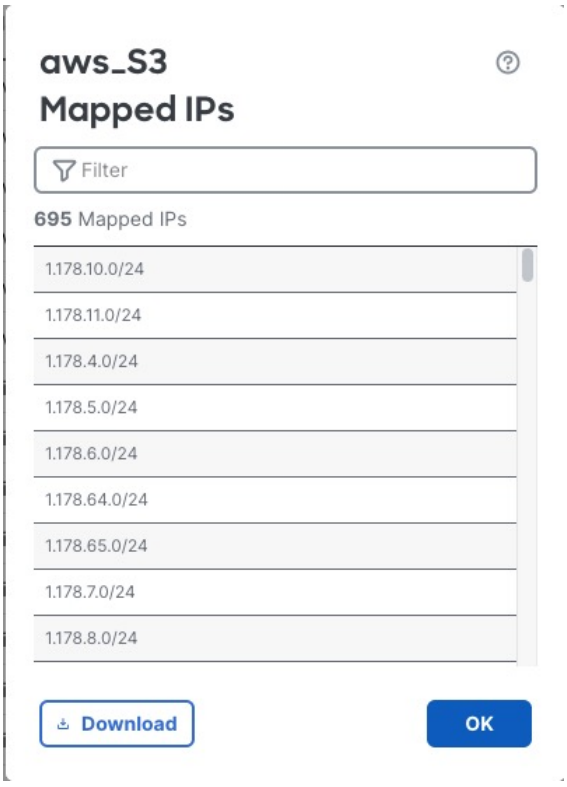
`APIC-site-name_tenant-name_application-profile-name_EPG-or-ESG-name`

Example.



Step 3 To view IP addresses associated with each dynamic object, click (IPs) at the end of the row.

Example:



What to do next

See Create access control rules or DNS rules using dynamic attributes filters, on page 77.

Create access control rules or DNS rules using dynamic attributes filters

This topic discusses how to create access control rules using dynamic objects (these dynamic objects are named after the dynamic attributes filters you created previously).

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

Before you begin

Create dynamic attributes filters as discussed in .

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

Procedure

Step 1 Log in to the

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

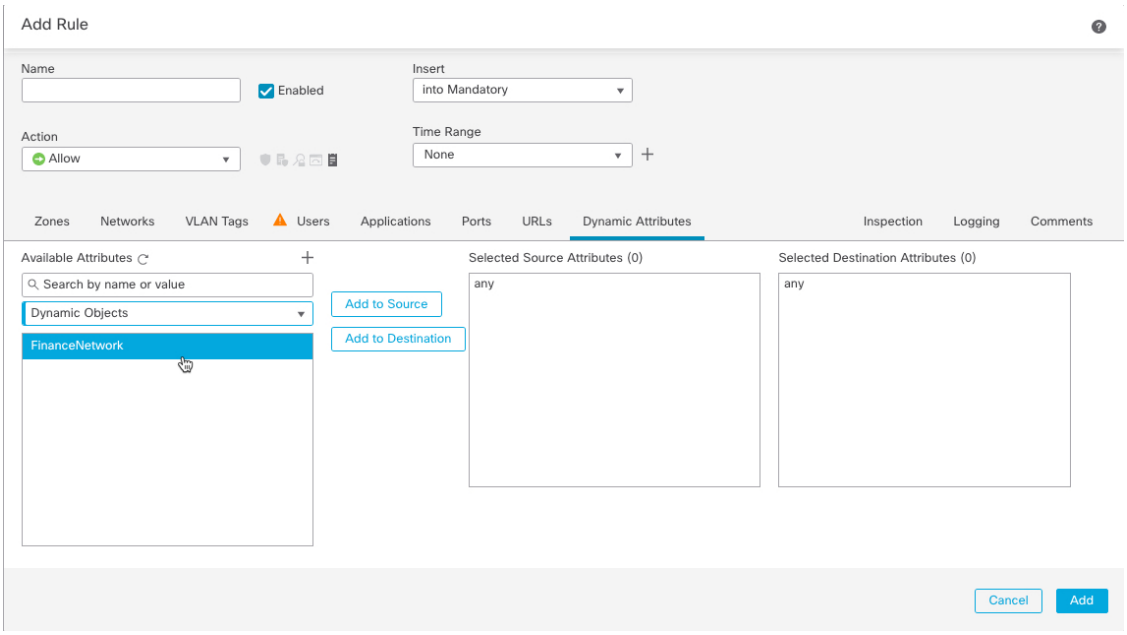
Step 3 Click **Edit** ( ) next to an access control policy.

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.



This 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.

Use dynamic objects in DNS policies

The dynamic attributes connector enables you to configure dynamic filters, seen in the as dynamic objects, in DNS rules. For information about DNS policies, see .

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

You can use these dynamic objects on the DNS rule's Dynamic Attributes tab page, similarly to the way you use Security Group Tags (SGTs). You can add dynamic objects as source or destination attributes, except for endpoint device type objects, which are source only.

Procedure

Step 1 Click **Policies** > **Access Control heading** > **DNS** and create or edit a DNS policy.

Step 2 Add or edit a rule.

Step 3 Click the **Dynamic Attributes** tab.

Step 4 In the **Dynamic Attributes** list, select the objects you want to use, then add them to the source or destination lists as appropriate. Initially, all security group and dynamic objects are listed, by you can uncheck the Security Group option to see dynamic objects only.

Step 5 On the **DNS** tab, select the appropriate list or feed to match the DNS requests you are targeting.

Step 6 Add other conditions to the rule if desired and set the action.

Step 7 Click **Save**.

How to use network object groups from Cisco APIC in ASA access rules

The following topics show how to use network object groups from Cisco APIC in ASA access rules.

Related Topics

Add network object groups to access rules, on page 79
View network object groups in ASDM, on page 81

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 35
- Create an ASA adapter, on page 52

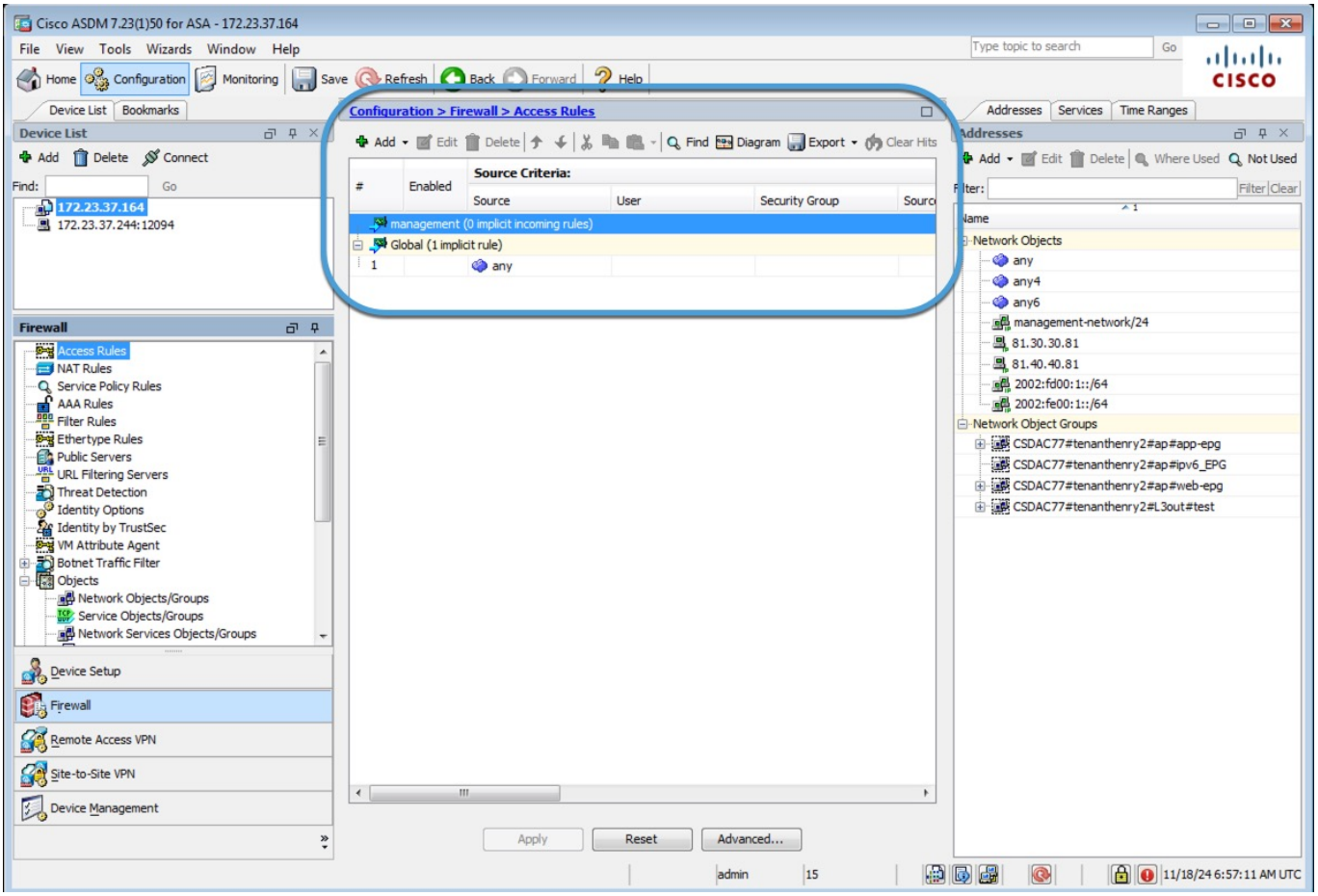
Procedure

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.

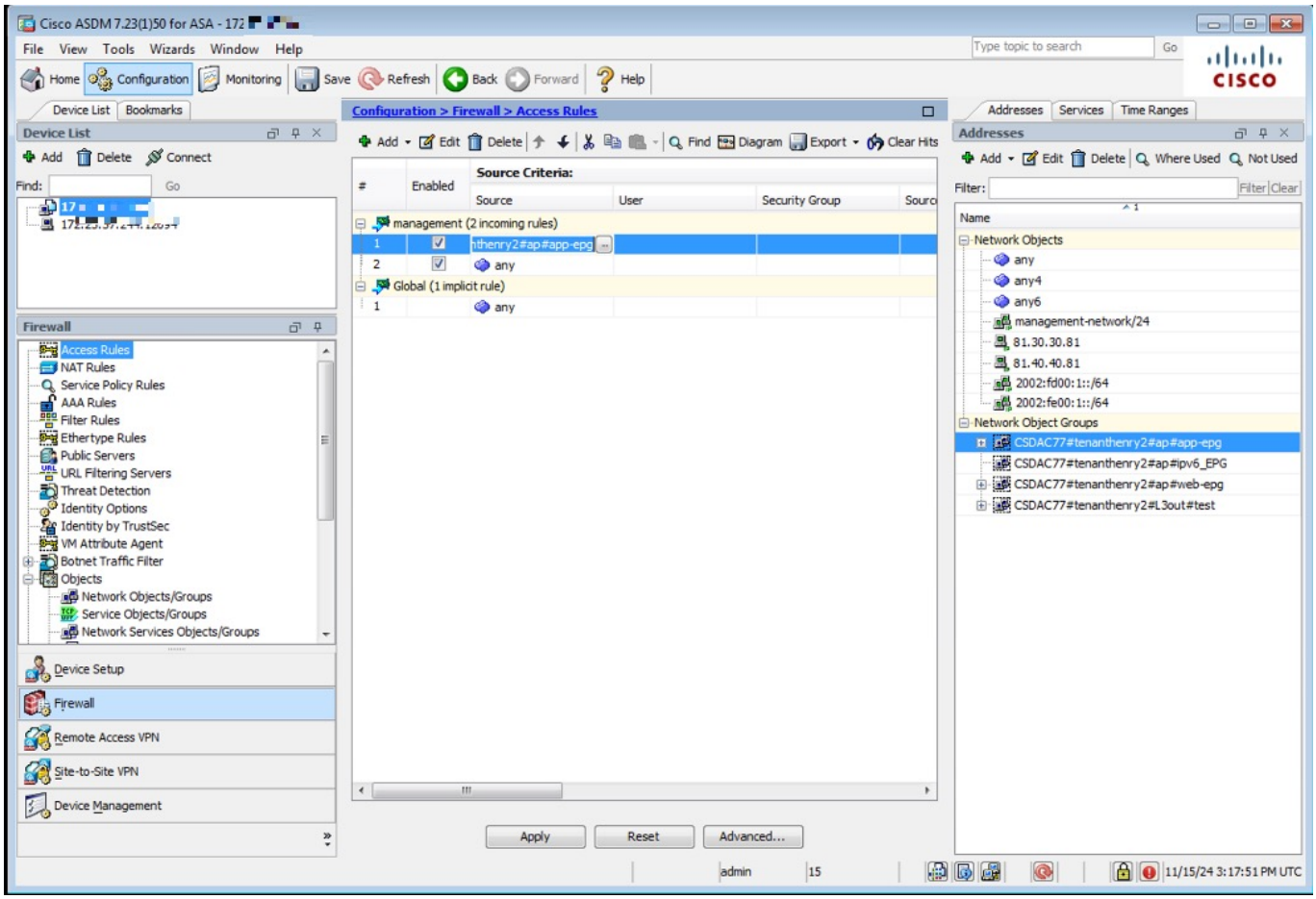
Step 2 Click **Configuration** > **Firewall** > **Access Rules** > **Network Objects/Groups**.
Access rules are displayed in the center pane as the following figure shows.



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.



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.

Related Topics

Add network object groups to access rules, on page 79
View network object groups in ASDM, on page 81

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 79.

Before you begin

Complete all of the following tasks:

- Create a Cisco APIC connector, on page 35

- Create an ASA adapter, on page 52

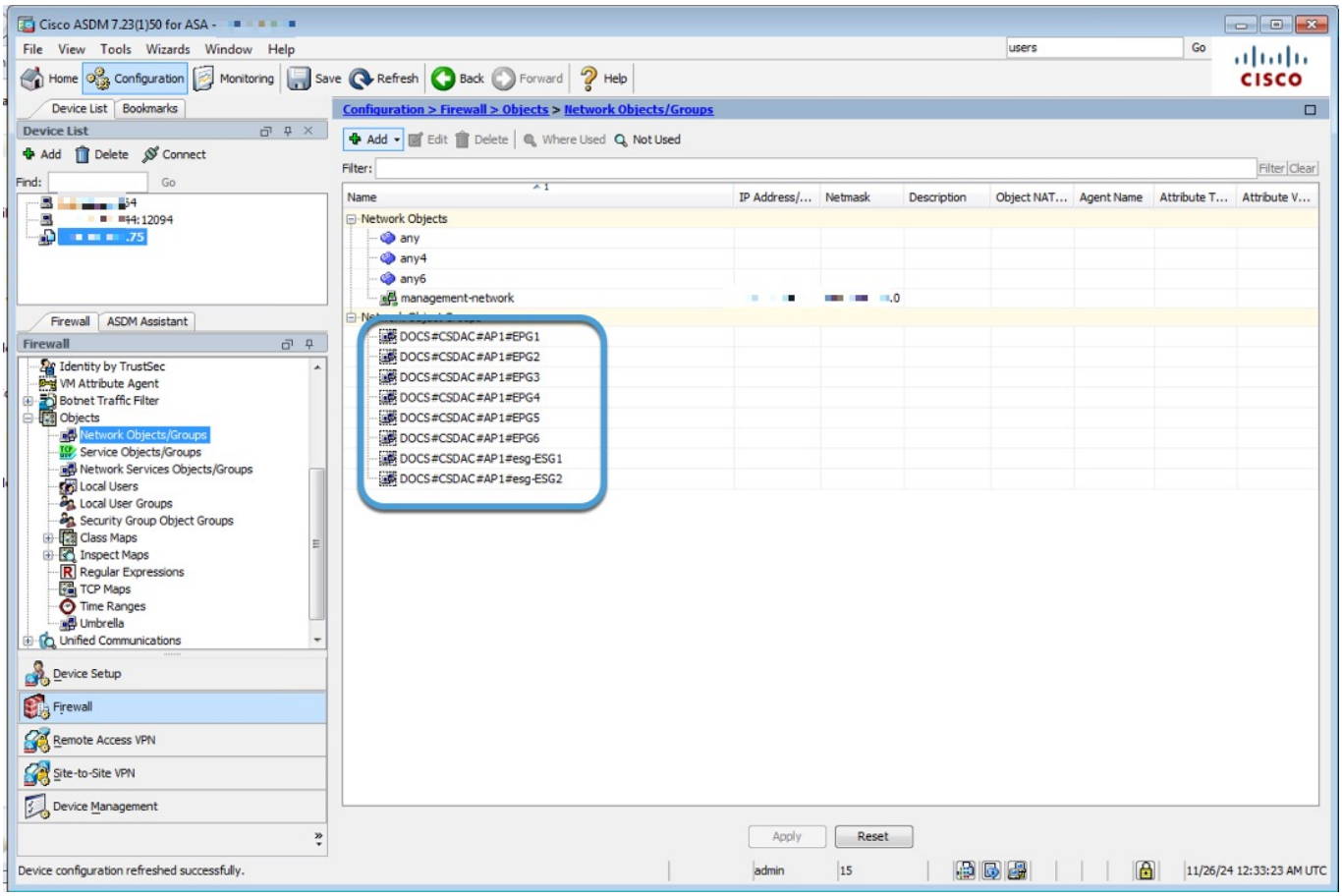
Procedure

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.



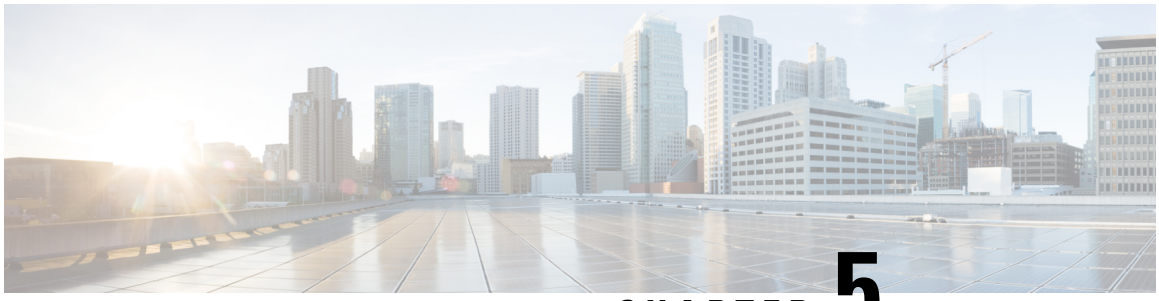
Network object groups are named as follows: `SiteName#TenantName#ProfileName#EPGName`

What to do next

See Add network object groups to access rules, on page 79

Related Topics

Add network object groups to access rules, on page 79
View network object groups in ASDM, on page 81



CHAPTER 5

Troubleshoot the Dynamic Attributes Connector

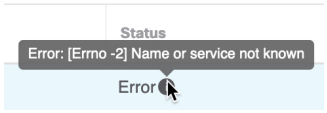
How to troubleshoot issues with the dynamic attributes connector, including using provided tools.

- Troubleshoot error messages, on page 85
- Troubleshoot using the command line, on page 87
- Manually get a certificate authority (CA) chain, on page 89

Troubleshoot error messages

Problem: Name or service not known error

This error is displayed as a tooltip when you hover the mouse over an error condition on a connector. An example follows; yours might look different.



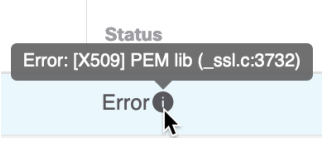
Solution: Edit the connector and check for:

- A trailing slash on a host name
- (On-Prem Firewall Management Center adapter only.) A scheme at the beginning of a host name (for example, `https://`)
- Verify the password is correct
- For an On-Prem Firewall Management Center adapter, verify the contents of the **FMC Server Certificate** field.

  For more information, see Manually get a certificate authority (CA) chain, on page 36.

Problem: [X509 PEM lib]

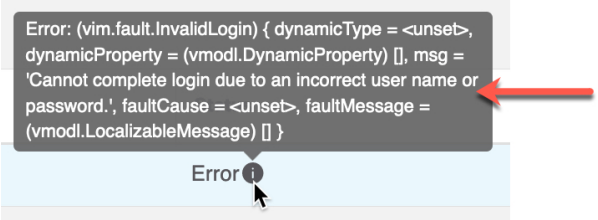
This error is displayed as a tooltip when you hover the mouse over an error condition on a connector.



Solution: Edit the connector and check the CA chain. For more information, see Manually get a certcertificate authority (CA) chain, on page 36.

Problem: Incorrect username or password

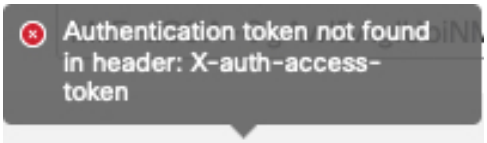
This error is displayed as a tooltip when you hover the mouse over an error condition on a connector.



Solution: Edit the connector and change the user name or password.

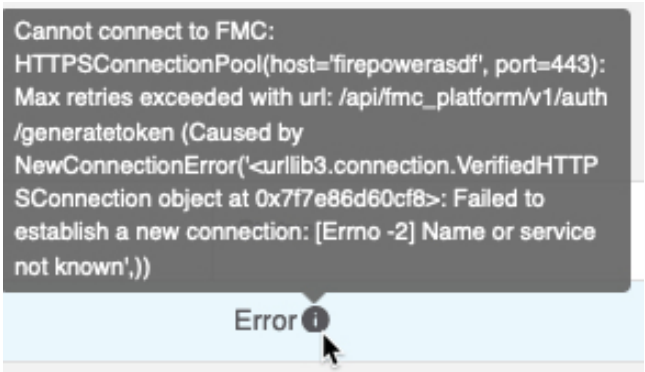
Problem: Authentication token not found in header

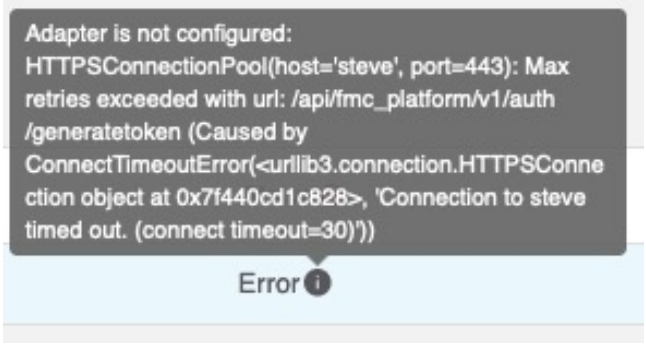
This error is displayed when you attempt to test the connection with an adapter user that does not have sufficient privileges on the :



Problem: Timeout or max retries error for an adapter

This error is displayed as a tooltip when you hover the mouse over an error condition on an adapter.





Solution: Do all of the following:

- Verify the management center is running and that it can be reached from the dynamic attributes connector.
- Verify the contents of the **FMC Server Certificate** field.
- Make sure the value you entered in the **IP** field exactly matches the certificate's Common Name.

For more information, see Manually get a certificate authority (CA) chain, on page 36.

Troubleshoot using the command line

To assist you with advanced troubleshooting and working with Cisco TAC, we provide the following troubleshooting tools. To use these tools, log in as any user to the Ubuntu host on which the dynamic attributes connector is running.

Check container status

To check the status of the dynamic attributes connector Docker containers, enter the following commands:

```
cd ~/csdac/app
sudo ./muster-cli status
```

Sample output follows:

```
============================== CORE SERVICES ==============================
      Name                     Command                  State    Ports
-----------------------------------------------------------------------------------------------
muster-bee     ./docker-entrypoint.sh run ...   Up             50049/tcp, 50050/tcp
muster-etcd    etcd                             Up             2379/tcp, 2380/tcp

muster-ui      /docker-entrypoint.sh runs ...   Up (healthy)
0.0.0.0:443->8443/tcp,:::443->8443/tcp
muster-ui-backend   ./docker-entrypoint.sh run ...   Up             50031/tcp
========================== CONNECTORS AND ADAPTERS ==========================
           Name                          Command               State     Ports
-------------------------------------------------------------------------------
muster-adapter-fmc.1         ./docker-entrypoint.sh run ...   Up      50070/tcp
muster-connector-vcenter.1   ./docker-entrypoint.sh run ...   Up      50070/tcp
```

Stop, start, or restart the Dynamic Attributes Connector Docker containers

If the **./muster-cli status** indicates containers are down or to restart containers in the event of issues, you can enter the following commands:

Stop and restart:

```
cd ~/csdac/app
sudo ./muster-cli stop
sudo ./muster-cli start
```

Start only:

```
cd ~/csdac/app
sudo ./muster-cli start
```

Enable application debug logging and generate troubleshoot files

If advised to do so by Cisco TAC, enable debug logging and generate troubleshoot files as follows:

```
cd ~/csdac/app
sudo ./muster-cli debug-on
sudo ./muster-cli ts-gen
```

The troubleshoot file name is **ts-bundle-***timestamp***.tar** and is created in the same directory.

The following table shows the location of troubleshoot files and logs in the troubleshoot file.

Location	What it contains
/csdac/app/ts-bundle-*timestamp***/info**	`etcd` database contents
/csdac/app/ts-bundle-*timestamp***/logs**	Container log files
/csdac/app/ts-bundle-*timestamp***/status.log**	Container status, versions, and image status

Verify dynamic objects on the

To verify your connectors are creating objects on the , you can use the following command on the as an administrator:

```
sudo tail f /var/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log
```

Example: Successful object creation

```
26-Aug-2021 12:41:35.912,[INFO],(DefenseCenterServiceImpl.java:1442)
com.cisco.nm.vms.api.dc.DefenseCenterServiceImpl, ajp-nio-127.0.0.1-9009-exec-10
** REST Request [ CSM ]
** ID : 18b25356-fd6b-4cc4-8d27-bbccb52a6275
** URL: POST /audit
{
  "version": "7.1.0",
  "requestId": "18b25356-fd6b-4cc4-8d27-bbccb52a6275",
  "data": {
    "userName": "csdac-centos7",
    "subsystem": "API",
    "message": "POST
https://myfmc.example.com/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f
/object/dynamicobjects Created (201) - The request has been fulfilled and resulted in a new
 resource being created",
    "sourceIP": "192.0.2.103",
    "domainUuid": "e276abec-e0f2-11e3-8169-6d9ed49b625f",
    "time": "1629981695431"
  },
  "deleteList": []
}
```

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, , Cisco APIC, or .

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
-
- 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 Cisco APIC, or . For example:

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

   If you access vCenter , or Cisco APIC, or 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, , Cisco APIC, or .

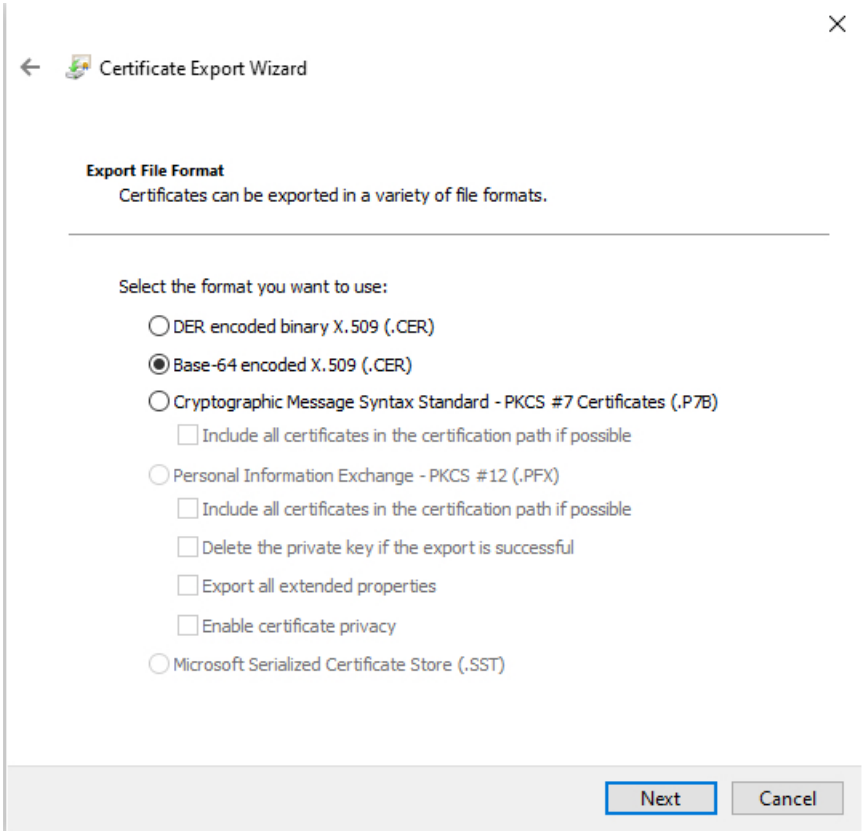
Get a Certificate Chain—Windows Chrome

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

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



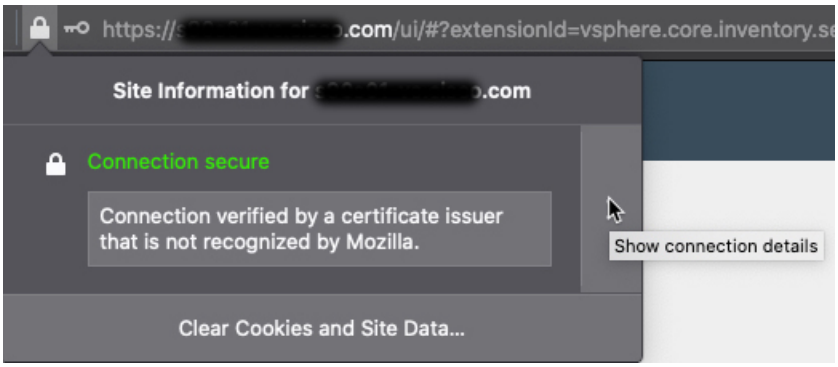
10. Follow the prompts to complete the export.
11. Open the certificate in a text editor.
12. Repeat the process for all certificates in the chain.

    You must paste each certificate in the text editor in order, first to last.
13. Repeat these tasks for vCenter, , Cisco APIC, or .

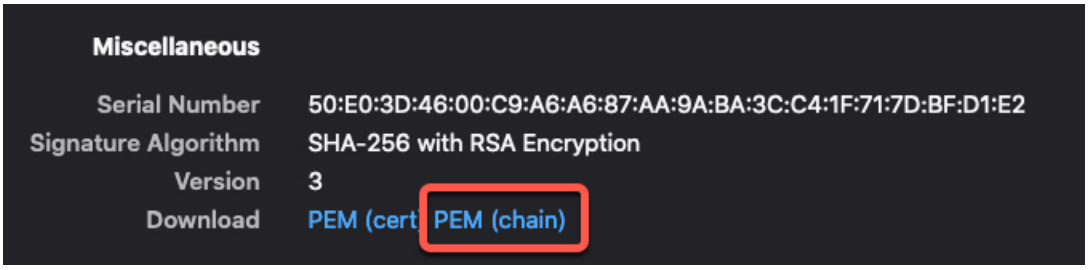
Get a Certificate Chain—Windows Firefox

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

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



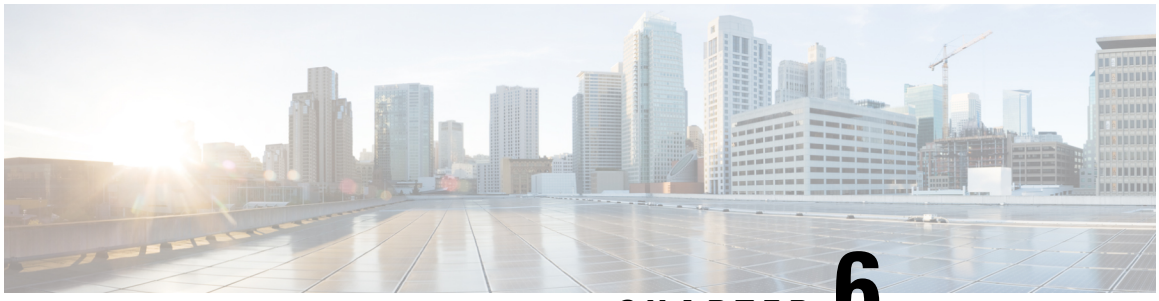
4. Click **More Information**.
5. Click **View Certificate**.
6. If the resulting dialog box has tab pages, click the tab page corresponding to the top-level CA.
7. Scroll to the Miscellaneous section.
8. Click **PEM (chain)** in the Download row. The following figure shows an example.



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

Related Topics

How to create an On-Prem Firewall Management Center adapter, on page 57
How to create a Cloud-Delivered Firewall Management Center adapter, on page 61
Create an adapter, on page 51
Create an ASA adapter, on page 52
Edit or delete an ASA adapter, on page 54
Create a user for the dynamic attributes connector, on page 55
Create a Cloud-Delivered Firewall Management Center adapter, on page 60
Get your base URL and API token, on page 60
Manually get a certificate authority (CA) chain, on page 36
System requirements for the integration with Cisco APIC, on page 31
Get required information for the integration, on page 31
Create a Cisco APIC connector, on page 35
Cisco APIC connector, on page 30
Requirements and prerequisites for, on page 30



CHAPTER 6

Migrate from the Cisco ACI Endpoint Update App to the Cisco APIC Integration with ASA

The following topics discuss the Cisco ACI Endpoint Update App to the Cisco APIC integration with ASA.

- About the migration, on page 93
- Migration step 1: Set up the dynamic attributes connector, on page 94
- Migration step 2: Prepare Cisco APIC, on page 94
- Migration step 3: Configure the dynamic attributes connector, on page 95
- Migration final step: Verify network object groups in ASDM, on page 95

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 . 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 the .
- 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 Cisco APIC can communicate with each other over the network. The dynamic attributes connector retrieves network object groups from Cisco APIC and pushes them to Cisco APIC so all systems must be able to communicate.

   See Migration step 1: Set up the dynamic attributes connector, on page 94

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 94

3. On the dynamic attributes connector, create .

See Migration step 3: Configure the dynamic attributes connector, on page 95

4. As a final verification step, make sure you see objects on the Cisco APIC.

   See Migration final step: Verify network object groups in ASDM, on page 95

Migration step 1: Set up the dynamic attributes connector

To use the integration, you must install the 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

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 9.

Step 2 Get the dynamic attributes connector software as discussed in Install prerequisite software, on page 10.

Step 3 Install the dynamic attributes connector as discussed in Install the dynamic attributes connector, on page 13.

What to do next

See Migration step 2: Prepare Cisco APIC, on page 94.

Migration step 2: Prepare Cisco APIC

Get required information

To migrate to the Cisco APIC integration with , 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 31.

Disable learning for the Cisco ACI Endpoint Update App

To prevent the Cisco ACI Endpoint Update App from communicating with Cisco APIC, 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 Cisco APIC.
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 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 94.

Procedure

Step 1 Log in to the dynamic attributes connector.

Step 2 Create the connector: Create a Cisco APIC connector, on page 35.

Step 3 Create the adapter: Create an ASA adapter, on page 52.

What to do next

See Migration final step: Verify network object groups in ASDM, on page 95.

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 dynamic attributes connector, on page 95.

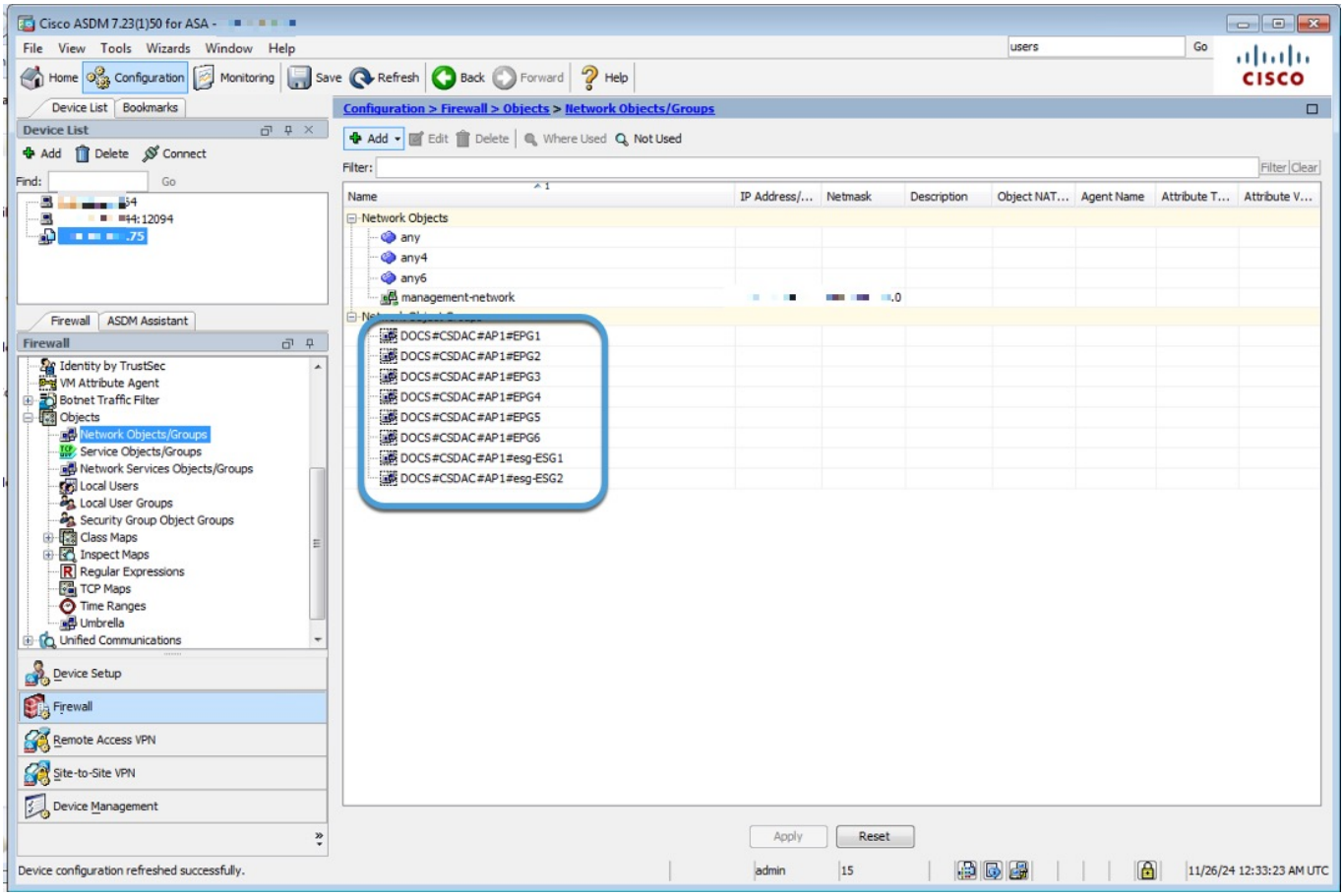
Procedure

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

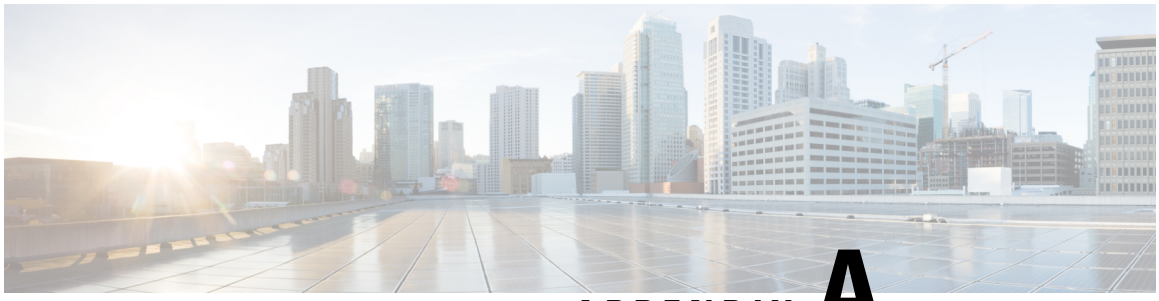
For more information about starting ASDM, see Start ASDM.

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`



APPENDIX A

Security and Internet Access

Lists of URLs used by the dynamic attributes connector when communicating with cloud service providers and the .

- Security requirements, on page 97
- Internet access requirements, on page 97

Security requirements

To safeguard the dynamic attributes connector, you should install it on a protected internal network. Although the dynamic attributes connector is configured to have only the necessary services and ports available, you must make sure that attacks cannot reach it.

If the dynamic attributes connector and the reside on the same network, you can connect the to the same protected internal network as the dynamic attributes connector.

Regardless of how you deploy your appliances, inter-system communication is encrypted. However, you must still take steps to ensure that communications between appliances cannot be interrupted, blocked, or tampered with; for example, with a distributed denial of service (DDoS) or adversary-in-the-middle attack.

Internet access requirements

By default, the dynamic attributes connector is configured to communicate with the Firepower System over the internet using HTTPS on port 443/tcp (HTTPS). If you do not want the dynamic attributes connector to have direct access to the internet, you can configure a proxy server.

The following information informs you of the URLs the dynamic attributes connector use to communicate with the and with external servers.

Table 4: Dynamic Attributes Connector access requirements

URL	Reason
https://*fmc-ip***/api/fmc_platform/v1/auth/generatetoken**	Authentication
https://*fmc-ip***/api/fmc_config/v1/domain/***domain-id***/object/dynamicobjects**	GET and POST dynamic objects

URL	Reason
https://*fmc-ip***/api/fmc_config/ v1/domain/***domain-id***/object/dynamicobjects/***object-id***/mappings?action=add**	Add mappings
https://*fmc-ip***/api/fmc_config/ v1/domain/***domain-id* **/object/dynamicobjects/***object-id***/mappings?action=remove**	Remove mappings

Table 5: Dynamic Attributes Connector vCenter access requirements

URL	Reason
https://*vcenter-ip***/rest/com/vmware/cis/session**	Authentication
https://*vcenter-ip***/rest/vcenter/vm**	Get VM information
https://*nsx-ip***/api/v1/fabric/virtual-machines/***vm-id*	Get NSX-T tag associated with the virtual machine

Migration from DockerHub to Amazon ECR

Docker images for the Dynamic Attributes Connector are being migrated from Docker Hub to Amazon Elastic Container Registry (Amazon ECR).

To use the new field packages, you must allow access through your firewall or proxy to all of the following URLs:

- https://public.ecr.aws
- https://csdac-cosign.s3.us-west-1.amazonaws.com
- https://d2glxqk2uabbnd.cloudfront.net
- https://d5l0dvt14r5h8.cloudfront.net

  For more information about Amazon Cloudfront URLs, see EKS Anywhere documentation.

Dynamic Attributes Connector Azure access requirements

The dynamic attributes connector calls built-in SDK methods to get instance information. These methods internally call https://login.microsoft.com (for authentication) and https://management.azure.com (to get instance information).